MSc Program
Renewable Energy in Central and Eastern Europe

CONTINUING EDUCATION CENTER

Application of Blockchain Technology for the Charging Infrastructure of Electric Vehicles - Technical, Environmental, Economic, Legal and Social Aspects

A Master's Thesis submitted for the degree of
"Master of Science"

supervised by
Univ. Prof. Dr. Dipl.Ing. Reinhard HAAS

Siegbert Zöhrer

08631568

September 18, 2018

CONTINUING
EDUCATION
CENTER

Affidavit

I, **Siegbert ZÖHRER**, hereby declare

1. that I am the sole author of the present Master's Thesis, "Application of Blockchain Technology for the Charging Infrastructure of Electrical Vehicles - Technical, Environmental, Economic, Legal and Social Aspects", 149 pages, bound, and that I have not used any source or tool other than those referenced or any other illicit aid or tool, and

2. that I have not prior to this date submitted this Master's Thesis as an examination paper in any form in Austria or abroad.

Vienna, 18.09.2018

Signature

Application of Blockchain Technology for the Charging Infrastructure of Electric Vehicles - Technical, Environmental, Economic, Legal and Social Aspects.

Abstract:

Switching to electric vehicles (EV), supported by a suitable charging station infrastructure, will take some time, as there is currently a lack of suitable infrastructure that allows convenient operation of EVs. The subject of this thesis is to investigate whether the application of BlockChain technology (BCT) for the charging infrastructure of EVs is possible and what advantages and disadvantages such a solution offers. Details of the BCT in terms of environmental, economic, legal and social aspects are analyzed. Many see the BCT as the biggest invention since the invention of the Internet. This technology makes it possible to achieve integrity in distributed systems without a centralized system. Distributed systems can reduce costs and provide more security in case of errors. It also provides an easy way to grow, as new systems can be easily integrated. The BCT also allows so-called "Micro Payments" with low costs for the payment, so that smaller electricity producers with solar modules on roofs will be able to sell their generated energy. Financial transactions must be conducted between actors who cannot build trust in the other party. The BCT also contains traps. One of them is an immense power consumption for consensus finding in distributed networks. All entries of BlockChain (BC) are public readable, can privacy be guaranteed here? The BC does not forget, how is the General Data Protection Regulation of the EU fulfilled here? The central question is whether it is possible with the BCT to build a distributed charging infrastructure, to implement this in a resource-saving manner, to allow micro-generators to participate in the electricity market, to enable privacy and to fulfill all legal requirements? To answer these questions, the technical requirements of the systems involved were analyzed and compared with the technical capabilities of the BC. Existing currency systems and crypto currencies were also analyzed for their possible uses. It was also

investigated whether a regulatory intervention must be possible and how to prevent monopolies and speculation. The right choice of BC shape and the right consensus algorithm allows the BCT to be used for the charging infrastructure of electric vehicles. Due to the open decentralized architecture, the BC also enables small power producers to economically participate in the power supply of these charging stations. Even an architecture without a central element enables trustworthy business relationships to be entered into. Smart contracts and coloured coins can be used to model complex business conditions. If regulative interventions are necessary, they must be transparent. Also, trading with Green Certificates is supported within the BC also with regulatory control of supply and demand. Within the BC, a cryptocurrency may be used, but to prevent speculation, it should be tied to a fixed currency and also support inflation.

Summary of the expected results

- The appropriate choice of form of the blockchain and of the correct algorithms the blockchain can be used for charging infrastructure of electric vehicles.
- The blockchain allows the open decentralized architecture also small energy producers such as solar systems on buildings economically participate in the power supply for charging stations.
- An architecture without a central element makes it possible for all trustworthy power producers to participate in the electricity market and also deprives large corporations of the power monopoly.

Table of Contents

1. Introduction

Currently, there is a lack of adequate area-wide infrastructure for charging electric vehicles. For small producers of renewable energy there is no possibility to offer their energy on the market with low administration costs and low billing costs.

The blockchain technology offers opportunities to conduct business relationships between two business partners without a trusting third party, to manage micropayments, to allow open transparent billing and offers protection against hidden manipulation and monopolies. Many of the current applications of blockchain technology, such as bitcoins, waste vast amounts of energy delivering their service.

1.1. Motivation

The decision to write on this topic was influenced by my personal interests in electric vehicles, solar power generation, and my interest in the possibilities of blockchain technology.

Electric cars are available in every price range today, but the short range is usually a problem, because cars that cover several hundred kilometers are too expensive for many. The short range, the high price and the poor charging infrastructure are currently the three major obstacles to electric mobility. Due to decreasing production costs and increasingly powerful batteries, the electric drive will spread more and more. But you cannot just load an e-vehicle anywhere because there is a lack of suitable charging stations. For any longer stay you could recharge your batteries, but due to lack of charging stations this is not possible.

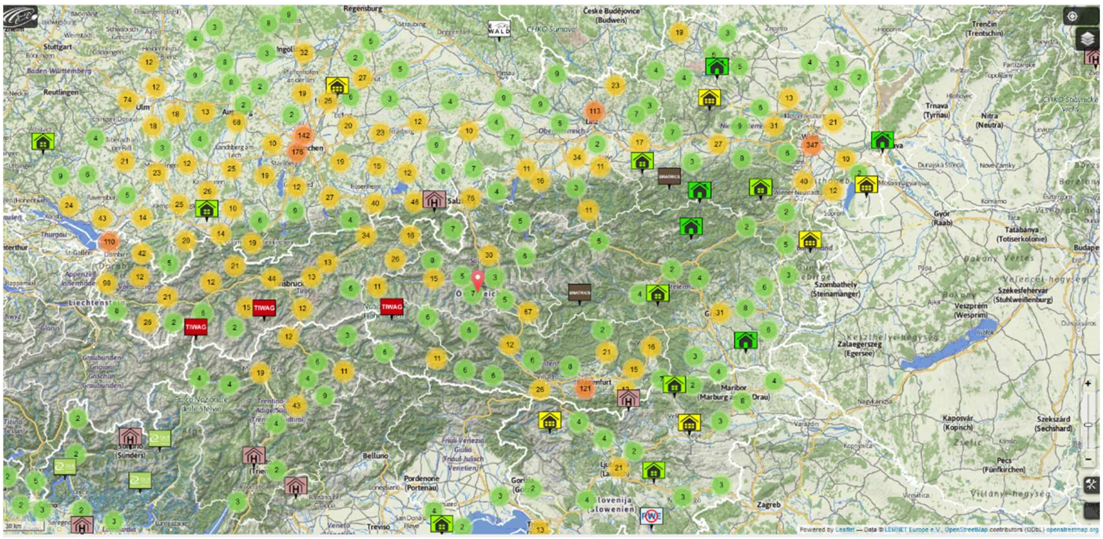


Figure 1: Number of Charging Stations for Electrical vehicles in Austria. (Sietas, 2018) (as on 18.9.2018)

Figure 1 shows the current availability of charging stations for Austria - in the other European countries it is no better.

With the previous charging infrastructure, only a small amount of money can be earned so that energy giants are still afraid of high investment costs. If the administration and the billing are automated, the costs will decrease. The Blockchain technology could enable such a system, so that the development of a charging infrastructure is cheaper, and even small energy producers such as households with a solar system, can also offer their energy.

1.2. Core objective

The main research question is whether it is possible to build a charging infrastructure with the blockchain technology that enables simple, cost-effective business relationships between energy producers, charging station operators and customers, without wasting large amounts of energy for the administration?

Does this technology also provide the opportunity for small producers of renewable energy to participate? Is a charging infrastructure possible without a central authority?

Summary of the expected results

- The right choice of blockchain form and correct algorithms can be used for the charging infrastructure of electric vehicles. There are also constellations of blockchain technology that are energy efficient.
- With the open decentralized architecture, the blockchain also enables small energy producers such as solar system owners to participate economically in the power supply of charging stations. The possibility of micropayments also allows the settlement of smaller quantities of energy delivered with low transaction costs.
- An architecture without a central element enables all trustworthy electricity producers to participate in the electricity market and deprives large corporations of the power monopoly.

1.3. Major references

An important introduction was to find out what blockchain technology is and how it works. The best document for this was the "white paper" by Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System". Satoshi Nakamoto - the pseudonym of the hitherto unknown person who designed bitcoins and programmed the original reference implementation. Further on other diverse technical books about blockchain technology up to the programming of the various blockchains - Andreas M. Antonopoulos: "Mastering Bitcoin").

After grasping the most important technical aspects, different perspectives on the subject matter were also necessary. Daniel Drescher's book "Blockchain Basics: A non-technical Introduction to 25 Steps", Daniel Burwinkels et.al. "Blockchain Technology: Introducing Business and IT Managers" and Henning Diedrich's "Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations" have been key sources of non-technical access to this topic.

It soon became clear that decentralized transaction systems and currency systems are also highly relevant, which further led to Elfriede Sixts book " Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie". The European Central Bank (ECB) was also a valuable source of information here. Only "Virtual Currency Schemes", "Report on Electronic Money" and "Impact of Digital Innovation on the Processing of Electronic Payments and Contracting: An Overview of Legal Risks" are cited here.

Not to mention the networking technology, Selected chapters of "Peer-to-Peer Computing" by Alfred Wai-Sing Loo. Cryptography is also an essential part of the technology. Helpful to understanding cryptography was the book by Christof Paar Jan Pelzl " Kryptografie verständlich ".

After blockchain technology offered a public ledger, literature was also required regarding privacy. An interesting manifesto by Eric Hughe was written in 1993: "Cypherpunk's Manifesto" - is attached at the end. In this context, information from Luis-Daniel Ibáñez, Kieron O'Hara and Elena Simperl from the document "On Blockchains and the General Data Protection Regulation" was also used.

I did not have to look for electrical engineering because I had attended a technical school in electrical engineering, but I had to complete only information about photovoltaic and charging stations from "Solar Powered Charging Infrastructure for Electric Vehicles" by Larry E. Erickson.

After the blockchain technology is a new technology and constantly new concepts and ideas emerge, the Internet was also a helpful source of information. The latest information on "Colored Coins", "Transcation Fees" latest consensus algorithms, implementations of various blockchains such as "Ethereum" or "Multichain" were obtained from official websites. The sources can be found in the attached bibliography.

Key insights into "governance and regulation" were gained in "Distributed Ledger Technology: beyond Block Chain" by the British Government Office for Science.

Vincenzo Morabito's "Business Innovation Through Blockchain" and "Bank Principles for Systemically Important Payment Systems" from the Bank for International Settlement also provided relevant information.

Intensive analyzes and categorisations of the found documents were necessary to find out the relevant parts for the master's thesis. After some sections had been built on other parts, a suitable structuring of the work had to be found.

1.4. Method of approach

First, the underlying technologies of the blockchains were analyzed for their impact on different areas. This includes technical, ecological, economic aspects as well as legal and social impacts. This includes a comprehensive literature review of blockchain technology, cryptography, economics, currency schemas, legal aspects of European legislation, smart charging, smart meters, renewable energy and the environment. After analyzing these possibilities, a suitable configuration as an application for a charging structure is sought, which corresponds to the requirement of a sustainable energy planning.

1.5. The application idea

The blockchain or distributed ledger offers a new approach to data management and data exchange between contractors. This approach can be used as an efficient solution for many industries. The contract negotiations and the implementation of contracts are simplified. Also, transactions can be performed without a trusted third party. Blockchain creates contract security - Trust in a trustless world.

In future, blockchain technology will always be used where third parties were previously involved between two contracting parties, which cost money, slowed down processes, and often also required the disclosure of sensitive data.

(Dannen, 2017, S. 165) (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 223)

1.6. The business case

After everything runs digitally within a system, the costs can be kept low. Costs can also be saved by eliminating third parties.

It also offers opportunities to run the micro business at no high cost. Small energy suppliers can also participate in a distributed charging system and offer their green energy. (Sixt, 2017, S. 141) (Office for Science, 2016, S. 76)

1.7. Aspects and Objectives of e-vehicle owners

Owners of electric vehicles need a good infrastructure to charge their batteries. So there must be a tight network of charging stations where they can easily charge their vehicles. These charging stations can be large charging stations of large operators that are used during a journey along the traffic arteries, but also small, possibly private, charging stations away from the metropolitan areas that can be used during parking. A tight network of charging stations in cities also allows electric vehicles to be recharged wherever they are parked. That would be of great value to electric vehicle owners. For example, an electric vehicle used for the outward and return journey to work may use a smaller battery if there is an infrastructure to charge the electric vehicle at work. A smaller battery would reduce the weight of the vehicle and also the initial cost. A good charging infrastructure gives electric vehicle owners a wider choice of when and where to recharge their batteries. This also increases the convenience.

The available charging stations should be available in an online database. Further information such as offered power sources, payment options, reliability and the availability of free charging stations must be available in a navigation system. It should also be possible to reserve this charging station in the area. This should be possible both domestically and abroad.

Before the loading process, the contract terms must be negotiated and fixed unchangeable. The measurements of the amount of energy charged must be within a defined tolerance range, which means that the accuracy of a charging station measuring device must be verifiable. In particular, for private charging stations, this must be easy because they cannot afford a high financial cost for regular calibrations. These stations must be trustworthy, no irregularities should occur during charging or paying. So there must be a trusted charging station system in which irregularities are prevented, or if they can nevertheless be eliminated.

Similarly, many owners want to determine the source of the charging current. It must be possible to select energy sources from renewable sources. This source should also be verifiable so that no fraud with the origin of the stream can be made.

As more and more companies equip their vehicle fleet with electric vehicles, accounting must also comply with the law. Since not every private charging station has a connected printer, it must also be possible to receive electronically signed invoices.

Many parking lots with charge lock are currently blocked by non-electric vehicles and you do not even get to charge the battery. Strictly speaking, such parkers are not even

false parkers, because the road traffic regulations have not yet been adapted for these situations. There is a lot of discussion, but it has not been implemented yet. It would help if there were parking spaces with charging stations only for e-vehicles, but also mixed usable for all vehicle types
(Doleski, 2014, S. 629).

Agendas that need to be considered:

- Good infrastructure of charging stations
- Have the best charging possibility for long travels or overnight parking.
- Key data available online
- Electricity supplier selectable
- Reservation system for charging stations
- Various payment systems
- Charging stations must be trustworthy.
- Electronically signed invoices
- Calibrated and certified measuring equipment
- Fraud prevention

(Doleski, 2014)

1.8. Aspects and Objectives of the charging station operators

Charging station operators want to create a pleasant climate for their customers, so that they also have an incentive to use the offered additional services. This improves the use case of petrol station operators. This can be done through a diverse range of charging options, power selection and payment options. If car owners are able to connect their vehicle to charging stations when they stop at the mall after work, especially when it is necessary to recharge the batteries in places other than at home, can help bring customers to a store, health club or restaurant. But customer loyalty programs are also possible here.

The operators want the highest possible utilization of their charging stations by their customers. If customers can already reserve charging stations in advance, this will increase the predictability of the operator. It even makes it possible to reserve these amounts of energy required in advance, which also helps the operators of power grids to make these available. Just a single Tesla Supercharger station can burden the network with 120kW (https://www.tesla.com/supercharger), as a predictive planning of the amount of energy is necessary.
(Sumedha Rajakaruna, 2015) (tesla, 2018)

Many customers want to support the environment and only refuel with green energy, so it must be possible for the operator of the gas station to provide a broad contingent of energy sources so that the customer can comprehensibly use it for the charging process. These renewable energy sources must be certifiable by certificates and be clearly attributable to the customer.

Due to the ever increasing distribution of crypto currencies and electronic payment transactions, the operator must be able to offer many payment channels. After there will be charging stations without an on-site care, the payment process must be regulated so that the owner of the charging station is guaranteed to get his money for the charging process. It must therefore be possible to reserve the agreed fee for the loading process before the start of the load, and to automatically credit the account of the operator upon completion of this transaction.

Large commercial gas stations are subject to regular maintenance, calibration and control so customers can be sure that the measured values are correct. Small private charging stations will not be able to perform maintenance and testing that often, so other verification methods must be used. One possibility is to compare the current measurements of the charging station with the measurement of the vehicle. With statistical methods, it can be determined here whether the measurement accuracy is still within a specified tolerance. A fully automated charging station could then even independently request a recalibration service. This allows charging stations to ensure that they work correctly - even small private stations.

The charging stations naturally require a suitable connection to the power supply network. From a normal power outlet, a maximum of 16 amperes can be purchased at 230 volts, which is just under 3.7 kilowatts. Using all three phases, with a phase to phase voltage of 400 volts, the power triples to 11 kilowatts. In a 3-phase power connection with a maximum of 32 amps per phase, it is 22 kilowatts and three times 63 amps, it is 43 kilowatts. Owners of private charging stations will therefore not be able to offer fast-charging services as standard systems with household characteristics typically have a maximum current of 25A per phase. It will therefore also be necessary to install fast charging stations in less populated areas as small charging stations cannot charge the batteries fast enough to allow the vehicle owner a comfortable journey. If the operator of the charging station has its own renewable energy source, of course, he will also want to offer this energy.

(Przemyslaw Komarnicki, 2017, S. 166)

Private charging stations should be able to carry out autonomously all actions, from the reservation of the filling station, the settlement of the charge, the execution of the loading until the automatic transfer of money and the production of the physical or electronic invoice.

Agendas that need to be considered:

- Want to have a high utilization.
- Attract the customers
- Offer range of energy sources, renewable or conventional.
- Offer certified renewable energy.
- Generate further sales through additional services.
- Good predictability of use.
- Offer various payment services.
- Offer reservation system for customers.
- Guaranteed to receive the reward for the loading process.
- Offer paperless payment procedures that comply with the tax standard.
- Disclose the quality of your measuring equipment.
- Know the trustworthiness of the customer. (Know your customer)
- Sell your own green electricity.
- Buy cheap electricity through better planning.

(Przemyslaw Komarnicki, 2017) (Veneri, 2017, S. 224)

1.9. Aspects and objectives of the energy providers

Charging stations can require a significant amount of electricity, Tesla Supercharger stations up to 120kW, private charging stations from 3.7kW to 11kW. If the majority of electric vehicle owners were to recharge their batteries at the same time, for example immediately after work, this would be a major drain on the grid at that time. To prevent this, consumers need to change their behaviour and use off-peak power when there is no high demand for the grid.

Price mechanisms motivate consumers to recharge their vehicles when there is a large supply of electricity, such as late at night and early in the morning. For the most part, consumers can save money and energy companies do not have to pay dearly for their energy production at these times. Consumers will be better informed at what times they should use their electrical appliances.

In general, electric power grids are designed for the maximum possible load. Reducing this peak load and shifting the energy required to charge the batteries during off-peak periods allows the grid infrastructure to be made smaller. This leads to cost advantages on the producer side. Cost advantages and security of supply are therefore incentives for network operators to avoid expensive peak loads. In order to obtain a load that is as constant as possible over time, it can be regulated by means of intelligent networks and automatic control or monitoring by consumers.

It would be best if the electrical companies could control what time which vehicles are loaded, as they will stay in these places for a long time. This could also be done at charging stations at the workplaces so that even here it does not come selectively to high loads of the network. If you offer the customer that they are loaded by a certain point in time, but the electric utility controls when, this would improve network load sharing and save customers money. This could flatten the peaks in power generation from wind power or solar systems, so that less control energy is needed.

(Sumedha Rajakaruna, 2015, S. 5) (Veneri, 2017, S. 18)

Agendas that need to be considered:

- Maintaining network stability.
- Prices depending on the time of day reflect the current demand for the power grid.
- Balanced load distribution throughout the day.
- Consumption-oriented generation through advance planning and reservation.
- Charging at home at the own charging station controlled by the power supply company (variable price over the time of day).
- Generation-oriented consumption.

1.10. Aspects and objectives of state and society

The economic aspects associated with the charging infrastructure of electric vehicles include some other positive social effects. It can reduce the costs of mitigating climate change and improve urban air quality. The construction of charging stations and the modernization of the network will generate new jobs in the construction, electrical engineering and IT sectors so that these infrastructural facilities can be installed. There will also be jobs in the area of planning and production of the materials needed to build the charging stations and manufacture the IT equipment.

Since the batteries in electric vehicles can store energy and electric car owners can decide when to recharge their batteries, e.g. if there is a surplus of energy and therefore electricity costs are low, electric vehicles can be advantageous for a grid with wind and solar energy production. This can help with smart charging strategies to reduce greenhouse gas production, which is a primary goal of our society.

After charging takes some time, this leads to compulsive breaks of drivers who can thereby recover in this time and therefore reduce the risk of accidents.

Agendas that need to be considered:

- Greenhouse gas reduction
- Improving urban air quality
- Create new jobs

(Larry E. Erickson, 2017, S. 77) (Larry E. Erickson, 2017, S. 5) (Office for Science, 2016, S. 14)

2. Background Information:

Bitcoin, blockchain and Smart Contracts: What do we need to know about the decentralized future and how can we use these technologies in the renewable energy sector? Does it make any sense to use these technologies if there are alternatives?

Blockchains are based on a series of innovations as well as legacy technologies in organizing, storing and sharing data.

With blockchain technology, you can create in real-time, a unique, up-to-date version of the truth about actions, transactions and ownership that is accepted and used by all participants of the blockchain system. (Dietrich, 2016, S. 20)

This in turn enables the development of new methods and models of complex systems based on the use of transparent real-time data, the immediate execution of transactions and the automatic execution of smart contracts. Even the business logic and contracts can be stored in the blockchain. (Burgwinkel Daniel, 2016, S. 58)

The name blockchain comes from its technical structure - a chain of blocks. The blockchain is also called Distributed Ledger. The aim now is to store transactions in this blockchain tamper-proof and correct. It must be ensured that the initiator of a transaction is authorized to execute it. The transactions are created and exchanged by the participants of the blockchain network, which, if considered correct by the distributed network, change the state of the blockchain.

Each block of the blockchain is a data structure that makes it possible to store a list of transactions. Each block of the blockchain is tamper-resistant associated with the previous block through a cryptographic hash. Only correct transactions are included in a Block and only correct block are included into the blockchain.

Blockchains offers a new approach to managing real and virtual goods and values which can be used as a solution to many inefficiencies today.

This technology enables a group of independent individuals or institutions to work with universal, up-to-date and unchanging information, and to automatically establish consensus among all parties, even without direct trust between the people involved.

In principle, any stored information could be represented in a blockchain, from the energy consumed in a charge, the source of the energy delivered, the ownership of assets, statistical data, the deviation of a charging station's energy metering, smart contracts, and more.

(Bashir, 2017) (Prusty, 2017)

Bitcoin, a crypto-currency based on blockchain technology, has allowed mutually suspicious companies to make financial payments without relying on a single trusted third party.

Blockchains are a distributed information technology with multiple mutually untrusting parties, each with different economic or political goals. Also, in countries that according to Transparency-International have a high corruption index[1] reliable transactions can be carried out.

So far, you always had to rely on a trusted third party to allow each other's mistrusting companies to exchange financial value or interact. In the economy, these were mostly clearing houses that could establish the consensus between the parties as an impartial third party.

In daily life, a bank controls the bank balance in an account database and ensures that every transaction is valid and authorized by the customer when money is moved. When money has been transferred abroad, the SWIFT system is used as a trusted intermediary.

Blockchains eliminate the need for trusted intermediaries, as the writing of entries in the distributed account book with multiple untrusted writers is governed by the blockchain technology.

(Hofmann, 2018, S. 43)

Reasons to prefer a block-chain-based infrastructure to a trusted intermediary may include lower costs, faster transactions, automatic reconciliation, and clearing of the clearing houses. Also, this technology allows to change the way society is built, acts and interacts - it revolutionize. It will take absolute power from the central organs of power, because everything is open and transparent, and they will be kept in the system as a maximum in a controlling role. (Morabito, 2017, S. 28)

The openness of the system and transactions is achieved by a distributed ledger. The leger is stored on all participating nodes. Whereby not every node builds up with every other node, but only forwards the information it receives to its known nodes, which forwards this information to its known nodes.

[1] https://www.transparency.org/news/feature/corruption_perceptions_index_2017#table

With the Internet, an infrastructure is available in which data is often copied so that many copies are available, sometimes with small changes or errors, but it is no longer clear what the original was. The blockchain can change this. It allows network wide to propagate only one truth, which was found by means of a consensus algorithm. In a consensus algorithm, the majority of all nodes agree on the validity of the transactions, and as long as more than 50% of all participating nodes consider the transactions supporting cryptography to be correct, it will also be true. As long as more than 50% of the nodes are honest, the information stored in the blockchain is the truth. So as long as a participant in a transaction can use cryptographic methods to prove that they own the resource they are trading, the other participants can trust it.

If all participants operate from their own local version of the information rather than having to query information at a central location, the overhead of querying and duplicating data and the associated costs and risk of error is reduced. There is no massive burden on a central institution, no single point of error, which reduces the risk of failure or congestion. Contracting parties may disclose information to each other without consulting a central authority.

(Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017)

Of course, a big question here is the privacy and the betrayal of company strategies. Even before the revelations of Edward Snowden, the Cypherpunks realized that the increasing digitization of the Web made it increasingly necessary to protect privacy. Today's cryptographic encryption technologies can now ensure the security and anonymity of highly sensitive data in public environments. Thus, it is in the interest of users to disclose only information that is required for the consensus of blockchain but otherwise remain anonymous. (Sixt, 2017, S. 149)

Blockchain technology creates a system for electronic transactions that is pseudo-anonymous, counterfeit-proof, and open and without us having to trust each other in business cases. It's a new and efficient way to consistently run system operations.

To understand a renewable energy application, we first need to break the technology down into its components. The blockchain is a series of innovations that build on each other and need to be understood separately.

Subsequently, we will be investigated how blockchain technology can be used in the energy market. But also the meaningfulness is analysed.

A system is then built up based on the blockchain technology and the associated innovations. We will look at the benefits and analyse the impact on different participants and parts of the system.

2.1. Charging stations

The manufacturers of electric vehicles, charging stations and the energy industry realize that only by standardizing the interface between the grid and the vehicle can safe and reliable energy transmission be ensured on a permanent and cross-border basis.

Charging stations have different connection capacities depending on the type of station. Large charging stations will have to have at least a 10kV and at least 100kW connection, small charging stations will need a connection to the conventional 3-phase power network with 230V (400V from phase to phase).

For optimum charging to take place here, communication between the vehicle and the charging station is required in order to determine, for example, the maximum charging power of the charging station.

In order to regulate this, standard IEC 61851 has been developed in international standardization committees. This standard regulates the charging stations and deals with the different charging modes, especially the conductive wired charging systems. A new standard has been developed, ISO 15118, which focuses on communication between vehicle and charging infrastructure.

If a driver has found a charging option, he can take care of loading the vehicle. For this he needs a charging cable. Simple cables that fit anywhere are equipped with a Schuko plug.

Due to the fact that only one phase can be charged and this plug is not suitable for 16-ampere continuous current, manufacturers are usually limited to a maximum of 10 ampere. (see Figure 2)

Contamination of the contacts increases the contact resistance, which then leads to even higher thermal losses between plug and socket in the following. To regulate this, appropriate standards have been developed.

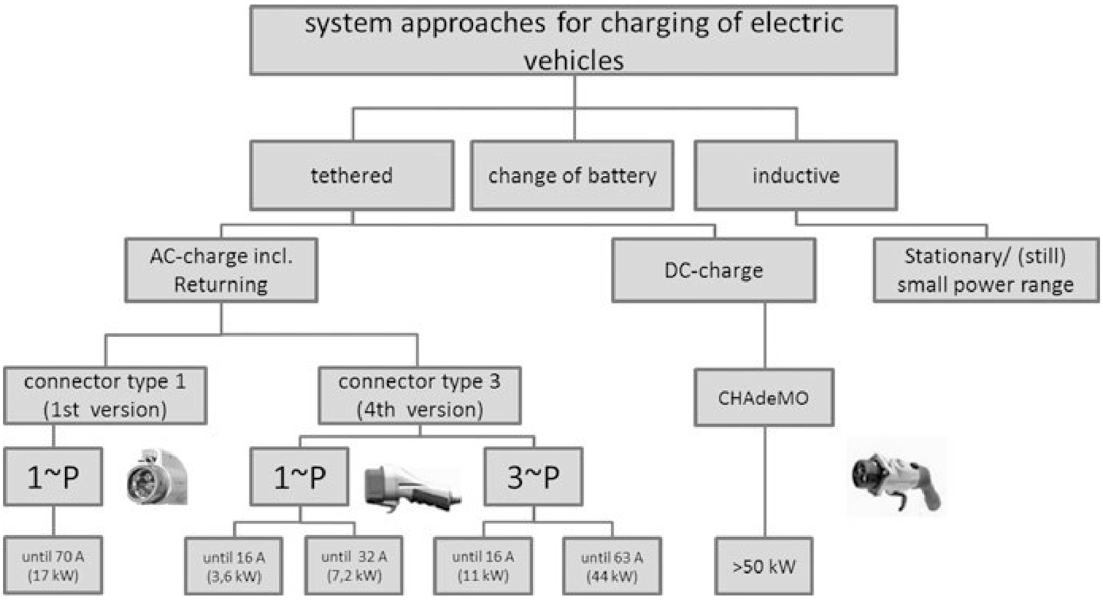

system approaches for charging of electric vehicles
tethered
change of battery
inductive
AC-charge incl. Returning
DC-charge
Stationary/ (still) small power range
connector type 1 (1st version)
connector type 3 (4th version)
CHAdeMO
1~P
1~P
3~P
until 70 A (17 kW)
until 16 A (3,6 kW)
until 32 A (7,2 kW)
until 16 A (11 kW)
until 63 A (44 kW)
>50 kW

Figure 2: Electric-vehicle charging systems (Przemyslaw Komarnicki, 2017, S. 166)

IEC 62196-1 refers to connectors (plugs), sockets, sockets and pre-assembled cables for electric vehicles used for wired charging systems. Specified for a range of

- 690 V AC, with 50 to 60 Hz, at rated current up to 250 A;
- 600 V DC, with rated current up to 400 A.

The charging modes are based on the specifications of IEC61851-1: [2]

- IEC 61851-1 "Mode 1" - slow charging to household sockets with earthing contact (Schuko) intended for single-phase or three-phase alternating current up to 16 amps.
- IEC 61851-1 "Mode 2" - one to three-phase charging is intended for device current up to 32 amperes. The signalling to the vehicle is limited to fixed values,
- • IEC 61851-1 "Mode 3" charge with specific charging kits for electric vehicles with pilot and control contact for fast charging up to 250 A. For higher charging currents, a suitable charging mode must be detected. Pulse width modulation is used to encode the maximum permissible charging current or the availability of digital communication.
- IEC 61851-1 "Mode 4" - fast charge controlled by an external charger for fast charging with DC up to 400A

The new communication standard ISO / IEC 15118 will in future be the central protocol for the communication between the vehicle and the intelligent power grid.

ISO / IEC15118 identifies the non-limited services, high-level standard for AC and DC charging, integration of renewable energy, network-friendly charging, as well as authentication (plug & charge) and value-added services.

Powerline (PLC) and a TCP / IP protocol stack are used as part of the communication between the car and the infrastructure, alternatively via User Datagram Protocol (UDP). The car is client, the charging point is server.

The vehicle uses an electric vehicle communication controller (EVCC), a charger, an ECU (microcontroller) and an HMI (operating unit).

The charging point requires a Supply Equipment Communication Controller (SECC), an Electric Energy Meter (eHZ), Contactor (contactor), Paying Unit (payment unit), HMI (operating unit).

The loading process will then proceed as follows according to this protocol:

- The vehicle authenticates.
- Then it asks for services such as charging charges or value-added services.
- In the next step, the energy network transmits the maximum possible charging power via the charging station and hands over a price table to the vehicle.
- The vehicle then responds with a desired charging schedule (time slot, charging power, source such as photovoltaic).
- Then the charging process starts.
- During loading there is always the possibility to adjust the loading plan.
- At the end of the charging process, the meter reading is acknowledged.

Modern charging stations also have a reservation system for the charging station.

The charging stations will divide into large commercial stations, small commercial and private stations, where the customer wants to initiate the same charging everywhere. Apart from the conventional charging and payment processes, as we already know at the large filling stations, it will be necessary to have another trustworthy option for smaller unmanned charging stations in order to have a nationwide charging system.

Thus the owners of electric vehicles are ready to use these unsupervised stations, they must build confidence in these. Trust that both the payment process is correct, as well as that the specified amount of charge and thus the amount to be paid is correct. To commercially operated charging stations here is the confidence that companies operate this, rather than in small private stations that are not subject to strict and permanent control.

It must therefore be created a trusting system in which the correctness of the billing can be checked at any time. Trust is an important component in a business - trust that you get what you paid for, or trust that you get payed for what you have delivered. (Veneri, 2017, S. 277) (Sumedha Rajakaruna, 2015, S. 203) (Przemyslaw Komarnicki, 2017, S. 172)

2.2. Energy Sources

As more and more vehicles are powered by electric power, new power plants need to be built to meet the increased power needs. After analysing the situation in Germany, there is only a 4% increase in energy demand if 25% of the vehicle were powered purely by electricity. (Doleski, 2014)

In the process, only the work was considered, of course, the current delivery to vehicles is distributed over the entire network, not equally in terms of time or power consumption.

This raises the question of the capacities and the amount of charging power of the network. It is crucial here whether all drivers want to load at the same time, or what from the point of view of the network would be desirable to load all in succession. This is crucial if the distribution network needs to be further expanded.

The expansion of the transmission and distribution network is a significant cost driver for the users of the network. A possible alternative to massive expansion is a controlling intervention in the charging times, the duration or the amount of charging energy.

Considering the driving or charging behaviour and the availability of regenerative generated energy, there are also times when regenerative generation is insufficient and conventionally generated energies are needed. Here is a shift of charging times in periods when renewable energy is available meaningful. The use of energy storage would also be useful.

The charging power of each vehicle can be very high, but it is also adjustable in many cases. This possibility of controllability and an intelligent network, which knows its load situation, make new approaches to grid-compatible charging possible.

An intelligent system that handles this control could solve this problem.

Renewable sources can be better integrated by anticipating the required energy gaps because the demand is known and conventional power plants can be better regulated.

The way energy is generated is becoming more and more important as more and more customers choose environmentally friendly energy from renewable sources, so the source of the electricity must be available and forgery-proof.

(Doleski, 2014) (Sumedha Rajakaruna, 2015)

2.3. Payment Services

Communities have created and circulated currencies for the exchange of goods and services they offer, thereby providing a medium for trade and settlement for that community.

It is difficult to determine the exact origins of the currencies. It seems that payments in the form of money are already around 2200 BC Christ were made.

(ECB, 2012, S. 9)

A brief summary of the most important changes: In 1609, the Bank of Amsterdam issued paper money for the first time, always paying attention to adequate coin cover. The Bank of England introduced the minimum reserve system at this time. This allowed the banks to re-lend most of their deposits, assuming that the sovereign, or rather the state, vouched for it.

In 1716, the French regent Philippe Duke of Orleans granted the Scottish economist and banker John Law the license to print money in France. John Law had the idea that not only the limited supply of precious metals but also real estate to cover the banknotes in circulation could be used, as well as its future earnings. But he put forward a more daring construction, the state could print at any time money and claim the necessary cover would be in the future tax payments of its citizens. The money cover was thus the tax debt or the tax payment of the future.

The ability to buy and sell new money "from the air" by buying government bonds also fuelled the recovery of the economy and thus a noticeable upswing in France. It came about that less than 10% of the paper money was covered by solid values. Finally, this system ended in 1720 in a fiasco.

This idea made John Law the "father" of the so-called fiat currency. The term fiat currency is derived from a Latin biblical quote "fiat lux" - "let there be light"

(Sixt, 2017, S. 49)

When silver became scarce for coinage, it was agreed at the International Monetary Conference in 1867 to take gold as the currency standard of value. This meant that from now on any banknote could be exchanged for gold at a fixed exchange rate. The advantage of the gold standard is avoiding any inflation. During the global economic crisis of the 1930s, gold price fixing reduced the US central bank's ability to raise new money to boost the economy through new lending.

(Sixt, 2017, S. 50)

In 1876, the newly founded Reichsbank introduced cashless payment transactions in the German Reich, the so-called book money or bank deposit on bank giro accounts. The book money is a means of payment that can be used in banking by transferring current account to checking account by means of bookings.

Where book money can arise in two different ways:

- by depositing cash into a bank account and
- by issuing a loan, by crediting the loan on the account of the bank customer e.g. demand deposits.

The book money creation is limited only by that commercial banks must hold a certain percentage amount of the loan amounts they awarded as minimum reserves.

Today in the developed economies the largest part of the financial system consists of book money. With cash only a small part of the liabilities is paid.

(Sixt, 2017, S. 52)

In the late 50s had accumulated large dollar holdings abroad, which could no longer be covered by the US gold reserves. In the 1960s, the flexible gold price created massive problems, and in 1971 Richard Nixon discontinued the Bretton Woods deal. Each state could now decide for itself on the extent of money in its domestic market. This was the basis for the globalization of finance, and the world economy prepared.

A fiat currency today is any legal tender issued by central government agencies and accepted in exchange for goods and services. It is money in which the issuer has no obligation to redeem another currency or a commodity. The confidence of the people in central banks or governments is the basis of this currency. The general acceptance is governed solely by legal regulations.

(Sixt, 2017, S. 50)

Today's central bank money, such as euro, is fiat currency.

> *“Now, following Goodhart (2005: 817), one can distinguish two main theories about the nature of money: metallism and chartalism.”*
>
> *(Rossi, 2007, S. 9)*

The metallistic school of thought considers money merely as an asset that has its own intrinsic value.

Metallists say:

- that money must be accepted as a barter in general and
- All goods that are generally accepted as bartered goods should be called money.

This metallic view is based on the idea that a currency should be a tangible material, or at least secured by such a material. (Rossi, 2007, S. 12) (Sixt, 2017, S. 53)

For the Chartalists, the value of money is not determined by its value, but by the following principles:

- On the one hand because of its social acceptance and on the other hand
- comes about through the state and its laws.

This group sees this as an agreement that encompasses the whole society.

The currency for the Chartalists is merely the coupon or symbol that is at the centre of this complex system.

In the classical theory of money, money had only the task of simplifying the exchange of goods and services, which corresponds to a metallistic view. Monetarism is based on relatively stable demand for money. Central banks should adjust the expansion of the money supply to long-term real economic growth. (Rossi, 2007, S. 16) (Sixt, 2017, S. 54)

The development of cryptocurrencies also plays an important role in the use of blockchain technology in charging stations. You could use your own currency. The phenomenon and the concept of cryptocurrencies fascinate many supporters of metallistic concepts, but these crypto coins have no intrinsic value, as in the classical metallic perspective.

Modern monetary constitutions in the developed countries are currently characterized by the following characteristics:

- The monopoly of money production is centralized.
- These central authorities are not bound by any cover rules to any substance value.

Trust is also the basic element of modern monetary systems, but all too often this trust has been destroyed.

Deregulation since the early 1980s has led to increasing speculation. There is a decoupling of the development of the real economy from developments on the financial markets and a massive redistribution of social wealth from wages to capital income. This should be avoided in the charging station accounting system, speculation possibilities reduce the users' confidence in the system.

However, since the 2008 financial crisis, it has become apparent that a credit boom is historically the most reliable single indicator of financial crises. Many Bitcoin enthusiasts do not consider coincidence in the publication of the White Paper by Nakamoto Satoshi in the midst of the 2008 financial crisis. The subsequent success of the Bitcoin system, in their opinion, goes back to the massive loss of confidence in the financial system.

(Sixt, 2017, S. 62)

Above all, Nakamoto has limited the amount of money in the Bitcoin code to 21 million bitcoins, which is the greatest evil of Fiat currency, to prevent the infinite money creation. If the majority of users of the Bitcoin payment system decide to increase these monetary units, it will be a majority vote of the users and not the lonely decision of a central authority. These majority decisions are made possible by the blockchain technology. (Antonopoulos, 2017, S. 216)

In the real world, too, the search for alternative payment systems to the state currency has been frequent over the last decades.[2] Especially in times of economic crises there was and is a high number of complementary payment and settlement systems. These complementary currencies form their own closed currency clearing, based in part on official currencies.

Many concepts or real experiments in the field of complementary currencies as an alternative payment system refer to the economist and social reformer Silvio Gesell. At the beginning of the twentieth century he propagated free money or fines as an effective means of stabilizing regional economic areas. During the world economic crisis it came in different places in Germany and Austria to actions with free money, which had great success. A built-in loss of value should increase the speed of circulation of money and boost the local economy. The aim was to stifle the receipt of unpaid income over interest and the tendency to hoard money.

(Sixt, 2017, S. 67)

Alternatively, you can use in a payment system, the new crypto currencies such as Bitcoins, ethers or other currencies. But it can also be built using the block chain technology own currency. This can have a direct link to a currency or even a currency that is created from "air" like the common crypto currencies.

According to European Central Bank one can divide Crypto currencies following: VIRTUAL CURRENCY SCHEMES (see Figure 27)

[2] Alternative currencies: Der oberbayrische Chiemgauer, Die belgische Regionalwährung RES, DasWörgl-Experiment, Der Schweizer WIR-Franken

> *“Depending on their interaction with traditional, ’real’ money and the real economy, virtual currency schemes can be classified into three types:*
>
> - *Type 1, which is used to refer to closed virtual currency schemes, basically used in an online game;*
> - *Type 2 virtual currency schemes have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can subsequently be used to buy virtual goods and services, but exceptionally also to buy real goods and services; and*
> - *Type 3 virtual currency schemes have bidirectional flows, i.e. the virtual currency in this respect acts like any other convertible currency, with two exchange rates (buy and sell), which can subsequently be used to buy virtual goods and services, but also to purchase real goods and services.”*
>
> *(ECB, 2012, S. 5)*

For use with charging systems for charging stations, type 2 or 3 can be considered here.

When electronic means of payment are used, latency is of great importance. But you have to distinguish between 2 times.

1.) How long does it take for the payment system to accept the transaction as valid: This only takes seconds for VISA cards. At Bitcoins, however, about 10 minutes.
2.) When is the transaction stored invariably on the recipient's account? This can take up to a month for Visa cards because the payer can cancel the transaction in that period. Bitcoin technology is faster here, about 1 hour, but bitcoins have only one probable settlement.

New applications such as a charging station system require the possibility of micropayments. The term micropayment refers to a method of payment of small sums. The Bitcoin block chain currently enforces a minimum amount that requires a fixed transaction fee that is above the Micropayment. This makes the micropayments impractical. Bitcoin developers are working on a draft paper on the "Lightning Network" with which you can downscale the fees to 0.00000001 Bitcoin.

All these currencies considerations must be considered when building a charging system. Expectations of a payment system are therefore multifaceted:

- The whole process should work quickly
- Offer many possibilities (cash, debit card, credit card, electronic transfer, cryptocurrency)
- Work reliably
- Be traceable at all times.
- Allow trusted transactions
- Low expenses, even with small transactions
- Be safe against hacker attacks or fraud
- Short time to the final processing.

(Settlements B. f., Core Principles for Systemeatically Important Payment Systems, 2001, S. 29) (Laurence, 2017, S. 133) (Karame & Androulaki, 2016, S. 52) (Poon & Dryja, 2015)

2.4. Background Information about Blockchain Technology

It is important to be aware of the similarities and differences between cryptocurrencies and blockchain technology, as these words are now used interchangeably, although cryptocurrencies are only one use case of blockchain technology. Blockchain technology requires decentralized consensus on the recording of events between untrusted entities. Therefore, many technical possibilities, such as digitally signed transactions, peer-to-peer networks, and a very robust consensus algorithm are needed to produce a chain of correct blocks. The blockchain technology enables direct transfers of economic goods via the Internet, without a trusted intermediary.
Bitcoin is not the blockchain, Bitcoins use the blockchain technology.

2.4.1. IT-technology needed to understand the Blockchain

2.4.1.1. Cryptographic checksum

A cryptographic hash is a special form of hash value. Calculating a hash value using a hash function is a daily business in computing. Mathematically speaking, a hash function is a function that calculates a unique value for data of variable length. The hash value can assume only a limited amount of values while the source data can be of any size. (see Figure 3) Hash functions should change about 50% of the output bits when changing one bit of the source data.

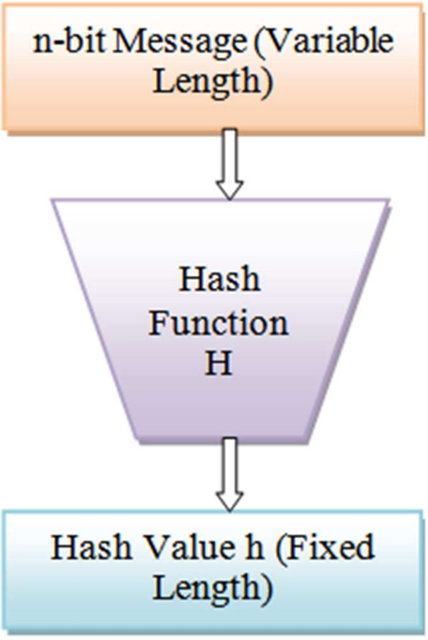


Figure 3: Hash function. (Kumar, 2015)

Hash methods are always used when it comes to finding a compact representation of large amounts of data in order to confirm their authenticity. So for example with crypto keys. The most important requirement is that every little change to the record leads to a change in the hash value. In addition, it must be virtually impossible for someone to create two records that produce the same hash value.

The algorithm of creating a hash value is not reversible, which means that you cannot return from a finished hash value to the origin.

To use a hash function for digital signatures (as we will use it), we must fulfil the following Security Requirements of Hash Functions as requested in the book “Understanding cryptography” (see Figure 4) (see Figure 14) (Paar & Pelzl, 2010):

> *“It turns out that there are three central properties which hash functions need to possess in order to be secure:*
>
> 1. *preimage resistance (or one-wayness)*
> 2. *second preimage resistance (or weak collision resistance)*
> 3. *collision resistance (or strong collision resistance)”*
>
> *(Paar & Pelzl, 2010, S. 296)*

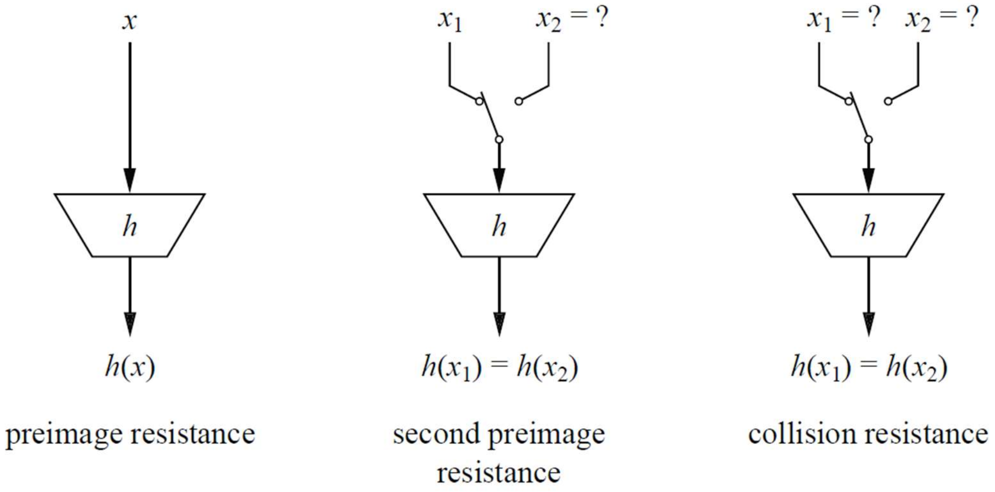


Figure 4: The three security properties of hash functions (Paar & Pelzl, 2010) (Paar & Pelzl, 2010, S. 297)

It is called a collision when two different source data produce the same hash value. This requirements are not trivial because collisions always exist if there is more possible output data than hash values.

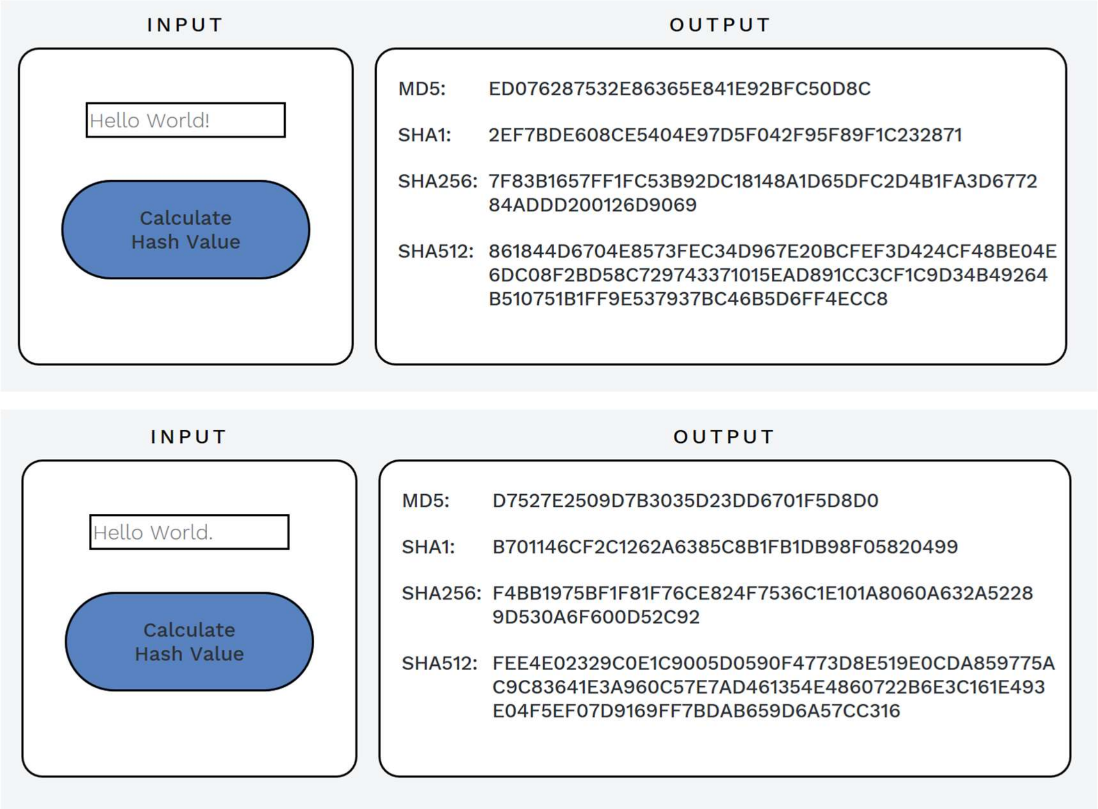
A hash function satisfying the said supplemental requirement is called a cryptographic hash function.

There are several cryptographic hash functions: md5, sha1, sha2, sha128 and sha256 for example. (see Figure 5) But not all of them are still secure. SHA-1 has been cracked since 2005. At that time, Chinese cryptologists presented an attack that significantly reduced the number of calculations needed to find a collision.[3] Following the attack on SHA-1 by Marc Stevens and colleagues in 2017, this hash process can finally be banned.[4] (Schmidt, 2005)

One of the currently widely used cryptographic hash functions is sha256. A cryptographic hash is a signature for data. The SHA-256 algorithm generates a near-unique, 256-bit, fixed-size hash.

[3] https://www.heise.de/newsticker/meldung/Kryptoverfahren-SHA-1-geknackt-135372.html

[4] https://www.heise.de/security/meldung/Todesstoss-Forscher-zerschmettern-SHA-1-3633589.html



Hello World!

```
MD5:    ED076287532E86365E841E92BFC50D8C

SHA1:   2EF7BDE608CE5404E97D5F042F95F89F1C232871

SHA256: 7F83B1657FF1FC53B92DC18148A1D65DFC2D4B1FA3D6772
        84ADDD200126D9069

SHA512: 861844D6704E8573FEC34D967E20BCFEF3D424CF48BE04E
        6DC08F2BD58C729743371015EAD891CC3CF1C9D34B49264
        B510751B1FF9E537937BC46B5D6FF4ECC8
```

Hello World.

```
MD5:    D7527E2509D7B3035D23DD6701F5D8D0

SHA1:   B701146CF2C1262A6385C8B1FB1DB98F05820499

SHA256: F4BB1975BF1F81F76CE824F7536C1E101A8060A632A5228
        9D530A6F600D52C92

SHA512: FEE4E02329C0E1C9005D0590F4773D8E519E0CDA859775A
        C9C83641E3A960C57E7AD461354E4860722B6E3C161E493
        E04F5EF07D9169FF7BDAB659D6A57CC316
```

Figure 5: Hash values for two minimally different sentences. (Drescher, Hash Function, 2017)

On the internet there are many pages that allow to calculate online cryptographic hash values according to the sha256 algorithm. An example of this is https://www.movable-type.co.uk/scripts/sha256.html (as of 2018), alternative sha256 calculators can be found on popular search engines with the keywords "SHA-256 Cryptographic Hash Algorithm online".

(Paar & Pelzl, 2010, S. 319)

How this technology will be used

We want to write data into the blockchain that should not be changed afterwards. This is achieved by writing the hash value cryptographically encrypted into the blockchain. If the output data is only changed for one bit, this is detected immediately because the hash value would be changed. So that the hash value cannot be manipulated, it is written into the blockchain using a suitable asymmetric encryption method. This Asymmetric encryption method guarantees that only the owner of the private key can generate this encrypted hash value. Those who have the public key can decrypt this encrypted data and read the correct hash value. If the decrypted hash value now matches the self-generated hash value of the output data, the authenticity of the output data can be ensured.

2.4.1.2. Asymmetric encryption / Asymmetric key pair

The most important task of cryptography is the protection of data against unauthorized access. This protection is provided by encryption with digital keys. The digital equivalent of closing a vault is encryption, while the digital equivalent of opening a vault is decryption. There are two different types of encryption/decryption - symmetric and asymmetric methods.

A symmetric algorithm uses a single key for encryption and decryption. If you have this key, you can encrypt and decrypt your messages, but anyone else who has the key can decrypt this message and also encrypt a message. This is not relevant for our application.

Blockchain technology uses an asymmetric key method. We've probably already seen in a movie that people break a banknote in two, so two people who have never met before know that they are talking to the right person when the two halves match. Similarly one can imagine asymmetrical keys.

Asymmetric methods use a key pair. These two different keys can be used for encryption and decryption. Data encrypted with one of the two keys can only be decrypted with the associated second key. It is irrelevant here which key is used for which process. If you use the 1st key to encrypt a message, the other person must use the 2nd key to decrypt it. If the other person now uses the 2nd key to encrypt his message, you can decrypt this message only with the 1st key.

With asymmetric algorithms, two different people can use these separate keys for private communication. It is practically impossible to generate the other key from one of the two keys and therefore impossible to decrypt a message with only one key.

Asymmetrical cryptographic techniques always use two keys to transmit an encrypted message, one known only to the recipient and one publicly known (the recipient's public key). The trick with this method is that an encrypted text can only be decrypted with the second associated key, which means the key used for encryption cannot be used for decryption, but only the second corresponding key can do this.

The two keys are interdependent, if one of the two keys is made publicly available two important functions can be achieved:

- Authentication: with the public key can verify that the owner of the corresponding private key has sent the message,
- Encryption, only the owner of the private key holder can decrypt the message encrypted with the public key.

(Paar & Pelzl, 2010, S. 173)

2.4.1.3. Digital Signature

A digital signature does not represent a hand-crafted signature that has been scanned in and stored digitally because it could easily be copied and misappropriated.

Digital signatures use hash codes as well as asymmetric key pairs with a public key. This is understood as a special checksum which, in the context of a digital document, has similar characteristics to a manual signature. They offer invincibility and integrity, but no secrecy.

So that everyone who has the document knows that you have written it, it can be provided with a digital signature. When you digitally sign an unencrypted message, allow anyone to read the content of the message. The digital signature only tells the recipient that the sender had access to the appropriate private key for the public key he has for that person.

For the hash code to be used for the signature, it must fulfill the following prerequisites:

- It must not be forgery.
- Their authenticity must be verifiable.
- It cannot be transferred unnoticed from one document to another.
- The associated document must not be able to be changed unnoticed.

It is not enough to just add the hash value to a document, because that way everyone could change the data and also the hash value. We still need a method to protect the hash value from manipulation. Here we can use asymmetric public key encryption.

To digitally sign a document and thus make it more counterfeit, the following basic steps must be taken.

1. Create the hash of the data. This ensures data integrity because the receiver can recalculate the hash value and compare it to the original hash to check if the data has changed during the commit.
2. Encrypt the created hash with the private key. Since only the creator knows the private key, the authenticity of the signature and thus of the signed data is guaranteed.
3. Attach the encrypted hash to the data.

This is now the signed message that can be sent to other parties.

The recipient can decrypt the hash of the message with the public key of the sender to obtain the unencrypted hash of the sent message. The receiver can now also generate the hash of the received message. If the two hashes match, the receiver is assured that the data was created by the sender, because only the sender can own the private key, and therefore only he can have created the encrypted hash.

Digital signatures have important features:

- Authenticity: The digital signatures can be verified by a receiving party. This check ensures that only the sender of the message can use the signing function with the private key.
- Immutability: Nobody is able to change the signed message because the signature is not correct.
- Non-reusability: The digital signature cannot be disconnected from a message and used again for another message.

(Paar & Pelzl, 2010, S. 263)

If the original message had been tampered with, anyone trying to compare the hash will get an error which tell the recipient that the message was changed.

We can now combine signatures and asymmetric key pairs.

Asymmetrical encryption allows two types of application:

- It allows a user to encrypt messages for a specific person so that only he can decrypt them.
- A person can send a message that can only come from him, since only he has the private key.

But there is another, combined application:

By combining the sender's private key with the recipient's public key, a message can only be read by the intended person and could only come from a particular sender. This allows a private encrypted communication of second participants only with the knowledge of the respective public key.

(Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 104)
(Paar & Pelzl, 2010, S. 259)

2.4.1.4. Communication with TLS (Transport Layer Security)

Securing data connections is state of the art today.

The three primary goals of using SSL / TLS are confidentiality, data integrity, and authenticity.

- *Confidentiality* is ensured by the encryption of the connection.
- By ensuring the *integrity* of the data, it is guaranteed that manipulation of the transmitted data is not possible.
- *Authenticity* means that the identity of the contacted server is verifiable. By ensuring the identity of the server, the client knows exactly who they are connected to.

> *“**Transport Layer Security (TLS):** [70] is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.”*
> *(Taylor, 2005, S. 145)*

This technique allows programs to take an encrypted (confidential) connection to an authenticated server and communicate with it tamper-free (integrity). Everything is open within the blockchain. Only the traffic between nodes is encrypted. But if you're a blockchain node yourself, you can see all the information and transactions.
(Schmeh, 2013, S. 655)

2.4.1.5. Network Architectures – Peer to Peer

If several computers are connected via network lines, then there is a computer network. A computer network provides the infrastructure through which the computers located at the connection points can communicate.

The topology has to be differentiated between physical and logical topology. Applications mainly use the logical topology, Peer-to-Peer (P2P) networks use a special logical topology called overlay networks. An overlay network is a computer network that is based on an existing physical network. Main features of an overlay network are a network above existing infrastructures with their own address space with its own addressing.

Peer-to-peer computing (P2P) is the sharing of resources between computers. These resources include processing power, knowledge, disk storage, and information from distributed databases. The concept of sharing resources is not completely new. P2P systems are a natural evolution in system architecture.

There are three types of networks on the Internet. (see Figure 6) The most common networks are organized centrally, such as Google or Facebook. A decentralized network, on the other hand, consists of equal servers that exchange data with each other for synchronization, and clients connect to one or more of these servers. A distributed peer-to-peer network, on the other hand, consists exclusively of equal peers and does not require a central server to function. Decentralised and distributed networks do not need a central server to work, all servers are eligible. (see Figure 9)

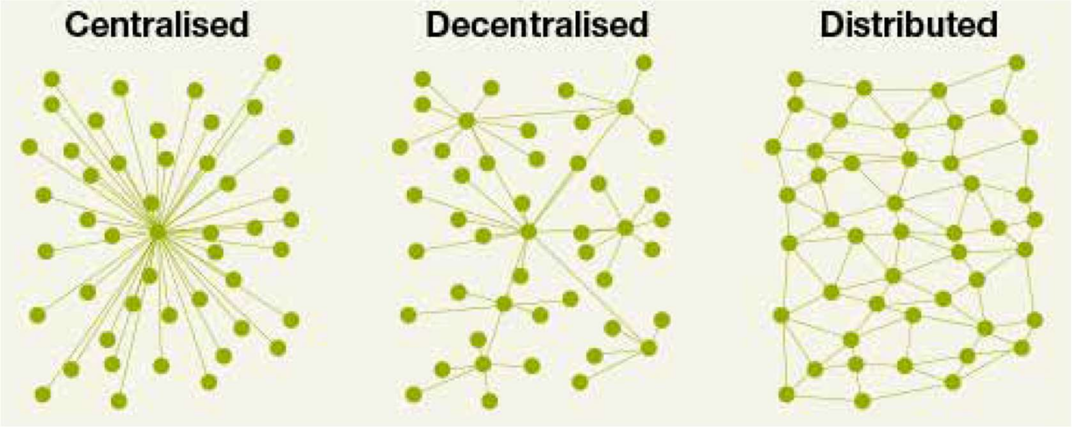


Figure 6: Topologies of Networks (Walport, 2016, S. 36)

Thus, a distributed network provides high availability and robustness because the infrastructure provided does not depend on individual central components, as is typically the case with centralized networks under the supervision of a single server.

Definition and Properties of P2P Systems.

> *"Peer-to-peer systems are distributed systems consisting of interconnected nodes able to self-organize into network topologies with the purpose of sharing resources such as content, CPU cycles, storage and bandwidth, capable of adapting to failures and accommodating transient populations of nodes while maintaining acceptable connectivity and performance, without requiring the intermediation or support of a global centralized server or authority."*
> *(Spinellis, 2004)*

In a P2P system, computers can act both as clients and as servers. Their roles in each task are determined according to the requirements of the system, as well as the role may change due to technical requirements.

Big advantage of P2P networks, the scalability:

Peers should be able to exchange resources directly with one another. These resources include files, storage, services, information, CPU performance, and above all, knowledge. Peers can easily enter or leave the P2P system freely. This allows users to retain control of their system and resources. Peers can belong to different owners. It is common that P2P systems have many owners, even each peer could have its own owner. The P2P network will continue to work if some of its peers are not working properly. Therefore, it is more forgiving than other systems. This ability to extend a network is called "scalability."

Centralized control and management are not required in a P2P network. Therefore, nodes in the operation of the P2P system take the same roles. In many system designs, this property is relaxed but not violated by the use of special peer roles such as mining peers, validator peers, super peers, or relay peers, as there are still many peer nodes with the same task. In this way, the cost of providing a central service with resilience and redundancy can be saved since this information is stored on all redundant nodes.

Peer-to-peer computing allows users to leverage collective power in the network. It generally takes less time to complete the task because peers can exchange resources directly without a server. Central, only simply available resources are always the bottleneck in a network. For certain tasks, the workload cannot be shared among the peers. (For example, if each node must prove the correctness of the shared data)

For a participant to be able to participate in a P2P system, it must be cost effective and easy to use.

To build trust, it must be safe to use. It should not rely on a software product from a single vendor, also promotes open-source software's confidence in this. The features of these products must be easy to extend.

(Loo, 2007, S. 6)

2.4.1.6. Important definitions of terms

Encryption: is fundamental to security and involves encoding (encrypting) data into something unauthorized persons without the proper key cannot understand.

Identify: We can identify participants or devices with signatures. A system can identify itself to partners with its signature.

Authentication: is used to verify the claimed identity of a user.

Authorization: involves checking that a user has the correct permission to perform a particular operation.

(Taylor, 2005, S. 134)

2.4.1.7. Micro payment

Micro-payment Small payment or micro-payment refers to a payment method that is primarily intended for the purchase of "paid content", including digital goods, such as music and newspaper articles incurred online. In these low-value goods, the cost-effectiveness of the payment is a central problem: Conventional methods, such as

credit card payment or direct debit are unsuitable, since the cost of payment often exceeds the value of the goods.
(Wikipedia, Micropayment - Wikipedia, 2018)

2.4.2. What is the Blockchain

The blockchain is similar in principle to the polygraph machine (see Figure 7). Many computers work together in a network. The blockchain is a technical system that allows many systems to write the state of a ledger into many local databases almost simultaneously.

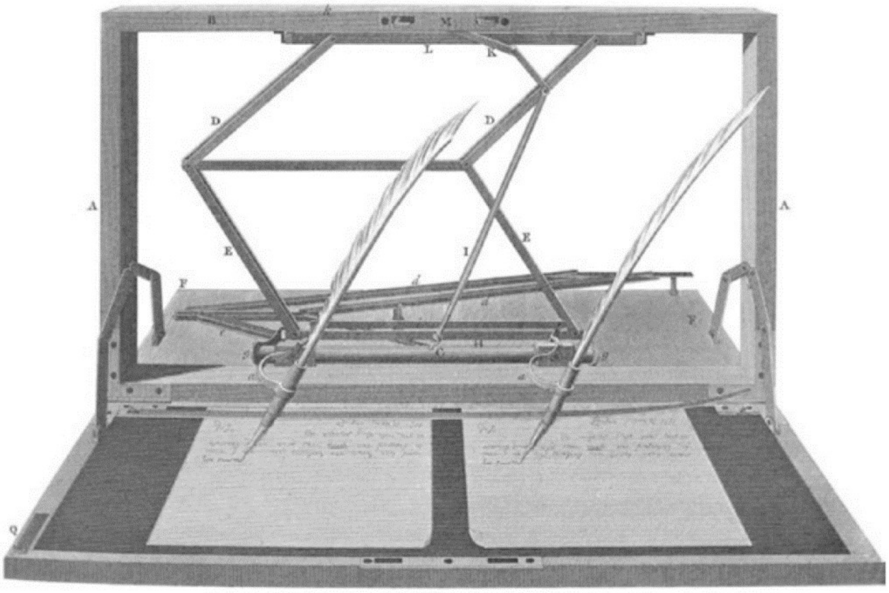


Figure 7: The polygraph machine was the first "copy machine," (Dannen, 2017, S. 25)

2.4.3. Current types of Ledger

Ledger books have been at the centre of commerce since antiquity and are used to record information, most commonly assets such as money, land and property. A Ledger is a recording tool in the form of a journal that contains all the material and capital movements of a company or society. All business transactions are recorded in a factual order and booked to individual accounts. From the general ledger, all details of the business transaction, such as the underlying transaction, the date of the transaction, the units transferred, such as money, materials, knowledge, energy, etc., must be visible.

Banks use a core banking system (also called core banking system, KBS or CBS). This core banking system is a database-driven software package for managing bank-based business transactions such as account management, savings processing, overdraft, credit, and ultimately, customer data management.

Banks track the customer balance sheets in a ledger. They control the Ledger database and ensure that each transaction is valid and authorized by the customer, so each transaction must be verified before it enters the general ledger.

In Austria, a land register with computer support is maintained in the district offices, in the past this was actually a hardcover book. Anyone can inspect the entries in the land register at any district court for free, or print out a written land register extract for a fee

The land register consists of the general ledger and the collection of documents, with each of them having its own general ledger and collection of documents.

Land register entries can only be made on the basis of written documents (e.g. purchase contract, condominium contract, loan agreement, marriage certificate). These documents are kept numbered in the collection of documents, organized by years, which is publicly available at the competent district court. (Österreich, 2018)

The only notable recent innovation, however, has been computerization, which initially involved only the transfer of information from paper to electronic media.

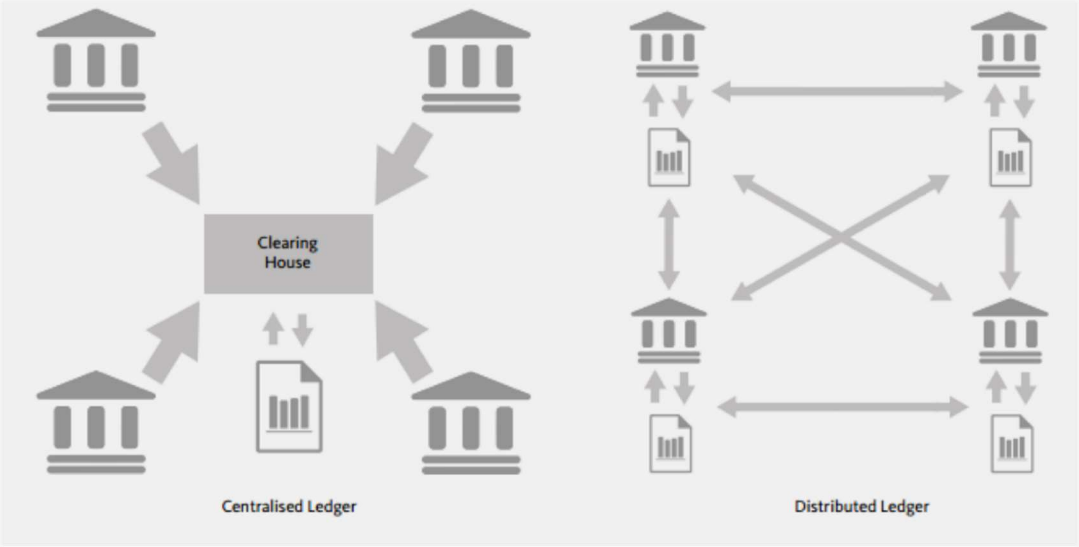


Figure 8: Difference between Centralised Ledger and Distributed Ledger. (René Wintjes, 2016, S. 11)

2.4.4. Central Ledger

Central ledger books are public and maintained from one central location, and can be mirrored to other instances. These central ledgers are under the control of a central authority. (see Figure 8) While many companies do business with each other, but do not necessarily trust each other because they have different interests, this central authority is usually run by a third party. In the case of international currency traffic, e.g. the Society for Worldwide Interbank Financial Telecommunication, abbreviated SWIFT. The consensus is made by the trust of all SWIFT organizations. For central ledger books, to gain consensus and trust among each other, a trusted third party is needed. All participants, who trust a version of the database maintained and made available by this third party.

A central instance, the ominous third party, is needed. In other words, a central authority!

(Settlements B. f., Distributed ledger technology in payment, clearing and settlement, 2017)

2.4.5. Conventional Distributed Ledger

A distributed general ledger is basically a distributed, replicated database. Represent tables that are duplicated many times on a computer network. (see Figure 8) This usually happens by copying data, with all the problems of distributed systems. Each participant may have a copy of some or all of the data, which reduces the probability of failure since there is no single point of failure. Consensus is ensured by one or more master systems. Replication is a major challenge for current database technologies and leads to high costs and complexity in IT projects. There are other ways to ensure that a database is distributed and permanent.

2.4.6. Blockchain Distributed Ledger

A blockchain is a type of distributed ledger, but not all distributed ledgers are blockchains. A distributed ledger is a database that can be shared across a network of multiple nodes. Information stored in a blockchain exists as a shared - and always reconciled - database. Not only is the blockchain database stored in a single location, this means that the records it performs are consistently stored in the entire network, there is no centralized version of this information. All changes to the general ledger are displayed in all copies after consensus. The information in the general ledger may be of a personal nature such as financial, legal, physical or electronic information. All participants within a network can have their own identical copy of the ledger, and each copy is synchronized by algorithms that have the ability to "consensus" on the status of the ledger.

If a node thinks that a user owns something, then by consensus all other computers on the network do the same. This information in a blockchain is therefore public and easily verifiable.

Blockchain technology has the algorithmic technologies that make it possible to use ledgers as tools to capture, activate, and secure a huge range of transactions.

Because digital information is distributed in the case of the blockchain, but cannot simply be copied, the blockchain technology is the backbone of a new kind of consistent consensus finding via a ledger. So blockchain is a technology that enables the creation of a global public database. In this database, it is not possible to add, change or remove data unnoticed.

It does not consist of the current data status, but of all data changes.

Transfers can be displayed in this database, the generation of green electricity and its associated "green certificates" are also documented, but also other transactions that represent ownership, for example. Since data cannot simply be copied in the blockchain, but is checked on admission, whether this information is plausible, e.g. "green certificates" or even digital money cannot be used or spent twice.

Blockchain, the distributed, decentralized ledger, ensures the integrity and authenticity of all transmitted data. The technology thus forms a basis of trust between actors who conduct digital and other transactions - thereby opening up a world of new possibilities.

In distributed systems, there is a requirement that all participating systems replicate a common status. This consensus can be found by suitable algorithms. To keep the state consistent, each node must apply the same operations in the same order to its copy of the blockchain. Consensus algorithms keep the state consistent across multiple unreliable asynchronously connected replicas.

Distributed-ledger technologies differ in the way the networked computers find a consensus:

- like Proof of Work like in Bitcoin,
- by proving economic interests, the "proof of stake" as in Ethereum Casper,
- by a coordinator like in Raft
- or through elections like Swirlds. (Https://www.swirlds.com/)

(Antonopoulos, 2017, S. 15-) (Nakamoto, 2009)

2.4.7. Shared Ledgers – Public, Private or Permissioned

A shared ledger generally refers to all databases and applications that are shared by a private group of users or are publicly available to all. It is the most general and important term for blockchain technologies.

There is a big difference in the accessibility of the distributed blockchain ledgers, depending on whether you want to allow anyone to write to the ds ledger, or just known, verified participants.

Public blockchains Ledger can be "public" in two ways:

- Anyone can write data without the permission of another node
- Anyone can read data without the permission of another node

When you talk about public blockchains today, you usually mean that everyone can write.

Especially public blockchains are particularly important because of the transparency offered by the technology, since everyone can view and check the data recorded in each block and therefore they can serve as a backbone for just about any democratized solution.

(Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 23-)

2.4.8. Public Blockchain

A public blockchain network is fully open and everyone is entitled to participate in and participate in the core activities of the blockchain network. Anyone can join or leave, read, write, and audit activities on the blockchain public network, which helps a public blockchain maintain its self-directed nature.

A public blockchain is designed as an "anyone-can-write" blockchain, in which participants cannot be verified and can easily add valid entries to the general ledger without requiring permission.

Therefore one needs defence mechanisms against attacks. Every attack on the blockchain requires high computing power which generates a high energy requirement and therefore costs. Each node that offers a solution for the next block has to solve a mathematical puzzle. This mechanism is called "proof of work". This creates cost and complexity at each node of this blockchain.

Public blockchains usually have an incentive mechanism that encourages new entrants to join the network and keep it mobile. That the rendering of computing power for a correct new block is paid for with digital money. Nodes that participate in consensus building are called miners, nodes that only test the correctness of the blockchain and new blocks are called Validator.

Public blockchains are of particular interest when it comes to solutions for truly decentralized, democratized and authoritarian operation.

In addition to the ease of use and ease of participation, a public block chain also has some disadvantages. One of the most important is the high power consumption required by the "proof of work" algorithm for maintaining the distributed public ledger. Another important issue is the lack of complete privacy and anonymity, resulting in a weaker security of protection of the identity of the subscriber.

In addition to reputable users, malicious users can participate anonymously, as consequences due to anonymity are very unlikely.

(Antonopoulos, 2017) (Hofmann, 2018, S. 42-) (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 215)

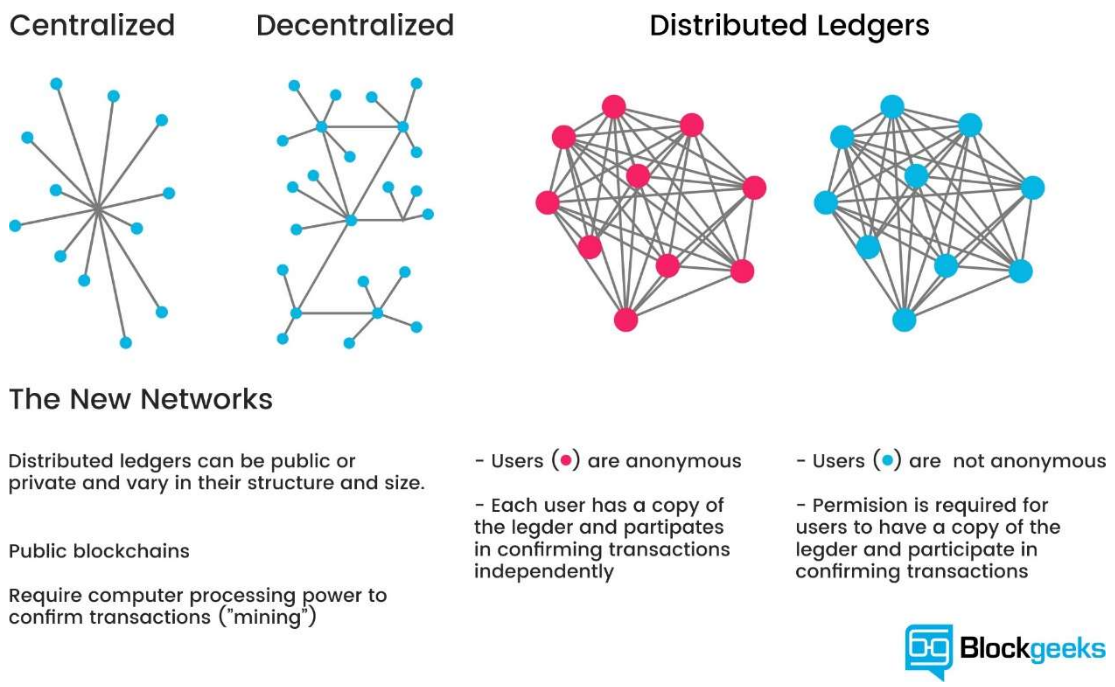
2.4.9. Private Blockchain, Private Ledger

A private chain is a block chain to which not everyone has access, but only a limited number of participants to be a miner or validator. In order to become a participant, a registration must be carried out. However, this application usually involves a registration process in which the identity in the real world is checked. (see Figure 9) (See Figure 33)

Miners become validators because miners are not necessary for a private chain. Validators validate the proposed blocks that come to the chain.

Private blockchains do not need a "proof of work" to protect against attacks because the network is protected in another way and the incentive to operate the network is not in the receipt of co-tokens but is negotiated in contracts outside the blockchain. Finding a consensus is easier for private chains. The miners or private chain validators are the people who actually operate and control them. Mostly, only the larger members of a consortium run validators, and the smaller members are content to just check the data on the blockchain so that if there is an error or collusion, it will be recognized.

Private chains are cheaper and safer.



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous
- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous
- Permision is required for users to have a copy of the legder and participate in confirming transactions

Figure 9: Centralized, Decentralized and Distributed Ledgers can be public or private (Tapscott, 2018)

(Dannen, 2017, S. 159-) (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 215)

2.4.10. Permissioned Ledger

The permissioned blockchains are a mix of public and private blockchains that allow for many customization options.

These blockchains are defined to grant each participant special privileges for certain functions, such as Reading and writing information on the blockchains. These permissions can also be assigned to specific roles, as validators must be able to read, and miners must also be able to write. Other user roles such as registrars, courts of arbitration, banks, etc. are also conceivable here. Roles and Asymmetric Encryption can also grant limited rights. The rights are also negotiated or stored within the blockchain. It may also be that just writing the blockchain requires special permissions, but reading the public, unencrypted information is possible for each participant.

In order to be able to perform a specific role in the blockchain, there may be a registrar that can grant each one a valid role in the approved ledger after properly verifying its identity. Through this role, the node is granted selected and assigned permissions, allowing it to perform certain activities in the blockchain.

For many applications, permissioned blockchain networks make sense, as they can be set selectively in the configuration of the networks, the necessary restrictions and the activities of the various participants in the desired roles can be controlled.

All parties involved may not necessarily need information about all the information in a business relationship. They may only need access to limited information, such as transfer volume, source and quantity of energy, to fulfill their necessary function in supporting such businesses. Allowed blockchains allow such limited implementation and limited permissions for these different participants.

Whether you need a blockchain and if so, which one, you can determine based on the criteria of the required copies of the general ledgers and on the basis of read and write permissions. (see Figure 10)

(Dhillon, Metcalf, & Hooper, Blockchain enabled Applications; Understand the Blockchain Ecosystem and How to Make it Work for You, 2017, S. 169) (Dannen, 2017, S. 159-)

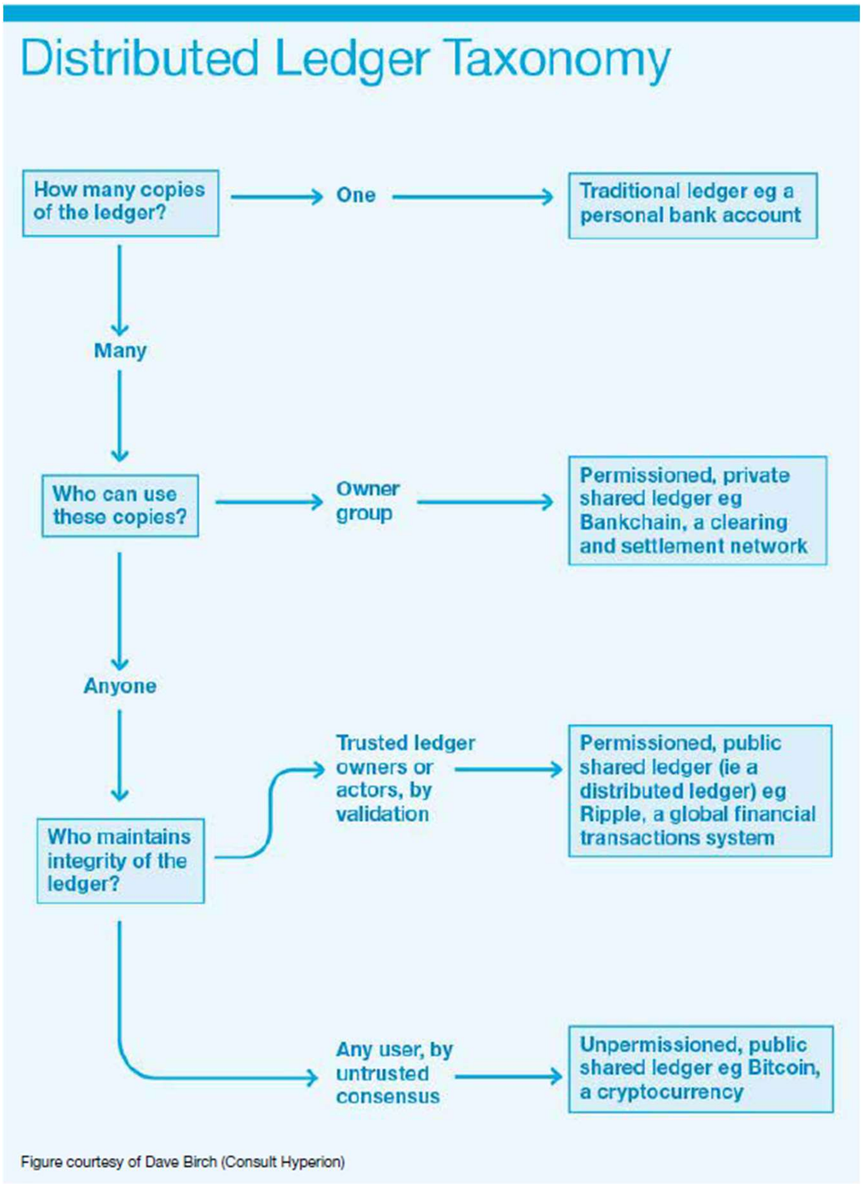

Distributed Ledger Taxonomy
How many copies of the ledger?
One
Traditional ledger eg a personal bank account
Many
Who can use these copies?
Owner group
Permissioned, private shared ledger eg Bankchain, a clearing and settlement network
Anyone
Who maintains integrity of the ledger?
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger (ie a distributed ledger) eg Ripple, a global financial transactions system
Any user, by untrusted consensus
Unpermissioned, public shared ledger eg Bitcoin, a cryptocurrency
Figure courtesy of Dave Birch (Consult Hyperion)

Figure 10: Classification of Blockchains: How to select proper Blockchain (Walport, 2016, S. 19)

2.4.11. Mining

Mining is the process of finding a new valid block for the blockchain - the general ledger. The majority of nodes determine which block will be added next to the blockchain. The responsibility that everything runs correctly is now no longer with a central authority, but is shifted by means of majority finding on the nodes. So that no manipulation can take place here, the algorithm and the associated source code must be openly available. This openness makes it possible for all those interested to administer the blockchain and create blocks. For the nodes to be interested in doing so, they must also receive a reward.

When a block is mined, it is considered unchangeable. If there are delays in the network causing two nodes to generate a valid block at the same time, either one will be discarded. This happens on the basis of defined rules. For example, with bitcoins, the branch is recognized as valid, which had to solve the more complex puzzle.
(Dannen, 2017, S. 12)

2.4.12. Merkle Trees

Transactions in the blockchain can be stored in Merkle Trees. For bitcoins, for example, Merkle trees are used to group all transactions together in one block. This will generate an entire digital fingerprint of all transactions in the block. A Merkle tree is created by repeated hashing of two nodes, until there is only one hash called root or Merkle root. (see Figure 11) (Nakamoto, 2009)

> *"Hashing also incorporates another old technology called Merkle trees, which take many hashes and squeeze them down to one hash, while still being able to prove each piece of data that was individually hashed."*
> *(Laurence, 2017)*

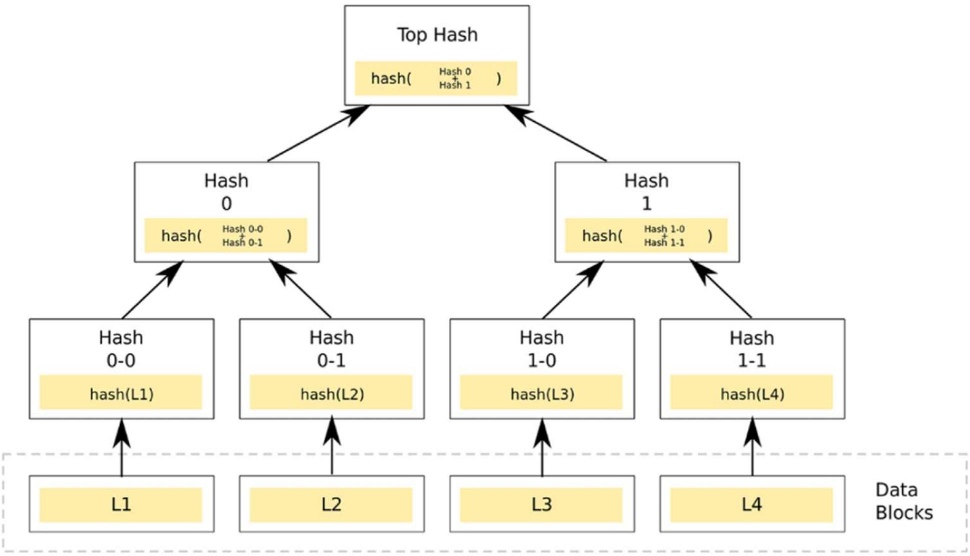


Figure 11: A Merkle Tree (Laurence, 2017, S. 43)

2.4.13. Consensus and accordance

Consensus means that the nodes agree on a specific status of the general ledger. This is difficult to achieve in any computer network. If a consensus can take place at the technical level without influencing individual nodes, then one can trust this consensus because it cannot be manipulated. If a node receives a suggestion for a new block from another node, it will only be accepted if it is correct. So as long as more than 51% of the nodes are honest, there will always be a correct view of the world.

Consensus is difficult to achieve when two or more parties want to share a database that neither party can control alone, can be written by each party, and anyone can rely on. The more difficult it becomes if the participating nodes have different goals and do not trust each other.

In such cases, the only solution is to introduce a trusted intermediary. This mediator manages a database centrally, and ensures that only audited, compliant transactions are performed. Each of the participating nodes is provided with access to the database so that anyone can check whether the database is correct.

This test is very complex and requires a lot of time and resources.

If you want to use a common writable database in the environment of limited trust, there is currently almost no alternative to blockchains. The basic requirement for this is that all nodes can control each other all the time. If all nodes agree, this is called consensus. This consistency and correctness can be achieved using cryptographic methods.

Only the consensus algorithm determines which transaction will be included in the blockchain. Many different technologies are needed for the writable database to work, and these technologies are provided by the blockchain concept.

Blockchain does nothing more than record transactions consistently and unalterably, provided that these blocks and the transactions they contain are cryptographically correct.

Public, private and permissioned blockchains can have different consensus procedures. One major difference is that private blockchains can use simpler methods because blocks are created only by a closed group of identified participants.

Individual nodes can work as miners or only validators, but all have in common is that only correct blocks are accepted. Stronger nodes will mine new blocks, but weaker ones will only validate them. If anyone can read the data of the blockchain, anyone without direct technical authority can check if there is an error or a collision.

Consensus is easier for private chains.

The mutual consensus check allows a network to agree on updates to the general ledger because the joint check ensures that the overall record is correct at all times. This works without the need for central coordinating authority.

> *“There are a number of different approaches to consensus protocols, but a common requirement is that there are adequate safeguards to prevent malicious manipulation (or cyber risk) and ensure that no single point of failure exists.”*
>
> *(Wyman, 2016, S. 6)*

(Laurence, 2017, S. 12) (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 165) (Sixt, 2017, S. 31)

Proof of Work

In an "unpermissioned" ledger system like Bitcoin, the successful miners are selected by lottery. The system seeks to ensure its integrity through economic incentives, such as reimbursement for quickly and correctly finding a new block, in a software-driven process.

> *“In a ‘permissioned’ distributed ledger system, verifiers are appointed by the system’s proprietor, and their integrity is assured through conventional means, such as a legal contract.“*
>
> *(Office for Science, 2016, S. 42)*

In a permissioned distributed ledger system, verifying participants are also appointed by the operators of the system. Again, their integrity is ensured by conventional means (see Figure 12). (Walport, 2016, S. 42)

Proof-of-work uses immense amounts of energy, as finding a mathematical puzzle solves the consensus. (see diagram 1) The puzzle is that in addition to the transaction data, a number - the nonce - must be found so that the SHA-256 has value starts with a certain number of zeroes. This number of leading zeroes varies, is called difficulty, and is given for example in bitcoins blockchain by the software. Criterion for Bitcoin is the minimum time that must be needed to find a new block - 10 minutes. If a block is found in a shorter time, the number of leading zeros required for the following blocks is increased.

> *“The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.”*
>
> *(Blockchain-Luxembourg, 2017)*

(Laurence, 2017, S. 46) (O’Dwyer & Malone, 2014)

The discovery of the nonce can only be found with a brute force method, since an expected target hash value cannot be calculated back to the initial data in SHA-256. Therefore, luck decides who finds the right nonce.

To keep the state consistent, the finder of the new block must present it to its neighbours in the network. These check the correctness of the block, and if it is given, accept it and forward that block to its other neighbours. If the block is faulty, it is discarded. Verifying a block, in contrast to finding the correct nonce, is very straightforward, as only once does the SHA-256 have to be computed with the nonce offered by the miner.

> *“nonce*
>
> *The ‘nonce’ in a bitcoin block is a 32-bit (4-byte) field whose value is set so that the hash of the block will contain a run of leading zeros. The rest of the fields may not be changed, as they have a defined meaning.”*
>
> *(Antonopoulos, 2017, S. xxvii)*

The puzzle to be solved and the found nonce are completely useless and it is not ecological that so much energy is needed. For Bitcoin, finding the consensus requires roughly the same amount of electricity throughout Ireland as many miners try to find the nonce in parallel, but only one can succeed. (Nakamoto, 2009, S. 3)

The complexity of the puzzles ensures that the creation of new blocks is distributed among different participants. It is unlikely that multiple consecutive blocks will be verified by the same party.

The honest finder of a new block at Bitcoin currently receives 4 Bitcoins - a very high sum. An additional incentive also arises from transaction fees that the subscriber is willing to pay for a transaction. In order to finance the electricity bill, the miners will normally change their coins into paper money. These monetary incentives can motivate knots to stay honest, because trying to add a wrong block to the blockchain will never cover the cost of using the computer. (Sixt, 2017, S. 100)

Since the found correct block cannot be distributed infinitely through the network, it can lead to the conflict that several miners have created a valid block at about the same time. Which block is the correct one for this branch?

This conflict usually does not last long, because the participants always opt for the "longer" blockchain, that is, those whose computation required more computational power.

There can only be different versions of the blockchain as long as not all participants know about all variants of the blockchain.

Each node continues to work on the block that they received at the first, but stores the other branch if it gets longer.

The balance is restored when a branch is longer than any other. All nodes that have worked on the other branch will continue to work on the longer one.

(Dannen, 2017, S. 123) (Antonopoulos, 2017, S. 261)

Therefore, only a probabilistic finality is achieved here. That is, if a transaction was put into a block, and that block was added to the blockchain, which does not mean finality. For bitcoins the rule of thumb is that after about 5 blocks the transaction is unalterable. After about every 10 minutes, a new block is generated, so this takes up to one hour, which is not applicable in today's financial systems. (Antonopoulos, 2017, S. 235)

This "proof of work" consensus is a reward system (miners receive money for the mine), but very energy intensive and environmentally questionable.

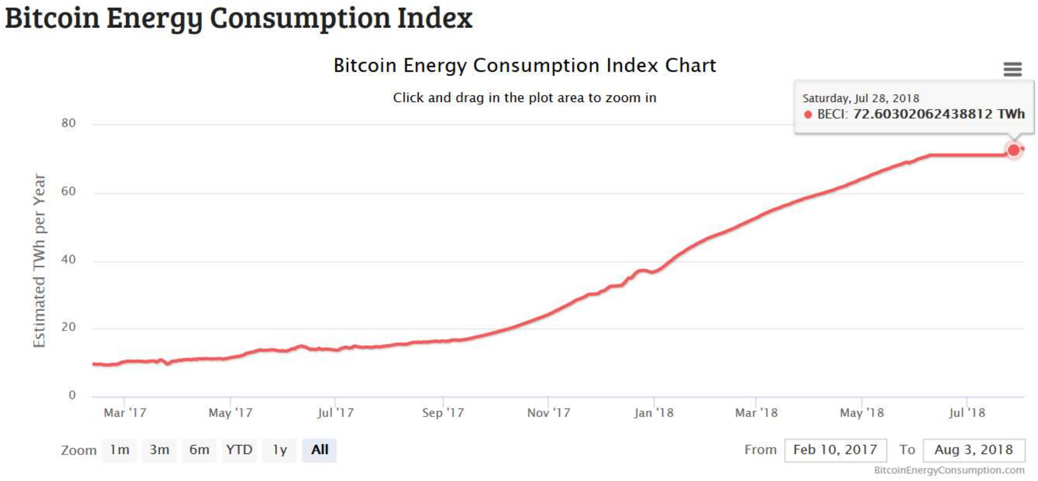


Diagram 1: Energy Consumption of Bitcoin Mining as representative Proof-of-Work consens system. (https://digiconomist.net/bitcoin-energy-consumption) (Digiconomist, 2018)

Proof of Stake

The Proof of Stake (PoS) attempts to solve this energy-intensive problem by introducing a penalty system in addition to the reward system. There are also rules for mines: A miner can only mine mines whose total cryptocurrencies are at least equal to his own balance (stake). With this approach, instead of wasting energy to answer proof of work puzzles, a proof of stake miner can create a new block with fewer calls to cryptographic functions, but only reduce the percentage of transactions that reflects its ownership. As a reward, he could get Coins according to his percentage of owned cryptocoins – but not in all variants of Proof-of-Stake. In some implementations proof of stake offers no block rewards, only transaction fees.

As a rule, validators put a certain amount of penny evidence in the core wallet of this blockchain. The network of that currency can then select them deterministically to construct the next block. The selection mechanism varies according to the algorithm, because it can be randomly selected or based on a combination of variables, such as total assets and the time that it was staked. (Prusty, 2017, S. 44)

With the pledge of their cryptocoins, the validators only need enough energy to run the core software of a blockchain. There is no need to waste energy on a computer with a cryptographic hashing program. (see Figure 12)

The blockchain holds for each miner a share, which he loses if he behaves badly in the sense of blockchain and promotes, for example, a fork. It can also happen with the proof of stake that a chain divides and two groups of nodes cannot agree on a branch. In this case, a node is not allowed to travel in a double track and mine on both branches, but has to choose a branch, which eventually leads to a consensus on the majority of votes. The nodes are under observation here from all other nodes, because as soon as a node scores in both branches, it loses its share of cryptocoins. About the rewards and punishments, the miners are encouraged to remain honest. In the case of Proof of Work, the miner does not get a reward if he tries to insert a wrong block because the other nodes discard it. In the case of Proof of Stake, the node also loses its cryptocoins in the event of fraud.

(Ethereum, 2018)

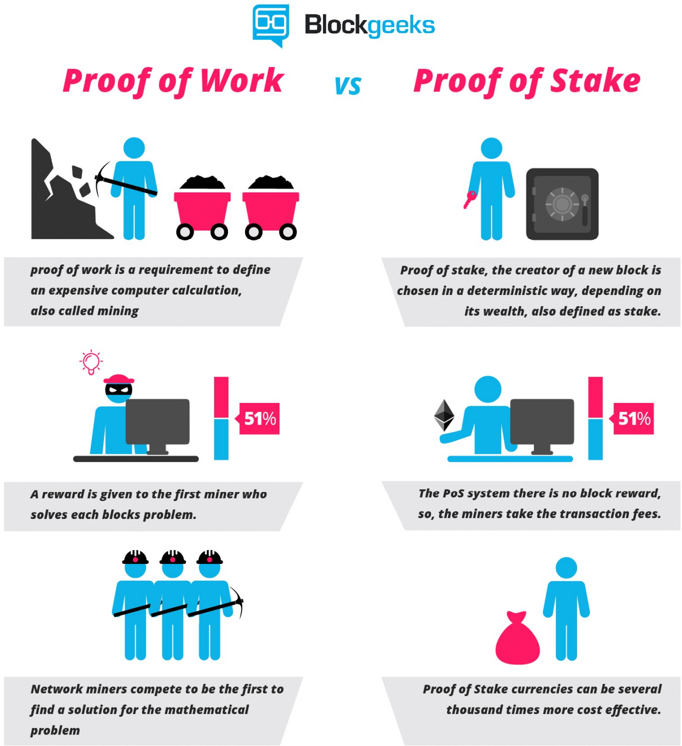

Blockgeeks
Proof of Work
vs
Proof of Stake
proof of work is a requirement to define an expensive computer calculation, also called mining
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.
51%
51%
A reward is given to the first miner who solves each blocks problem.
The PoS system there is no block reward, so, the miners take the transaction fees.
Network miners compete to be the first to find a solution for the mathematical problem
Proof of Stake currencies can be several thousand times more cost effective.

Figure 12: Difference proof of work and proof of stake (Buterin, 2017)

2.4.14. Content of Ledgers

Various information can be stored in a general ledger, information about material goods, immaterial goods, intellectual property, contracts, etc.

Thus, for example, the production of green energy by a producer can be documented, the associated "green certificate" can be assigned to a single source here and cleared in the case of a sale on the account of the buyer. Actually, conceptually, accounts are managed whose content is money, energy produced, authorizations for specific activities, number of green certificates - the possibilities are endless.

The integrity and current status can be checked at any time: For example, if a participant has sufficient licenses (permissions) to carry out an activity, a customer has enough money to buy energy. Information that otherwise needs to be checked for inquiries from third parties.

This ability to provide subscribers with the security and accuracy of the data in the blockchain will also prevent privileged insiders from engaging in illegal acts.

The resulting possibilities are multifaceted: Since all suppliers in the block chain are equipped with appropriate authorizations, consumers in the energy market can enter into a direct supply relationship with the various electricity producers. Companies can buy directly from producers "green certificates" whose correctness is guaranteed. Endless possibilities limited only by the creativity of the participants.

(Laurence, 2017, S. 101) (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 95)

2.4.15. True finality versus probabilistic finality.

Finality means that once a particular operation has been performed, it is forever carved in stone and nothing can reverse that operation. This is especially important in areas where trust is needed. Imagine having a specific asset and having to return ownership to the seller through a small flaw in a software process. All planning and investment in this asset will then be lost.

No system in the world ensures 100% finality, because it is possible to penetrate into a system and manipulate it. That's a big problem with centralized systems. However, distributed systems also have the same problem, but after the current status of the blockchain is determined by the majority, 51% of the nodes would have to be manipulated.

Bitcoin blockchain, the best known application of the proof-of-work mechanism, has had at least three major issues with finality. The reason for these problems was firstly a software bug, and secondly, a planned change in the block size limit from 1 MB to

8 MB, which not every participant agreed to, which led to a split in the blockchain - a so-called hard fork. From Bitcoin BitcoinCash has split off - with 8MB block size. Ethereum also experienced a split. Due to a protocol error, one could steal from a decentralized autonomous organization (DAO) Cryptomoney. Here a change of the software was carried out, which was not accepted by all participants on the basis of the principle "Code is law". From Ethereum a second blockchain was fined, Ethereum Classic, which kept this error.

Regardless of the change of the blockchain by mistake or by a hard fork, one speaks in the consents in the blockchains of true finality and probabilistic finality.

With true finality there is no possibility to change data from the past - except for the above-mentioned samples. Period!

For a blockchain with proof-of-work, there is only Probabilistic Finality. Suppose we have a situation like in Figure 13. There is a blue main chain and a red chain branching from the main chain at block 50.

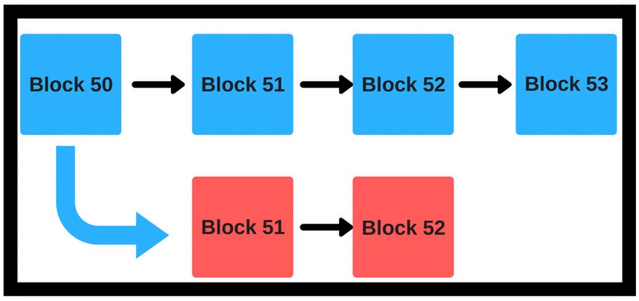


Figure 13: Blockchain split at Block 50. (Vasa, 2018)

Now if a node only sees the red blocks, it keeps them for the current truth, until it also receives the information about the blue chain. After more processing power has been used for the blue path, this is the correct path, according to the proof-of-work algorithm. All transactions in the red path were "Probabilistic Finality" and are therefore discarded again. The transactions are of course not lost, but may already be stored in the blue path, or will be saved there later - if the account still exists (see Double Spending Problem)

So blockchains "proof-of-work" consensus can only give very probable information about what is a fact, but it's eventually considered a final. With Bitcoin one assumes that after 5 blocks the probability of the finality is already so big that this branch is final (after approximately one hour). This is called probabilistic finality.

Private chains can provide true finality. Private chains that use traditional, fault-tolerant consensus protocols can provide real instead of probabilistic finality-but only with the right consensus algorithm.

The finality is always a relationship between strict finality, speed, availability, and scaling.

(Athanassiou, 2017, S. 29) (Settlements B. f., 2012, S. 23) (Settlements B. f., Distributed ledger technology in payment, clearing and settlement, 2017, S. 23) (Dietrich, 2016, S. 229)

2.4.16. Decentralization by the Blockchain

Most management systems are currently centralized, meaning that there is one single central authority responsible for their administration. This form of management has several significant disadvantages, as it is the only point of failure in the system.

Decentralization is the process of distributing power from a central authority to all participants.

Blockchain technology enables this decentralization by storing information decentral on all nodes and giving each individual the ability to actively participate in correctness. This creates a censorship resistance, meaning that no actor can prevent a transaction from being made.

Any malfunction of a centralized system, whether inadvertent or deliberate, will inevitably have a negative impact on the entire system.

2.4.17. Wallets and accounts

An account in the blockchain is similar to an account with a bank. You have a unique number for this account and the bank always knows the current account balance. The same applies to the blockchain: each account is identified by a number, and the blockchain or node always knows the current account balance.

An account in a blockchain consists of a key pair. The account is identified within the blockchain by the hash code of a public key of an asymmetric key pair - this is the account number. (see Figure 14)

A user creates one or more asymmetric key pairs outside the blockchain. For his account, this forms a hash code over the public key and uses it in the blockchain as his account. This account will become known to the blockchain as soon as a transaction is made to this account.

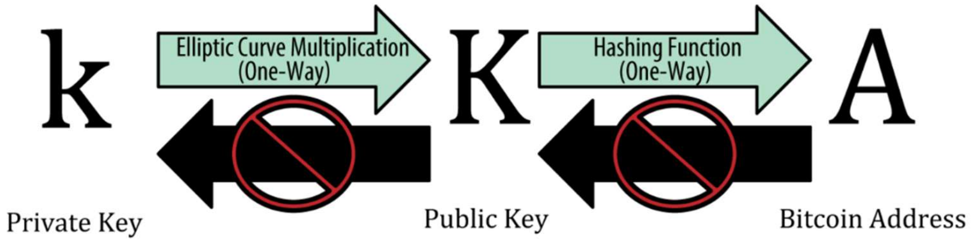

k
Elliptic Curve Multiplication (One-Way)
K
Hashing Function (One-Way)
A
Private Key
Public Key
Bitcoin Address

Figure 14: From private key to Address in Blockchain, only one way calculation possible (Antonopoulos, 2017, S. 57)

With this key pair, the user can manage his account within the blockchain. The hash value of the public key identifies the account. During a transaction, the public key is used to allocate the account balance of his account (= hash). The private key signs the transaction so that any other participant in the blockchain can verify that he is the legitimate owner of the account. The private key serves as access authorization to the account, and must therefore be kept secret by the owner. Anyone who has the private key has access to the stored values of this account.

Digital signatures are used in transactions for:

- Signing a transaction that can only be the owner of the key pair
- Verify a transaction. This can all nodes, since they know the public key of the account holder, and from this can form the hash, which corresponds to the account number.

(Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 107)

These two use cases of the signature result in the following consequences:

- With the signature, the owner of the account agrees that he transfers ownership to another account.
- The signature is unique and cannot be calculated from the public key or its hash to prevent authorization of transactions without the consent of the author.
- Only the owner of the account can create such a signature that transfers ownership of an asset.
- The signature can easily be verified by anyone at any time.
- Only validly signed transactions are included by the nodes in the ledger - the blockchain.

To simplify management for the user, he has a so-called wallet to each of his accounts. In a wallet, the secret keys of Bitcoin addresses are managed, so they are also referred to as digital purses. Wallets can store accounts with a wide variety of

information. These can be electronic currencies, available Green Certificates, entitlements, and more.
(Antonopoulos, 2017, S. 93) (Hofmann, 2018)

2.4.18. Blockchain transactions

Transactions are the ability to transfer the ownership of digital assets from one user (specifically its wallet) to other users, and serve as a way to confirm ownership. A transaction is an operation that may include one or more source accounts and destination accounts (see Figure 15). The input to the transaction is a source account or several source accounts, which are addressed by the public key of the previous transaction. At the exit of the transaction, the number of units and the hash values of the public keys of the accounts are specified. The public key of the recipient accounts is not yet relevant at this time, the amounts are stored in the outputs of the transaction. The owner only needs the public keys if he wants to transfer the amount from these accounts (hashes) to another account. Likewise at the exit conditions are deposited which have to be fulfilled for this transaction to be carried out and the target accounts can redeem this credit. The conditions that must be met for an output to be used are scripted, and only the recipient who can create the correct condition for the script can access the target account and reuse the digital values stored therein. An example of this is that an amount may only be debited from a source account if the recipient can confirm that he has received an agreed amount of energy.

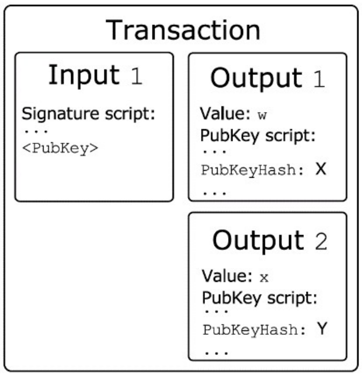


Figure 15: a Blockchain transaction (Karame & Androulaki, 2016, S. 38)

Figure 15 shows a simplified transaction with a source account identified by the public key and two target accounts identified by their hash value (see Figure 18) . In this transaction, w units are credited to account X (hash of the public key of an account) if the script that is selected via a public key authorizes, and transfers are made to the address of Y with x units. This values are provided to the output, if the specified script is true. The input value is always consumed as a whole amount - as when paying with a banknote you get the change back. This is done in the form of a destination that points to the same account as the source, or refers to another account of the transferring due to anonymization. The sum of the amounts for the receivers may never be greater than the sum of the amounts of the sources, otherwise Crypto money would be generated like fiat money generated from air, but for which there is no guarantor in the case of blockchain. It is usual for bitcoins that there is a difference between the sender and the recipient; this share may be credited to the miner's account as a transaction fee. (Nakamoto, 2009, S. 5)

Transactions inputs refer to accounts in previous transactions. (see Figure 16) Thus, transactions effectively form a chain of transactions, and account balances are technically stored only in the outputs of the transactions, not in addresses. The blockchain knows at any time the number of units of a transaction, and knows whether they have already been issued to avoid a "double spending scenario".

(Antonopoulos, 2017, S. 119)

An account can be:

- An external operated account (EOA) that means it is controlled by a user who knows the key pair. This is used for transfer payments.
- A smart contract that has control over its accounts and status through its code.

(Dannen, 2017, S. 61)

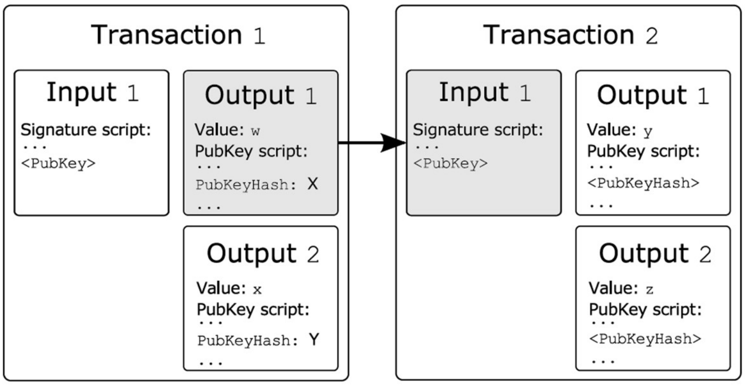


Figure 16: Chaining of transactions (Karame & Androulaki, 2016, S. 38)

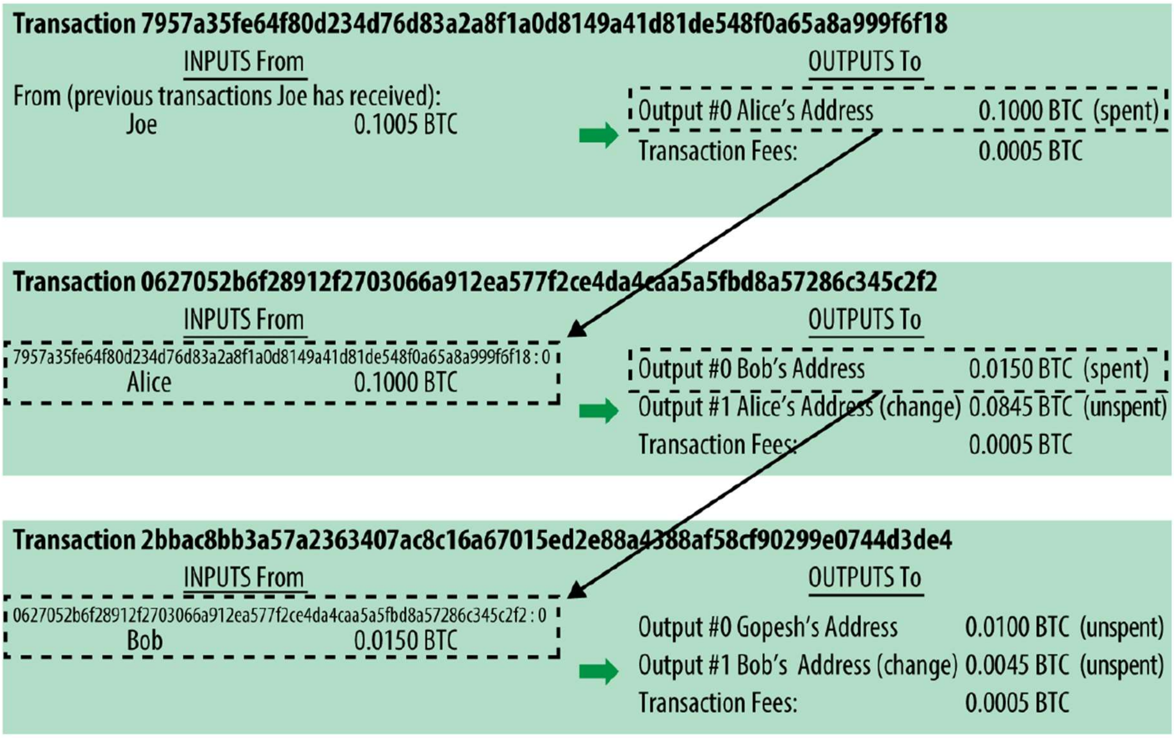

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
INPUTS From
OUTPUTS To
From (previous transactions Joe has received):
Joe
0.1005 BTC
Output #0 Alice's Address
0.1000 BTC (spent)
Transaction Fees:
0.0005 BTC
Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
INPUTS From
OUTPUTS To
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice
0.1000 BTC
Output #0 Bob's Address
0.0150 BTC (spent)
Output #1 Alice's Address (change)
0.0845 BTC (unspent)
Transaction Fees:
0.0005 BTC
Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4
INPUTS From
OUTPUTS To
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob
0.0150 BTC
Output #0 Gopesh's Address
0.0100 BTC (unspent)
Output #1 Bob's Address (change)
0.0045 BTC (unspent)
Transaction Fees:
0.0005 BTC

Figure 17: Chained Transaction in Bitcoin Blockchain, showing also Transaction Fees. (Antonopoulos, 2017, S. 20)

In Figure 17 you can see a typical Bitcoin transaction: in the middle Transaction (0627052b6f28912f2703066a912ea577f2ce4da44caa5a5fbd8a75286c345c2f2) Alice 0.1 Bitcoin (BTC) has in their account, pay to BOB 0.0150 BTC, the miner she will pay 0.0005 BTC and receives as change 0.0845 BTC back to her address. You can also see that each transaction has a unique identifier.

To perform a transaction, the owner of the account must do the following:

1. The data required for the transaction, such as the account numbers involved, the units to be transferred, the conditions that must be met for them to be carried out, or additional information required for the transaction, must be available.
2. Now the sender creates the cryptographic hash value of this transaction data.
3. This hash value of the transaction data is now signed (encrypted) with the private key of the owner's account.
4. Now, the signature of the owner of the source account is added to the transaction as a digital signature.
5. This transaction is forwarded to the mining nodes for inclusion in the blockchain.

In this way, transactions can be performed on the network. However, a transaction by forwarding to the Mining Nodes is not finally confirmed. For finality, it must first be stored in a block of blockchain visible to all participants.

Now the transaction can be verified by the blockchain and if this is correct it will be included in the blockchain.

To verify a transaction, the mining nodes must do the following:

1. The hash value is created from the transaction data without the signature data.
2. The digital signature is decrypted with the sender's account number, which is the associated public key of the account and has units from an earlier transaction.
3. Now the hash value decrypted from the signature is compared with the hash value generated from the transaction data. If this matches, the owner of the account, and only the latter, has authorized the transaction and transferred ownership of the units to a new owner. If an additional script has been specified, it will also be checked, because only if successful can the transaction be executed.
4. If the transaction is correct, it will be included in the blockchain, otherwise it will simply be discarded.

There are several possibilities of transactions. Any number of inbound accounts can be used in the transactions if the amount of an account is insufficient (Figure 20). Or in businesses where multiple recipients are involved, one can send units from one account to multiple accounts (Figure 19).

(Antonopoulos, 2017) (Scherer, 2017, S. 41)

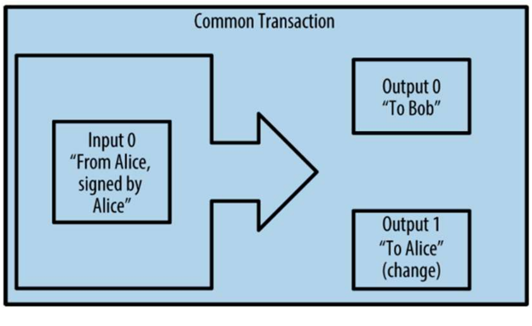


Figure 18: Common Transaction (Antonopoulos, 2017, S. 21)

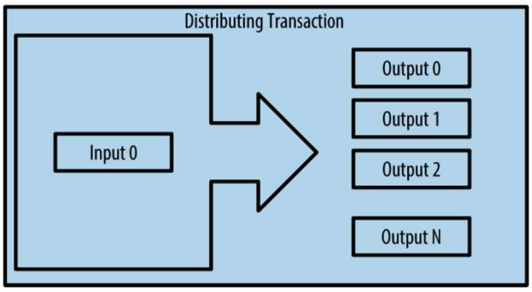


Figure 19: Distributing Transaction (Antonopoulos, 2017, S. 22)

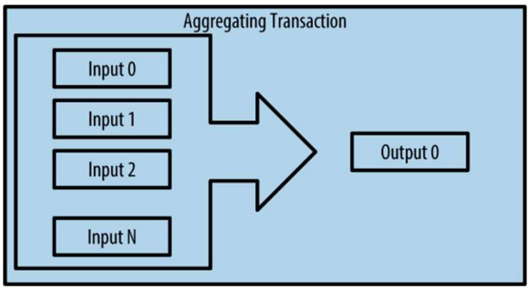


Figure 20: Aggregating Transaction (Antonopoulos, 2017, S. 21)

Each amount of a transaction can only be used by a single subsequent transaction. The blockchain knows that the units of a previous transaction have already been used and therefore prevents an attack known as a double-spending attack in which the same bitcoins are sent to multiple recipients. (https://en.wikipedia.org/wiki/Double-spending)

This method of transferring any digital assets works because cryptographic hashes of each transaction are unique and can be seen as digital fingerprints.

The property of public-private-key cryptography that key-encrypted data can only be decrypted with the corresponding key is the basis of this transaction security. The assignment of both keys is unique. The successful decryption of the signature with the corresponding public key of the account serves as proof that it was created by the account holder with the associated private key.

A false digital signature shows everyone that the message has been changed against the will of the owner of the account.

To prevent participants from modifying transaction data or their copy of the code to modify or create transactions for their benefit, each transaction must be reviewed before it enters the general ledger.

There is also the possibility to save a bitcoin address by multiple signatures. Multi-signature addresses secure account balances by requiring more than one signature for a payment. For example a multisig 2-of-2 (Quorum) need the signature of both participants.

> *"Quorum of Control*
> *Multisignature constraints in scripts impose a quorum of authorization, predefined in the multisignature scheme. The M-of-N requirement is enforced by the consensus rules."*
> *(Antonopoulos, 2017, S. 277)*

Blockchains also give two subscribers the ability to create and sign a barter transaction, ensuring that it only succeeds or fails as a whole. This allows delivery against payment in a common ledger, without the need for a trusted intermediary to manage the process. More complex transactions can be done even better with smart contracts. In these smart contracts additional transaction-specific conditions can be defined under which the agreed tangible or intangible goods are exchanged.

Mining the Blockchain: Store transactions in Blockchain for ever.

In a block of block chain transactions of the participants are stored immutable. This security and immutability is guaranteed by the fact that a hash value is always formed over the entire block which serves as a unique signature of the preceding block for the subsequent block and is also stored there. This signature of the last block is also part of the current block, this value is also used to calculate the signature of the current block. Likewise, the block data contains a current timestamp. (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 137)

The name blockchain therefore comes from the fact that not every transaction is inserted individually in the database, but is added as a bundle of transactions together (as a "block"). Each block then refers to the predecessor by the signature of the predecessor. The blockchain is thus structured as a list of transaction blocks. Each block also contains a checksum, which would be recognized immediately if the transactions were subsequently changed. Blocks with incorrect checksums are not accepted by the nodes and discarded. (see Figure 21)

With the information about the respective predecessor node one comes back to the node number 0, known as the "Genesis Block". The "Genesis Block" is used to initialize the blockchain. (Antonopoulos, 2017, S. 198)

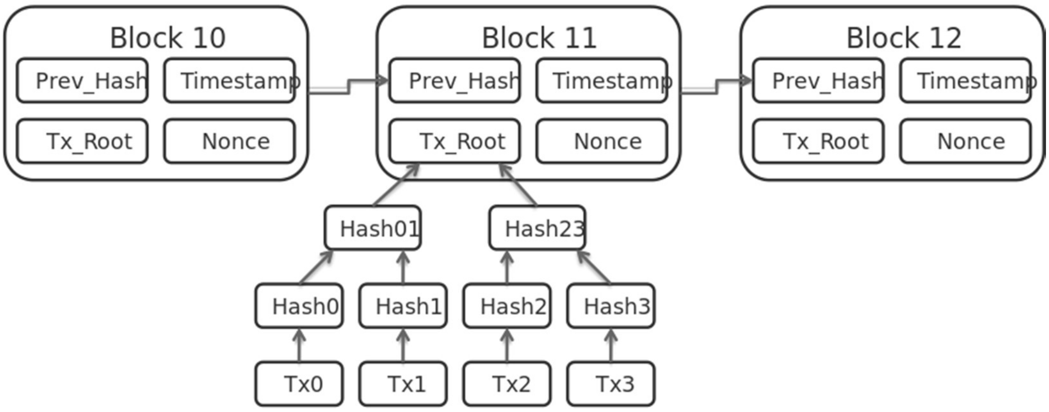


Figure 21: Sequence of blocks, Tx (n) are the stored transactions (By Matthäus Wander - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=26816920) (Wikipedia F. , 2018)

The transactions of users and possibly of smart contracts are constantly coming into the blockchain network. When they arrive at the nodes their correctness is checked. If the transaction is correct, it will be added to a pool of unsaved transactions. When miners construct a new block, they add transactions from that pool to the new block and try to establish it as a new block through the consensus algorithm.

Which transactions are added to the block is determined by the node. Here it depends on the rules and conditions of the respective blockchain which criteria are relevant for the node. If the amount of the transaction fee can be freely chosen by the account holder, the transactions with the highest fees are selected first.

Each miner begins building a new block as soon as he has received the previous correct block from the network. He immediately creates a new block, stores in it the fingerprint (hash value) of the previous block, and fills in his chosen transactions and begins to process the consensus algorithm. (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 139)

The following procedure is used to create a new block:

1. The hash value of the previous block is stored in the new block
2. When a node receives new transactions, these are sent to other nodes.
3. Each node collects the new transactions and creates a new block for itself.
4. Each node works to fulfill the consensus algorithm.
5. When a node finds a valid block, it sends it to all other nodes.
6. The other nodes only accept this block if all transactions in it are valid.

The other nodes accept these blocks by taking them as the basis for the calculations of their next block. (Consensus) (see Figure 22)

Blockchain nodes always assume that the longest chain is the correct one and are working to extend it. (Dannen, 2017, S. 114)

Basically, the data that contains a blockchain is a sequence of transactions. It is important that no transaction is ever forgotten.

The blockchain is a chain of validated blocks, each linking to its predecessor all the way back to the genesis block.

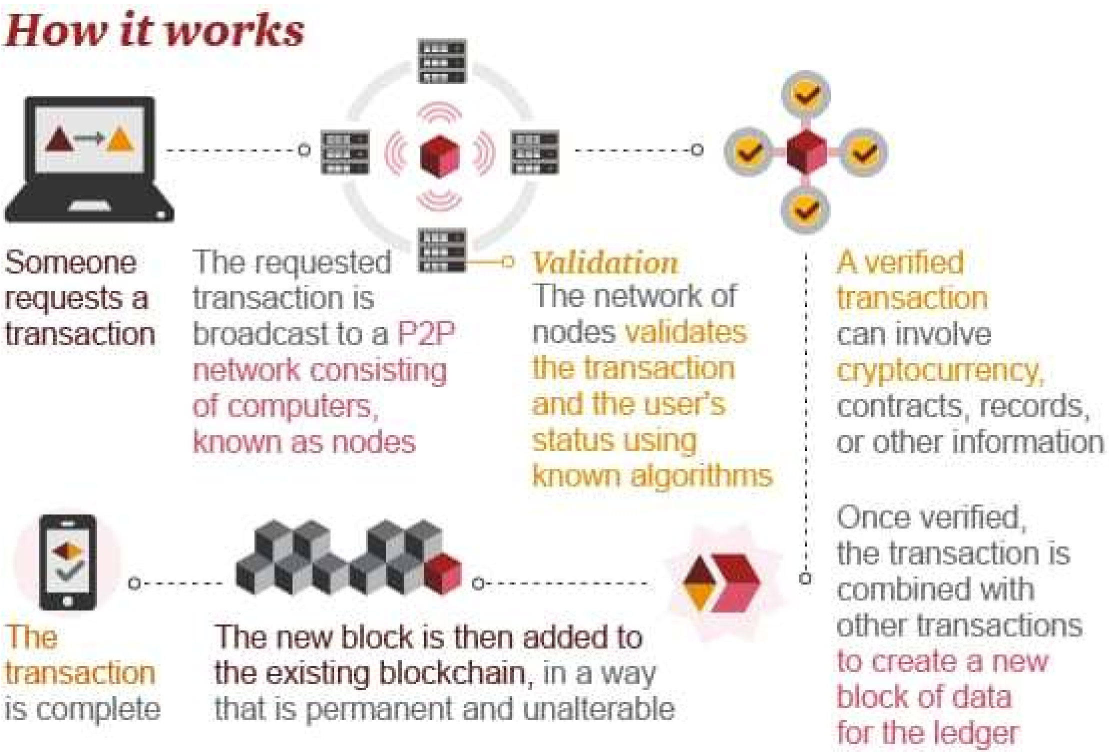

How it works
Someone requests a transaction
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes
Validation
The network of nodes validates the transaction and the user's status using known algorithms
A verified transaction can involve cryptocurrency, contracts, records, or other information
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger
The new block is then added to the existing blockchain, in a way that is permanent and unalterable
The transaction is complete

Figure 22: How does Blockchain work (PricewaterhouseCoopers, 2016)

2.4.19. Transaction Fee

Miners in public blockchains have the task of validating transactions and adding them to the blockchain.

You need here depends on the consensus algorithm very powerful computers and therefore give large amounts of money on computing power and energy to get a financial reward for this: With each block they have successfully mined they receive in the case of Bitcoin block chain new Bitcoins to her Account added.

Similarly, Bitcoins charges for each transaction. These fees can be set by the user himself for his transaction. The more willing he is to pay a higher fee, the more likely he is to get his transaction into the next block. As a result, up to $ 37 per transaction had to be paid in December 2017 (see Diagram 2). A typical value is currently $ 0.75 (https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#3m) as of 8.8.2018

For a comparison of charges, see Appendix A.

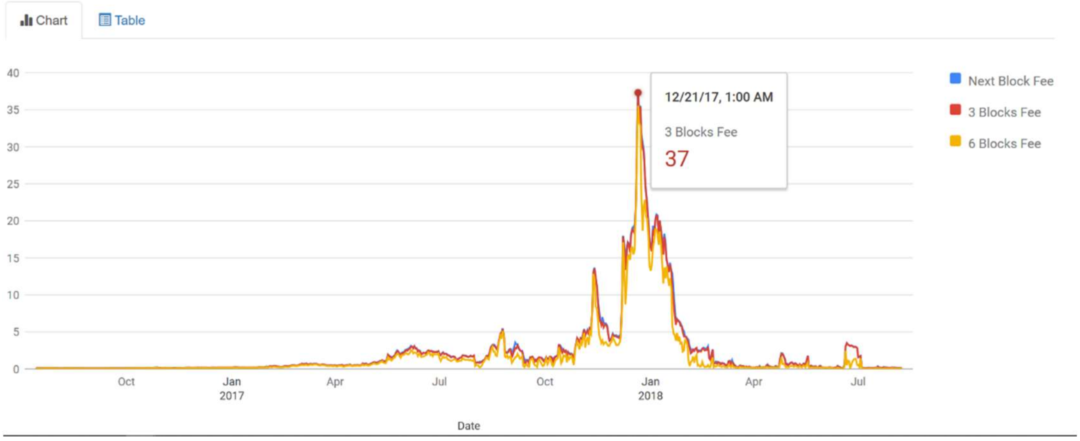


Diagram 2: Historic daily average Bitcoin transaction fees (in dollars per transaction) (bitcoinfee, 2018)

Because of these variable transactions, miners have a financial incentive to favour the validation of transactions with a higher fee. If you want to send money quickly you have to pay the corresponding high fee.

Although the fee does not depend on the amount you want to send, it depends on the network conditions at the time and the data size of the transaction.

Users compete to secure their transactions in the next block by including higher and higher fees. This will give the market a maximum transaction fee that users are willing to pay. As soon as demand decreases again, the transaction fee will decline again. This process can lead to unpredictable costs for a transaction because there is no upper limit.

Proof of work always has high transaction costs because the consensus requires a lot of energy. Therefore, a mature, cheaper consensus system should be used for consensus on a network.

Private chains are cheaper and more predictable, as consensus can be more easily achieved here.

There are no direct hard-working miners on private blockchains, but validators that validate the proposed blocks and add them to the blockchain. In private blockchain, the value-added chain is typically not within the block chain, but is clearly regulated in contracts outside.

(Nakamoto, 2009, S. 4) (Antonopoulos, 2017, S. 126)

2.4.20. Latency, Throughput and Scalability

In today's IT infrastructure, adding nodes means distributing the work across more nodes and increasing performance. This is not the case with blockchains, as new nodes perform the same tasks as all other nodes to ensure the correctness of the blockchain, increasing integrity and availability. If more nodes improve system resilience then perfect scalability would not cause overhead, but overall system performance will not improve.

Blockchains are not scalable by adding more nodes. Here, it is necessary to invest in the algorithms used and in the computing power of the individual nodes (Indicate the processor speed, number of cores, memory, and so on) in order to improve overall performance. Even a split into several blockchains would bring an improvement in throughput.

(Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 206) (Karame & Androulaki, 2016, S. 52) (Sixt, 2017, S. 95)

This metrics apply when applying Blockchains

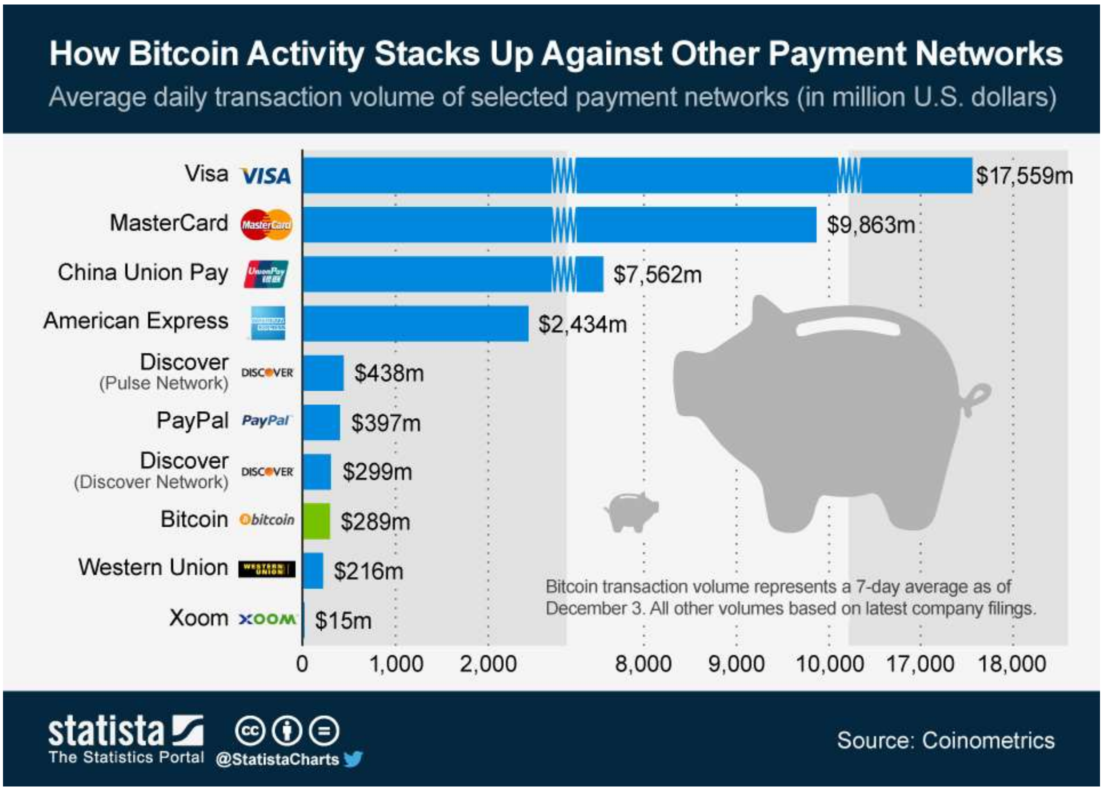


Diagram 3: Compare Transactions per second, Visa versus Bitcoin. (Richter, 2013)

Transaction Latency

Transaction latency is the time that elapses between the sending of the transaction and the final confirmation of inclusion in the blockchain. This time is defined by the generation rate of blockchain blocks. For bitcoins, a block is generated approximately every 10 minutes, at Ethereum about every 17 seconds. (Dietrich, 2016, S. 218)

Transaction Throughput

Transaction throughput is the rate at which valid transactions were finally confirmed by the blockchain in a defined period of time. This rate is also expressed as transactions per second (TPS). (Dietrich, 2016, S. 221)

Visa should be able to deal with an average of 2,000 tps with peaks of 40,000. Bitcoin can perform about 7 TPS, and Ethereum about 10 TPS. (see diagram 3) In these two blockchains, the TPS rate lags far behind today's financial transaction systems. For Bitcoin this is especially due to the proof of work consensus algorithm and the small block sizes. (The block size determines how many transactions can be stored in a block.

However, a blockchain transfer is fast in the finality - it is about 1000 times faster than the stock exchanges and 100,000 times faster than the credit card payment. In order for a credit card payment to actually be made, it takes about two to four months, and the customer still has the option to file a claim. This final finality is reached much earlier at blockchains. For bitcoins, after 5 blocks, a transaction is final, which is about 1 hour - at Ethereum, a transaction after 12 blocks, so after 3.5 minutes as finalized. Finalized means that the money, the asset has arrived on the account of the recipient unchangeable, so that a transaction is completed and cannot be stopped or reversed. After that, a trade has been completed and finalized, such as a credit card bill when the deadline for the chargeback has expired.

Private chains can be orders of magnitude faster. A private chain that uses faster consensus protocols can be much faster and have much higher capacity than public chains.

It takes a different kind of algorithm - not PoW - to find a consensus among many nodes.

However, the transaction data must always be transferred so that each node knows and can verify all transactions. With a large number of nodes, this takes time depending on the network topology.

Private chains can find a consensus much faster here. Since a very small number of nodes are accepted here. In addition, this can be a form of proof-of-stake or Byzantine Fault Tolerance be used which brings a massive increase in performance.

So right now you have to be careful choose between:

- strict finality
- speed
- Availability
- scaling

But there are already new approaches to solving these problems:

> *"This is another proposal for addressing scalability, throughput, and speed issues in the bitcoin blockchain. Next Generation (NG) protocol is based on a mechanism of leader election which verifies transactions as soon as they occur, as compared to Bitcoin's protocols, where time between blocks and block size are the key limitations in relation to scalability."*
> *(Bashir, 2017)*

Scaling Client side:

Client side can scale at the expense of client security. By so-called light clients or thin clients, the effort on the clients can be massively reduced. These clients do not scan the entire blockchain - which is what clients usually do - but trust other nodes to a degree. When they join the blockchain network, they do not check the new blocks for their validity. They may do some testing, but in the end they need a full client to work with. (Sixt, 2017, S. 36)

This type of client already exists in Bitcoin and Ethereum.

(Dannen, 2017, S. 117) (Dhillon, Metcalf, & Hooper, Blockchain enabled Applications; Understand the Blockchain Ecosystem and How to Make it Work for You, 2017) (Morabito, 2017, S. 12) (Dietrich, 2016, S. 221)

2.4.21. Smart Contracts

In a blockchain, an account can be managed either by a person or by a program code. These program codes are called Smart Contracts.

A smart contract is an autonomous software that can make decisions. A smart contract is a contract that has been translated into code and can handle even the most complex applications. The code is law and cannot be changed or obstructed by any outside authority. Therefore, it is very important to check this code very carefully before its first use. Once the code is on the blockchain, it is immutable.

> *“Legal code vs technical code: Two types of rules*
> *The financial system is both a set of legal obligations between institutions and a set of digital records of these obligations. Both the legal and the digital spheres are governed by rules, but the nature of these rules is different. In a seminal text on the subject1, Lawrence Lessig of Harvard University addressed how these legal and digital rules interact to govern activity. Lessig argued that in a digital environment both laws (legal code) and software/hardware (computer code) regulate activity, and that the impact of both needs to be considered when constructing a theory of regulation.”*
> *(Walport, 2016, S. 41)*

> *“There are three key elements that distinguish smart contracts from ordinary contracts:*
> 1. ***Autonomy**: Once a smart contract is launched and running, it does not need to be in further contact with its initiating agent.*
> 2. ***Self-sufficiency**: A smart contract has the ability to independently marshal any kind of resource. For example, a smart contract could raise funds by providing services or issuing equity and could spend them on needed resources, such as processing power storage.*
> 3. ***Decentralisation**: Smart contracts are registered into blockchains and are thus distributed and self-executed across a wide network of nodes.”*
>
> *(Hofmann, 2018, S. 44)*

The contract can itself determine whether the conditions for the execution of the contract are fulfilled. This involves using data from external sources (see oracles) that may trigger further steps in a contract, such as releasing payments or initiating any kind of exchange of digital assets.

These payments can also be payments by conventional means, initiate a credit card payment or use PayPal, or transfer cryptocurrencies.

Smart contracts can be built around many different use cases.

Once the transfers are in place, the blockchain with the smart contract will then act as an independent third party, ensuring that the transfers agreed in the code are executed. No legal or illegal tricks are possible, no delayed payments, which greatly improves business conditions for small businesses.

The goals of smart Contract are the fulfillment of common conditions, minimizing both malicious and accidental exceptions and minimize the need for external trusted intermediaries.

After all nodes are equal and therefore Smart Contracts is executed on all nodes, the program is unstoppable. This equality of nodes is the basis for the unstoppable programs on the blockchain. Since all nodes execute the program logic in exactly the same way, it does not matter if some nodes are unavailable, they crash, and some make deliberate or unintentional errors.

Digital possessions can be settled directly within the blockchain, while real values outside the blockchain are considered to be settled only when external sources have provided this information securely.

These external inputs are also consensual, as only data from trusted sources provides a secure, same initial state for all other nodes for all subsequent transactions.

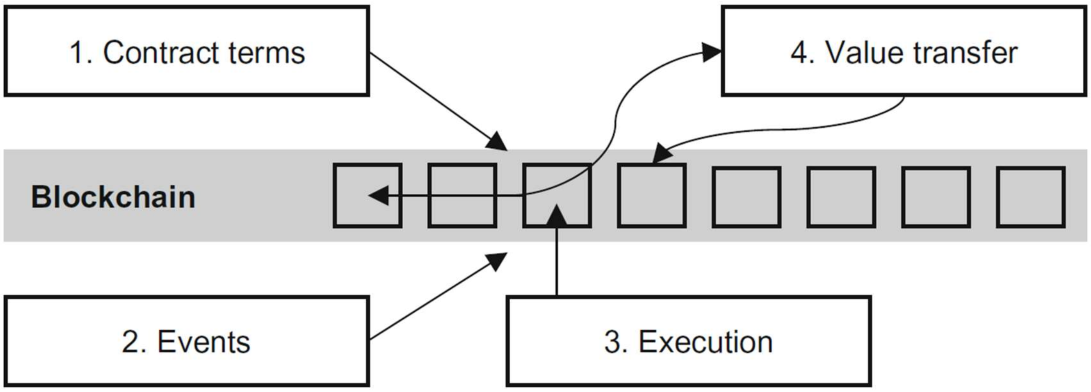


Figure 23: Operations during the execution of a smart contract. (Hofmann, 2018, S. 44)

Figure 23 shows the processes involved in a smart contract.

1. First, the contract conditions are defined. Counterparties establish obligations and settlement instructions. Assets are put under custody of smart contracts. Conditions for execution is checked.
2. Followed by events that trigger the execution of the contract. Events can be:
   - by other transaction initiated,
   - external information is received.
3. The contract is executed. Terms of business logic dictate movement of value based on conditions met.
4. The values from previous transactions are stored as output of a new transaction in the blockchain. That means values are transferred to intended

recipients as defined in the contract. For digital assets on the blockchain accounts are automatically settled. For assets represented off the chain, accounts are settled when accounts off-chain match settlement instructions.

> *“The magic formula here is a combination of three powerful effects.*
> *A smart contracts is an agreement that is binding, not only in theory but in practice as it can move information and money around based on the concrete terms of the agreement.*
> *It is unstoppable an ‘automatism‘ that is guaranteed to resolve itself, Not resting on a legal system and its enforcement but on the blockchain instead.*
> *And it is way more precise and arguably easier to read than legal texts and the millions of pages of rules that define their actual meaning.*
> *A smart contract is decentralized code that moves money based on a condition.” (Dietrich, 2016, S. 167)*

The big advantage of blockchain technology is that contracts are executed on a permanent basis and are resistant to corruption and external interference that used to be just ink, paper and a trusted authority. This is a milestone in affected businesses - the code is law and there is no need for external enforcement by courts. Smart contracts ensure that a contract is executed as written in the code. The blockchain acts as a mediator and executor.

Smart contracts can create new markets, markets that were too burdensome in the past, enforce honesty. They help to open up market opportunities for people where there is no exchange of information, no sharing of it and no common ground. They can establish a sustainable form of justice without judges, lawyers and court fees.

Blockchains have an integrated Turing full programming language (Buterin 2013). The programming language allows anyone to create and write code, commands, and distributed applications on a blockchain to create proprietary rules for ownership, transaction formats, and state transition functions (Buterin 2013).

One programming language is Turing complete, if, in simple terms, it can solve any problem. This feature also includes loops, which programmatically can cause endless loops, and the program cannot stop. This would block all nodes of the network. This holding problem must be solved. In Ethereum, this is resolved by execution costs in smart contracts. A caller of a smart contract must provide GAS (equals money). If the GAS is used up during the execution of the Smart Contract, the script terminates and the contract was not executed and the GAS units are cleared.

(Laurence, 2017, S. 30-) (Dannen, 2017, S. 89-) (Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 240-) (Antonopoulos, 2017, S. 275-)

2.4.22. External events – Oracles.

Sometimes external events are needed as sources in the blockchain. This can, for example, the successful delivery of energy, the valid creation of a "Green Certificates" the transfer of a sum of money. This functionality is provided by so-called Oracle outside the blockchain. The blockchains (actually the nodes) cannot make requests to the Internet that could lead to different responses at each node, or even run-time restrictions and run-time delays if external services are unavailable or congested. That could destroy the whole network.

External information can be requested by means of control flow inversion. That is, if you need information about an external event, you can request this through a special entry in the blockchain. This information can then be provided by an external Oracle as it becomes available.

Oracles are the interfaces from the digital world to the real world. They feed smart contracts from outside the blockchain. Oracles can be services that provide digital, signed evidence of an event. A Uniform Resource Locator (URL) is a unique Internet Address.

> *“The way in works is by:*
>
> 1. *writing the URL - or often just a part of it - into the blockchain, as value,*
> 2. *let it be read by an off-chain service that pulls for such values,*
> 3. *that calls the URL, and*
> 4. *writes the result back on to the blockchain for the decentralized code to read.”*
>
> *(Dietrich, 2016, S. 163)*

Oracle provides trusted, signed information to the blockchain. This may be the current value of an energy meter needed by a smart contract within the blockchain.
(Dietrich, 2016, S. 187) (Morabito, 2017, S. 137)

2.4.23. Save digital values in Timelock in the Blockchain.

A timelock prevents the use of digital values before a certain future time. Timelocks are an important part of many smart contracts. This roughly corresponds to time locks in vaults - which can only be opened again at a certain time in the future.
(Antonopoulos, 2017, S. 157)

2.4.24. Save digital values in a Hashlock.

A hash lock is a type of lock that prevents the output of a digital value until a particular code (the key) is publicly released. Once a hashlock has been opened, any other hashlock saved with the same key can also be opened.

Typically, the transaction is encrypted with the hash value of a secret code. Only someone who knows the initial value can unlock the transaction. This initial value is also called "preimage".

This makes it possible to create multiple transactions that all have the same hash locks and are therefore all available at the same time.

(Athanassiou, 2017, S. xxvi)

2.4.25. Hash Time Lock Contracts (HTLC)

Are another special kind of smart contracts, they expand payment options. So-called Hash Time Lock Contracts allow participants to combine digital values with expirations in addition to a required secret.

Anyone who knows the secret code can use the digital value. If the code is not revealed in time before the timeout expires, nobody can use the digital value for themselves. This is done by the fact that the receiver creates a secret (preimage) at the beginning of the transaction and transmits from it only the hash value to the payer. This now uses this as a digital hashlock to secure the digital values.

This method requires the recipient of a digital value to acknowledge receipt of this before expiration of the HTLC, which is done by revealing the preimage of the hash in the blockchain as a cryptographic proof of payment. The recipient of a payment thus either confirms that he has received the payment before the timeout has expired, or he loses the authorization to request the payment and this is returned to the payer. The cryptographic proof of payment that the recipient provides can also be used to trigger other actions in other transfers. As for example, the confirmation of the receipt of a certain amount of energy can trigger the payment of this, as well as the creation of a "green Certificates" can be confirmed. This makes HTLCs a powerful technique to enable conditional transfers of goods.

(Poon & Dryja, 2015, S. 30)

2.4.26. Payment channels and state channels

Payment channels are a trusted mechanism for exchanging digital values between two parties outside a block chain. This means that continuously signed transactions are generated which are not immediately stored in the blockchain. They are like bonds that may be redeemed. Streams such as videos, or continuous power deliveries can be billed. (see Figure 24)

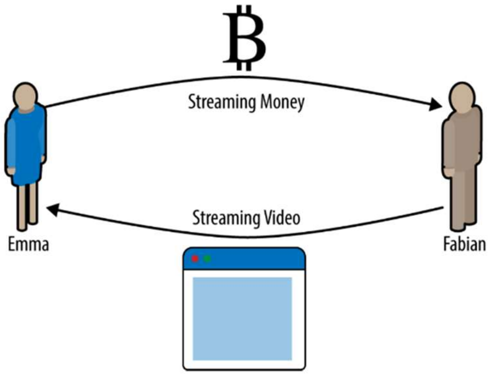


Figure 24: Emma purchases streaming video from Fabian with a payment channel, paying for each second of video (Antonopoulos, 2017, S. 287)

The two parties agree to a 2-of-2 transaction with Timelock, which blocks the digital assets of previous transactions as a means of payment. This is a so-called funding transaction, which also sets the maximum transfer value. The value of the previous transaction (the result of a previous transaction) can only be used if both parties release the key to unlock, or the timelock has expired and the payer can use the amount otherwise. This is seen as ensuring the payment to the supplier and also the buyer has the assurance that in case of no delivery no transaction can be made. This is the only transaction that must be mapped to the network before and during the haulage operation in the blockchain.

Now the transfer of digital or real goods can begin. The two parties are now exchanging digitally signed transactions that represent the current delivery status. These transactions are valid transactions where they can be submitted by both parties for settlement, so-called commitment transactions. These transactions are performed outside the blockchain and can therefore be quickly created. They represent the current status of the transaction.

Upon receipt of a commitment transaction, it invalidates the previous commitment, so the only commitment that can be redeemed is always the most recent commitment transaction. The contract ends either when all agreed goods (video streaming, Generated Energy, green certificates ...) have been transferred, or together the finalization has been agreed. When the transfer ends, each of its received values, which were signed off-chain by the other partner, is placed in the blockchain.

For example, if a buyer has purchased energy and the associated green certificates, he will place the certificates in the blockchain with the green certificates signed by the electricity supplier, and he will received the electricity off-chain during the contract

period. The vendor also places the signed transaction with the paid cryptocurrencies in the blockchain, so that he has new means of payment available. Contractors will only copy the latest, largest confirmed (signed) value into the blockchain as prior confirmed transactions would include a lesser amount. The last transaction is called settlement transactions. By preventing "double-spending" by the blockchain, a digital unit can only ever be used once.
(Antonopoulos, 2017, S. 285)

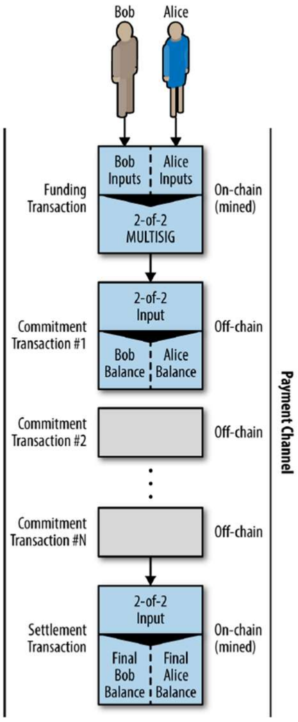


Figure 25: Processes in a Payment Channel, showing the funding, commitment, and settlement transactions (Antonopoulos, 2017, S. 286)

A payment channel has the following transactions: (see Figure 25)

1. A funding transaction is transferred to the blockchain. It ensures that the buyer can pay.
2. Commitments outside the blockchain are permanently transmitted by both partners during the forward transmission
3. When the transfer is complete, each one transfers the already signed commitment transaction with the highest digital value to the blockchain. This is the most recently committed commitment transaction, also called settlement transaction.

(Antonopoulos, 2017, S. 287)

2.4.27. Payment

When trading economic or digital assets in the blockchain, secure transaction facilities must be provided. If you fill up your energy storage at a conventional gas station, you can also pay using conventional means of payment such as cash, credit cards or direct debit.

For small service stations that are not supervised by operating personnel, these can only be used with difficulty or not at all due to the necessary investments and expenses. So far, small-scale electricity producers have had no real access to the private energy market and this has not been facilitated by the privileged utilities. This has severely limited the economic benefits of micro-generation to end-users.

Blockchain technology, in combination with smart metering systems, has the potential to open up the energy market for micro-generation. Smart counters could capture the micro generated energy in a distributed ledger and be settled in a currency managed within the blockchain. (Office for Science, 2016, S. 76) (Bründlinger & Bletterie, 2007, S. 33)

For currencies within the digital world, there are several options, according to the European Central Bank (ECB): (see Figure 26)

> *“In some cases, these virtual communities have created and circulated their own digital currency for exchanging the goods and services they offer, thereby creating a new form of digital money (see Table 1). The existence of competing currencies is not new, as local, unregulated currency communities existed long before the digital age. These schemes can have positive aspects if they contribute to financial innovation and provide additional payment alternatives to consumers. However, it is clear that they can also pose risks for their users, especially in view of the current lack of regulation.”*
> *(ECB, 2012, S. 11)*

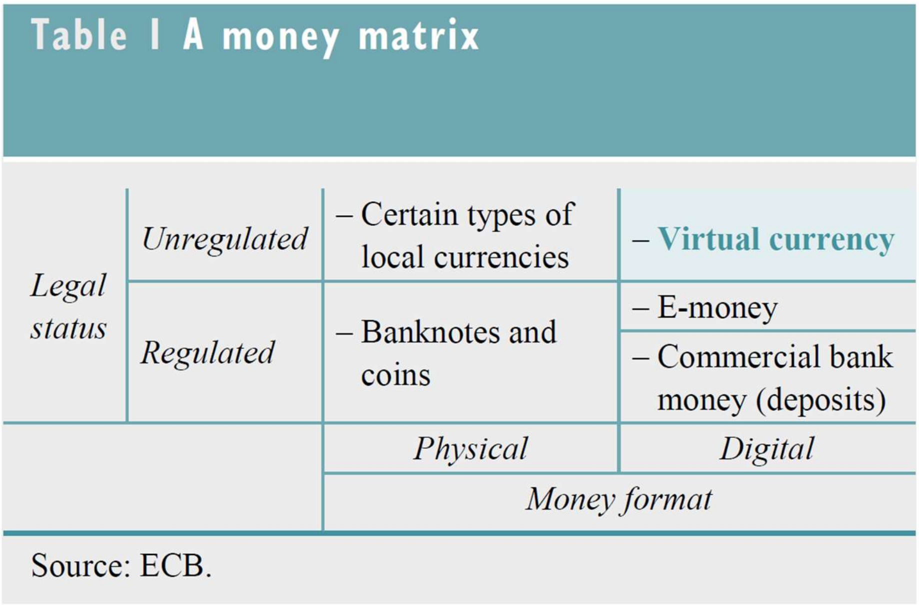


Table 1 A money matrix

Legal status	*Unregulated*	– Certain types of local currencies	– **Virtual currency**
	Regulated	– Banknotes and coins	– E-money – Commercial bank money (deposits)
		Physical	*Digital*
		Money format	

Source: ECB.

Figure 26: A money matrix according to ECB (ECB, 2012, S. 11)

Virtual Currency: A virtual currency serves as a medium of exchange or as a settlement unit within a virtual community. But in the virtual world, there is no institution like a state that provides guarantees for the value of the currency. Bitcoin is an example of this - there is no state that guarantees the value of a bitcoin. Within the Bitcoin virtual community, the Bitcoin has a value so that they can be exchanged for assets or other currencies. This system is based only on trust, as long as the owners have confidence in the bitcoin, it has a value. It is generated money from air, similar to bankroll, only with bankroll a bank is liable for the value. Therefore, it will be useful for a payment service in a blockchain to use a currency tied to a real one. Having your own independent cryptocurrency would also allow for speculation that would reduce trust in this service.

According to ECB, virtual currencies can also be classified according to their changeability into other currencies and their usability. (see Figure 27)

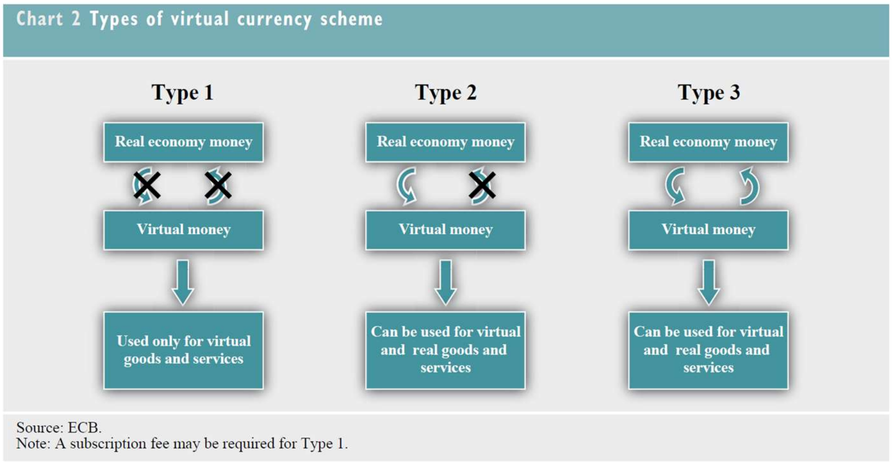


Chart 2 Types of virtual currency scheme

Type 1
Type 2
Type 3
Real economy money
Real economy money
Real economy money
Virtual money
Virtual money
Virtual money
Used only for virtual goods and services
Can be used for virtual and real goods and services
Can be used for virtual and real goods and services

Source: ECB.
Note: A subscription fee may be required for Type 1.

Figure 27: Types of currency scheme according to ECB (ECB, 2012, S. 15)

Another possibility enabled by the distributed Ledger technology is the ability to add specific attribute information to the virtual coin to create "coloured coins". For example, coins may present green certificates, physical assets or virtual assets, but one can tie the allowed uses to a coin.

This opens up the possibility of money with more than one value, attributes such as the permitted use, expiration date, inflation, exchange rates or place of permitted use can be tied.

> *“A single ledger carrying the identity and entitlements of potential claimants, updated in real time, could be a radical innovation that is much more efficient, reducing both operating and development costs. Adding attributes to a particular payment could mean that as well as the amount, the purpose and timeline of expenditure could be both specified and tracked. This would, of course, involve extensive negotiations with stakeholders, and may require some management of this form of currency to ensure any desired parity with sterling.”*
> *(ECB, 2012, S. 59)*

Adding attributes to a particular payment method may mean that both the amount and the purpose and of the spend timeframe can be both specified and tracked. In order to avoid exchange rate speculation, the purpose of use such as "buying energy" but also the possibilities of switching to other currencies could be regulated - e.g. Digital coins may only be exchanged for their original currency.

So there may be multiple currencies in parallel in a blockchain, coins for the purchase of energy, coins for the sale of energy, coins as Green Certificate, etc. It would also be useful for some currencies to include an inflation function so that currencies are not hoarded. This has already been used with alternative currencies in the past.

> *"Alternativwährungen*
>
> *Change occurs when there is a confluence of both changing values and economic necessity,not before. (John Naisbitt)*
>
> *Viele Konzepte oder real ausgeführte Experimente im Bereich der Komplementärwährungen beziehen sich auf den Ökonomen und Sozialreformer Silvio Gesell, der Anfang des letzten Jahrhunderts das Freigeld oder Schwundgeld als wirksames Mittel zur Stabilisierung regionaler Wirtschaftsräume propagierte. Durch einen eingebauten Wertverlust sollte die Umlaufgeschwindigkeit des Geldes erhöht und die lokale Wirtschaft angekurbelt werden. Der Bezug von leistungslosem Einkommen über Zinsen und die Neigung zur Geldhortung sollten dadurch erstickt werden. Die meisten praktischen Versuche, solche Systeme zu installieren – der berühmteste fand 1932/1933 in Wörgl/Tirol statt und konnte tatsächlich die Folgen der Weltwirtschaftskrise lokal abfedern – waren jedoch nicht nachhaltig."*
>
> *(Sixt, 2017, S. 63)*

Translated (by translate.google.at)

> *Alternative currencies*
>
> *Change occurs when there is a confluence of both changing values and economic necessity,not before. (John Naisbitt)*
>
> *Many concepts or real experiments in the field of complementary currencies refer to the economist and social reformer Silvio Gesell, who at the beginning of the last century propagated free money or fading money as an effective means of stabilizing regional economic areas. A built-in loss of value should increase the speed of circulation of money to boost the local economy. The purchase of non-income over interest and the tendency to hoard money should be stifled. The most practical attempts to install such systems - the most famous took place in Wörgl / Tyrol in 1932/1933 and was able to cushion the impact of the global economic crisis locally - were, however, unsustainable.*
>
> *(Sixt, 2017, S. 63)*

Binding to existing Fiat currencies, which is issued as legal tender by central authorities, simplifies the transfer of money from a traditional bank account into a digital wallet and back again. But the question of the source of the money has to be asked here. Who is allowed to produce the coins? Only the central bank (central bank money), or even the banks (wallet money) - money from the air, for which banks must guarantee and include in their balance sheets, or they make available the amount of an existing account in the blockchain. In Estonia, the largest local banking institute is conducting a field trial to provide the first fiat money as a cryptocurrency.

> ***“A pioneering bank issues cryptocurrency securities***
> *Earlier this year, LHV Pank — the largest independent Estonian bank — became the first bank in the world to experiment with programmable money when it issued €100,000 worth of cryptographically-protected certificates of deposits. The experiment followed the establishment of a new LHV subsidiary, Cuber Technology, focused exclusively on Bitcoin-based digital securities. Cuber’s work comprises two strands: CUBER securities and the Cuber Wallet.*
> *CUBER (Cryptographic Universal Blockchain Entered Receivable) securities are simply bank certificates of deposits recorded in the Bitcoin block chain. They are denominated in euros, may pay interest and are suitable for various purposes — as a store of value, medium of exchange, trust and escrow services, and even for machine-to-machine transactions, opening potential applicability in the Internet of Things (IoT). LHV views CUBER securities as the Lego building block for their future financial innovation.*
> *The Cuber Wallet is the first demonstration of CUBER usability. It is a piece of software for mobile phones, enabling instant and free peer-to-peer euro transactions, and low cost instant payments for merchants and consumers, using underlying CUBER securities.”*
> *(Office for Science, 2016, S. 81)*

(Sixt, 2017, S. 63)

2.4.28. Perseus Hydra

A blockchain will persist as long as a node remains upright, as Perseus Hydra.

Even after a catastrophic failure of many nodes, the state of the blockchain is preserved and all failed nodes are re-synchronized over time so that the ledger continues without data loss.

The blockchain can only be terminated if all nodes are switched off.

(Dietrich, 2016, S. 39)

2.4.29. Privacy

A blockchain transaction has a set of inputs and outputs. Each input is connected to an output of a previous transaction, back to the Genesis Block. Nodes only need to parse the transaction to evaluate whether the sender's conditions are valid. The nodes do not have to know the identity of the owners of the accounts, it is enough to know only the account number. This provides good privacy protection when used correctly. All necessary transaction data, the amount transferred, including the sender account number and recipient account number, are fully public and are present on every node in the network, so anyone can read the blockchain entries.

The traditional banking model has a better level of data protection because access to the transactions is limited to people involved and trusted third party. The traditional banking method eliminates the need to publish all transactions.

The privacy of blockchain transactions is thus much less well protected than traditional financial systems. Disclosure of accounts in the traditional financial system requires demonstrable suspicions and regulatory approval.

A blockchain is not anonymous, it is pseudo-anonymous. Because all transactions ever made exist because old entries cannot be deleted. You can see that a transaction has been made, but not by whom - as long as the identity behind the account number is unknown. But once the identity is known behind an account number, all transactions are traceable. In order to maintain the privacy nevertheless the flow of information must be interrupted at another place. The owner of an account can create a new account for each transaction, or use a payment service such as banks, credit card companies, so that the sender of the payment is the account of this service is deposited and not his own.

The cryptographic codes are extremely difficult to crack up to nearly impossible to crack, but they can be e.g. be bypassed by social hacking. For example, people may accidentally or deliberately hand over the key, or fall for a fishing attack, or even be present due to software code backdoors. Therefore, it makes sense to provide functionality to completely lock an account. This can be done, for example, by a Revoke key pair linked to this account, of course only under the control of the account holder.

Private Key Infrastructure

Key management can be performed, for example, by the Public Key Infrastructure (PKI) Federations based on an X.509 encryption standard.

Hide private information in transactions with asymmetric encryption.

The blockchain nodes only need to know part of the transaction data for the correct knowledge of the account balances. Information that should not be public but only accessible to specific institutions or participants can also be encrypted with an asymmetric key pair. If, for example, non-public information for a regulatory authority is also to be available in the blockchain, this part of the transaction can be encrypted with the public key of this institution. Then only the authority in possession of the associated private key can read this information.
(Karame & Androulaki, 2016, S. 179) (Office for Science, 2016, S. 22)

2.4.30. General Data Protection Regulation (GDPR) – regulation in EU law

Of course, the blockchain must also meet the requirements of the GDPR. This includes the following points in relation to this application case:

- Pseudonymisation
- Right of access
- Right to erasure
- Keep records of the processing activities

The GDPR demands "Pseudonymisation", this is immediately guaranteed by the anonymous accounts in the blockchain.

The "right of access" means that everyone has access to the data stored about him. This is guaranteed in the blockchain, since everyone can access the blockchain and thus also read the data of its accounts.

Right to erasure is the right to have data deleted at the request of a participant. This is not so easy to do in blockchain, because usually the blockchain does not forget anything to understand each transaction. Likewise, after expiration of the retention period for documents, companies should be able to permanently delete them. However, these deletions can be achieved by appropriate storage of the blockchain data in a Merkle Tree. This Merkle Tree allows parts of the tree to be deleted without loss of integrity. (see Figure 28)

> *“To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.”*
> *(Nakamoto, 2009, S. 4)*

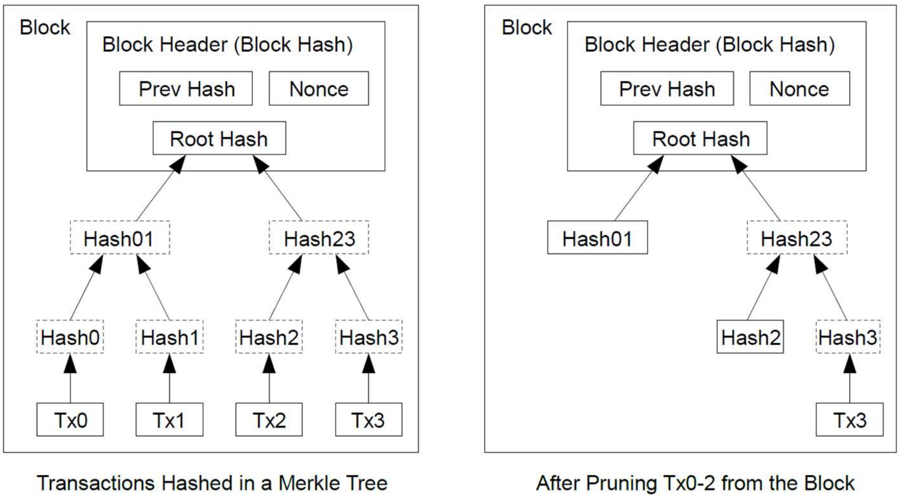


Figure 28: deleting an old part of the Blockchain stored in a Merkle-Tree (Nakamoto, 2009, S. 4)

The duty to keep records of the processing activities can also be done very easily as the purpose of blockchain is publicly known. The individual institutions that receive information about their own encryption must provide this information themselves.
(Lyons, 2018, S. 16) (Ibáñez & Kieron O'Hara, 2017)

2.4.31. Trust in a trustless world

Trust is the basis of all human relationships, whether private or business. Blockchain technology adds the dimension of trust to the data.
Since all transactions must be signed in the blockchain, one does not have to trust the business partner, but can trust that the blockchain will do everything correctly. For example, a subscriber can only use digital values that he actually owns in the ledger. This eliminates any possibility of misuse and gives the users control. Even the initiator of the chain has no possibilities to manipulate here.

> *"Trust is a risk judgement between two or more people, organisations or nations. In cyberspace, trust is based on two key requirements:*
>
> - *Prove to me that you are who you say you are (authentication)*
> - *Prove to me that you have the permissions necessary to do what you ask (authorisation)"*
>
> *(Office for Science, 2016, S. 74)*

Confidence in government in developing countries is lower than in countries where there are stable and accountable legal and regulatory structures. With the use of blockchains there is a mechanism to ensure accountability and security.

Overall validation replaces central control, eliminating the need for a privileged master node. All nodes are effectively equal.

Public verifiability allows anyone to verify the correctness of the distributed ledger. Every change in the ledger is checked and confirmed by miners and each observer.

Like any other software, Bitcoin must be regularly maintained to implement new features or remove bugs if necessary. It is important for trust who writes the software and how the software is accepted and distributed by the nodes. Those who undertake this adaptation and development have a great influence on the function of the blockchain itself. In order to operate a digital business in cyberspace, the software must be trustworthy. A manipulated software can fundamentally change the accounting and ownership rules in favour of individuals.

An open-source code and an open application program interface offers protection here. If the source code is readable by everyone, no one can insert illegal functions without attracting the attention of other SW technicians. This openness of source code is one of the most important conditions for trust in the new Distributed Ledger books. An open source code makes the traceability of the function and the principles of the respective blockchain system possible.

Attendees can trust developers that blockchain programs running on their own computer will not misuse data on the computer. Open source code makes it possible to believe in the security of your network.

In addition, the control of the state or regulatory institutions, which also have no opportunities for manipulation, can further increase the confidence of the participants. (Laurence, 2017, S. 9-) (Antonopoulos, 2017, S. 271)

2.4.32. Social aspects, influence on society

The application of blockchain technology in a widely used system such as power generation and power consumption has potential to disrupt the entire economic system and society in a sustainable way.

Technological revolutions in the past had little or no impact on hierarchical organizational and governance systems, but the blockchain opens up new transparency about their activities.

A radical technical innovation could lead to revolutionary changes in society. Companies have to rethink their business model in order not to be replaced by technology. Also the way society is organized could change - the power of Central Organizations can move to the majority.

> *"Previous technological revolutions had little or no impact on pyramidal, hierarchical systems of organisation and governance. But some suggest that our new technological era enables a potentially emergent 'Collaborative Commons', in which society is motivated by collaborative interests rather than individual gain[6]. This could imply distributed, consensual community structures that do not depend on intermediaries organised in hierarchies (such as banks and governments). Distributed ledger technology (DLT) represent a challenge in precisely this way."*
> *(Office for Science, 2016, S. 55)*

To run a digital business in cyberspace, an organization must be trustworthy and self-trusted. Trust and interoperability are essential in cyberspace.

Hierarchies that have individual control over entire systems can lead to potential abuse of power, such as the denial of payments to WikiLeaks by credit card companies a few years ago.

> *"The Icelandic judiciary decided that Valitor (a company related to Visa and MasterCard) was violating the law when it prevented donation to the site by credit card. A justice ruled that the donations will be allowed to return to the site after 14 days or they would be fined in the amount of US$6,000 a day."*
> *(Wikipedia, Wikileaks - Wikipedia, 2018)*

Public ledgers such as Bitcoin do not have a single owner - they cannot be owned, so they cannot be controlled or manipulated by individuals. A public ledger's job is to allow anyone to bring in data. This creates a censorship resistance, meaning that no actor can prevent a transaction from being added to the ledger.

Previous banking systems allow censorship or manipulation due to their technical central structure. Physical money is fundamentally different from all other forms of money today. Only physical money can be transferred without the permission of another - it is "censorship-resistant". This is also the case with cryptocurrencies in public chains.

For Private or Permitted Ledgers, this is not implicit. Here, the one who holds the highest authority in the system determines the read and write access to the system and can also cancel it. With suitable authorization systems, which must be an integral part of these blockchains, the majority can decide who gets a specific authorization for the system. This must be determined by clear technical rules.

The world increasingly relies on digital economies. These revolutions require us to do more than apply computer technology to existing models. We need to re-evaluate and

re-structure our understanding of what drives a digital economy, as well as its constituent actors and activities.
(Sixt, 2017, S. 26)

Transparency for all

Current systems rely on "security through obscurity" which is obsolete today. In many cases, the safety model can be overridden by reverse engineering. A new approach is "Security through transparency" which allows everyone to see and analyse the source.

Blockchain technology is not as uncontrollable as it is sometimes portrayed. The underlying architecture makes it easy to track transactions, and with additional information from the interfaces to the real world, it is possible to identify the identity of persons acting. This is especially valuable when people try to abuse the system.

Through this transparency, which all actors can use, the partially lost trust in banks and other institutions can be regained. This is due to the ability of distributed ledger technology to pinpoint where and from whom transactions have been made.
(Dannen, 2017, S. 15) (Karame & Androulaki, 2016, S. 151)

Privacy

Early on, the Cypherpunks already recognized that the increasing digitization would make the protection of privacy in the digital economy a major challenge. Even before Edward Snowden's unveiling in 2013 revealed the extent of the National Security Agency (NSA) spy programs, they were already thinking of the important privacy of the individual.

> *"One of their founders, Eric Hughes, wrote in 'A Cypherpunk's Manifesto' in 1993:*
> *'Privacy is necessary for an open society in the electronic age. .. We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy .. We must defend our own privacy if we expect to have any'"*
> *(Dietrich, 2016, S. 255)*

Cypherpunks seek privacy and not secrecy and also want to make a clear distinction. Private sphere controls who private information is shared with.

> *"Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."*
> *(Dietrich, 2016, S. 256)*

> *“For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society."*
> *(Dietrich, 2016, S. 257)*

The transparency of data is a requirement for public verifiability. However, not all data must be visible to everyone. Subdivisions of the data in distributed ledgers can be made non-transparent using asymmetric encryption methods. Data protection is an important feature of blockchains, so there is a clear need to differentiate between privacy and transparency.

Today's generation wants to reveal as much information as possible in social networks, despite the fact that some people have lost their jobs due to entries in social networks.

(Office for Science, 2016, S. 51) (Dhillon, Metcalf, & Hooper, Blockchain enabled Applications; Understand the Blockchain Ecosystem and How to Make it Work for You, 2017, S. 189)

General benefits

At present, Internet commerce is almost exclusively with financial institutions such as banks or payment services tied to a bank account or credit card. Here they act as the trusted third person to conduct the transactions. Distributed ledger systems could extend this function or even take over. But banks are afraid of taking this step, as it could have gone as bad as the music Compact Disk (CD) producers did. The CD production was taken away by music services like Napster, iTunes, Spotify and similar a large market share. For this reason, banks should also offer these services, otherwise innovative startups will take away this market.

With blockchain technology, companies can offer new products and services. But it also offers micro enterprises such as power generators on rooftops the opportunity to participate in the market.

Also, blockchain technology can complicate tax collection for the benefit of the general public.

(Drescher, Blockchain Basiscs: a non-technical introduction in 25 steps, 2017, S. 19) (Sixt, 2017, S. 46)

> ***“DLT proposition***
> *The development of an EU-wide series of Value-added tax (VAT) standards and protocols would enable DLT to be deployed across Europe, with unilateral alignment of all VAT accounting transactions, from invoices to bank receipts.*

> *The system could include smart contracts designed to outsmart the tax quasi-compliant economy, which would also help to address the various threshold differences in VAT applicability across EU member states."*
> *(Office for Science, 2016, S. 71)*

The power of the code

A contract pictured in code will by default have no ethics. When programs make decisions, you must explicitly code ethics in those contracts. With these new technologies, we not only need to ensure that the technology is robust and scalable, but also recognize and treat ethical and social influences.

The current financial system follows rules determined by the legislature and the banks. Like these rules, technical code must be created by people who define the rules that the code embodies. But we have to ask ourselves the question: Who makes the rules?

Code is law, once distributed in a blockchain it cannot be changed. Therefore, this must also comply with legal rules and obligations. Code must comply with the governance rules of the participants and the rules of the authorities. (Athanassiou, 2017, S. 38)

> *"Legal code vs technical code: Two types of rules*
> *The financial system is both a set of legal obligations between institutions and a set of digital records of these obligations. Both the legal and the digital spheres are governed by rules, but the nature of these rules is different."*
> *(Office for Science, 2016, S. 41)*

2.4.33. Governance and Regulation

There must be control over the blockchain, but only the majority can control it. Data and programs in the blockchain are auditable by auditors and governments but cannot be manipulated. Due to the technology - open source and public ledger - activities of regulators in the blockchain can also be audited, so even these cannot operate in secret changes, manipulations or censorship. Regulators, governments should not play a special role, but should only be seen as a group of users who are also subject to rules and obligations.

But mechanisms to ensure accountability and security must be integrated into the concept and business processes. If there is misuse or attempted abuse, it may be the case that the community or regulatory authority makes it public and, if necessary, corrects it.

The problem here, however, is to find a good balance between protecting the interests of system participants and the broader interests of society. These rules must be transparent and must not hinder the application of the technology. They require interdisciplinary features, and computer experts, lawyers, and government officials must work together to create a concept and rules that will do the job and be accepted by the rest of the community.

(Office for Science, 2016, S. 11, 41) (Farell, 2015, S. 11)

> ***“Core Principle X - The system’s governance arrangements should be effective, accountable and transparent.***
> *7.10.1 The quality of governance arrangements is important for all private and public sector institutions and organisations. For systemically important payment systems, effective, accountable and transparent governance is particularly important, because there are normally only a very few such systems in a country, the services they provide involve large values, and they give rise to interdependencies among participants.”*
> *(Settlements B. f., Core Principles for Systemeatically Important Payment Systems, 2001, S. 53))*

The initiators of a blockchain also want to have legal certainty and for this reason it makes sense to involve the supervisory authorities in the design and changes. For example, the state wants to levy taxes, administer Green Certificates, prosecute crimes, and prevent the use of a distributed general ledger for criminal purposes. When a new system is introduced to this extent, it must be resistant to market failure and risk because of its importance.

> *“Recommendation 4: Government needs to consider how to put in place a regulatory framework for distributed ledger technology. Regulation will need to evolve in parallel with the development of new implementations and applications of the technology. As part of the consideration of regulation, government should also consider how regulatory goals could be achieved using technical code as well as legal code. The DCMS Digital Economy Unit could take ownership of this recommendation.”*
> *(Office for Science, 2016, S. 12)*

The way regulators seek to solve the problem today is to monitor the interface between regular money and blockchain currencies. They want to enforce the rules for know-your-customer (KYC) and anti-money laundering (AML) for every customer of crypto-currency exchanges. (Sixt, 2017, S. 127)

In order not to form the basis for speculation, the inflow and outflow of digital currency to the distributed charging infrastructure must also be regulated. The coins that are used in the blockchain for the transfer of goods must be regulated, it must not arise from nothing coins, but must be introduced by institutions similar to banks in the blockchain according to fixed rules. These institutions must also be able to guarantee their value, similar to bank deposits. The rule for individual currency units can be different. It could Green Certificates have built-in inflation, so that they are not only hoarded, but used as CO_2 compensation.

> *“Regulation and legislation: Fitness for purpose*
> *Disrupters in other industries (such as Airbnb and Uber) have adopted an ‘act first, seek forgiveness later’ approach to regulation. Innovations in financial markets, however, require the explicit blessing of regulators well ahead of time. New regulatory principles may be needed where blockchain technologies become an integral part of the market infrastructure, and where consensus protocols are run through an international network of nodes. For example, the responsible parties for system integrity would need to be decided.”*
> *(Wyman, 2016, S. 14)*

> *“1.2.1 Payment systems oversight*
> *As part of their payment systems function, central banks monitor developments in the field of payment and settlement systems in order to assess the nature and scale of the risks inherent in these and to ensure the transparency of the arrangements concerning payment instruments and services. Where necessary they define principles and standards for the promotion of safe, sound and efficient payment and settlement systems. They ensure that the systems, whether these are operated by the central banks themselves or by private operators, comply with these principles and standards.”*
> *(Settlements B. f., Payment system in the euro area, 2003, S. 79)*

The way authorities are trying to solve the problem of money laundering or illegal trades in today's cryptocurrency is to monitor the interface between regular money and blockchain currencies. Therefore, you want to enforce the rules for know-your-customer (KYC) and anti-money laundering (AML) at the interfaces to the system for every customer of the crypto currencies.

What is currently happening in these blockchains in illegal business is beyond their control. That is, the business relationships within a blockchain for charging stations or green certificates should be clearly defined and secured by "code is law". If it is not possible to carry out illegal transactions, then you do not have to identify the acting persons, because they have been checked on entering the virtual world (KYC) and cannot do anything illegal within the virtual world.

We will need some kind of identity system that manages the access control that grant licenses for certain activities, but also needs to allow them to be revoked. This should not be open to anyone in every detail, but in the case of court orders, it can provide all relevant data.

> *“The lack of a central legal entity also makes it more challenging for public regulators to regulate distributed ledger systems via legal code. Governments should therefore also consider ways of regulating distributed ledger systems by influencing the technical code that defines their rules. In finding the right blend, the government should consider the strengths and weaknesses of both technical code and legal code, recognising that the two interact and should be designed accordingly.”*
> *(Office for Science, 2016, S. 45)*

2.4.34. Technical roles of node

The individual nodes in the block chain network can have a variety of technical roles. Examples are (see Figure 29):

- Asset Issuer: is entitled to issue new Cryptocoins
- Validator: is authorized to confirm the validity of proposed blockchain status changes.
- Auditor: is authorized to view the ledger but not to perform any updates.

These roles depend on the use case of the blockchain.

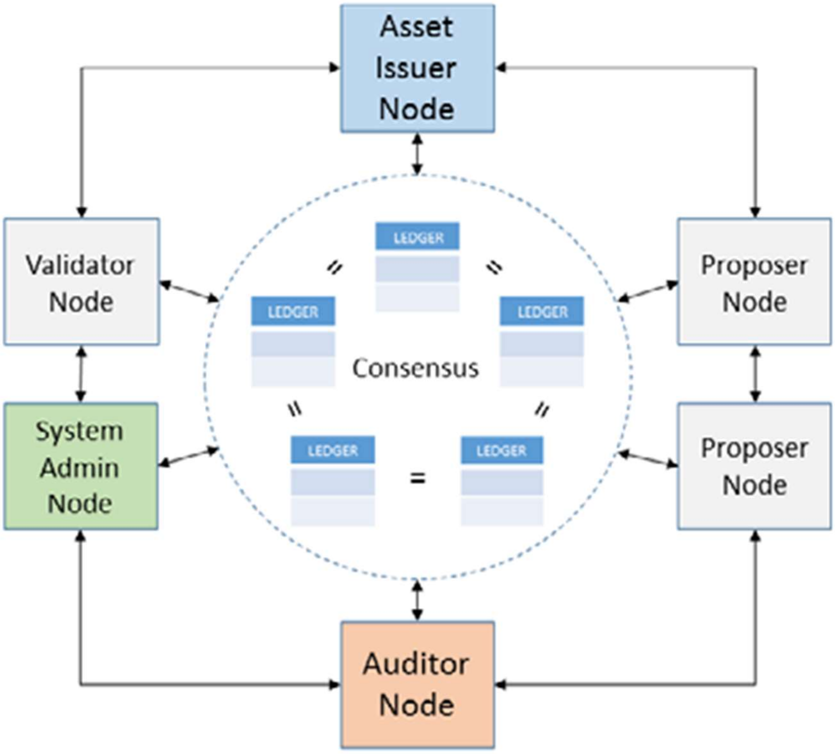


Figure 29: Distributed Ledger with different Type of Nodes. (Settlements B. f., Distributed ledger technology in payment, clearing and settlement, 2017, S. 5)

3. Ecological and economic aspects of the blockchain technology.

The CO_2 production of today's blockchain applications is immense. With the technologies and algorithms used, Bitcoin alone needs the same amount of energy as Ireland. This is caused by the enormous need for computing power to find a consensus of the ledger. Every successful miner proves by solving a mathematical puzzle that he has spent work on it. This proof requires high computing power which is provided by specialized computer systems in server farms. These systems lead to high costs for acquisition and operation, generate additional large amounts of CO_2. This type of application does not make much sense in the renewable energy sector, as the avoidance of unnecessary energy is part of a sensible energy strategy for the future. (O'Dwyer & Malone, 2014)

3.1. Analyse the different aspects of a Blockchain in terms of energy consumption.

The investment costs are made up of the expenses for the acquisition of the construction and operation of the distributed blockchain. Too high a cost can make the energy production of small solar power plants unprofitable and therefore would not be traded on the electricity market. Likewise, it must be avoided that the operation of the blockchain massively wastes energy and does not affect the advantage of generating less CO_2 with renewable energies.

Several subareas affect the ecology and economics of the application of blockchain:

- Current algorithms for finding a consensus require high computational power, resulting in high operating costs due to the power consumption and cost of the particular hardware. This is currently the largest share of costs and unnecessary CO_2 production.
- All participating nodes try to find a solution to the mathematical problem in parallel. Here, energy is consumed unnecessarily through parallelism.
- Network traffic is necessary to synchronize all nodes. Existing structures are used, but their operation also produces costs and pollutants.
- The storage of data requires Hardware (HW) resource. By redundantly storing data, the same HW is needed in the same way on all involved nodes. This causes costs and energy requirements in the acquisition (production) and operation.

(O’Dwyer & Malone, 2014)

3.2. How can energy consumption be minimized

By selecting the right type of blockchain and the appropriate algorithms, the energy requirement can be optimized.

3.2.1. Consensus Algorithms (Proof of Work, Proof of Stake)

Since the Blockchain is not a central system, a consensus must be found among the individual nodes. There are several approaches that differ in the type of blockchain. Public ledgers currently need the most energy they need to provide through the "proof of work" consensus, evidence of work done. This is inefficient because this proof is provided by the solution of a mathematical riddle whose solution otherwise has no further value at all. Following the miners in gold mines, these nodes are also called Mining Nodes. Gold diggers, however, end up with physical gold, bitcoin miner virtual coins, and the solution of a meaningless complex mathematical puzzle. Permissioned and Private blockchains have better ways of finding consensus here, as the trading systems and their operators are known, and therefore preventing fraud is easier. The blockchain comes to a consensus with these algorithms but much easier.

For the application of blockchain in the renewable energy sector, a better consensus finding algorithm must be used. The proof of stake is an alternative consensus algorithm. To create a block here, it must prove ownership of a certain amount of currency (its "share" in the currency) for the consensus, and the node will be allowed to create the block that can prove the largest share. This percentage is used as a guarantee, as a deposit system so that the node does not try to manipulate the blockchain and remains honest. The advantage of the proof of deposit can be seen in the resource conservation, but promotes "wealthy" nodes that they get a block fee, thus even more possession - if one is paid.

Another option would be the delegated proof-of-stake algorithm. It is a variant of the proof-of-stake algorithm that also allows lower-denomination nodes to create a new block and possibly receive the transaction fee. In Delegated Proof of Stake algorithm, each node with its coins can vote for other nodes to use for generating the new block. You choose a representative for your voice here, so it has more focus on efficiency and fair access.

3.2.2. Hashing algorithms

If an algorithm uses massive hashes, specialized hardware can be used here. Since Bitcoin miners had an incentive to find more and more powerful computing devices, there has been a rapid evolution in hardware that can calculate hashes.

Originally, mining of hash values was performed by CPUs (central processing unit) of normal workstations. For the repeated calculation of block hash values with different nonces, the graphics card processors, the "Graphical Processing Units", proved to be up to 100 times faster, with significantly lower power consumption. In 2013, the specialized Bitcoin mining hardware came on the market: FGPA (Field Programmable Gate Arrays) which then also displaced the graphics cards as unprofitable. The hashrates of most of these graphics cards were below 1 GH / s (gigahash per second), a single Application-specific integrated circuit (ASIC) unit could reach more than 1000 GH / s and needed less energy. Therefore, it makes sense to use the appropriate hashing hardware.

When using an algorithm that uses massive hashing algorithms, it makes sense to use suitable hardware that helps to consume less power for the calculations.

3.2.3. Not everything has to be logged in the Blockchain

Storage of data in the blockchain is expensive compared to local storage, in addition the data must be transmitted to all nodes and stored there as well. Therefore, only data that is relevant for the account balances in the ledger, authorizations of the individual participants, data for contract negotiations and similar relevant information should be stored in the blockchain. Messages during the initiation of a business transaction need not be stored in the blockchain, only a final offer, as a result of these negotiations should be filed.

If contracts are active for longer periods, it is not necessary to regularly update the current delivery statuses in the blockchain. There are suitable methods such as hashed time locks that enable a secure business relationship here. The only downside is that the transferred goods can only be accessed after settlement has taken place. Blockchain technology prevents fraud by double-spending.

For transactions, not all information is relevant to the operation of the blockchain. Data about any taxes to be paid can also be stored outside the blockchain in a cloud service or on a local computer. Hashing and cryptographic functions can be used to prevent manipulation of this data. The data can be encrypted with public key of a key pair and stored outside the blockchain. Within the blockchain the location and the digital signature of the data are stored so that authorized institutions can request this data from the owner of the data and check their correctness. Similar to tax law, companies are legally obliged to keep tax-relevant invoices for a certain period of time.

(Wyman, 2016) (Greenspan, Scaling blockchains with off-chain data, 2018)

3.2.4. Client Side savings consumption on Thin- Clients,

Not every node has to mine or validate. If small power producers also need all the hardware and network traffic, then the cost of doing so would exceed profits and much more CO_2 would be generated by power consumption. To avoid this, there are the so-called thin clients for some blockchain variants. They trust other full nodes and can query the relevant data for transactions at any time. After the blockchains are publicly readable, the operators of these thin clients can, if so, use a workstation to verify past transactions. (Sixt, 2017, S. 36)

> ***“Compact data proofs***
>
> *In a blockchain, blocks are filled mostly by the transactions that they confirm. However each block also has a compact ‘header’, which contains important information such as a timestamp and a link to the previous block. For public*

> *blockchains based on proof of work hashing (https://en.bitcoin.it/wiki/Proof_of_work), the input for the hashing algorithm is this block header alone. This means that the authority of a chain can be assessed by a '**lightweight client'** without downloading most of its content. For example, as of November 2015, the complete set of bitcoin headers is 30 MB in size, compared to 45 GB (https://blockchain.info/charts/blocks-size) for the full chain. That's a ratio of 1500:1, making a crucial difference to mobile devices with limited bandwidth and storage."*
>
> *(Greenspan, Gideon Greenspan | MultiChain, 2015)*

This brings a big advantage through lower costs and lower CO_2 emissions through lower power consumption. Photovoltaic systems can be equipped with Smart Meters that have already installed this functionality.

3.2.5. Split into regional Blockchain- Sidechains

Cryptographic currencies have a blockchain distributed all over the world, that is, all nodes worldwide must get the same information and agree on the same consensus. Charges that are an energy transaction between a local generator and a local charging station do not require the entire world to be informed. You can create local blockchains with fewer nodes, and therefore less traffic and less redundant data, but also have a Smart Contracts-controlled interface to other blockchains. If an electric vehicle is to be loaded in another region, the identity of the vehicle and that of the charging station operator can optionally be checked via this interface. The negotiation, money reservation and payment can also be done through this interface, as in a local blockchain. This idea can be implemented as sidechains that are of the same type of blockchain. (see Figure 30)

> *"Sidechains are blockchains that can be interoperable with Bitcoin and with each other. This allows assets to move freely across all blockchains."*
>
> *(Karame & Androulaki, 2016, S. 173)*

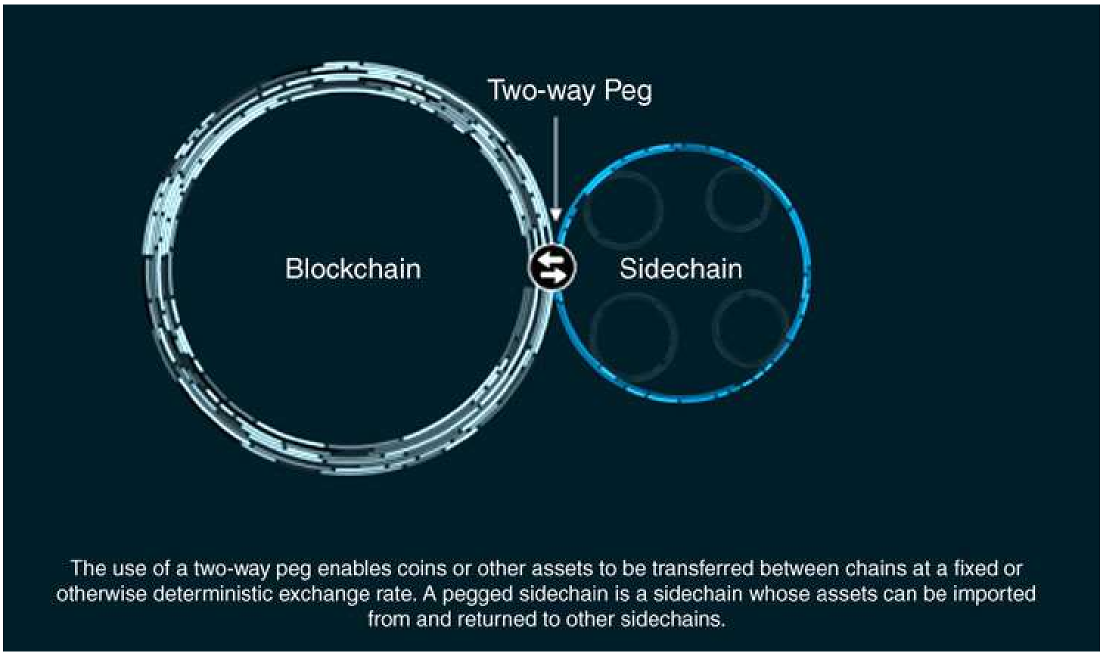

Two-way Peg
Blockchain
Sidechain
The use of a two-way peg enables coins or other assets to be transferred between chains at a fixed or otherwise deterministic exchange rate. A pegged sidechain is a sidechain whose assets can be imported from and returned to other sidechains.

Figure 30: Sidechains are blockchains that are with each other (Sixt, 2017, S. 116)

3.2.6. Optimize transport losses through planning.

Electricity network operators also have access to blockchain data and can therefore predict the expected electricity consumption of the future using statistical means and plan energy purchases from past usage patterns. Appropriate analysis can also identify the regional energy needs and plan for the need to build new local renewable energy sources and, where appropriate, local buffer storage.

If the vehicle owners plan their routes ahead and reservation systems already reserve charging stations along the route, the charging station operators know in advance how much energy is needed at what time. This allows you to pre-charge or discharge local energy storage such as battery systems, supercapacitor systems, hydrogen storage or other storage media. (Komarnicki, Lombardi, & Styczynski, 2017, S. 48)

3.2.7. Flexible pricing, so green energy is consumed.

After you can predict the production profile of solar systems to a certain extent, you can adjust the prices depending on this offer. If an electric vehicle is parked and needed again in 8 hours (typical working hours), the charging station will have 8 hours to charge it. As a result, only solar energy can be used selectively. Likewise, with a surplus of wind energy, the charging current can be increased so that this energy is used meaningfully. If there are no renewable energy sources, or if they are not sufficiently available, the missing energy can also be obtained from the non-renewable energy grid. Likewise, private charging stations in the homes of the owners by intelligent algorithms select the time when a battery is charged. These smart strategies must be implemented at the charging stations and the electricity supplier and can be handled with smart contracts and oracles in the distributed charging infrastructure. Customers can be motivated to use this functionality by cheaper energy costs.

3.3. How energy suppliers can adjust their energy to the energy supply

By storing the energy needs of the past in the blockchain anonymously, energy producers can anticipate the need for the future. The possibility of controlling the private investments of participants who are in the blockchain can also be exploited using Smart Contract. The possibility of Smart Contracts simplifies contracting as these processes can be fully mapped in the blockchain.

Depending on the supply of renewable energy, the energy supplier can make the charging process dynamic at the private charging station.

3.4. Traded goods and wallets

Most public blockchains currently only govern the ownership of cryptocurrencies. It also makes sense to manage other assets in the blockchain when using this technology for a charging infrastructure. In addition to a valid currency, these can be green certificates, charging station reservation processes, thus covering all processes in the charging infrastructure. Similarly, the permissions of individual nodes can be stored in the blockchain, and the blockchain software regulates that these nodes can only perform functions assigned to them. Electricity stations can sell energy, electric vehicles can only create an account, transfer money and pay with it. So it will be useful to have a universal digital ledger in which all aspects of the charging infrastructure are stored.

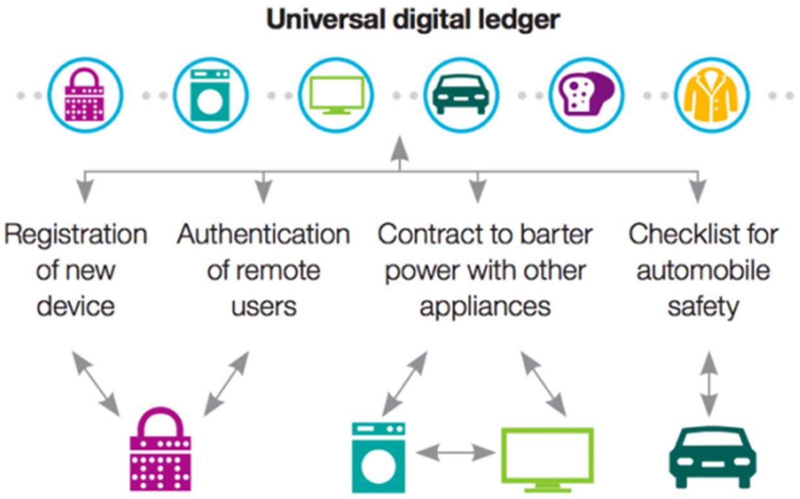

Universal digital ledger
Registration of new device
Authentication of remote users
Contract to barter power with other appliances
Checklist for automobile safety

Figure 31: Universal digital ledger. (Groopman, 2017)

The goods that are captured in a block chain can be purely virtual, or even an image of real goods. Thus, the amount of energy delivered in the blockchain is a reflection of the amount of energy delivered in the real world, reservations do not correspond to real goods. (see Figure 31) Important here are the oracles that send trusted, signed information into the blockchain. For example, these can be calibrated smart meters that provide energy values.

4. Result: Model of an IT infrastructure of charging stations under ecological and economic points of view.

Most popular Internet applications, including the World Wide Web, use a Central Server architecture. This has one major drawback - there is a single point of failure. If this central server fails, all associated services will stop working. Even if the number of clients accessing in parallel increases, this can lead to a bottleneck and this can lead to the server being unable to answer any queries.

In decentralized systems, where peers work independently without centralized services, these disadvantages do not exist. Here the communication takes place between the peers. These peers do not require a known centralized service to exist as a network. The individual nodes communicate with each other, but not every node with each, but like in a distributed network (see Figure 6) only with its neighboring nodes to optimize the network traffic.

Peer to Peer (P2P) networks are able to provide high availability resources. They can provide more useful and robust solutions than current technologies in many different situations. For the application of the blockchain technology for a system of charging stations, only a peer-to-peer network makes sense, since there are no central instances, and also a maximum failure safety is given. If a single node fails, this does not affect the overall system and clients can then contact other nodes on the P2P network.

4.1.1. Logical layer on Top of existing infrastructure

This P2P network resides on top of the physical networks as its virtual network overlay (see Figure 32). Peers use the networking technology of TCP / IP to communicate with each other. This technology is now available on all technical systems, from fixed line communication to mobile communication in GSM / 3G / 4G radio networks.

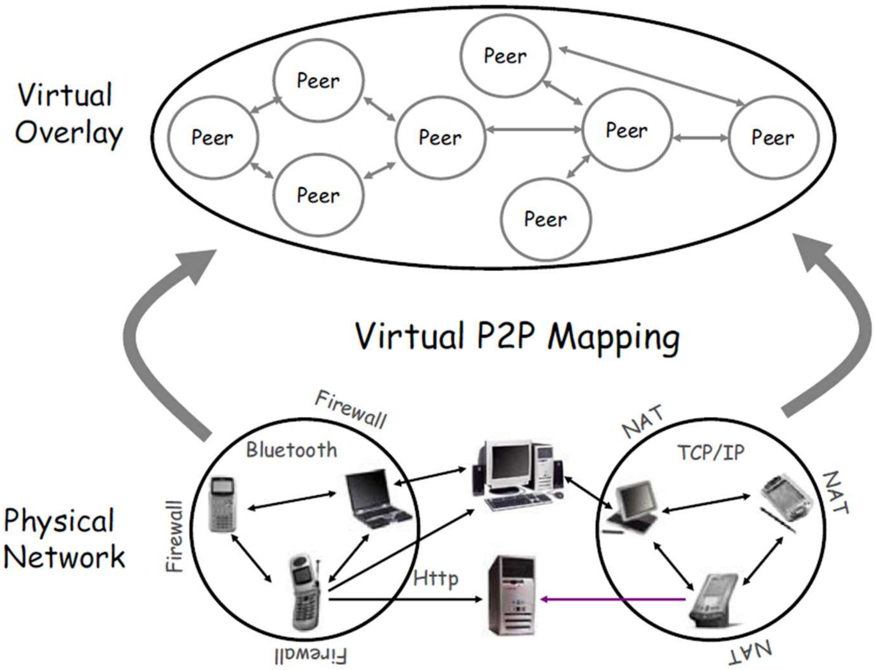


Figure 32: Virtual P2P mapping on existing Physical Network (Taylor, 2005, S. 36)

> *"An illustration of the notion of an overlay network. Modern P2P infrastructures typically overlay a virtual view of the nodes on the network to abstract the underlying mechanisms that actually connect these devices; this example was taken from Jxta [15]."*
>
> *(Taylor, 2005, S. 36)*

To build a charging infrastructure, it is easier and less expensive to build on an already existing distributed infrastructure, as there is no need to pay for installation and maintenance. We also do not have to pay for security, the network itself is secure.

The physical TCP / IP network is available nationwide and can therefore be used as the basis for the charging station P2P network. (see 2.4.1.5)

4.1.2. Enough IP addresses are available with IPv6

After the end of a nationwide charging infrastructure each charging station needs an IP address, IP addresses of version 6 (IPv6) should be used because in this address space enough addresses are available.

For a computer to communicate with other computers on the Internet, it must have a unique IP address. An IP address (version 4) (IPv4) is a unique 32-bit number that indicates the location of your computer on a network. There are theoretically 4,294,967,296 unique addresses. With the expansion of the Internet, the number of available IPv4 addresses is simply not enough. A solution has been developed called IPv6, which is an increase in the address space of IPv4 with 2^{32} (≈ 4.3 billion = 4.3×10^9) addresses to 2^{128} (≈ 340 sextillion = 3.4×10^{38}) addresses in IPv6. According to Google (https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption), communication worldwide is currently about 22% with IPv6 addresses. (6.25% in Austria) (Google, 2018)

The addressing of the individual charging stations should be done with IPv6 addresses in order not to have to change the network at a later time.

4.1.3. Communication between nodes (TLS)

Although the data inserted into the blockchain is all digitally signed, communication should be encrypted from the individual clients to the nodes. By unencrypted communication, for example, a "man in the middle attack" can be made to inject the wrong data into the communication and subsequently into the general ledger of the charging station system.

The problem of protecting the communication between two subscribers has long since been solved. There are two widely used communication protocols used for encrypted communication.

> *“The following technologies are examples of secure channels:*
>
> - *Secure Socket Layer: is a standard for encrypted client/server communication between network devices. A network protocol, SSL runs on top of TCP/IP. SSL utilizes several standard network security techniques including public keys, symmetric keys, and certificates. Web*

sites commonly use SSL to guard private information such as credit card numbers.

- *Transport Layer Security (TLS): [70] is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.“*

(Taylor, 2005, S. 145)

TLS was defined in document (https://www.ietf.org/rfc/rfc2246.txt).
(see 2.4.1.4)

4.2. Public or Private Blockchain for Distributed Charging Infrastructure.

A public blockchain allows anyone to read the contents of the general ledger and thus check the validity of the stored data. In a private blockchain, only a limited number of participants are allowed to read the data.

With all types of blockchains, it is possible to use cryptographic methods to ensure privacy for subscribers. Privacy-relevant content can be hidden by encryption.

With a public blockchain, the shared ledger can easily be checked for correctness by all participants without revealing details of the digital transaction.

To provide evidence in a decentralized system, the ledger must therefore be publicly available. However, since not all data is to be published, permissions must be set up for different types of users.

- Based on the previous considerations, the use of a public block chain is recommended.

4.3. Permissionless or Permissioned Blockchain

Permissionless blockchains grant write access to all. Each user or node can check transaction data and create and add new blocks to the blockchain data structure. This leads to complex consensus protocols because each node can create a new block and this means a large communication station infrastructure and therefore many nodes to considerable communication effort.

A permissioned blockchain restricts the nodes. Only certain nodes can create blocks and propose them to the other nodes as the next block. Ultimately, this limits who may contribute to the consensus of the global ledger. They grant write access to only limited groups of preselected nodes or users, namely users trusted by KYC and KYB processes. The identification of nodes by KYC, KYB and AML laws makes the permissioned blockchain interesting for shared ledgers in an open charging station infrastructure. Thus, here only the group of nodes that have write access may insert transactions and participate in the distributed consensus procedure.

For permissioned blockchains, wallet addresses are usually issued by a trusted third party. This function can also be displayed directly in the blockchain, if Oracles can verify the authenticity of a person, Smart Contracts can create users directly, but their identity does not necessarily have to be stored in the blockchain, but their cover name, the wallet address, is sufficient. These trusted instances, which are mapped as Smart Contract or external Oracle, grant the authority to participate in the system and allow transactions within the system to be sent to Mining Nodes so that they check the transactions for correctness.

In the distributed charging world, this type of verification might be necessary to scale a product for the masses. Blockchain network users undergoing a registration process as an end user or institution will be granted their privileges. Whether they are regulators, power generators, financial institutions, charging station operators or just customers.

A user may have different identities (aliases) in a public blockchain. Bitcoin and Ethereum addresses are inherently pseudonymous; they are not linked to your real name or information. But every transaction they send is public, in the sense that anyone can see the transaction on the blockchain. For this reason, public blockchains are being touted for their transparency.

The permissioned blockchain makes it possible to use consensus-finding mechanisms that are not based on proof-of-work, but more efficient ones such as proof-of-stake or Byzantine fault-tolerant protocols.

Permissioned block chains provide verifiable records that many nodes can validate. This creates a high degree of confidence in the security of the system. A legitimate ledger is usually faster than a Permissionless ledger.

> *“The key distinction is that whereas permissioned blockchains are merely distributed solutions, open blockchains offer real decentralization.”*
> *(Dhillon, Metcalf, & Hooper, 2017, S. 197)*

As a basis of a billing system for a distributed system of charging stations with different types of power generation offers a permissioned public block chain.

Public so that it is verifiable by every participant, and therefore trustworthy. Permissioned to use a simpler, faster and more energy efficient consensus algorithm.

Permissioned also allows regulators with restricted rights to be censored by individual interest groups.

Not all charging stations need to be mining nodes, but can also be thin clients. Small private charging stations can trust multiple full nodes and use them to put their transactions in the general ledger.

- For a distributed public charging infrastructure, it is recommended to use a permissioned public blockchain.

4.4. Permissions in the Charging Station System

After a permissioned blockchain is used, permissions must also be set.

For a participant to be allowed to participate in the blockchain he needs a unique identity (see Figure 33). This identity can be the address of a wallet analogous to Bitcoin or Ethereum and can be called a unique user identity (UID). This UID can be the hash value (for example: sha256) of the public part of an asymmetric key pair, or just the public part directly. The private key of the subscriber allows him to sign his transactions so that each other participant knows he has the right to do so. This verification takes place with the help of the public key. By decrypting the signature which must give the hash code of the transaction, any other node can check this (see Asymmetric encryption / Asymmetric key pair; paragraph 2.4.1.2; page 26). Checking whether it is the correct account is done via the unique UID.

This UID allows for principal participation in the blockchain. Depending on the role, the user's wallet may have entries about its permissions.

Permissioned systems recognize their users, whose identity has been verified by a KYB (KYB) or KYC (KYC) verification procedure, similar to the requirements of traditional financial systems. The information about the identities is not stored in clear text in the blockchain, but can be stored encrypted using cryptographic methods. Only the owner with his private key, or the institution that carried out the exam, can release the identity. The release must be clearly defined by rules.

In addition to legal considerations, there are also social and ethical responsibilities for knowing the ultimate beneficial owners (UBOs) of companies doing business in blockchain. Because it could be companies that hid their profits from legal taxation in tax havens. These hidden funds would create a larger tax burden for the rest of society. (Hofmann, 2018, S. 42)

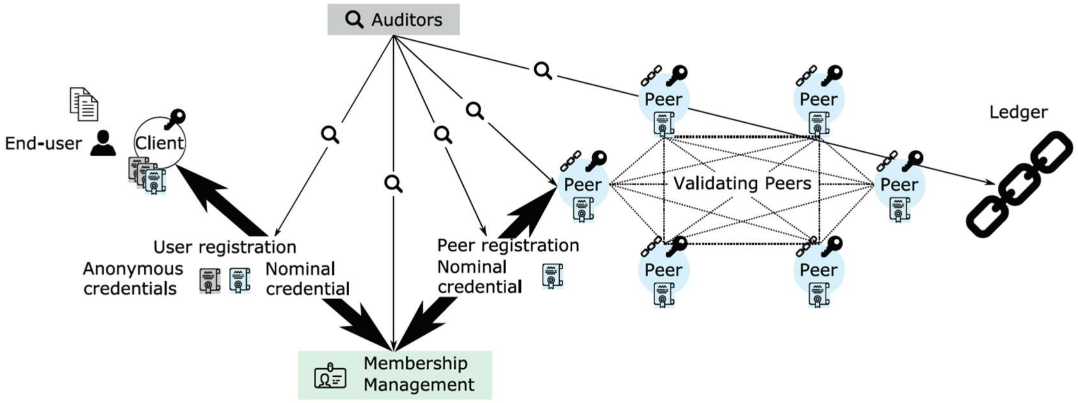


Figure 33: Basic architecture of Open Blockchain with registration process (Karame & Androulaki, 2016, S. 178)

> *"Open Blockchain is a permissioned blockchain network, where end users or organizations go through a registration process that would authorize them to submit (as users) or process transactions (as validators) that are announced in the system. The permissioned nature of Open Blockchain allows the latter to mainly rely on nonproof-of-work based mechanisms, such as Byzantine fault-tolerant protocols, to achieve consensus in the network on transaction validation."*
>
> *(Karame & Androulaki, 2016, S. 178)*

4.4.1. Right to participate in the Charging Station System

If Electro Vehicle (EV) users wish to purchase energy from a charging station, they must identify and authenticate themselves at the charging stations. This permission is bound to its UID. If a user has an UID, he may register with the stations and try to conclude a contract for the loading process. This right automatically includes the right to check the correctness of the blockchain. Depending on how strictly the access to blockchain is regulated, this authorization can already presuppose a KYC process, which checks the identity of the participant. If access is generally allowed for everyone, the KYC process will required for the other rights. (see Figure 33)

4.4.2. Right to use of means of payment in the charging station system

Since there will also be roles that are only allowed to observe the operations in the blockchain, they must or cannot perform any transactions. This application of means of payment can be subdivided into send (pay) and receive (get paid). It is up to the developers and the designers how different wallet types are treated. Goods of the blockchain can not only be coins, but also green certificates and other useful goods. All goods could also be seen as a means of payment (actually, they can be interpreted as goods for bartering). If all goods are to be considered as means of payment this use of means of payment must be defined separately. There are tuples of the kind (currency type, application possibilities). Permissions can also be limited to one country, so that they are valid there.

For example, if you want to buy GreenCertificates within the blockchain, you must have the permissions (Cryptocoin, Send) and (GreenCertificates, Received). These permissions do not allow me to resell the certificates.

4.4.3. Right to own a wallet

Not every user needs a wallet, because he can also use the conventional payment services such as cash, debit or credit card. However, this assumes that the charging station can offer them. Large charging stations, similar to today's filling stations, can easily reproduce this in their business model, but in the case of small decentralized stations, this will not be the case in cost terms because the running costs and the necessary technical equipment will be too high in relation to the expected profits. This permission can also be tied to the one KYC process,

4.4.4. Right to feed renewable energy into the electricity network

Not every node is allowed to feed power into the grid. The basic prerequisite is the suitable production possibility of renewable energy and the availability of suitable calibrated measuring systems so-called smart meters which also have a connection to the blockchain. This authorization may be accompanied by the production of green certificates.

4.4.5. Right to sell renewable energy to EV owners

If the operator of the solar system also wants to sell electricity directly to customers on site, he needs the permission to offer and sell this electricity. This requires a renewable energy source and the appropriate measuring equipment.

4.4.6. Right to sale of conventional (non-renewable) energy to EV owners

In order to build a nationwide charging system, it must also be possible to provide electricity from the conventional energy market. This requires suitable measuring equipment.

4.4.7. Right to mine new blocks

After the mining nodes have to be particularly trustworthy, their identity must be checked. It must be clear who runs the business, pulls the strings behind the scenes and profits from the business - so who is the UBO. The danger of a 51% attack can be prevented, since never a UBO may never own 51% of the mining nodes.

4.4.8. Permission to contribute money to the Blockchain

Not everyone is allowed to bring money into the blockchain. Money can be created as usual in the banking world by entries in an account, or be circulated by the central bank. In the real world, you only need a bank license. There must be a similar function in the blockchain. These institutions must be able to demand this money in bank accounts, thus serving as an interface to real currencies. These features will typically be real-world payment services: banks, online payment services, credit card companies.

4.4.9. The right to intervene regulatory in the charging station system

If there are legal problems in providing the service, or a subscriber attempts to cheat by manipulated technical devices or even a software error leads to a malfunction then there must be a way to correct this. This is done by a regulatory intervention by one or more authorized nodes. Depending on the intervention, a certain number of regulators must be involved, so that democratic structures emerge. However, this intervention can only trigger new transactions, but not alter old transactions, because that would contradict the finality of the blockchain. An example would be that a charging station regulator blocks access because it has been compromised, or accounts could be blocked if its owner stole digital assets by manipulation. They can also unlock the access again. Various regulatory interventions may be possible, but each of these rights should be governed by its own permissions. However, these interventions must be stored transparently in the blockchain in order to prevent misuse of this function.

The rationale for this role lies in the fact that an attack on a system such as the Decentralized autonomous organization (DAO) hack at Ethereum must be governed by predefined rules.

4.4.10. Right over the granting of authorizations within the charging station system

If new nodes want to accept a new or additional role in the blockchain, the associated permissions must be granted through transparent operations. To make this process democratic, this can be done by vote. Nodes already have the roles to vote on whether another node should be assigned this role. This makes sense only for more privileged roles, for the participation in the blockchain a KYB exam will suffice.

4.4.11. Right to send transactions to the Blockchain Miners.

If a node wants to sell digital assets such as green certificates or energy to EV owners, they must send this transaction to the blockchain miners. To do this, he needs the right to send transactions to the Mining Nodes, at least one node must have this right when executing contracts, otherwise the transaction cannot be immortalized in the blockchain. Which transactions a node may send for validation must be clearly regulated in its role within the system.

4.4.12. Right to perform KYC and KYB checks for the charging station system

In order for newly participating nodes to be included in the blockchain as participants, their identity must be checked in accordance with KYC, KYB or AML regulations. This test must be carried out by specific roles. These nodes need the right to do so and work like Oracle, which can bring external information about transactions into the blockchain.

4.4.13. Right to trade with all economic goods of the charging station system

This would correspond to a stock exchange, thus allowing for speculation and therefore should not be used, as this would create uncertainty among the operators and users, as there would be a currency risk through speculation.

4.4.14. Right crypto transfer coins within the charging system to accounts outside the Blockchain.

If profits are made within the blockchain, they may be used within the blockchain under the rules of smart contracts for other digital assets or transferred to a conventional account at a bank or other payment system. These interfaces will be special nodes that interface with these systems. The owners of these accounts will be just these service providers.

4.5. Roles in the Charging Station System and assignment of this.

The roles in the blockchain determine the processes that a participant is allowed to perform within the system. The roles that own a node are placed in the blockchain and checked during the execution of Smart Contract. A set of rules in the Smart Contract ensures that roles are not exceeded. In order to give roles, a vote among the participants is generally to be aimed at in privileged roles. Depending on the roles, a certain percentage of the nodes that already have this role must vote for the node. If they are roles that have specific economic or technical functions, KYB or KYC exams must be performed, which also check the technical competence. If checked by external checkpoints, then this information is copied to the blockchain upon successful completion of this check - this is equivalent to the function of an external trusted Oracle. The rules for granting roles and associated privileges must protect against being able to monopolize individual nodes or roles, which would destroy the principle of an open charging structure.
(see 2.4.34)

4.5.1. Electric Vehicle User

EV users want an easy way to charge their battery systems. They want to find charging stations in their area with simple means, where they can choose a suitable charging strategy, renewable energy sources and pay for the amount of energy you have received. To be able to use the charging infrastructure you need at least the right to participate in the network. If you do not want to own a wallet directly, you can pay via payment services. When charging, the payment service provider is included in the smart contract, as this guarantees the payment of the charge and will pay. Of course, the EV operator needs a contract outside the blockchain with this payment service.

In order to find charging stations within his radius or along a planned route, he will use a service outside the blockchain. Of course, this service can be tightly linked to the blockchain, that is, it can obtain the information about the location and its offered service and availability directly from the blockchain.

If the EV owner himself wants to have a wallet and wants to pay with it, he needs the right to own it and the right to use digital money in transactions.

4.5.2. Operator of a small charging station that only offers energy from own renewable energy sources:

A renewable energy operator needs the right to sell energy to EV owners and to the grid, the right to own a wallet, the right to receive cash. When green power is generated, "green certificates" are also generated. If you look at "green certificates" like digital currencies, then you also need the right "money" in the form of green certificates. Digital currency and green certificates are both digital goods and can therefore be treated equally, that means have the same authorization structure. After the transacted transactions have to be immortalized in the blockchain, this role must also be able to send transactions to the mining nodes.

When examining this role, it must of course be checked by an external Oracle whether the electricity comes from renewable sources. For example, solar power or from a small hydroelectric power station.

4.5.3. Operator of a small charging station that offers energy from any renewable and conventional energy sources.

This role has the same rights as a producer of renewable energy sources, it only needs to be guaranteed that green certificates are generated only from renewable sources.

4.5.4. Operator of a small charging station that offers energy only from conventional energy sources.

An operator of a charging station needs the right to sell energy to EV owners, the right to own a wallet, and the right to receive cash. So that he cannot be speculated here, he must not sell energy to the grid because he could buy energy cheaply and sell more expensive. Likewise, he may not sell Green Certificates because he does not generate any.

4.5.5. Operator of an energy storage system for renewable energy

This role can buy energy from renewable energy sources, even with the associated "green certificates" but not pure certificates without the associated energy, because this would allow an exchange trading with "Green Certificates". This can be limited in the Smart Contract for this transaction. Of course it must also be allowed to sell its electricity and the "Green Certificates".

4.5.6. Operators of large charging stations offering all types of energy

These have the same rights as a small charging station that sells energy from different sources. If this operator also operates an energy storage device, it may only be subject to the same rules as pure energy storage - no trade in "Green Certificates" without purchasing the associated green energy. But you can also operate each charging station as a separate small station, of course, the accounts must then be billed separately.

4.5.7. Miner

These have as only role the right to mine new blocks. After this service has to be paid, they must also have the right to an account and also be allowed to send the Cryptocoins from their own account to accounts outside the blockchain. If they try to create wrong blocks, these nodes can be kicked out by the regulators and their accounts frozen. When reviewing the block, all supervisors must realize that it is wrong and they can collectively revoke this node's permissions by voting. False blocks are detected and discarded by all nodes in the blockchain due to cryptographic procedures.

4.5.8. Auditor, state institution

They ensure compliance and review of the rules of blockchain. After all transactions of the blockchain are readable by all participants, these auditors can analyse the behaviour of the users and, if necessary, initiate legal action outside the blockchain. Tax authorities can check whether profits from transactions in de blockchain are also taxed.

4.5.9. Regulators in the charging station system

Can work in concert with the other regulators in common to influence certain functions. These can block incorrectly behaving nodes in the blockchain. These rules must be disclosed and be comprehensible at all times and also stored in the blockchain. If a fixed value is defined for a digital value, such as Green Certificates, these nodes can change this by consensus. These rules may be hard-coded or dictated by external Oracle controlled by a state agency. Thus, the state can reduce the number of available certificates. Inflation avoids that goods are used and not hoarded. (Analogous to alternative currencies, see chapter 2.4.27) (see chapter 2.4.33

4.5.10. Payment services for the charging station system

These nodes offer financial services. If an EV owner does not want a wallet in the blockchain, he can delegate the payment to a payment service. Of course, the EV owner must then have a contract with these service providers outside the blockchain. An advantage of this type of payment is that the EV owner's UID is not included in the blockchain transaction. The EV owner receives a direct debit on his account outside the blockchain. Likewise, these payment services can also transfer crypto coins from the blockchain to an account outside of them. You therefore need the right to use funds for Crypto Coins, the right to own a wallet, the right to bring money into the blockchain, for which they also have liability. They can also perform the KYC or KYB check for your customers outside the blockchain, which means they have the right to grant authorizations. This service must be disclosed to governmental authorities in the event of a legitimate request confirmed by a court order.

4.5.11. KYC, KYB test instance

These nodes serve as external oracles, which with reasonable care confirm their trustworthiness and identity to users. You grant the roles after successfully checking in the blockchain by creating a corresponding transaction in the blockchain. Thus, the role is linked to the UID in the blockchain and the user is allowed to carry out the possible transactions.

4.6. Payment within the charging station system

Services rendered, real goods or digital goods must be paid. In the real world, this is done through cash, or electronic cash transfers. Crucial for money transfers is the settlement - when do I really have the money. With cash, this is very easy, as soon as I physically own the money it belongs to me. This is different with bank accounts - only from the value date the money belongs to me - if the payer does not have the right to reclaim the money. For credit cards, the payer has about 1 month to complain about a paid bill - so the money belongs to the account holder earliest after one month. This settlement is achieved with cryptocurrencies, with the corresponding consensus process, immediately upon entry of the transaction into the blockchain. This transaction cannot be undone within the blockchain. Regulators can block accounts if allowed by law outside the blockchain. This is a clear improvement over the previous banking system.

Decisive for the business model are also which coins or currency I use within the blockchain - a separate crypto currency with variable exchange rate to existing currencies, or a digital representation of existing currencies.

The crypto-currency used guarantees the energy supplier that the amount to be paid is credited to his account immediately after the end of the delivery.

4.6.1. Cash and coloured coins

If a currency is used within the blockchain, it can not only have the attribute value. Due to its digital origin, but can also have other properties.

Thus, coins can have an attribute only for the purchase of certain goods, be used only for transfer to a real account, only to be changed into a specific national currency and so on. These restrictions can prevent this Crypto currency from being used for speculative purposes.

The following restrictions would be useful:

- When a user transfers money to the blockchain through a payment server, it may only be used to purchase energy, but no other goods can be purchased.
- A charging station can only transfer its business profits to a real account in its home country.
- Coins should have a built-in inflation so that it is not hoarded. They are not used as a store of value and hoarded thereby.
- If money is transferred to a digital account from the existing banking system, then it may, if it has not been used, only transferred back to the same account.
- They can be divisible or indivisible, which means that the amount of assets in a transmission can be an integer or a decimal.

These limitations make sense to prevent misuse of the blockchain because the only purpose is to provide a stable, reliable system for a charging infrastructure.

This additional feature of coins is called "Coloured Coins", they provide the possible use cases.

(Rosenfeld, 2012) (Assia, Buterin, Hakim, & Rosenfeld, Year not specified in document, maybe 2016) (Sixt, 2017, S. 167-)

4.6.2. Conventional procedures (credit card, debit card, cryptocurrency)

If customers want to pay conventionally with cash, the cash register system of the charging station must make this possible. The cash register is an external oracle that assigns the corresponding number of coins to the seller of the energy via a payment service. The accounts within the blockchain can also have their coins transferred to an external account via these services.

With electronic payment services such as automated teller machine card (ATM-card) or credit card, payment is also made via an external oracle. Once the transaction is done in the real world, the oracle writes the transaction to the blockchain.

These two methods will most likely not be provided by small charging stations, since on the one hand there will be no on-site personnel and, on the other hand, a connection to an electronic payment system will be too costly.

Micro Business will make sense only through a digital currency with low expenses.

4.6.3. Own cryptocurrency in the Blockchain

If a currency is used within the block chain for the payment of goods, this may be a separate floating currency with variable exchange rate to existing currencies, or a currency with constant exchange rate to existing currencies. The money within the blockchain should only be a means of payment and cannot be used as a store of value or a speculative object. There are already banks and stock exchanges for these business models.

4.6.3.1. Own money, own cryptocurrency

Blockchains allow you to create your own currency. This would be fiat money, a digital asset with no intrinsic value. The value exists only as long as the participants believe in it. The problem with this currency is the undefined exchange rate to government fiat money such as the euro. It would come as with other crypto currencies to price fluctuations that could destroy the business models of the charging station operators. There is no assurance that the purchasing power of the coins received will be the same in the near future, and the owner of these coins will incur high losses by no fault of his own.

Own digital money also brings benefits in terms of transaction costs. There is no need to pay high fees in the blockchain as opposed to banks as this is one of the main tasks of the system and therefore can be implemented very efficiently at a low cost.

Digital money can also be easily divided into units under a EuroCent, so that even small amounts can be settled. Many companies are already spending too much money on using EuroCents in physical money, so they stop accepting 1, 2, and 5 EuroCent pieces. For bitcoins, you can divide a bitcoin into a hundred-millionth bitcoin (0.00000001 BTC) - a satoshi is currently the smallest unit of bitcoin currency that can be stored in the bitcoin block chain.

4.6.3.2. Blockchain fiat money should be tied to the euro

Having your own currency - even fiat money with a fixed link to an international currency like the euro makes sense, because here there will be no losses or profits due to changing exchange rates. If other currencies are used for payment, the payment services must convert this to digital euro coins at current daily exchange rates.

4.6.3.3. Alternative money

Another alternative would be a currency equal to the amount of energy, so that, for example, a micro-solar power company charges its account with kilowatt-hours, which it can withdraw from the grid at another time. The problem with this is that one kilowatt hour at peak time has more value than one at off peak time. Here, the current load situation would have to be considered.

Money is actually a medium of exchange. In former times also commodity money, as salt, rice, gold or silver was used as medium of exchange. So you can call Green Certificates actually money and use accordingly. If a subscriber generates green Certificates and has them on his account, he could later use it against energy to charge his vehicle. This could create an incentive to buy an EV vehicle and a photovoltaic system.

4.6.3.4. Coloured coins

Coloured coins make it possible to create digital assets on the Energy blockchain by using their functionalities beyond the currency. Coloured coins allow the money and flows of goods within the block chain to be defined and regulated. This shows that currency systems can be integrated that provide rich functionality beyond the current currency system.

4.6.3.5. Money with built-in inflation

So that money is not only hoarded within the charging system, but also used, one can install an inflation function. If money is not used for a certain amount of time, it loses value.

This is especially interesting when implementing Green Certificates as the currency of built-in high inflation. As a result, Green Certificates cannot be hoarded and must be used. By implementing Green Certificates as coloured coins, which makes this inflation rate dependent on other parameters, a regulator can very well control the use of these certificates. For example, the Green Certificates at the producer could have a lower inflation rate than the buyers. Companies would not buy many certificates in stock and bunker them.

4.6.3.6. No speculation object

None of the traded commodities or currencies should be able to be used as a speculative object, providing them with uncertainty and additional costs, extra costs due to speculators' profits and additional costs due to unnecessary new transactions.

4.6.3.7. Green Certificate from the perspective of a currency

Green Certificates can also be viewed from the perspective of a currency. A green certificate is normally issued per 1 MWh of renewable energy. By divisibility of the certificates even small producers can generate this. If the certificate prices result from the interplay of supply and demand for certificates. The more renewable energy is generated, the cheaper Green Certificates will be, which reduces the incentive to produce them. Inflation and possibly also an expiration date can be used to intervene regulative and increase demand again.

If the certificates are also considered as coloured coins, i.e. other attributes are bound to this currency, the source of the green energy can also be linked to the certificates.

4.6.3.8. Smart contracts with Payment channels

A smart contract is an agreement that is binding as it can move digital asset based on the specific terms of the agreement. These contracts are stored as programs in the blockchain and are applied as needed. If an EV owner wants to buy energy at a charging station, the two contracting parties conclude a contract. Once agreed, this is unstoppable, guaranteed the negotiated terms and conditions are met. This implementation is not based on a legal system and its enforcement, but on the blockchain. Smart contracts must therefore be carefully checked before they are included in the blockchain.

Since a loading process is a continuous process, but can also be cancelled, the units are also billed continuously. In order not to produce permanent entries in the blockchain, payment channels can be used. Initially, it is agreed what the maximum charge quantity and the price will be, starting with a smart contract that generates an initial transaction that ensures the payment and delivery of the energy. Now, outside the blockchain, the current amount delivered is billed, and payment channels allow a covered transaction (see Payment channels and state channels; chapter 2.4.26 page

67). As soon as the loading process is finished or cancelled, this parallel settlement is included as a transaction in the ledger and the contract is fulfilled.

- It makes sense to use fiat money in the blockchain, which has a fixed bond to the euro.
- The coins should be coloured coins that have other attributes besides their value.

4.6.4. Initial Cash Distribution in the Charging System

Since the energy charging system should not create money from nothing, there would be no coverage by any authority, there must be authorized agencies to bring money into the blockchain. There are two possibilities here:

- Bank money, introduced by banks, or payment services.
- Central bank money created by the central bank.

After transactions of accounts within the block chain with accounts in payment services take place during use of the charging point system, it makes sense that the banks first bring the money into the block chain. However, they must also have collateral for them, such as money, on the customer's accounts. This deposit insurance serves to protect the digital assets of the participants. This ensures the functioning of the system in the event of bank insolvency.

4.6.5. Fulfillment of GDPR regulation in EU law

The blockchain does not forget anything. But this would violate the right to forget about the GDPR of the EU. But there is a solution: If the blockchain is set up according to the Merkle-Hashtree, individual transactions can be replaced by their hash values and the transaction can be deleted. Possible copies of the records can no longer be checked for correctness within the blockchain since the transaction data no longer exists. But the blockchain is still consistent

Blockchain subscribers can put a delete request to the blockchain to delete transactions that were made with a specific wallet address. Likewise, transactions can already be provided with a deletion date when they are created. For Austrian companies that would typically be the law at the earliest after 7 years.

Authorities may view and analyse the data of a participant only according to legal principles. For example, during a financial audit, you can ask the public UID of the participant, and then include that year's data in your investigation. For companies, it is advisable to create a new account for each fiscal year and thus create a new public UID.

All other conditions are given by the structure of the charging system. (see chapter General Data Protection Regulation (GDPR) – regulation in EU law. Chapter 2.4.30 page 76)

4.7. Selected processes within the charging station infrastructure

4.7.1. The processes within the charging infrastructure can be handled with smart contracts.

If two or more business partners want to enter into a business relationship then they choose a smart contract filed in the blockchain or jointly create a new one that meets their requirements.

4.7.2. Infrastructure has to be payed

The miners must be paid - by transaction costs. These transaction costs are paid by the nodes that send the transactions to the miners. These can be paid to the miners as the difference between the amounts in the transaction. Miners can also demand minimum amounts. If these are too high, regulators can limit these.

4.7.3. Charging a EV

If an EV owner wants to load his vehicle in the distributed charging system, he must comply with the following processes.

4.7.3.1. Register in distributed charging system.

In order to be able to use the charging infrastructure as a user, it has to register in the network. The following steps are necessary for this:

1. Create an asymmetric key pair. The public part will be his UID and if he wants to create a wallet, it will be the wallet's address.
2. He turns to a KYC instance to register. He provides his UID and personal details. He also states whether he wants to own a wallet, or only wants to pay via payment services.
3. The KYC instance checks the identity and, if successful, creates a transaction that meets the requirements using a smart contract in the blockchain. The UID gets a role and the associated permissions provided by the authorized body. The KYC instance signs this block with its private key. The private data is stored secured for traceability at the KYC site.

Everyone on the network knows that this UID has the right to charge at charging stations and which KYC instance has checked it.

4.7.3.2. Loading the account with money.

In order for the account to be used for payment within the charging system, an amount has to be transferred to the account. The following steps are necessary for this:

1. The subscriber turns to his bank or other payment service, which is also registered as a payment service in the blockchain, and gives them the order to transfer a certain amount from his external bank account to his UID in the blockchain.
2. The payment service now executes a transaction which carries out a transfer of funds from one of its accounts to the account of the party taking part. If blockchain uses coloured coins, then with this money you will only be able to load your EV vehicle.

The EV owner now has money in his account, which is assigned to his UID.

4.7.3.3. Charging the EV

In order for an EV owner to be able to charge his vehicle, he has to drive to a charging station and arrange a charging process with it.

1 Depending on what type of charging the EV owner wants to load his vehicle, he is looking for a charging station with an online tool. He can be on a journey and looking for a fast charging station along the route, or at work, looking for a station with solar charging and parking for 8 hours. This tool can get the information about charging stations directly from the blockchain.

2 The EV owner reserves online the charging station for a specific time window.

3 A contract with the charging station operator is agreed and started on the type of electricity and the duration of the load.

4 If the EV owner has his own account in the blockchain, he will indicate this as a payment account. If he does not have an account, he will contact his payment service outside the blockchain so that they will make the payment with the charging station owner.

5 A transaction is created with both signatures and the guarantees for payment and delivery.

6 The charging process is carried out. Billing can be done via a payment channel outside the blockchain.

7 When the loading process is completed or the process is terminated prematurely, the amount confirmed outside the blockchain is passed to the mining nodes as information. They include this transaction in the ledger.

The success of the loading process can also be sent to review portals.

4.7.4. Operation of a small charging station for renewable energies

4.7.4.1. Register in distributed charging system.

In order for a solar system owner to make his charging station available in the system, the latter must register in the network as a charging station. The following steps are necessary for this:

1 Create an asymmetric key pair. The public part will be his UID.

2 Contact a KYC KYB authority to register. He provides his UID and personal details. Once the node is a charging station, it must also provide technical support for the charging infrastructure.

3 If everything is correct, a corresponding transaction will be sent by the authority to the mining nodes and they will create the correct entry in the blockchain.

4 Everyone in the blockchain now knows that this charging station exists and knows all the technical features. The charging station owner enters his charging station in appropriate search engines, so that his station can be found.

The charging station is now known in the network with location and UID.

4.7.4.2. Offer energy and charging on the market

The operator of a private solar charging station can offer various types of charging. The choices can be the power source - it can also offer conventional energy sources in addition to solar power at too low solar power. Also, the length of stay is a criterion that charging the vehicle during a long stay on site is a common application.

This information is managed off-chain and sent to appropriate servers. It would not make sense to store this information directly in the blockchain.

4.7.5. Get the permission to be a mining node.

Mining nodes carry the actual workload in the blockchain. They have the necessary infrastructure, such as processing power, network connections, and disk space, to complete this function. They are paid by participants using transaction fees. Alternatively, the solar station operators could pay a fixed monthly usage fee.

For a node to be accepted as a mining node, the following process must be performed.

1 Create an asymmetric key pair. The public part will be his UID as well as the address of his account.

2 Contact a KYC KYB authority to register. He provides his UID and personal information. After being a mining node, he must also have the technical ability. These requirements are also checked.

3 If the verification was successful, the audit authority will submit a transaction for inclusion in the blockchain.

4 Depending on the blockchain setup, a certain percentage of other mining nodes must agree to this. The more restrictive the blockchain is at its mining nodes, the more other miners will have to agree.

5 If enough participants have agreed, the node will be included in the Mining Nodes and will in future also check transactions and create new blocks

When a node creates a new block, it gets the mining fee on its account. This transaction is part of the newly created block.

4.7.6. Get permission for other kind of nodes.

Roles can be issued by KYB, KYC instances following an identity check and also their technical requirements, similar to the roles listed above.

4.7.7. Genesis, the first block.

In the first block of the blockchain all initial roles must be defined and already assigned to the first audited participants. Likewise, all basic smart contracts must already be created initial, so that the first participants can already apply them.

5. Conclusion

Blockchain technology, also known as Distributed Ledger, is a new technology that will take a lot of evolutionary steps. It has many degrees of freedom that offer many possibilities. For the application of the blockchain technology in the renewable energy sector, the parameters and algorithms must be chosen carefully, because there are some configurations that lead to an unnecessarily high energy consumption. It also has disruptive potential, so big players in the power industry should use the power of this technology as small startups will conquer the market.

Analyzes have shown that the algorithm for finding consensus in distributed networks is one of the most important parameters for energy efficiency. Consensus finding should not be based on a proof-of-work process, but on a proof-of-stake or other energy-efficient algorithm. The storage of data also costs a lot of energy, the use of which can be optimized. On the one hand, instead of one large global blockchain, many small local blockchains can be used, requiring the individual nodes of each chain to store less data. The individual chains are not autonomous, but can communicate via gateways or Oracles with the other chains analogous to sidechains. This ensures that the users of the charging infrastructure worldwide can load their vehicles without additional effort, the system fetches the relevant data from the respective homechain of the user. Not all information of a transaction needs to be stored within the blockchain. Information that is not needed for billing, or for proof of possession can be stored in external databases backed up by cryptographic methods. Another option is the use of thin clients. These do not store all the information of their own chain, but only information relevant to them, and trust one or more full nodes that control the general ledger. This reduces not only the memory requirement of the node but also its network traffic caused by the consensus algorithm. By using a Peer2Peer architecture, each node does not have to communicate with all the nodes, but only with its neighboring nodes, which passes that information back to its neighbors.

Because all the nodes in a chain store all the general ledger information, there is no way that one or more nodes can manipulate the system or monopolize it. This distributed architecture also provides greater resiliency than centralized systems because failure of individual nodes cannot disrupt the overall system.

In order to create a censorship-resistant open system, a public block chain should be chosen, which allows no monopolists to operate in secret and everyone has an insight into the amount of all transactions. This transparency and openness of the transactions creates trust of the participants in the system. This openness also requires that no backdoors are hidden in the code and therefore the code should be available as open source, as is customary in many areas today.

This openness of transactions requires special measures to protect the privacy of their subscribers. Cryptographic techniques provide mechanisms for protecting them. The use of pseudonyms or payment services is the minimum requirement for privacy, but can be further improved by further procedures. By becoming aware of the identity behind a pseudonym, the complete movement pattern and the business relationships of a user could be determined. (Together from other information of the system)

The individual actors of the distributed charging system have different interests, so each of these actors needs different permissions. This led to the idea that a permissioned public blockchain should be used. In this case, the required authorizations can be selectively assigned depending on the scope of functions of the node.

In this system there will be different types of nodes: customers who want to use the infrastructure for charging, small private charging stations who want to sell their solar power directly to the network operators or EV owners, large charging stations with optional buffer storage the energy from various sources with guaranteed certificate of origin, payment systems that provide an interface to real banks, miners who want to offer their resources and get paid, but also regulatory authorities who want to monitor the function of the blockchain.

The individual actors need legitimacy. These can be obtained through a system with different roles. These roles must be initially set in the code. The code is trusted for the proper functioning of the roles, as this code is publicly available. But it still has to be determined who may hold which role. It will not be possible to avoid external institutions that examine the identity of the participants and then give them the authority to trust. So that no monopoly position arises here, the authorization for this authorization must also be clearly regulated. One possible solution here is that the new candidate for a role must meet certain external requirements (for payment systems, for example, have a banking license) before all other nodes agree on the inclusion. One can also apply the 51% principle here, if 51% are honest, then a new participant also needs at least 51% of the votes so that only new honest accounts are added to it. Important for the confidence in the system is the new participants must meet fixed rules before they are taken into a role by democratic vote. These rules are only necessary for roles with special rights, for pure users of the charging stations as EV users checking the identity is sufficient.

By outsourcing the identification and authorization of users to external systems, they offer privacy. However, this requires trust in one or more entities in the system.

The massive automation can reduce the costs of operation. The cost of operating the infrastructure of the Blockchain's validators may be covered by a monthly fee or a fee per transaction. These costs should be fixed and very low. Each node must pay for the operating costs themselves.

In order to spare small producers a cost-intensive billing using the existing banking system, a separate crypto currency must be used within the system. The producer has his wallet within the blockchain where coins can be credited with little effort. If he wants to use the money in the real world, he has to transfer this via a payment service to his bank account. Important when using your own currency is that there are no possibilities of speculation. Speculation only creates uncertainty, as no one knows if his cryptocoins have the same purchasing power the next day. Therefore, the cryptocurrency used must be permanently fixed to a real currency and colored coins can also be used to regulate the flow of money within the blockchain.

The producers need to prove their technical equipment, the correctness of the counters, an asymmetrical keypair with the public key as UserId and an identification and authentication by a KYC, KYB test facility. Once done, all participants know that a new charging station is online and can be reserved and used. Of course, the charging station operators have the possibility to provide their charging station with all relevant data on various online platforms that offer information about these stations.

With the concept of a charging station system based on blockchain technology, an energy-efficient transparent infrastructure can be set up for all open, unbureaucratic, transparent infrastructures. The system is also robust and scalable. There are no central authorities required for the operation, but it will make sense to incorporate regulatory elements that can influence according to transparent rules. These regulators have no monopoly positions, but can only act according to the defined rules.

We have a system for charging stations that does not rely on trust between the participating parties but can rely on blockchain technology.

During the analysis, another application of the distributed charging system has opened up. If energy suppliers generate energy from renewable sources, a further cryptocurrency within the blockchain can also be used to generate and trade "green certificates". The certificates are to be regarded as divisible coins. In order to prevent these certificates from being hoarded but to be traded, they should have built-in inflation like alternative currencies (see Chapter 2.4.27). In order for the state to be able to intervene here too, it can control inflation by means of a regulator according to fixed rules, so that there is always adequate supply and demand.

Once again the key points for the application of blockchain technology for a distributed charging system:

- Public blockchains should be used for the system to be trusted and open.
- Permissioned blockchains should be used to use a simple energy-saving consensus method, to assign different roles in the network, and not to give a censorship to any user group.
- The blockchain and the associated ledger are final.
- The system should avoid centralization, which is a single point of failure and also has monopolistic structures. The blockchain is a distributed structure with democratic open structures.
- Blockchain technology makes it possible to set up a distributed charging infrastructure in which even private charging stations can be integrated.
- The blockchain allows even small energy suppliers such as solar system operators to participate in the charging station system.
- A blockchain-based charging station system does not require a central instance or central authority.
- A blockchain-based charging station system does not require a trusting third person as with many other business processes.
- The existing Internet network structure can be used. With the new IPv6 addressing there are enough addresses for all nodes. The network of nodes is used as a logical P2P network on top of the internet
- The communication between the nodes is encrypted using TLS to prevent external manipulation.
- Saving in the blockchain is expensive, so only important information for the general ledger should be stored directly in the blockchain.
- There must be a regulatory unit that can perform actions in the blockchain according to established rules. These must be transparent and must not have a monopoly position.
- It makes sense to use a cryptocurrency within the blockchain that is linked to the existing euro currency. This prevents speculation with exchange rates.

- The cryptocurrency should have coloured coins that specify the possible purposes of dilution.
- Green Certificates can have built-in inflation to manage supply and demand.

Sufficiently radical technological innovation can lead to revolutionary changes, not only in business models or industries, but ultimately also in the way how the company organized and governed.

5.1. Personal conclusion:

Blockchain technology is a new technology and there is sure to be a lot to talk about. But there are many things that have already been said, and therefore do not have to be put into new words. Therefore, my personal conclusion is a sentence by Stephan Hessel from the book "Engage you!" (Engagiert Euch!) Stéphane Hessel, (20 October 1917 - 26 February 2013) born in Berlin, was a French citizen since 1937. French Resistance member and Buchenwald survivor. From 1945 he represented France at the United Nations in New York, 1948 as co-signatory of the UN Charter of Human Rights. On behalf of the UN and the French Ministry of Foreign Affairs, he worked as a diplomat.

We have to put an end to this growth fetishism of "still more".

6. Literature

Antonopoulos, A. M. (2017). *Mastering Bitcoin, Programming the Open Blockchain* (Second Ausg.). United States of America.: Published by O'Reilly Media, Inc.,.

Assia, Y., Buterin, V., Hakim, L., & Rosenfeld, M. (Year not specified in document, maybe 2016). *Colored Coins BitcoinX - Whitepaper*. Abgerufen am 1. 8 2018 von Colored Coins BitcoinX - Whitepaper: https://bravenewcoin.com/assets/Whitepapers/ColoredCoins-BitcoinX.pdf

Athanassiou, P. (2017). *Impact of digital innovation on the processing of electronic payments and contracting:*. Abgerufen am 23. 3 2018 von https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf

Bashir, I. (2017). *Mastering Blockchain.* Birmingham, B3 2PB, UK.: Packt Publishing.

bitcoinfee. (6. 8 2018). *Bitcoin Transaction Fees.* Abgerufen am 6. 8 2018 von Bitcoin Transaction Fees: https://bitcoinfees.info/

Bründlinger, R., & Bletterie, B. (2007). *Network of DER Laboratories and Pre-Standardisation* (49 Ausg.). 34119 Kassel/Germany: European Commission.

Burgwinkel Daniel, M. M. (2016). *Blockchain Technology, Einführung für Business- und IT Manager.* 4057 Basel: Burgwinkel Daniel.

Buterin, D. (2017). *https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.* Abgerufen am 11. 2 2018 von Proof of Work vs Proof of Stake: Basic Mining Guide: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Dannen, C. (2017). *Introducing Ethereum and Solidity.* Brooklyn, New York: Apress.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). *Blockchain enabled Applications; Understand the Blockchain Ecosystem and How to Make it Work for You.* Orlando, Florida, USA: Apress.

Dietrich, H. (2016). *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations* (1 Ausg.). CreateSpace Independent Publishing Platform.

Digiconomist. (3. 8 2018). *Bitcoin Energy Consumption Index*. Abgerufen am 3. 8 2018 von https://digiconomist.net/bitcoin-energy-consumption

Doleski, C. A. (2014). *Smart Market, Vom Smart Grid zum intelligenten Energiemarkt.* (C. A. Doleski, Hrsg.) Hochschule Kaiserslautern: Springer Vieweg.

Drescher, D. (2017). *Blockchain Basiscs: a non-technical introduction in 25 steps.* Frankfurt am Main, Germany: APRESS.

Drescher, D. (2017). *Hash Function*. Abgerufen am 11. 12 2017 von http://www.blockchain-basics.com/HashFunctions.html

ECB, E. C. (2012). VIRTUAL CURRENCY SCHEMES. In 2. European Central Bank, *VIRTUAL CURRENCY SCHEMES* (S. 55). European Central Bank.

Ethereum. (12. 9 2018). *Proof of Stake FAQ*. Abgerufen am 16. 9 2016 von Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs

Farell, R. (2015). *An Analysis of the Cryptocurrency Industry.* Pennsylvania: University of Pennsylvania. Abgerufen am 14. 6 2018 von http://repository.upenn.edu/wharton_research_scholars/130

Google, S. (2018). *IPv6 – Google*. Abgerufen am 01. 5 2018 von IPv6 – Google: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

Greenspan, G. (2015). *Gideon Greenspan | MultiChain.* Abgerufen am 29. 04 2018 von https://www.multichain.com/blog/author/gdg

Greenspan, G. (13. 6 2018). *Scaling blockchains with off-chain data*. Abgerufen am 5. 9 2018 von Scaling blockchains with off-chain data: https://www.multichain.com/blog/2018/06/scaling-blockchains-off-chain-data/

Groopman, J. (20. 11 2017). *The intersection of blockchain and IoT is all about trust*. Abgerufen am 7. 8 2018 von The intersection of blockchain and IoT is all about trust: https://www.experfy.com/blog/the-intersection-of-blockchain-and-iot-is-all-about-trust

Hofmann, E. (2018). *Supply Chain Finance and Blockchain Technology.* St. Gallen, Switzerland: SpringerBriefs in Finance.

Ibáñez, L.-D., & Kieron O'Hara, E. S. (2017). *On Blockchains and the General Data Protection Regulation.* University of Southampton.

Karame, G., & Androulaki, E. (2016). *Bitcoin and Blockchain Security.* Boston, London: ARTECH HOUSE.

Komarnicki, P., Lombardi, P., & Styczynski, Z. (2017). *Electric Energy Storage Systems.* Magdeburg: Springer.

Kumar, S. N. (2015). *Review on Network Security and Cryptography*. Abgerufen am 1. 10 2017 von Science and Education Publishing: http://pubs.sciepub.com/iteces/3/1/1/index.html#Figure7

Larry E. Erickson, J. R. (2017). *Solar Powered Charging Infrastructure for Electric Vehicles A Sustainable Development.* 6000 Broken Sound Parkway NW: CRC Press.

Laurence, T. (2017). *Blockchain.* 111 River Street, Hoboken, NJ 07030-5774: John Wiley & Sons, Inc.

Loo, A. W.-S. (2007). *Peer-to-Peer Computing.* Lingnan University, Hong Kong: Springer.

Lyons, T. (2018). *Blockchain Innovation inEurope.* European Commission: the european union blockchain observatory & forum.

Morabito, V. (2017). *Business Innovation Through Blockchain.* Bocconi University: Springer.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Abgerufen am 2. 5 2017 von https://bitcoin.org/bitcoin.pdf

O’Dwyer, K. J., & Malone, D. (2014). Bitcoin Mining and its Energy Footprint. *ISSC 2014 / CIICT 2014, Limerick, June 26–27* (S. 6). National University of Ireland Maynooth: Hamilton Institute.

Office for Science, G. U. (2016). *Distributed Ledger Technology: beyond block chain.* London SW1H 0ET: Open Government Licence (c) Crown.

Österreich, R. (17. 7 2018). *HELP.gv.at: Grundbuch – Allgemeines*. Abgerufen am 17. 7 2017 von HELP.gv.at: Grundbuch – Allgemeines: https://www.help.gv.at/Portal.Node/hlpd/public/content/60/Seite.600500.html

Paar, J., & Pelzl, C. (2010). Understanding Cryptography. In D.-I. J. Prof. Dr.-Ing. Christof Paar, *Understanding Cryptography - A Textbook for Students and Practitioners* (S. 293-317). 44780 Bochum, Germany: Springer.

Poon, J., & Dryja, T. (2015). *The Bitcoin Lightning Network: Scalable O.*

PricewaterhouseCoopers, P. (22. 02 2016). *Making sense of bitcoin and blockchain: PwC*. Abgerufen am 3. 5 2018 von Making sense of bitcoin and blockchain: PwC: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

Prusty, N. (2017). *Building Blockchain Projects.* BIRMINGHAM - MUMBAI: Packt Publishing.

Przemyslaw Komarnicki, P. L. (2017). *Electric Energy Storage Systems.* Magdeburg: Springer.

René Wintjes, G. A. (2016). *Business Innovation Observatory, Trend report, Optimal recycling, big data from space, and blockchain applications: disruption and policy response.* European Union.

Richter, F. (3. 12 2013). *Chart: How Bitcoin Activity Stacks Up Against Other Payment Networks | Statista*. Abgerufen am 12. 12 2017 von Chart: How Bitcoin Activity Stacks Up Against Other Payment Networks | Statista: https://www.statista.com/chart/1681/daily-transaction-volume-of-payment-networks/

Rosenfeld, M. (2012). *Overview of Colored Coins.* WhitePaper.

Rossi, S. (2007). *Money and Payments in Theory and Practice.* New York, NY 10016: Routledge.

Scherer, M. (2017). *Performance and Scalability of Blockchain Networks and Smart Contracts.* Umea University.

Schmeh, K. (2013). *Kryptografie: Verfahren, Protokolle, Infrastrukturen.* 69115 Heidelberg: dpunkt.verlag.

Schmidt, J. (2005). *Kryptoverfahren SHA-1 geknackt | heise online*. Abgerufen am 15. 2 2018 von Kryptoverfahren SHA-1 geknackt | heise online: https://www.heise.de/newsticker/meldung/Kryptoverfahren-SHA-1-geknackt-135372.html

Settlements, B. f. (2001). *Core Principles for Systemeatically Important Payment Systems.* Basel: Bank for International Settlements.

Settlements, B. f. (2003). *Payment system in the euro area.* BIS.

Settlements, B. f. (2012). *Principles for financial market infrastructures.* bis.org.

Settlements, B. f. (2017). *Distributed ledger technology in payment, clearing and settlement.* Bank for International Settlements.

Sietas, H. (18. 09 2018). *LEMnet - Map.* Abgerufen am 18. 09 2018 von LEMnet - Map: https://www.lemnet.org/en/map/?destination=austria

Sixt, E. (2017). *Bitcoins und andere dezentrale Transaktionssysteme.* Wien, Österreich: Springer Gabler ist Teil von Springer Nature.

Spinellis, S. A.-T. (2004). A Survey of Content Distribution Technologies. In S. A.-T. Spinellis, *A Survey of Content Distribution Technologies.* ACM Computing Surveys, 36(4).

Sumedha Rajakaruna, F. S. (2015). *Plug In Electric Vehicles in Smart Grids.* Perth, WA, Australia, Australia: Springer Science+Business Media.

Tapscott, D. &. (2018). *What is Blockchain Technology?* Abgerufen am 9. 7 2018 von What is Blockchain Technology?: https://blockgeeks.com/guides/what-is-blockchain-technology/

Taylor, I. J. (2005). *Computer communications and networks, From P2P to Web Services and Grids.* London: Springer Verlag.

tesla. (2018). *Supercharging | Tesla*. Abgerufen am 11. 05 2018 von Supercharging | Tesla: https://www.tesla.com/supercharger

Vasa. (2. 07 2018). *ConsensusPedia: An Encyclopedia of 30 Consensus Algorithms*. Abgerufen am 2. 8 2018 von ConsensusPedia: An Encyclopedia of 30 Consensus Algorithms: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f

Veneri, O. (2017). *Technologies and Applications for Smart Charging of Electric and Plug-in Hybrid Vehicles.* Naples, Italy: Springer.

Walport, S. M. (2016). *Distributed Ledger Technology: beyond block chain* (GS/16/1 Ausg.). London SW1H 0ET, UK: Government Office for Science.

Wikipedia. (2018). *Micropayment - Wikipedia*. Abgerufen am 1. 5 2018 von Micropayment - Wikipedia: https://en.wikipedia.org/wiki/Micropayment

Wikipedia. (01. 08 2018). *Wikileaks - Wikipedia*. Abgerufen am 1. 8 2018 von https://en.wikipedia.org/wiki/WikiLeaks

Wikipedia, F. (01. 07 2018). *Blockchain, Bitcoin Network*. Abgerufen am 1. 7 2017 von Blockchain, Bitcoin Network: https://en.wikipedia.org/wiki/Blockchain

Wyman, O. (2016). *Blockchain in Capital Markets: The Prize and the Journey.* Euroclear.

7. Abbreviations:

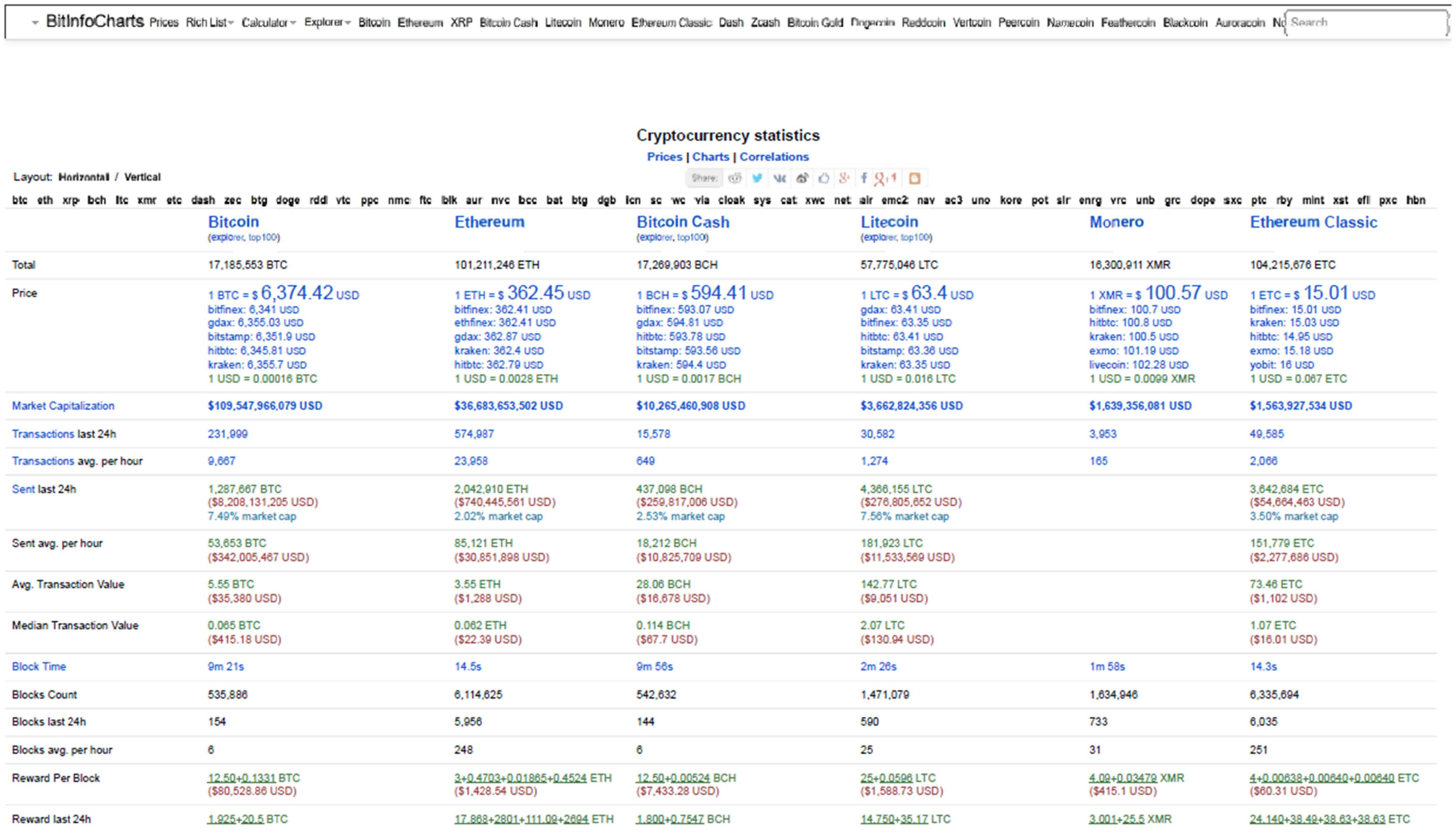
3G	3G, is the third generation of wireless mobile telecommunications technology.
4G	4G is the fourth generation of broadband cellular network technology, Long-Term Evolution
AC	Alternating current
AML	anti-money laundering
ASIC	Application-specific integrated circuit
ATM	Automated teller machine
BC	Before Christ
BTC	Bitcoin
CBS	Core Banking System
CD	Compact Disk
CIICT	China-Ireland International Conference on Information and Communications Technologies
CO2	Carbon dioxide
CPU	Central Processing Unit
CUBER	Cuber Technology is based in Estonia. The fintech company is a subsidiary of LHV Group and is the developer of Cuber Wallet.
DAO	Decentralized autonomous organization
DC	Direct current
DLT	Distributed ledger
ECB	European Central Bank
ECU	Electronic control unit
eHZ	Electric Energy Meter
EOA	External Operated Account
EU	European Union
EV	Electric Vehicle
EVCC	electric vehicle communication controller
FPGA	Field Programmable Gate Arrays
GAS	Gas is the execution fee for every operation made on ethereum
GB	Giga Byte
GDPR	General Data Protection Regulation
GH	Giga Hash
GH/s	Giga Hash per Second
GSM	Global System for Mobile communication
HMI	Host Micro Interface
HTLC	Hash Time Lock Contract
HW	Hardware
IEC	international Electro technical Commission
IP	Internet Protocol
Ipv6	Internet Protocol Version 6
ISO	International Organization for Standardization
ISSC	Irish Signals & Systems Conference

IT	Information Technology
KBS	Core Banking System / Kernbanksystem
KYB	Know Your Business
KYC	Know Your Customer
LHV Pank	LHV Pank is an Estonian banking and financial services company headquartered in Tallinn.
MB	Mega Byte
MWh	Megawatt hour
NG	Next Generation
NSA	National Security Agency
P2P	Peer to Peer
PKI	Public Key Infrastructure
PLC	Power-line communication
SECC	Supply Equipment Communication Controller
SHA	Secure Hash Algorithms
SSL	Secure Sockets Layer
SW	Software
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPS	Transactions per Seconds
UBO	Ultimate Beneficial Owner
UDP	User Datagram Protocol
UID	User Identifier
UK	United Kingdom
URL	Uniform Resource Locator
US	United States
VAT	Value added tax
VISA	multinational financial services

8. List of Figures

9. List of Diagrams

Appendix A: Bitcoin, Namecoin, Dogecoin, Peercoin, Ethereum stats (https://bitinfocharts.com/)



BitInfoCharts Prices Rich List Calculator Explorer Bitcoin Ethereum XRP Bitcoin Cash Litecoin Monero Ethereum Classic Dash Zcash Bitcoin Gold Dogecoin Reddcoin Vertcoin Peercoin Namecoin Feathercoin Blackcoin Auroracoin N Search
Share:
btc eth xrp bch ltc xmr etc dash zec btg doge rdd vtc ppc nmc ftc blk aur nvc bcc bat btg dgb icn sc wc via cloak sys cat xwc net air emc2 nav ac3 uno kore pot slr enrg vrc unb grc dope sxc ptc rby mint xst efl pxc hbn

Cryptocurrency statistics

Prices | Charts | Correlations

Layout: Horizontal / Vertical

	Bitcoin (explorer, top100)	Ethereum	Bitcoin Cash (explorer, top100)	Litecoin (explorer, top100)	Monero	Ethereum Classic
Total	17,185,553 BTC	101,211,246 ETH	17,269,903 BCH	57,775,046 LTC	16,300,911 XMR	104,215,676 ETC
Price	1 BTC = $ 6,374.42 USD bitfinex: 6,341 USD gdax: 6,355.03 USD bitstamp: 6,351.9 USD hitbtc: 6,345.81 USD kraken: 6,355.7 USD 1 USD = 0.00016 BTC	1 ETH = $ 362.45 USD bitfinex: 362.41 USD ethfinex: 362.41 USD gdax: 362.87 USD kraken: 362.4 USD hitbtc: 362.79 USD 1 USD = 0.0028 ETH	1 BCH = $ 594.41 USD bitfinex: 593.07 USD gdax: 594.81 USD hitbtc: 593.78 USD bitstamp: 593.56 USD kraken: 594.4 USD 1 USD = 0.0017 BCH	1 LTC = $ 63.4 USD gdax: 63.41 USD bitfinex: 63.35 USD hitbtc: 63.41 USD bitstamp: 63.36 USD kraken: 63.35 USD 1 USD = 0.016 LTC	1 XMR = $ 100.57 USD bitfinex: 100.7 USD hitbtc: 100.8 USD kraken: 100.5 USD exmo: 101.19 USD livecoin: 102.28 USD 1 USD = 0.0099 XMR	1 ETC = $ 15.01 USD bitfinex: 15.01 USD kraken: 15.03 USD hitbtc: 14.95 USD exmo: 15.18 USD yobit: 16 USD 1 USD = 0.067 ETC
Market Capitalization	$109,547,966,079 USD	$36,683,653,502 USD	$10,265,460,908 USD	$3,662,824,356 USD	$1,639,356,081 USD	$1,563,927,534 USD
Transactions last 24h	231,999	574,987	15,578	30,582	3,953	49,585
Transactions avg. per hour	9,667	23,958	649	1,274	165	2,066
Sent last 24h	1,287,667 BTC ($8,208,131,205 USD) 7.49% market cap	2,042,910 ETH ($740,445,561 USD) 2.02% market cap	437,098 BCH ($259,817,006 USD) 2.53% market cap	4,366,155 LTC ($276,805,652 USD) 7.56% market cap		3,642,684 ETC ($54,664,463 USD) 3.50% market cap
Sent avg. per hour	53,653 BTC ($342,005,467 USD)	85,121 ETH ($30,851,898 USD)	18,212 BCH ($10,825,709 USD)	181,923 LTC ($11,533,569 USD)		151,779 ETC ($2,277,686 USD)
Avg. Transaction Value	5.55 BTC ($35,380 USD)	3.55 ETH ($1,288 USD)	28.06 BCH ($16,678 USD)	142.77 LTC ($9,051 USD)		73.46 ETC ($1,102 USD)
Median Transaction Value	0.065 BTC ($415.18 USD)	0.062 ETH ($22.39 USD)	0.114 BCH ($67.7 USD)	2.07 LTC ($130.94 USD)		1.07 ETC ($16.01 USD)
Block Time	9m 21s	14.5s	9m 56s	2m 26s	1m 58s	14.3s
Blocks Count	535,886	6,114,625	542,632	1,471,079	1,634,946	6,335,694
Blocks last 24h	154	5,956	144	590	733	6,035
Blocks avg. per hour	6	248	6	25	31	251
Reward Per Block	12.50+0.1331 BTC ($80,528.86 USD)	3+0.4703+0.01865+0.4524 ETH ($1,428.54 USD)	12.50+0.00524 BCH ($7,433.28 USD)	25+0.0596 LTC ($1,588.73 USD)	4.09+0.03479 XMR ($415.1 USD)	4+0.00638+0.00640+0.00640 ETC ($60.31 USD)
Reward last 24h	1,925+20.5 BTC	17,868+2801+111.09+2694 ETH	1,800+0.7547 BCH	14,750+35.17 LTC	3,001+25.5 XMR	24,140+38.49+38.63+38.63 ETC

	($12,401,444.82 USD)	($8,508,378.04 USD)	($1,070,392.63 USD)	($937,350.44 USD)	($304,417.11 USD)	($363,997.21 USD)
Difficulty	5,949,437,371,610	3.608 P +1.17% in 24 hours	548,889,195,596 -5.94% in 24 hours	9,217,686	55.229 G +4.98% in 24 hours	208.603 T -7.1% in 24 hours
Hashrate	47.049 Ehash/s +12.21% in 24 hours	298.141 Thash/s +2.12% in 24 hours	3.78 Ehash/s -6.95% in 24 hours	263.852 Thash/s -8.37% in 24 hours	468.555 Mhash/s +5.7% in 24 hours	15.317 Thash/s -6.96% in 24 hours
Mining Profitability	0.2636 USD/Day for 1 THash/s	0.0285 USD/Day for 1 MHash/s	0.2832 USD/Day for 1 THash/s	3.5526 USD/Day for 1 GHash/s	0.6497 USD/Day for 1 KHash/s	0.0238 USD/Day for 1 MHash/s
Top 100 Richest	3,277,903 BTC ($20,894,734,885 USD) 19.07% Total		4,168,249 BCH ($2,477,662,658 USD) 24.14% Total	25,558,702 LTC ($1,620,371,468 USD) 44.24% Total		
Wealth Distribution Top 10/100/1,000/10,000 addesses	6.09% / 19.07% / 35.48% / 56.44% Total		7.43% / 24.14% / 44.68% / 66.57% Total	13.81% / 44.24% / 62.53% / 77.50% Total		
Addresses richer than 1/100/1,000/10,000 USD	15,268,671 / 4,951,128 / 1,914,037 / 469,443		5,637,635 / 1,180,278 / 315,107 / 92,552	1,479,597 / 619,346 / 180,956 / 22,064		
Active Addresses last 24h	547,671	358,731	32,897	74,429		31,539
100 Largest Transactions	last 24h: 231,385 BTC ($1,474,947,072 USD) 17.97% Total	last 24h: 512,536 ETH ($185,766,856 USD) 25.09% Total	last 24h: 266,789 BCH ($158,583,047 USD) 61.04% Total	last 24h: 2,007,915 LTC ($127,297,835 USD) 45.99% Total		last 24h: 1,680,773 ETC ($25,222,769 USD) 46.14% Total
First Block	2009-01-09	2015-07-30	2009-01-09	2011-10-08	2014-04-18	2015-07-30
Blockchain Size	209.21 GB	667.10 GB	161.24 GB	18.38 GB	57.21 GB	86.37 GB
Reddit subscribers	909,516	374,557	35,765	198,973	135,992	21,919
Tweets per day	36,169	11,572	1,102	2,174	594	642
Github release	v0.16.2 (2018-07-26)	v1.8.13 (2018-07-31)	v0.17.2 (2018-05-30)	v0.16.2rc1 (2018-07-24)	v0.12.3.0 (2018-07-10)	v5.5.1 (2018-08-02)
Github stars	33834	19844	660	3117	3165	368
Github last commit	2018-08-08	2018-08-08	2018-05-31	2018-06-17	2018-07-27	2018-07-26
	Bitcoin	Ethereum	Bitcoin Cash	Litecoin	Monero	Ethereum Classic

2018-08-09 07:23:17

Light / Dark | Advertising | Privacy Policy / Disclaimer | Contact: bitinfocharts@gmail.com

Appendix B: Whitepaper Bitcoin from Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

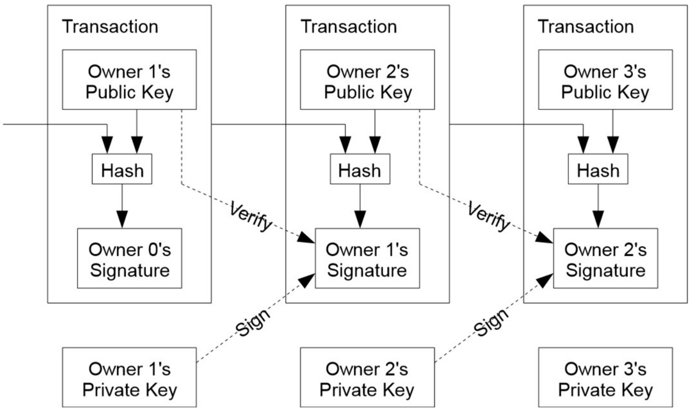
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

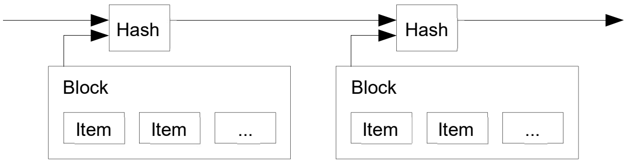


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

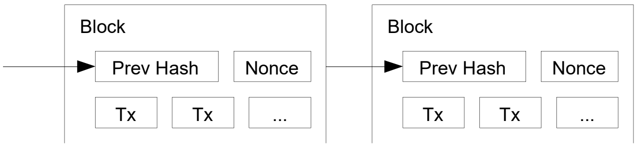
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proofof-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proofof-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

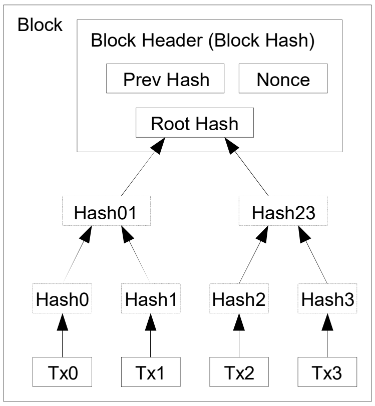
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

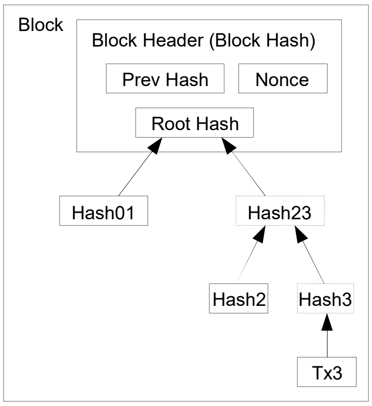
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Transactions Hashed in a Merkle Tree

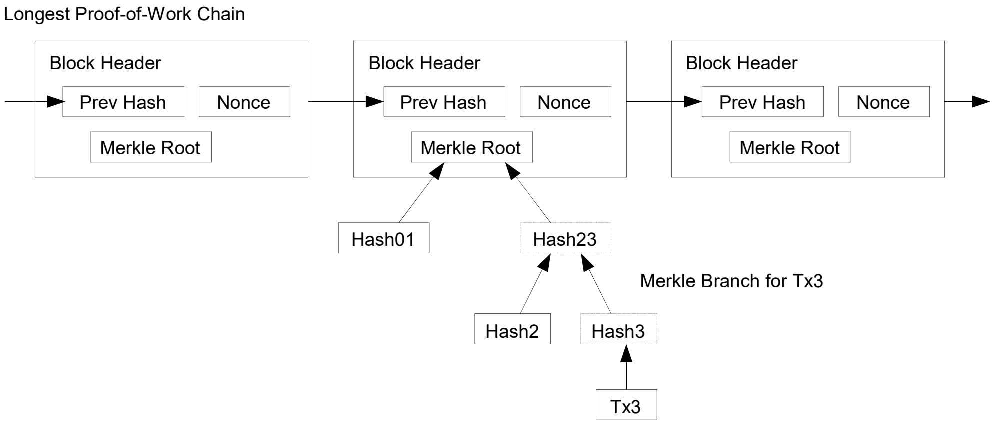


After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

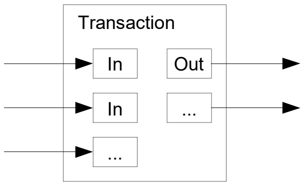
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

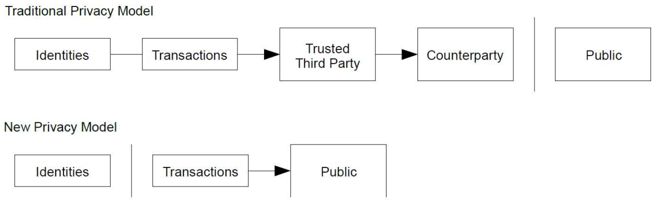
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{Bmatrix} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{Bmatrix}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

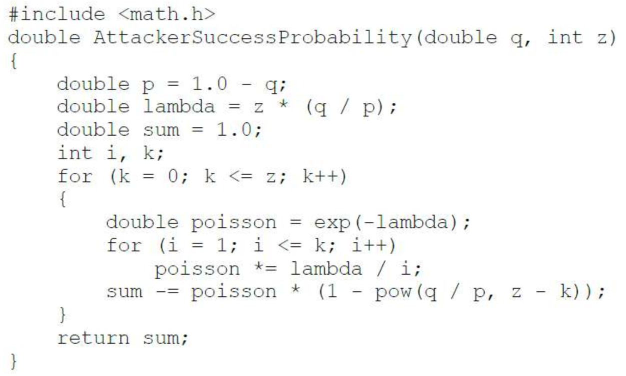
To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{Bmatrix} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{Bmatrix}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

Converting to C code...



```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1 z=0
P=1.0000000 z=1
P=0.2045873 z=2
P=0.0509779 z=3
P=0.0131722 z=4
P=0.0034552 z=5
P=0.0009137 z=6
P=0.0002428 z=7
P=0.0000647 z=8
P=0.0000173 z=9
P=0.0000046 z=10
P=0.0000012

q=0.3 z=0
P=1.0000000 z=5
P=0.1773523 z=10
P=0.0416605 z=15
P=0.0101008 z=20
P=0.0024804 z=25
P=0.0006132 z=30
P=0.0001522 z=35
P=0.0000379 z=40
P=0.0000095 z=45
P=0.0000024 z=50
P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001 q=0.10
z=5 q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

13. References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Appendix C: “A Cypherpunk's Manifesto” by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward. Eric Hughes <hughes@soda.berkeley.edu>

9 March 1993