Blockchain: Hype or Innovation

Christoph Meinel, Tatiana Gayvoronskaya,
Maxim Schnjakin

Technische Berichte Nr. 124

des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam | 124

Christoph Meinel | Tatiana Gayvoronskaya | Maxim Schnjakin

Blockchain

Hype or Innovation

Universitätsverlag Potsdam

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de/ abrufbar.

Universitätsverlag Potsdam 2018
http://verlag.ub.uni-potsdam.de/

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 2533 / Fax: 2292
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam.

ISSN (print) 1613-5652
ISSN (online) 2191-1665

Druck: docupoint GmbH Magdeburg

Translated by Dr. Sharon Therese Nemeth from the German language edition:
Blockchain: Hype oder Innovation. Technischer Bericht Nr. 113, ISBN 978-3-86956-394-7

ISBN 978-3-86956-441-8

Zugleich online veröffentlicht auf dem Publikationsserver der Universität Potsdam:
URN urn:nbn:de:kobv:517-opus4-414525
http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-414525

The term blockchain has recently become a buzzword, but only few know exactly what lies behind this approach. Many see blockchain technology either as an all-purpose weapon – which only a few have access to – or as a hacker technology for secret deals in the darknet. The innovation of blockchain technology is found in its successful combination of already existing approaches: such as decentralized networks, cryptography, and consensus models. This innovative concept makes it possible to exchange values in a decentralized system. At the same time, there is no requirement for trust between its nodes (e.g. users).

With this study, the Hasso Plattner Institute would like to help readers form their own opinion about blockchain technology and distinguish between truly innovative properties and hype.

The authors of the present study analyze the positive and negative properties of the blockchain architecture and suggest possible solutions that can contribute to an efficient use of this technology. We recommend that every company define a clear target for the intended application, which is achievable with a reasonable cost-benefit ratio, before deciding on this technology. Both the possibilities and limitations of blockchain technology need to be considered. The relevant steps that must be taken in this respect are summarized for the reader in this study.

Furthermore, this study elaborates on urgent problems such as the scalability of the blockchain, appropriate consensus algorithm and security, including various types of possible attacks and their countermeasures. New blockchains, for example, run the risk of reducing security as changes to existing technology can lead to holes in security and failures.

After discussing the innovative properties and problems of the blockchain technology, its implementation is discussed. There are a lot of implementation opportunities for companies available who are interested in realizing blockchain in their own enterprise. The numerous applications are either based on a company's own blockchain or their use of an already existing and widespread blockchain systems. Various consortia and projects offer "blockchain-as-a-service" and help other companies to develop, test and deploy their own applications.

This study provides a detailed overview of diverse relevant applications and projects in the field of blockchain technology. As this technology is still a relatively young and fast-developing approach, it lacks uniform standards to allow the co-operation of different systems and to which all developers can adhere. Currently, developers are orienting themselves to Bitcoin, Ethereum and Hyperledger systems, which serve as the basis for many other blockchain applications.

The goal is to give readers a clear and comprehensive overview of blockchain technology and its capabilities. The authors are very thankful to ***Dr. Sharon Therese Nemeth*** for the translation of this technical report from the German language edition.

Contents

List of Figures

1 Introduction

The term "blockchain" keeps making headlines. More and more articles, as well as reports and studies, attempt to explain to the public at large the "phenomenon" of the blockchain. An effort is being made to clarify the technology, the first blockchain project "bitcoin", and the new areas of application. But in spite of all these explanations, many are still in the dark about the new technical expressions and functionalities. The polarized headlines often put readers in the position of taking a stand for or again blockchain technology instead of helping them develop their own point of view.

Is blockchain technology really a cure-all or just a new, unnecessarily complicated fantasy of computer scientists that the media has made their latest hype?

With this study we hope to help readers form their own opinion about the blockchain, and in doing so acquire the ability to differentiate between innovation and hype.

1.1 So, What is Blockchain Anyway?

The history of blockchain technology is still young. It originated from a desire to revolutionize the financial sector and develop a third-party independent digital payment system.

For many, the first thing that comes to mind at the mention of a digital payment system is classic online banking – transactions no longer carried out at the local bank branch but instead at home or via a mobile device. Whether facilitated by a bank teller or online, an account transfer can take several days to complete, as in both cases it is ultimately the bank itself that processes the transaction.

But what if a transaction could be carried out between bank customers directly without a central instance, such as a bank, involved in the process? It was this idea that inspired Bitcoin "founder" Satoshi Nakamoto in 2008, when he first outlined his concept for a cryptocurrency called bitcoin; that is, a digital currency with a decentralized and cryptographic secure payment system [3].

The omission of a central instance in financial transactions saves a great deal of time and money. It was, however, initially very difficult to imagine how such a system could function independently without an administrator keeping an eye on things and intervening if problems or errors should occur. At the beginning it seemed like a utopia: a payment system that administered itself, in which all users have the same rights and where transferring money is not dependent on trust in third party or between users. The underlying blockchain technology would take care of it all.

The idea of a secure, decentralized payment system made up of a network of interacting users (in technical terms called "nodes"), without a central adminis-

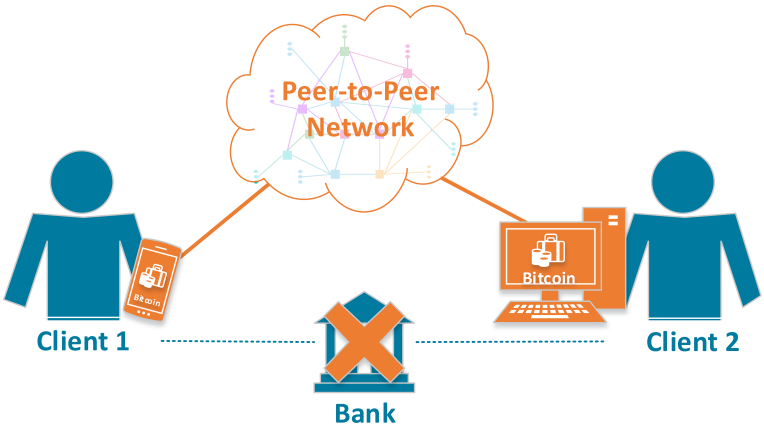


Figure 1.1: Bitcoin principle

trative instance, already existed before bitcoin. However, previous attempts failed to withstand the test of time due to either errors in conception or problems with security ("double spending problem", see section 2.4.3).

Blockchain is thus a new and successful combination of already known technologies.

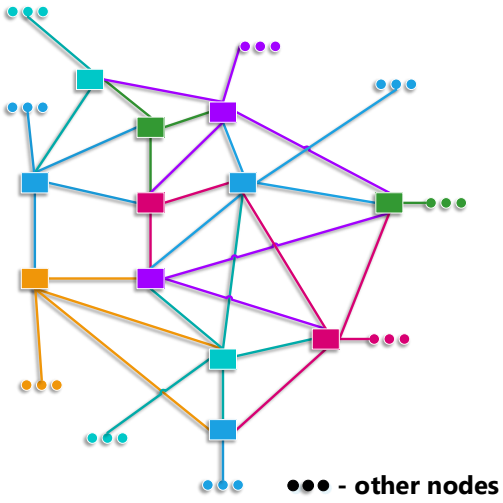


Figure 1.2: A decentralized network (peer-to-peer network)

The terms "blockchain" and "bitcoin" are often used as synonyms. However, blockchain is a technology and bitcoin is a system that uses the technology for the digital payment processing. The entire source code of the bitcoin system is publicly available (open source) and all users may use the code for their own blockchain applications. The digital currency of the bitcoin system is likewise called bitcoin

(BTC[1]). It is protected by a cryptographic proof and is thus called a cryptocurrency (see section 2.2.1). Blockchain is understood as a list of all transactions that have ever been carried out in the respective system (e.g. bitcoin) and which, in turn, are divided into blocks (e.g., in bitcoin there are between 900 and 2500 transactions per block). The blocks form a chain (blockchain), so that each one of the blocks that follow carries a cryptographic reference to the previous block. In transactions, assigned values from one address (comparable to a bank account number) are transmitted to another. In the bitcoin system, for example, the values are the bitcoins that are transmitted in each transaction. Besides cryptocurrency, the values can represent property (e.g., a rented apartment that changes its tenant) or a certain event (e.g. the right to unlock an office door), which are then registered in the blockchain "land registry". For this reason, the blockchain technology is also called the "Internet of Value" (see figure 1.3).

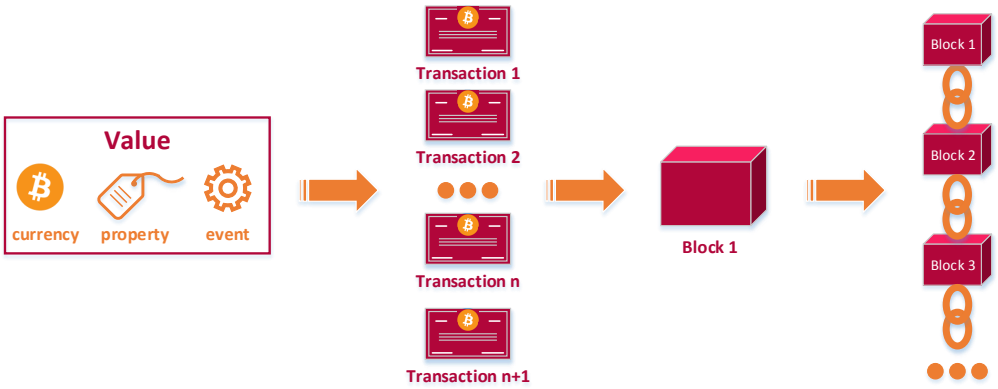


Figure 1.3: Blockchain technology as an "Internet of Value"

The blockchain is not stored centrally at a server where it is managed and subsequently distributed to all users. Instead, every "full node"[2] saves and manages the blockchain according to a system's fixed rules.

Transactions are carried out between individual participants, and without the intervention of third parties (e.g. banks), in such a way that once they have already been executed they cannot be revoked.

[1] BTC is the designation of the bitcoin currency. Bitcoin has several decimal metric units, e.g. 0.1 BTC is a deci-bitcoin (dBTC), 0.01 BTC is a centi-bitcoin (cBTC), 0.001 BTC is a milli-bitcoin (mBTC), 0.000001 BTC is a micro-bitcoin (µBTC) and 0.00000001 BTC is the smallest unit and is called Satoshi.

[2] A user who locally stores the complete blockchain (all block contents) with all transactions and is involved in the complete verification of all transactions and blocks based on the system's fixed set of rules.

1.2 Bitcoin Was Only the Beginning

Bitcoin was born in 2008. It was in November of that year when Satoshi Nakamoto published a white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System". As early as January 2009 the first version of the open source software was released.

> „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. [131]"

As the name "Satoshi Nakamoto" was completely unknown, many assumed it to be a pseudonym, behind which a group of developers was hiding.

To be able to manage bitcoins (save, transfer and receive) the user needs a bitcoin wallet, which takes the form of mobile, desktop and web applications. At the same time, physical bitcoin wallets are also available as hardware and paper wallets[3] (Figure 1.4).

Figure 1.4: Hardware and paper wallets [19, 23, 32]

Like every other currency, bitcoins can be bought at numerous Internet platforms for a fee and also exchanged, for instance at CoinBase, BitPay or Anycoin Direct. Because the demand for bitcoins fluctuates strongly, the price is also subject to considerable change. For example, in the past, within the course of a week the price changed by 25 percent. The bitcoin exchange rate is continually setting new records. In August 2017, a bitcoin (BTC) cost 3,588.94 euros and in December of the same year the bitcoin exchange rate exceeded the 10,000 euro threshold.

The bitcoin system ensures a constant flow of new bitcoins. This process is called mining (a detailed description can be found in section 2.2.3). In 2013 there were

[3] More on the topic of the hardware wallet in section 2.4.6.

eight million bitcoins in circulation. The upper limit of 1.2 million bitcoins, set by Satoshi Nakamoto in the bitcoin architecture, will be reached by 99 percent in 2023 [54]. Due to a defined upper limit of existing bitcoins it is not possible for a situation of endless inflation to occur [12].

The bitcoin currency is already accepted by many companies – ranging from IT service providers to food service businesses – as a means of payment (see figure 1.5).

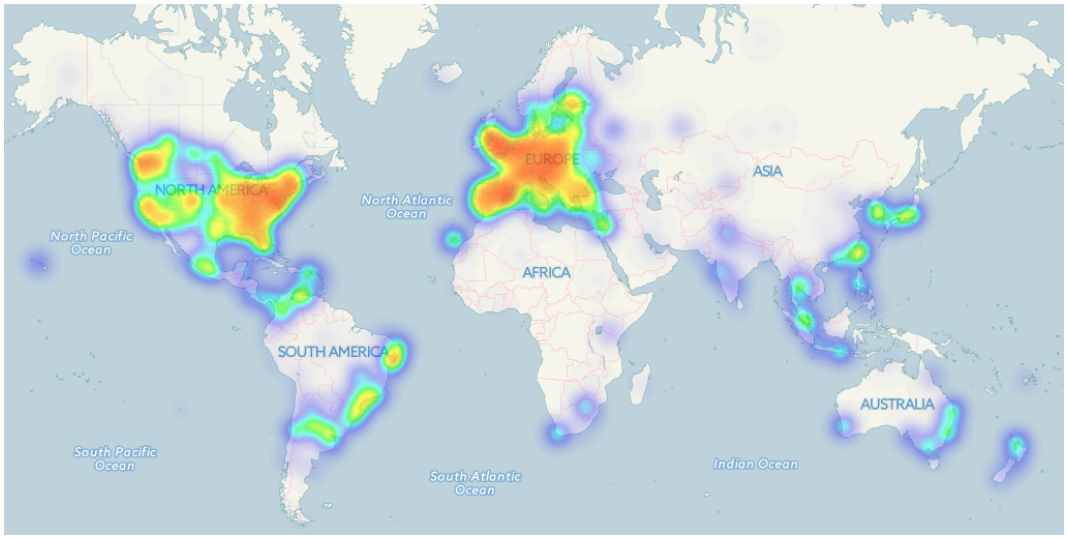


Figure 1.5: Spread of bitcoin currency worldwide (coinmap.org)

The first application launch of blockchain technology (bitcoin and other cryptocurrency systems) was in the finance sector. In the meantime, numerous projects have emerged, based on blockchain technology and a variety of services and products. Science, medicine, identity management, cloud computing, the Internet of Things, as well as many more areas all profit from it.

2 Where Does the Hype End and the Innovation of the Blockchain Technology Begin?

Although blockchain technology is still relatively young, it has already become a widespread topic of interest. The first implementation of the technology – the bitcoin project, and its rapid proliferation into many different branches – led to the blockchain hype. Media reporting has focused on new, incredible value increases, dramatic downturns or speculated about a bitcoin crash.

The consulting firm Gartner Inc.[4] pointed out the strong impact blockchain technology would have on the economy. In its "Hype Cycle for Emerging Technologies 2016"[5] the Gartner research team placed blockchain technology immediately before the "peak of inflated expectations" (see figure 2.1). At this stage, mass media devotes much attention to the technology and expresses many, though not always realistic, expectations. The result has been more and more companies attempting to use the technology for themselves.

After the initial interest of the media faded – likely due to the fact that the technology still finds itself in its infancy, regarding elaborated cross-technology standards, uniform interfaces and proven cases of application – the blockchain technology, according to Gartner's "Hype Cycle for Emerging Technologies 2017", experienced a descent into a "trough of disillusionment" (see figure 2.2).

Specific standards and uniform interfaces will likely be set after the new technology overcomes its expected decline and the unfulfilled expectations and negative reports that accompany it. This will lead to the next phase, the so-called "slope of enlightenment", from which the "plateau of productivity" will then be reached. Realized in this phase will also be a greater application on the market. As long as blockchain technology lacks mature and uniform standards, it will hang in the balance between the hype of unrealistic expectations and its place as an innovation whose solutions are still marked by random difficulties.

We would like to devote this entire chapter to helping readers in distinguishing between exaggerated expectations (hype) and the innovation of the features of blockchain technology.

[4] Gartner Inc. is a leading US consulting firm that focuses on market research and analysis in the IT sector.

[5] Gartner's "Hype Cycle for Emerging Technologies" serves as a guide for businesses in the field of new technologies, thereby providing assistance in distinguishing between hype and economically viable technology in the form of five phases.

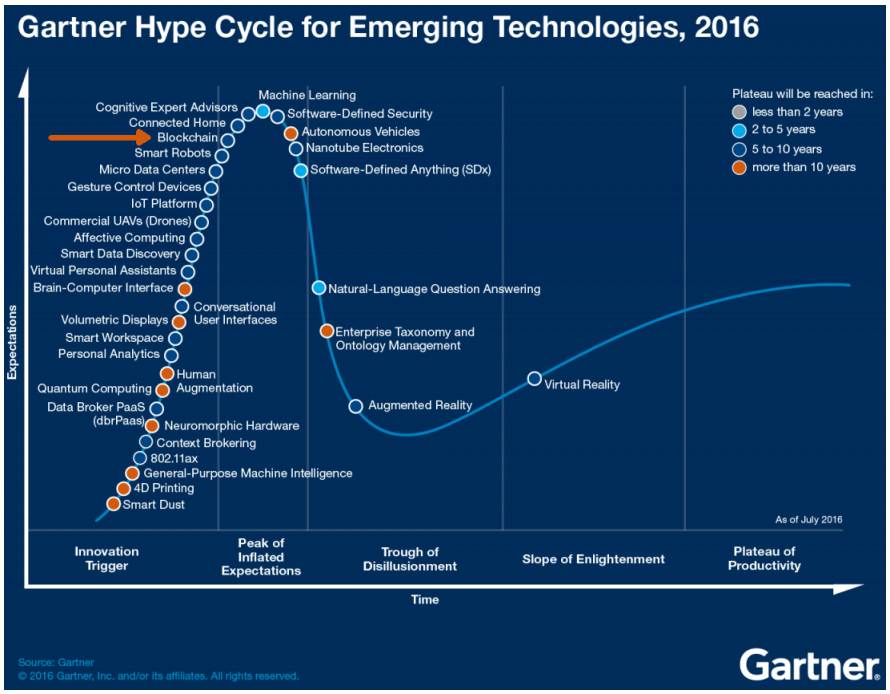


Figure 2.1: Hype Cycle for Emerging Technologies 2016 – Gartner Inc.

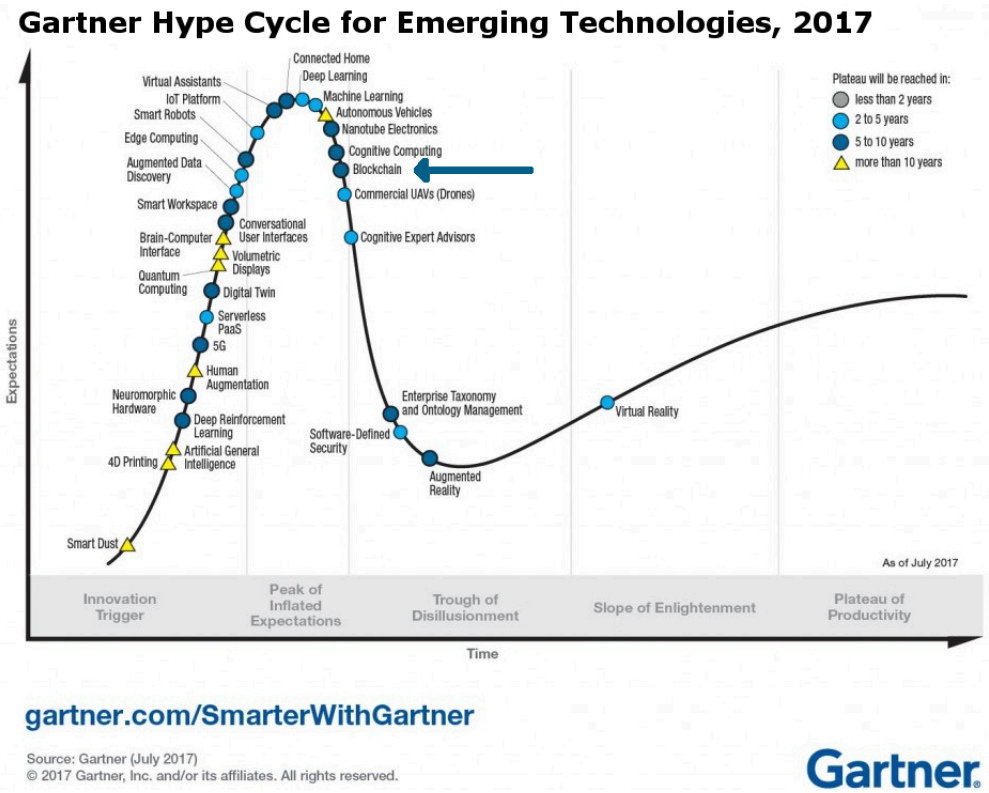


Figure 2.2: Hype Cycle for Emerging Technologies 2017 – Gartner Inc.

2.1 The Possibility of Partial Anonymity – In Spite of Transparency

Most people are very sensitive when it comes to personal matters concerning money. Hardly anyone likes to talk about their money in public, much less disclose private assets. For this reason, we entrust a third party, such as a financial service provider, with our savings. The party promises to adhere to strict standards of confidentiality in handling our assets.

In contrast, blockchain technology operates with transparency[6] regarding all transaction contents. Every user can see all of the transactions that have ever been carried out in the blockchain system. In the system of bitcoin this means, for example, that the information about who received bitcoins from whom, when the transaction took place and how much was received is accessible to the public. The "account balance" and all transactions of an address[7] are also transparent [59].

To disguise the identity of the user, many blockchain applications, including bitcoin, use pseudonyms (anonymous user addresses) that are difficult for the end user to trace (see section 2.1.2 and 2.4). Besides these pseudonyms, other possibilities for concealment are used, for example for bitcoin systems:

- Use of the anonymous network TOR for obfuscation of IP addresses,
- Anonymous mixing services (also called "tamblers") intended to conceal the transaction receiver. Whereby, the bitcoins to be transferred are split into several parts and sent to several of the addresses proposed by the mixing service provider. Subsequently, the same number of new bitcoins from these addresses are sent to the final receiver. This service naturally assumes the trust of the user, and it is not legal in every country.

Cryptography plays a leading and decisive role in blockchain technology. With the help of cryptography the described pseudonyms, transactions and blocks are generated.

Therefore, we will briefly look at the basics of the cryptographic methods used in blockchain technology.

2.1.1 Cryptography

The term "cryptography" comes from an ancient Greek word meaning "writing secretly". It describes an area of science that deals with safeguarding messages (encryption, decryption, etc.) [122]. In the course of the long history[8] of cryptography, several methods have established themselves. These include the public-key method, which is among those methods used in blockchain technology.

The basic idea of the public-key cryptography is that all participants of an encrypted communication have a pair of different keys (a secret key – called a private

[6] This applies to the public blockchain and the consortium blockchain (see chapter 3.1).
[7] Comparable to a bank account number, more in section 2.1.2.
[8] Cryptography was already used in ancient Egypt some 3000 years ago [8].

key – and a public key) instead of having a shared secret key for decrypting the received message. The public key is made freely available to all communication partners. The private key should remain secret and is used for signing and decrypting the messages. Let us consider an example with two interaction partners called Alice and Bob. Alice wants to send a message to Bob. Alice encrypts the message with the public key from Bob before she sends it. Only Bob is able to decrypt the message with his private key (see figure 2.3). [118]

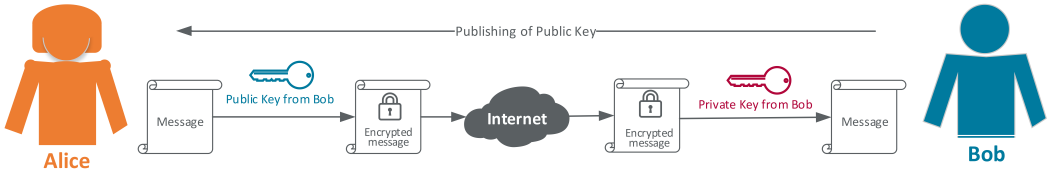


Figure 2.3: Public-key cryptography

A digital signature is a number of bits or a sequence of bits calculated from a message using public-key cryptography procedure and whose authorship and affiliation with the message can be checked by anyone [119]. By signing the message, Alice confirms that the message is actually from her (to do this she uses her private key). Bob can check this through verification (using the public key from Alice, see figure 2.4).

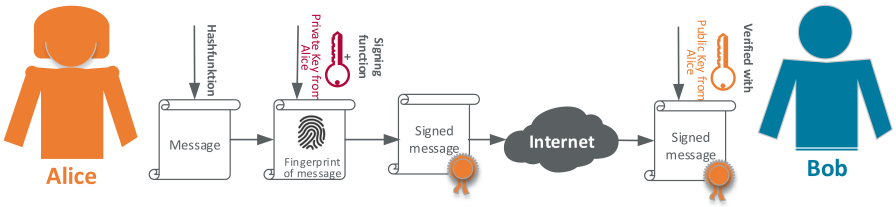


Figure 2.4: Digitally signing and verifying a message

In order to create a digital signature, a cryptographic hash function is used. Hash functions are categorized as one-way functions. This means that while in one direction[9] mathematical calculation is simple, in the opposite direction[10] it is extremely difficult or impossible [118]. The hash function converts an amount of data of different lengths into an alphanumeric value of fixed lengths – a hexadecimal string. The hash value consists of a combination of numbers and letters between 0

[9] To calculate from a plaintext message, for example, a hash value from the name Alice.
[10] To calculate the original message only on the basis of the hash value and the hash algorithm.

and 9 and between A and F (as a substitute for the numbers 10 to 15). This method makes the unambiguous identification of a message possible, without having to reveal the contents of the message. For this reason, the hash value is often called a fingerprint.

The most-often used hash function in blockchain technology is the SHA-256 (Secure Hash Algorithm), whereby 256 indicates the length of the hash value in bits. Even the smallest change in the message produces a completely different hash value. The following example, using the name "Alice" and the SHA-256 algorithm, shows how great the difference in hash values can be if even just one character in the name changes:

- Alice
  3bc51062973c458d5a6f2d8d64a023246354ad7e064b1e4e009ec8a0699a3043
- Alice1
  9d328d8b7ac56e1f71ce94ed3c7975d63c8b6f1a54d5186de8881cf27dd8b3a9
- alice
  2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90

In blockchain technology, digital signatures are used for the confirmation of authorship of corresponding values (e.g. bitcoins).

2.1.2 User Identification

In the financial sector, "bank account" and "account number" are often-used terms. A lending institute uses an account number to identify a customer. Because in blockchain technology there is no central instance who administers user accounts, in the case of cryptocurrency, for example, all expenditures incurred are registered in the blockchain. User applications (for example cryptocurrency wallets) analyze the blockchain and present an overview of the user's incoming and outgoing transactions and current cash holdings.

In many blockchain applications, special pseudonyms identify users. These are called addresses (e.g. bitcoin address). Just as emails are sent to an email address, bitcoins are sent to a bitcoin address.

Originally in the bitcoin system it was possible to send bitcoins to an IP address [68]. This method, however, opened up the possibility of attacks. For this reason, when a user is credited a bitcoin value cryptographic methods are only carried out in address generation. To do this, a cryptographic key pair is generated at the user, for example in the wallet. The private key is used for signing the transaction[11] and the public key for generating the address.

The key pair in the bitcoin system and in many other different cryptocurrencies (e.g., Litecoin or Dogecoin [68]) is generated with the Elliptic Curve Digital Signature Algorithm (ECDSA).First, the private key is generated as a random number.

[11] See section 2.2.1.

The public key is derived from the private key and then "hashed"[12]. The address is essentially a 160 bit long alphanumeric value (e.g., 16UpLN9Risc3QfPqBMvKofHfUB7wKtjvS). Such an address is often called a "Pay To Public Key Hash Address" or a P2PKH address.

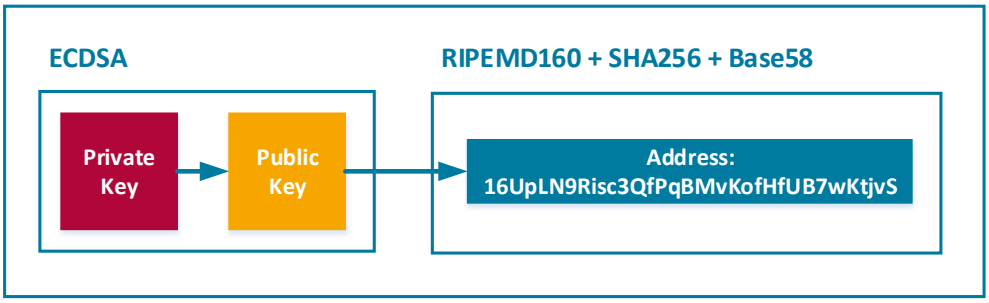


Figure 2.5: Address generation in the bitcoin system

Some wallets offer so-called multi-signature addresses. For these addresses several private keys are created [28], which in turn increases security. The recipient who receives the credit must have all the necessary private keys in order to be able to use the credit received. Multi-signature addresses can be used, for example, in a company that accepts bitcoins in order to confirm expenditures from individual employees upon their approval by controlling. In this case, both the employer and the controller each have a private key for a common bitcoin address [65].

Since all transactions in a blockchain[13] are public for all users, it is always possible to track the previous owner (the P2PKH address) as well as the entire "history" of the amount and to see the account balance (all transactions carried out with the address) of every user. This is the reason it is recommended for users to use their address one time only and then to generate a new address for every new transaction [59].

An individual account balance is also associated with every user address. It is additionally possible to use different wallet for different purposes.

These usually include the following information:

- one or more cryptographic key pairs,
- an address generated with the key pair,

[12] In order to generate the address from the public key, two cryptographic hash functions are used one after the other on the public key (RIPEMD-160 and SHA-256) and the result is then encoded using the Base58 scheme (without the number 0 (zero), O (capital letter o), I (capital letter i), and l (small L)) (more in appendix 6.1).

[13] This applies to the public blockchain and the consortium blockchain (see section 3.1).

- a list of transactions addressed to and executed by the user,
- other functionalities depending on the software vendor.

Above all, it is important that the users protect their private key sufficiently. For whoever has access to the private key may also spend the credit associated with it or with the P2PKH address (for more information see section 2.2.1).

2.1.3 Exchange Among Equals

One of the key strengths of blockchain technology is its architecture. It provides its many users with a decentralized, autonomous, secure and transparent system.

Below we introduce the decentralized system behind blockchain technology and explain how the values transferred via the transactions (e.g., bitcoins) are assigned to their new owner.

A blockchain system is based on a so-called peer-to-peer network (P2P). The users of this system are represented by the nodes in the network. They are all on equal footing and can use services as well as providing them to other users. In the case of the bitcoin system, users are those who transfer bitcoins to others or who receive them. In the Internet of Things, on the other hand, the IoT devices interact with each other in the decentralized network.

Communication takes place via an unencrypted Internet connection (see figure 2.6).

As the network has no authentication and no central administration for the user nodes, methods from P2P networks[14] (see figure 2.7) are used for locating other nodes and for information dissemination [116].

Generally in blockchain[15] networks all nodes are on an equal footing and can be both clients and servers. Given the size of the bitcoin blockchain (in December 2017 it was 147 GB), it is understandable that not every user has enough resources for storage and verification at its disposal. Above all, the application should be as "thin" as possible for mobile users. Against this background, two kinds of users are possible in the blockchain network [116]:

- "Servers" or full nodes. They have both incoming and outgoing connections with other users, store the complete blockchain and are involved in its verification.
- "Clients" or lightweight nodes (the "thin client" or the less common SPV[16] node) are the most common[17] users in the bitcoin network. They just provide

[14] A Peer-to-Peer Network is a network in which all nodes have equal rights. This means that, on one hand, each node provides functions and services to other nodes and, on the other hand, it can equally use the functions, resources, services and files provided by the other nodes. The data is distributed over many nodes. The P2P concept is a decentralized concept, without a centralized server, like the Internet. Every node in such a network can be connected with numerous other nodes [15].

[15] Applies to the public blockchain and the consortium blockchain (see section 3.1).

[16] SPV - Simplified Payment Verification (see section 3.2.4).

[17] An estimated 13 times as many clients as servers [116].

outgoing connections and store only a part of the blockchain [120]. They set up a connection to the full nodes to obtain information that only applies to them. Also included among the clients are users who outwardly[18] have a different IP address than (for example) in their company network.

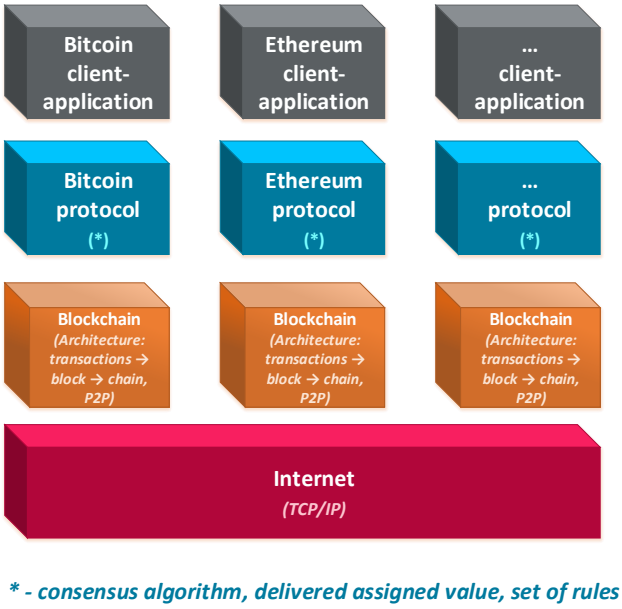


Figure 2.6: Abstract representation of the blockchain layer architecture

Bitcoin users (client and server) support eight outgoing connections with other users. In addition, the server supports up to 117 incoming connections. If one of the eight outgoing connections is no longer active (e.g., because the user is offline), this connection will be replaced by a new one [116]. Information is exchanged via these connections (e.g., information like a new transactions, blocks and IP addresses[19] of the full nodes/server). Every user (client and server) keeps a list of IP addresses of other users (servers) in the network and updates it regularly through exchange with other users. The IP addresses are not connected with the cryptographic addresses.

Let us return to the example of Alice and Bob. Alice is often on the go and wants to use the bitcoin system on her laptop. We assume there is not enough memory and computing capacity to run as a full node. We also keep in mind that Alice often logs in to different networks: at home, in the library or at work. She therefore installs the bitcoin software and sets up a lightweight wallet. The

[18] For example, the users behind Firewall and NAT.
[19] In the bitcoin network: IPv4, IPv6 and OnionCat addresses [120] [116].

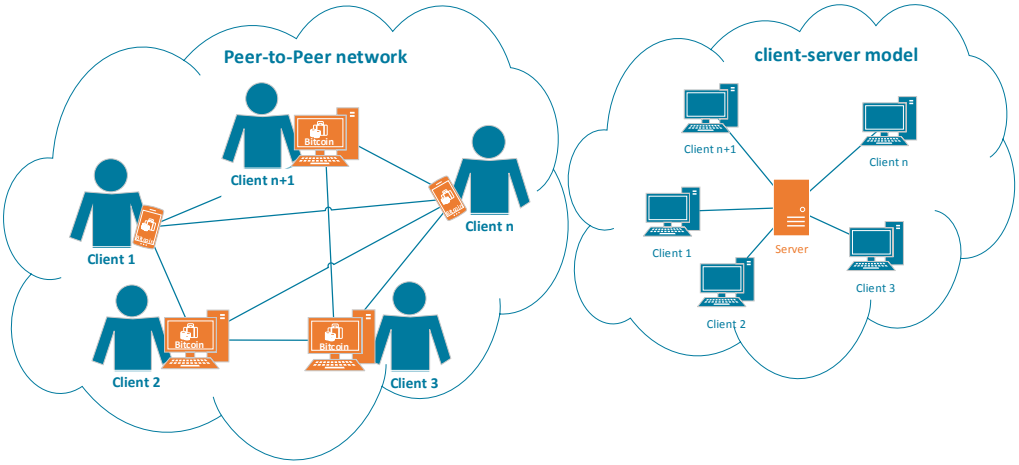


Figure 2.7: Comparison of the P2P and the client-server networks

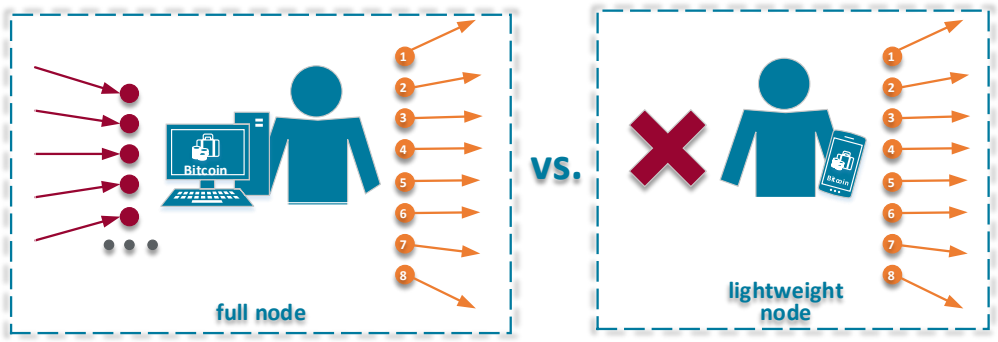


Figure 2.8: Comparison of user types (full and lightweight nodes)

software already contains hard-coded DNS[20] names (also called DNS seeds – e.g. seed.bitcoin.sipa.be, seed.bitcoinstats.com, etc.) that include multiple IP addresses of full nodes (see figure 2.9).

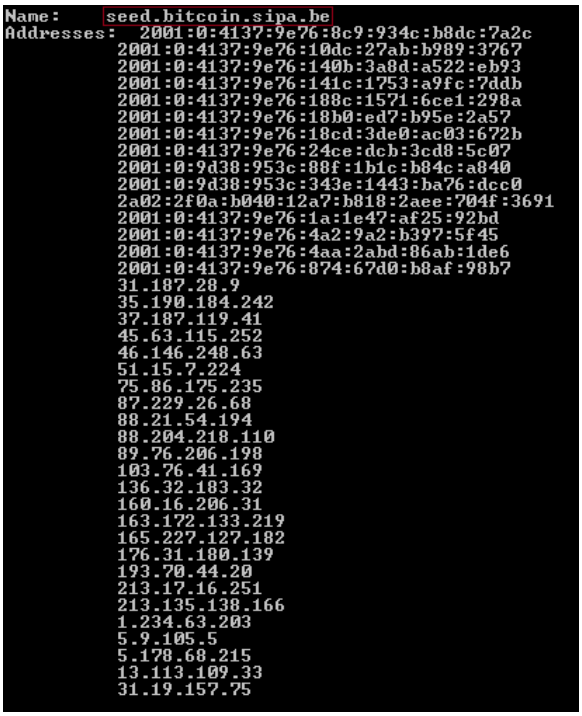


Figure 2.9: Resolution of the domain names of a DNS seed

The software establishes connections with some of the full nodes in the list and asks for additional IP addresses. The list of IP addresses is continually updated. The software from Alice can support up to eight connections, which means that Alice can exchange information with eight additional users, in this case full nodes. First, the "thin" version of the current blockchain is downloaded. Alice also sends her transactions to the users and receives information from them that is intended for her specifically. The disadvantage of a lightweight node is found in its reduced security. Alice must place complete trust in the full node as she only uses the "thin" version of the blockchain and thus cannot verify all earlier transactions.

The information in the blockchain network is exchanged according to defined rules. These prevent, for example, that an already sent file (block, transaction, IP address) by a user is resent to the same user. In this way, network overload is also avoided.

[20] The Domain Name System (DNS) connects numerical (IPv4) and alphanumerical (IPv6) IP addresses with easy to remember domain names. In this way, instead of having to remember a long series of numbers, users instead remember a meaningful name. For example, behind the DNS name hpi.de is the IPv4 address 141.89.225.126.

In contrast to the example with Alice, let us assume that Bob operates a full node. He has a complete copy of the blockchain and besides the eight outgoing connections to other users he may have up to 117 incoming connections. Via the incoming connections, he receives all new transactions and blocks of the other users and verifies them according to fixed rules. The valid blocks and transactions are cached and sent on to other full nodes. The invalid ones are discarded. The full nodes are the backbone of the bitcoin system. They allow the system to grow and to remain secure and decentralized.

All files (new blocks, transactions and IP addresses) are sent from one user to the other users (see figure 2.10). The full nodes pass on their own new transactions with those just received, so that it appears to the other users as if they were their own.

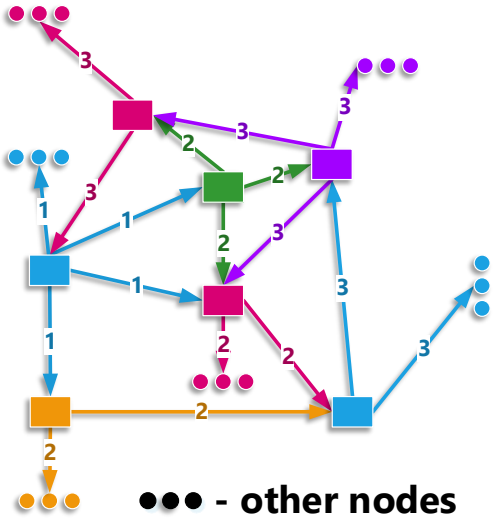


Figure 2.10: Dissemination of Information in a blockchain-based network

The received file is verified each time by the user according to defined rules. If the user has already received the file from another user and has already saved it in its cache, the user discards the newly arrived file.

2.1.4 Obfuscation

As already mentioned, transparency is one of the key features of blockchain technology. However, in many application areas this feature would infringe on the user's privacy. At the same time, if the issue is, for example, the different ingredients[21]

[21] The company ClearKarma offers the food industry a solution for the end-to-end traceability of ingredients [73]. The company plans a cloud-based platform with extensive

in foodstuffs or the traceability of information along the supply chain related to the storage of a drug[22] (temperature or moisture), transparency is of the utmost importance. In private finances, on the other hand, it is usually unwanted.

It is necessary to note that the anonymity of the user created by the pseudonym is only partial, as it is still possible to determine the identity of the user from the IP address and by tracing the user's transaction history (see section 2.4.5).

Bitcoin therefore recommends its lightweight nodes deploy the anonymous TOR network in order to disguise the IP address [59]. With the standard software Bitcoin Core[23], the full nodes can automatically use the "TOR Hidden Services" for more anonymity (see appendix 6.2) [66].

The TOR network provides a service that makes the connection data anonymous. The initials TOR stand for "The Onion Routing". So-called onion routing is characterized by the multiple encryption of a message. The TOR client searches for a route through the network that consists of a number of "onion servers" ("onion routers"), each of which provides a public key (see figure 2.11).

Generally the route runs via three servers. Having found a route, the TOR client first encrypts the message with the public key of the last onion server (Router C) and adds its address. Afterwards, the already encrypted message and the address of router C is encrypted with public key of the next to last server (Router B) and its address added, and so on. Subsequently the message is decrypted during transmission layer by layer.

Each server involved in the routing process can decrypt the message intended for it with its own private key. In the message it finds, in turn, an encrypted message and another address. The message is sent to the specified address. Hence, every onion server "knows" only its predecessor and its successor. Only the last link in the routing chain is able to read the message in plaintext.

The use of the TOR network is only possible for outgoing connections – thus only for lightweight nodes. To also support incoming connections in the TOR network, the user can make use of its so-called hidden services. In this case, the full node acts as a service provider and arranges a "meeting point" with the service receiver (another user) – a secure onion server, also known as a "rendezvous point". In this way, secure and anonymous communication can be ensured (see figure 2.12) [66].

Because in the bitcoin system there are no sender addresses[24], users are strongly recommended to use a new address for each new transaction to protect their privacy. The previously mentioned mixing services can be used to further disguise the recipient. The legality of using such services can be subject to different rules depending on the law of the specific country [59].

---

information on foodstuffs, whereby the history of all information changes are verified and stored on the blockchain.

[22] The company Modum.io offers a solution for end-to-end data integrity in a supply chain with the help of blockchain technology [97].

[23] That is, since version 0.12.0, published on 23 February 2016.

[24] Simply put, each transaction contains the bitcoin value and the receiver address, and it is subsequently signed by the sender. The user can only output the obtained bitcoin value with its private key, which it has generated for the transaction (see section 2.2.1).

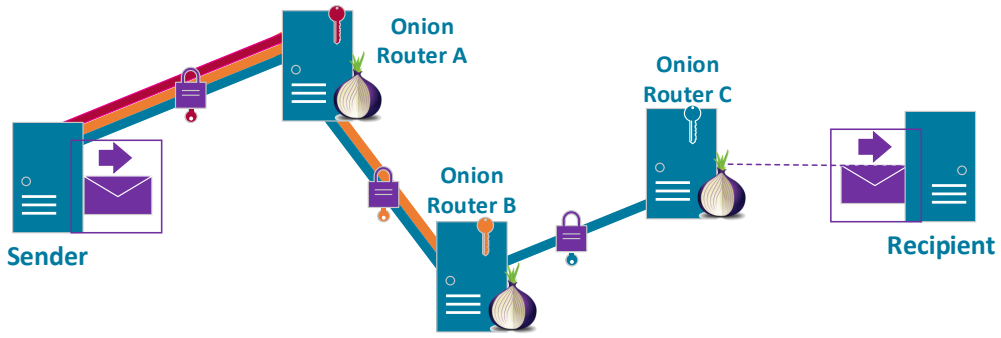


Figure 2.11: TOR network

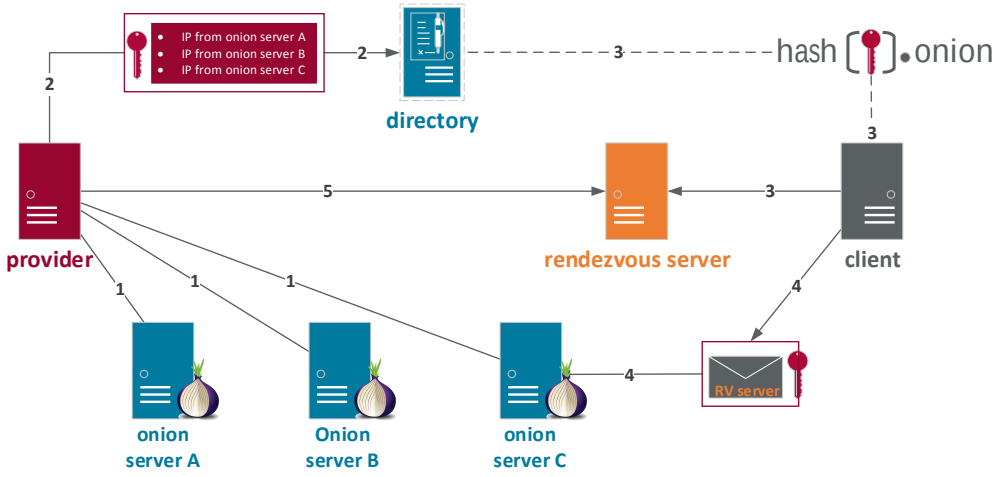


Figure 2.12: Tor hidden services (for further information see [105])

The listed methods provide greater anonymity in the transparency of the blockchain system. Nevertheless, users should heed a number of safety instructions to protect their privacy as well as the blockchain values (e.g., cryptocurrency such as bitcoins, ownership of, for example, a rented bicycle, or events such as unlocking the door to a room).

2.1.5 Data Protection and Liability

As noted, a blockchain-based system has no central instance. Accordingly it functions in a decentralized and autonomous manner and works with an unprecedented level of transparency [59]. From what seem to be highly positive characteristics, arise several data protection issues.

Because of the transparency of all transaction information, the business and, basically, the personal circumstances of the users can be recognized [133]. Trust-critical transactions between the parties are carried out without an obligation to reveal the identity of the contract partners to each other or to the public. Anonymity or pseudonymity thus become instruments of data protection [78].

According to Pesch and Böhme [133], bitcoins can neither be classified as a "legal object" in the sense of a "thing", nor as a "legal object" in the sense of "money". Therefore, because of the prohibition of tortious analogy[25] in criminal law, bitcoins cannot be the object of a criminal act whose offense centers solely on money or a thing [133]. It remains to be seen whether other blockchain values can be considered a "legal object" in the sense of a "thing".

One of the most common applications of blockchain technology is the smart contract[26]. It has an impact on areas of life that are traditionally regulated by analogous law or institutions [78]. The company Agrello [57] has taken up this problem and found a solution in the form of legally binding smart contracts. Agrello offers a product with a user-friendly interface (see figure 2.13) that supports the user in the creation of a legally-binding contract. The generated contract is converted into a smart contract and saved in a blockchain. At the same time, a legally binding contract in natural language is created and digitally signed [57]. The user is supported throughout the creation of the contact by an AI[27] agent.

2.2 Reliability, Counterfeiting Protection, Traceability

Blockchain applications vary from application to application. Some are much more complex than others. But all have in common their underlying architecture (transactions, blocks, chain, consensus algorithm[28]). For example, the identity system

[25] "An analogy prohibition exists in particular in criminal law. Accordingly, a judge is prohibited from convicting a non-criminal offense, even if he or she considers the act to be criminal or similar to, but not entirely in accordance with, another criminal law. This ban applies in particular to loopholes." – Definition according to [7].

[26] For more information on the smart contract see section 3.3.

[27] AI – Artificial Intelligence.

[28] siehe Kapitel 2.3.

Figure 2.13: Agrello-App [57]

Blockstack takes the advantages of blockchain technology and logs only the blockstack operations in the blockchain (see figure 2.14). The other functionalities, such as management and data storage, are controlled outside the blockchain (for more information see section 4.5).

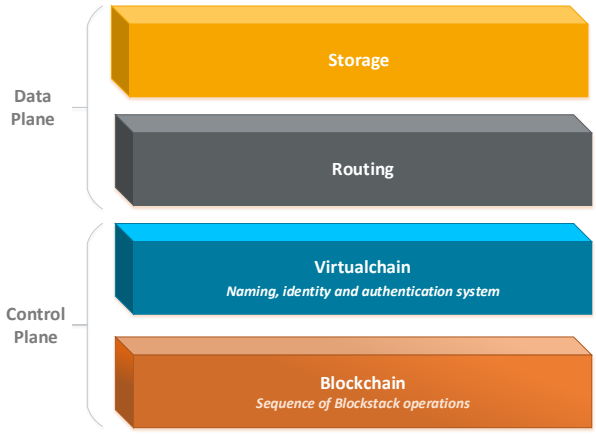


Figure 2.14: Blockstack layer architecture

In contrast, pure cryptocurrencies have a simpler architecture (see figure 2.6):

- underlying blockchain,
- specific rules for each cryptocurrency (among them the consensus algorithm) and
- a user application that implements everything.

Because of the way information is distributed in a blockchain system, every user has either a full copy or a "thin" version of the blockchain, which is updated regu-

larly. The distribution of the blockchain over many machines that are independent of each other provides security in the case of system failure or data loss.

Features such as counterfeiting protection and transaction traceability first become clear with a good understanding of the blockchain architecture. In the following chapters we will therefore look at, first, the smallest unit of a blockchain (in cryptocurrency this is the digital coin, for example a bitcoin) and how it is entered in a transaction. Finally, we will explain how the transactions are recorded in the blocks and how this results in a chain.

2.2.1 The "Smallest Component" in a Blockchain

A network designed on the basis of blockchain technology is also called the "Internet of Value". Instead of exchanging information in the Internet in a manner that is sometimes encrypted and sometimes decrypted, end users in a blockchain network exchange values that are tamper-proof. A value can consist of a cryptocurrency, an event or a possession.

These values are the smallest "conceptual components" in a blockchain. The corresponding units are not defined in the blockchain system code as extra messages, data packets or variables, but rather as part of the transaction. Therefore, technically, a transaction is the "smallest component" in a blockchain.

Through such a transaction in the blockchain, a certain value is transferred between users, thus changing its owner. A newly created end value, whether it be a digital coin in a cryptocurrency or a new apartment for rent, has no previous history. In the course of time when the value is transferred from user to user, the entire history is stored in the blockchain – specifying who had possession of something and when. In this process, the value is also displayed as a reference to a previous transaction.

A transaction has two main elements: an input and an output. Upon input an existing value is entered, that is, the reference to the previous transaction, in which the value was transferred to the current receiver at an earlier point in time. The references to the previous transactions are their hash values (see section 2.1.1 – Cryptography). In the output, the address of the recipient is entered and additionally for example in cryptocurrency the number of digital coins to be transferred. The transaction is then signed by the sender.

As previously noted, the address is derived from the public key and represents its hash. The user can therefore only then use the transaction value addressed to it when it has the private key corresponding to the public key. By signing with a corresponding private key the transaction can be "spent"/passed on.

A transaction may also include multiple inputs and outputs. In the bitcoin system, for instance, all previous transactions, which are addressed to a user and have not yet been spent, are listed in his wallet as his current bitcoin assets. These earlier transactions are used in new transactions as inputs of this user. Multiple outputs are provided if the value to be transferred is to be split up among multiple recipients.

If the sender wants to transfer a smaller amount of money than is available at all inputs, he has the possibility of sending the remaining balance to himself. If the sender has a transaction balance that he does not transfer to himself, the amount

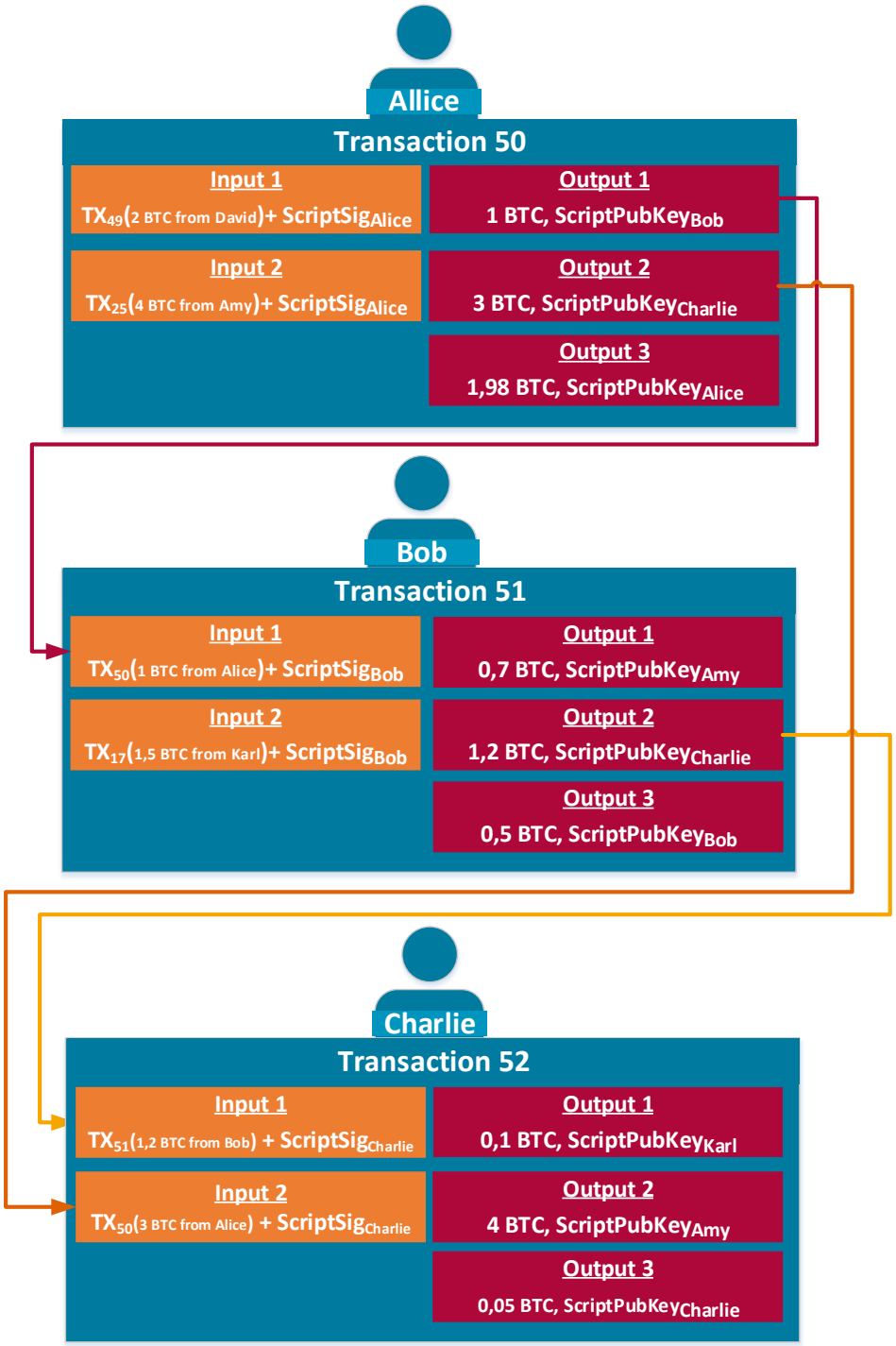


Figure 2.15: Transactions in the Bitcoin system

will be understood as a transaction fee (see section 2.15). Transactions cannot be undone.

Once a transaction has been generated, it will be shared with other users with whom a connection exists. Every full node verifies the received transaction according to defined rules (see section 6.3) and stores it in its buffer memory (memory pool) until it is accepted in a block by a so-called blockchain updater (miner or minter). The process in which a blockchain is updated is called mining or minting (depending on the consensus algorithm, see section 2.3). New transactions are thereby summarized in blocks and the blocks linked in a specific order (more about this in section 2.2.3).

Here are four examples of transaction verification rules:

- a transaction has been signed,
- a transaction has never been "spent" before,
- if the transaction was sent to me, it would be added to my wallet,
- if the transaction was added to a valid block, it would be deleted from the cache.

A transaction is considered valid if it is included in a block that already has at least five successor blocks. This number was chosen based on the assumption that potential attackers do not have enough computing power (or want to exert it) to recalculate six blocks.

2.2.2 Block and Chain

After transactions are distributed to the full nodes in the blockchain network, and after being successfully verified and stored in their memory pools, full nodes can summarize them in a defined list with additional information and receive a reward for doing this. In blockchain technology such a list is simply called a "block". The user (full node) has only then chance to create a valid block, and thus get the reward, by executing the predefined requirements in his system. In the bitcoin system, for instance, the user should correctly solve a fixed cryptographic task (for more information see section 2.2.3).

Transactions and blocks are the most important components in a blockchain. Additional information is contained in the "block header", followed by the list of transactions in the "block body". This information is necessary for the proper construction of the blockchain and its verification.

In the bitcoin system, the block header contains the following information:

- Nonce[29] – an important clue to the proper construction of the block, and used for mining (32 bits),

[29] In cryptography the term "nonce" (abbreviation for "used only once" or "number used once") refers to a number or letter combination that is used only one time in a particular context [109] (for more information see section 2.2.3).

- a reference to the previous block: a SHA-256 hash of the previous block (hash of the previous block header),
- a value that is important for block construction, which shows a "difficulty target"[30] for the cryptographic task,
- a time stamp of when the block was created,
- a reference to all transactions in the block, also called the root of the Merkle tree ("Merkle root", 256 bits) and the
- specification of the software version of the bitcoin application, utilized by the user who created the block (block version number).

The hash of the previous blocks, the nonce and the difficulty target of the cryptographic task are relevant for mining (for more information see section 2.2.3).

As shown in the chapter "Cryptography", the hash function allows a clear and relatively simple identification of the data. In blockchain technology the hash values help to preserve the sequence of entered data. They are used as references. A transaction contains, for example, the hash values of the previous transactions; these are the inputs of the transaction – the value base (in the bitcoin system the coin asset). In this way, it is possible to trace the entire history of the transaction or of the end value in the blockchain.

The blocks include two different references, one for the previous block (hash of its block header) and another for all transactions carried out in the block. These references are the so-called "finger prints". They help to quickly prove whether a transaction has been introduced in the block retroactively.

The Merkle root is the last hash value in the so-called hash tree. The hash tree ("Merkle Tree") involves a tree structure (graph theory) made up of consecutive hash values[31]. In figure 2.16, for example, it can be seen that from Transaction 1 (**TX1**), first a double hash value **dh1** is created. This is **dh1=SHA256(SHA256(TX1)**). Then, the same thing happens with transactions **TX0**, **TX2** and **TX3**. Further hash values are calculated from the first double hash values of the original transactions. The root of the tree **dh0123** is in this case the Merkle root.

The block size in the bitcoin system is limited to 1 MB. Thus, a block can contain approximately between 900 and 2500 transactions. For a long time the bitcoin community has discussed whether the block size should remain at 1 MB or be increased to 2 MB. On August 1, 2017, a spinoff of the bitcoin system resulted in "Bitcoin Cash". Here, the size of the block is fixed at 8 MB.

One of the specifications for block creation in the bitcoin system (mining), is that a new block must be generated in ten minutes.

The first transaction in the block body is made by the user who created it – called a miner in the bitcoin system – and is addressed to himself. This transaction is the reward for the miner and consists of 12.5 newly created bitcoins. This transaction has no input since the bitcoins are newly created bitcoins without a history.

[30] The value of this "difficulty target" is shared by all users in the bitcoin system.
[31] In the bitcoin system the hash function SHA-256 is applied twice.

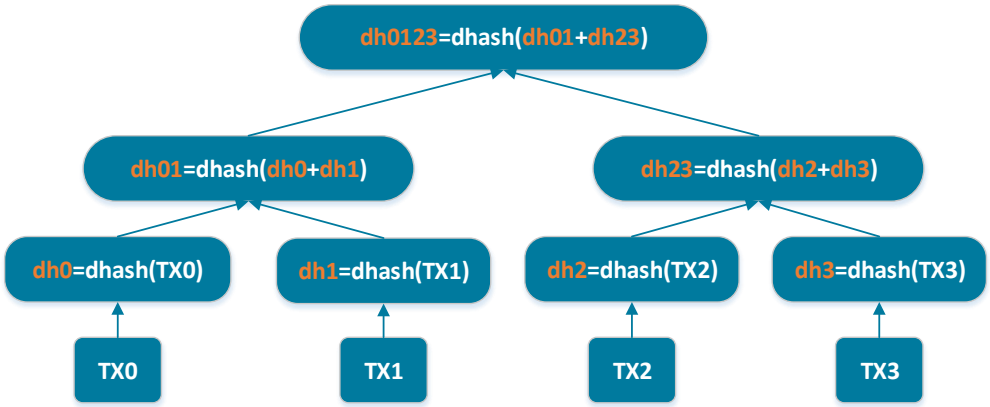


Figure 2.16: Hash tree from transactions

After 210,000 blocks have been surpassed, the reward paid to the miner is cut in half (roughly every 4 years; for example, from 2020 onwards, it will be only 6.25 bitcoins).

To be certain whether the created transaction is valid, users should wait until the transaction is included in a block that already has at least five succeeding blocks. Since each new block is created in ten minutes, the waiting time is between one and two hours. The larger the transaction fee, the faster the transaction is included in a new block by the miner. Miners receive the transaction fees of all the transactions contained in the block.

Once the block has been created, it is distributed to the users. Each full user (full node) verifies the received block according to defined rules and adds it to the chain. Thereby, a chain made up of joined blocks connected by references is created. The first block in the chain is also called a genesis block.

Blockchain technology lists all transactions that have ever been carried out in the respective system, and which in turn are divided into blocks. The listed blocks form a chain with each block containing a reference to its predecessor. In this way, a sequence of blocks is created – the origin for the name blockchain.

Because the blockchain network is decentralized and no arrangements are made between the users as to the priority of the created blocks, it is possible that multiple miners may generate a new block simultaneously. If these blocks fulfill all the rules and use the last block in the chain as their reference, this can result in a forked chain. In bitcoin terminology this is called a "fork". The solution here is at the same time the most important rule in the bitcoin system: "The longest chain is valid" (for more information see section 2.2.3). The shortest chain is ignored; its blocks are called "orphan blocks" (see figure 2.17).

The size of the bitcoin blockchain in December 2017 was 147 GB.

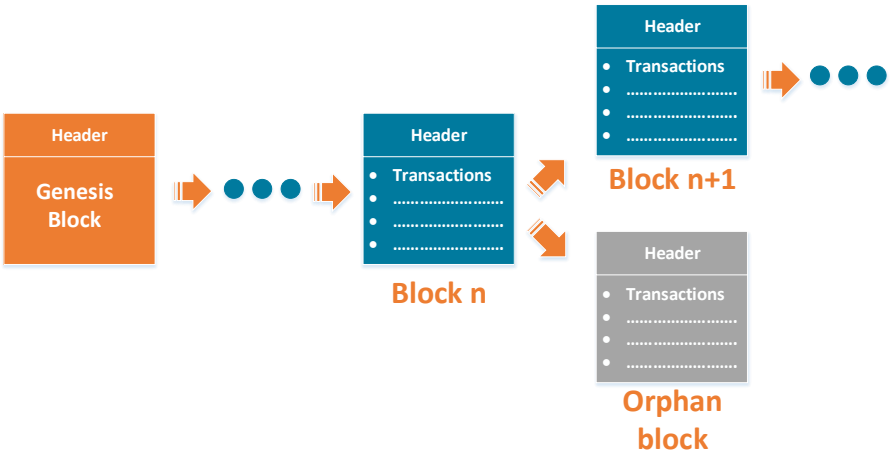


Figure 2.17: Blockchain

2.2.3 Updating the Blockchain

The blockchain is updated by merging new transactions into blocks and chaining the blocks together in a specific order. In the bitcoin system this is called mining; the users who update the blocks are miners. In fact, there is a definite similarity between the process and the extraction of raw material in a mine: whoever mines, has to exert a great effort to uncover the resources they are after.

The blockchain protocol is tamper-proof in regard to when, between whom and what information is exchanged. New values (cryptocurrency, ownership, events) are securely registered in the system and already existing values are not assigned more than once (double spent). In this way, a reliable, manipulation-free consensus is achieved between all users.

The defined requirements a user must fulfill in creating a valid block are among the many rules for consensus-building in a decentralized and autonomous system and of crucial importance.

The requirements vary depending on the system and exist insofar as the user is obliged to prove that he has either wasted specific resources for block creation or that he has been chosen by other users for block creation (more on this topic in section 2.3).

The work necessary in mining is resource-intensive and with an intentionally complicated design. The block-building process thus remains constant and possible attackers are discouraged from manipulating blocks or flooding the network with counterfeit blocks. Attackers must, after all, also carry out the same intensive work involved in the creation of new blocks. The Proof-of-Work is checked by other users in terms of its correctness and confirmed when accurate. Users involved in block creation are rewarded with newly generated bitcoins (first transaction in the new block; for more information see section 2.2.2) and transaction fees. Thus, the reward in the bitcoin system serves in the creation and dissemination of new bitcoins as

well as motivating users to take an active part in the mining process and thereby maintaining the security of the system [64].

After transactions have been distributed to all users, the users verify them. The transactions are then stored in the users' memory pools until being included in a block.

Before a miner can put the transactions in a valid block, he must perform a cryptographic task with a certain level of difficulty[32]. The cryptographic task consists of finding a hash value below the given "difficulty target". Every two weeks (after 2016 blocks have been reached) the level of difficulty and the "difficulty target" are adjusted in such a way that it takes ten minutes to build a block. When the computing power of the entire network increases and the 2016 blocks can be found in less than two weeks, the level of difficulty is raised.

The hash value is calculated by using the double hash function SHA-256 from the block header and a nonce[33]. The nonce, a 32-bit long, variable hexadecimal string, is adjusted again and again until the hash value is smaller or equal to the target (see figure 2.18).

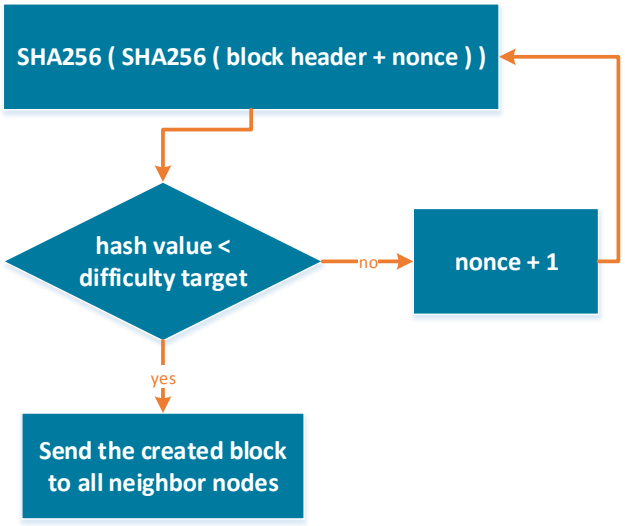


Figure 2.18: Mining process; solving the cryptographic task

The target is a 256-bit hexadecimal string, which is shared by all bitcoin users. The smaller the target (that is, with several zeros at the beginning) the greater the

[32] The level of difficulty indicates how hard it is to find a hash value below the given target.

[33] In cryptography, the term "nonce" (abbreviation for "used only once" or ""number used once") indicates a number or letter combination that is used only once in each context [109].

level of difficulty. If a specific number of zeros results at the beginning of the string when the hash is calculated, then the task has been solved (see figure 2.19).

Target for block 100,000	
Hexadecimal	000000000004864c000000000000000000000000000000000000000000000000
Decimal	186131131498380012681564362292723007636833484581425336990197350 4

Hash for block 100,000	
Hexadecimal	000000000003ba27aa200b1cecaad478d2b00432346c3f1f3986da1afd33e506
Decimal	153326787264777690215432048793065921179506558199844584874022631 0

Figure 2.19: Hash calculation of blocks [22]

The probability of a user finding the right solution is proportional to his applied computing power (his hash rate[34]). After the appropriate solution is found, the created block is distributed to all the users.

Each full node verifies[35] the block received. Depending on the verification result, the block is accepted (added to the main chain[36] or to the "side branch"[37]) or discarded ("orphan block"[38]). When it is accepted, the block is distributed to other users.

Due to the latency of the network, dissemination of the blocks occurs at different rates of speed. When multiple miners solve the task at the same times and distribute their blocks into the network simultaneously, ultimately only a single chain will prevail. Here is an example. Alice and Bob have simultaneously found a solution for the cryptographic task and distribute their newly created blocks **a** and **b** in the network. Each user saves the first block received, after successful verification, as a part of the main chain ("main branch"). User **K** gets block **b** from Bob after he has already received block **a** from Alice. He adds it to the side branch after verification and waits for the next block. Charlie is also a miner and got block **b**

[34] Hash rate – or computational power; how many hashing operations can be performed in a second.
[35] First a check is made of whether the block was correctly constructed and whether the references in the block header (hashes) are correct. For a detailed description of block verification see [13].
[36] Also called the main branch – the longest chain that has been validated by all nodes.
[37] A side branch is created by the forking of the chain.
[38] Orphan blocks are either those blocks that have no predecessor block or blocks from the shorter chain that have not prevailed.

first. He builds another block **b+1** and distributes it to all users. User **K** gets block **b+1**. After verification he adds it to his side branch (since block **b** is stored by Bob) and redefines it as a main chain, because in the end the longest chain becomes a main chain. The blocks from the side branch become orphan blocks and their valid transactions are again moved to the user's memory pool. As the chain with Bob's block prevailed, after 100 blocks (waiting time) Bob gets a reward in the form of newly created bitcoins and transaction fees. Alice does not receive a reward for her block **a**. The number of newly created bitcoins are cut in half every four years (by 2012 it was 50 BTC, by July 2016 the number was at 25 BTC and by 2020 it is 12.5 BTC, etc.).

Every full bitcoin user can be a miner and construct new blocks. In the first years of the bitcoin system all members were miners. Over time, however, the number of users as well as the computing power used in mining has quickly risen. The level of difficulty of the cryptographic task has been adjusted, which means a further upgrade of mining hardware and an increase in power consumption.

Today, in order to stay in the race, miners must provide special hard- and software or take part in cloud mining. Many miners join so-called mining pools to pool their computing capacity with other users.

For mining, either a computer with a powerful graphics card is used or, for the mining of bitcoins, the specially manufactured bitcoin miner (e.g., ASIC[39] mining hardware). In December 2017, bitcoin miners were on the market with energy efficiency of between 0.29 J/GH[40] and 0.098 J/GH and performance between 3.5 TH/s[41] and 13.5 TH/s. Their consumption is approx. 1,200 watts. The hash rate[42] of the bitcoin network at the time was approximately 12,337,091 TH/s [33]. This means the bitcoin network consumed about 49 GWh a day at this time. We can compare this to an average German household of four that uses 4,000 kWh of energy a year. This means that approximately 12,250 such households can consume as much energy in a year as the bitcoin network needs in a day. The estimated energy consumption of the bitcoin network varies greatly according to the source. For example, according to information from Digiconomist in September 2017, it was said to be about 19 TwH while another source[43] states it as 5 GWh annually.

A potential attacker would have to solve the task with the same level of difficulty as any other user, and also bear the "losses" in energy resources in order to create a valid block.

In order to fake a block that has already been included in the blockchain, an attacker would have to convert all subsequent blocks as well. Because even the smallest change in a block leads to a new hash, the references in the block would no longer agree. For the successful manipulation of block contents, the attacker must have over 51 percent of the computing power of the complete bitcoin network.

---

39 Application Specific Integrated Circuits.
40 Joule per Gigahash.
41 Terahashes per Second.
42 Hash rate – or computational power; how many hashing operations can be performed in a second.
43 Mishra, Sailendra Prasanna. Bitcoin Mining And Its Cost (University of Texas at Dallas) 2017.

2.3 Consensus Building in a Decentralized Network

To avoid chaos in a decentralized network – where every participant is equal and there is no trustworthy central instance – specific rules and a decision-making model (consensus algorithm[44]) are necessary. All participants subscribe to these rules and can adapt to them accordingly.

As previously described, every user application contains a set of rules, such as how transactions and blocks are constructed, verified and distributed. Rules outline how connections are established with other users in the network and how the proper order of blocks in the blockchain is ensured and made tamper-proof. The last mentioned rule varies from system to system and requires a consensus between all users regarding how to handle proof of eligibility in the creation of new blocks. In this chapter, several consensus algorithms will be introduced and compared.

The problem of reaching a consensus in a system that is distributed across multiple computers (in which some machines could be faulty and thus distribute the wrong information) is also known as the Byzantine Generals Problem (a description may be found in appendix 6.4).

According to Lamport [127], unity between the nodes (computers/users) in a synchronous system[45] can even be reached if up to a third of the nodes involved are malicious. The error tolerance is thus around 33 percent (unity can be achieved if the number of faulty or malicious nodes is under 33 percent).

Error tolerance is correspondingly lower in an asynchronous system[46]. For example, the FaB Paxos protocol[47] tolerates up to one-fifth of malicious nodes (also called Byzantine errors). Agreement in an asynchronous system with 20 percent of malicious nodes can thus be reached [140].

By introducing further restrictions, several algorithms exist that allow an improvement in the fault tolerance of asynchronous systems with an increased number of nodes (e.g., use of digital signatures, establishment of user groups, etc.).

At this time there are a number of blockchain projects from different branches that are based on various consensus algorithms. The following algorithms are currently the most widespread:

- Byzantine Agreement Algorithmus (BA),
- Federated Byzantine Agreement (FBA),
- Proof-of-Work (PoW),

---

44 Consensus is defined here as an agreement on common values [44].

45 Activities are carried out in synchronization between each other (controlled by common clocks or other synchronization mechanisms) [138].

46 No synchronization used [138].

47 Martin, J-P. and Lorenzo Alvisi. “Fast byzantine consensus”. Dependable and Secure Computing, IEEE Transactions on 3.3 (2006): 202–215. The protocol demonstrates solvability of the consensus problem in “semi-synchronous” systems and enters into various compromises regarding the number of processors, the number of message delays before learning the agreed value, the activity level of the individual subscriber, the number of sent messages and the types of errors [110].

- Proof-of-Stake (PoS),
- Proof-of-Burn (PoB).

The Byzantine Agreement algorithm provides a solution to the Byzantine Generals Problem, thus allowing agreement to be reached between nodes ("generals") in a synchronous system where one-third of the nodes are faulty or malicious. According to Lamport [127], each node (computer/user) creates a vector with the values it has received from other nodes. After the vectors have been created they are exchanged. Each node checks all the values obtained from every single vector and makes a majority decision, which is then used as the result of the algorithm. In his work, Lamport places two restrictions on the solution: the sending of verbal and signed messages. As a result, two algorithms have been developed (see [142]). For use of the algorithm in a distributed network with equal nodes (whose number grows dynamically) further restrictions need to be made.

The Byzantine Agreement was further advanced in the context of the Stellar Consensus Protocol (SCP). Stellar is a public finance platform that enables the simple transfer of money in different currencies. SCP is based on a new consensus algorithm, which is described for the first time in the SCP White Paper[48] It is called the Federated Byzantine Agreement (FBA). The BA and the FBA differ in several criteria. The BA allows unity despite faulty nodes. This requires that all nodes in the network know each other and are verified early. In the FBA it is unnecessary that nodes have complete knowledge of each other. The FBA allows every node the possibility eliciting the service of trusted membership groups – so-called "quorum slices". A quorum is a number of nodes that is sufficient to reach agreement. A quorum slice is the subset of a quorum that can convince a specific node of the agreement. Each node can have several slices, which it can choose based on reputation or financial arrangement.

If the quorums have common nodes, they can overlap. In order to come to an agreement, the FBA nodes reach a consensus among themselves. They use federated voting to do this. The overlapping of quorums means that slices can influence each other in decision-making. New digital coins in the stellar systems, also called lumens, are awarded weekly by such a vote to the nodes (a one percent yearly rate of creation).

The already introduced consensus algorithm for the bitcoin system, Proof-of-Work (PoW), is used for updating the blockchain as well as for creating new bitcoins (mining). For every newly created block, the miner gets a reward in the form of newly generated bitcoins and transaction fees from the users (nodes). In the Proof-of-Work concept, energy resources are used to solve a cryptographic task.

The charge of wasted electricity is the biggest criticism of the proof-of–work concept. In contrast, Proof-of-Stake (PoS) is based on the share of digital coins of a cryptocurrency and not on the effort expended in solving the cryptographic task. A user (node) who owns **n** percent of the digital coins, may create **n** percent of the blocks.

[48] White Paper of February 25, 2016.

In the peercoin system[49] (which uses PoS), for example, the usable share of digital coins is based on the so-called "coin age". The number of digital coins owned by a block producer is multiplied by the number of days in which the digital coins were kept at the block producer (if, for example, Alice has received 5 coins from Bob and has already stored them for 10 days in her blockchain wallet, the coin age is 50 coin days). For successful block production the coin age must be between 30 and 90 days. These digital coins are used in block creation in the first transaction sent by the block producer to himself. Only after this are they valid for minting (block generation in PoS) again in 30 coin days. Each node in the peercoin system can create a block and receive a reward for it annually worth a maximum of one percent of the held digital coins. The reward consists of newly created peercoins. In this system, the transaction fees are not forwarded to the block producer but instead destroyed in order to minimize the inflation of the peercoins and the tendency to confirm only one's own blocks (and not those of other minters[50]).

In addition to the Proof-of-Stake concept in the peercoin system, the Proof-of-Work concept is also used (hybrid consensus).

In contrast to the peercoin system, in the NXT cryptocurrency all digital coins are available from the beginning (genesis block) and the transaction fees serve as motivation for the block producer. NXT uses a modified PoS algorithm [124].

A pure PoS concept confronts the specific problem called "Nothing at Stake". In the event that it comes to a forking of the chain, minters can build new blocks parallel on both forks without significant losses. This means that the same single digital coin can be spent more than once ("double-spending problem"). Since loss is not as noticeable in this case as, for example, in the PoW concept, PoS is more susceptible to attacks.

This problem is solved with an expanded form of PoS, called "Delegated Proof-of-Stake". Here delegate (confidant) users are especially chosen in accordance with specific rules (e.g., dependent on the number of the digital coins owned or the votes cast by other users). They are allowed to participate in minting and to verify the blocks generated by other delegates. So that a new block is accepted, several delegates must sign it after a successful verification. To avoid attacks, the digital coins of the delegates are blocked in the case of any malicious behavior.

An alternative to PoW and PoS is called the proof-of –burn concept (PoB). Here in mining, digital coins are destroyed (figuratively speaking "burned"). The more digital coins are destroyed, the higher the chance that the newly generated block is accepted and entered into the chain. The coins to be destroyed are sent to an address where they are no longer usable.

In distributed networks, decentralized control is an essential feature. Proof-of-Work is the best-known decentralized consensus algorithm and distinguishes itself through its use of physical resources (energy consumption through the expenditure of computing power). To keep losses at a minimum and to win the reward, miners must adhere to the rules (build correct blocks) or, through the application of the

[49] Peercoin is a peer-to-peer cryptocurrency, which is based on the design of Satoshi Nakamoto's bitcoin [126].

[50] Block generators in PoS.

highest computing power (more than 51 percent), convince other nodes of the correctness of the blocks.

Under these circumstances the "punishment" for malicious behavior is relatively high. This motivates individual miners further to act according to the rules specified in the system. The probability is very low that in a system with numerous nodes (like bitcoin) one of them has more computing power than all of the other nodes put together (over 51 percent of the total computing power).

Because the reward for newly generated blocks in the bitcoin system consists of created bitcoins and transactions fees – and the number of created bitcoins is halved every four years – it is indeed the transaction fees that remain the primary motivation for miners in block creation. The energy consumption depends on the difficulty of the cryptographic task, which in turn is adapted to the computing power of the bitcoin network. If the computing power of the bitcoin network, and thus the energy consumption, continue to rise, the transaction fees must be increased as well so that mining continues to be worthwhile.

Concepts such as PoS and PoB solve the problem of wasteful energy use by shifting the focus from physical to electronic resources. However, at the same time, this increases the likelihood of the branching of the chain and the double-spending problem, which in turn can be solved with further restrictions, e.g., the Delegated Proof-of-Stake concept.

Algorithm	Decentralized control	Low latency	Flexible trust	Asymptotic Security
Proof-of-Work	+	-	-	-
Proof-of-Stake	+	maybe	-	maybe
Byzantine Agreement	-	+	+	+
Stellar Consensus Protocol	+	+	+	+

Figure 2.20: Comparison of the consensus algorithms and their properties [129]

The Federated Byzantine Agreement solves the problem of trust between the nodes without assuming resource ownership; federated voting is carried out for this purpose.

According to the SCP[51] White Paper, SCP offers four properties for a consensus algorithm: decentral control, low latency, flexible trust model, and asymptotic security (see figure 2.20).

In comparison to Proof-of-Work and Proof-of-Stake, SCP has lower requirements regarding computing power and is open to new participants.

2.4 Security

Blockchain architecture provides a high level of security. Its cryptographic algorithms are among the best. There is of course a risk that quantum computing could crack these in the future [89], but, at the same time, the developers of the bitcoin system have pledged to switch to better algorithms if this danger becomes reality [67].

The source code of the bitcoin system is public and widely used by many IT experts who analyze its weak spots and improve it continuously. In the last three years there have been no more serious, security-relevant weak spots found [67, 61]. During this time, many changes have been made to secure the bitcoin system against numerous attacks. We list the best known among them here.

2.4.1 Denial-of-Service Attack

In a targeted overload of network nodes, for example, the full nodes are no longer available. Overload can result from the transmission of a flood of messages to the victim; whereby vast resources are consumed in handling the messages received.

In response, bitcoin implements a reputation-based rule: any user, who sends a faulty or manipulated message gets penalty points. When the number of points reaches 100, the IP address is blocked for 24 hours [116]. Because an attack can come from multiple IP addresses, for example from a botnet, bitcoin sets up further rules against DoS[52] attacks, such as the following:

- Not to forward orphan transactions and blocks to other users,
- Not to forward transactions whose contents (bitcoins) have already been exhausted (double spend transactions),
- Not to resend a message (transaction, block, address of another user) to the same user,
- Not to exceed the block size of 1 MB.

[51] Stellar Consensus Protocol (SCP).
[52] Denial-of-Service.

2.4.2 Flood Attack – Spam Transactions

The attacker generates several transactions and sends them to himself. The goal is to fill the new block with his own transactions and thereby delay the acceptance of transactions from other users. No transaction fees are involved.

The bitcoin system, however, allows only five percent of fee-exempt transactions in a block. This means that an attack is only possible if the attacker is willing to spend his bitcoins to carry it out [67].

2.4.3 51 Percent Attack

A miner with a large computing capacity (hash rate) can create new blocks faster than other miners with a lower capacity. When an attacker has more than 50 percent of the entire computing capacity of the network at his disposal, the following blockchain manipulation are possible:

- to monopolize the mining of new blocks and to keep the reward gained for himself alone,
- to force the creation of his own blockchain – which is also the longest chain,
- to includ only his own transactions in the blocks or to block the transactions of specific users (i.e., not accepting them in the blocks),
- carrying out double spending[53]. In generating blocks, the miner needs to verify if the values were already "given out" by the user in earlier transactions (i.e., if he is the owner). The attacker can ignore this rule in generating blocks and reuse values that he has previously issued.

To change earlier blocks, an attacker must recalculate from the block to be changed through the whole chain (blockchain) that is, regenerate all of the previous blocks starting back from the last block. In this case, the attacker can only change the order of the transactions in the chain or take them out; however, no new values can be generated (e.g., bitcoins, only by reward). Nor can values from other users' transactions be redirected to him. This is only possible if the attacker has the users' private key [115].

Lightweight nodes do not have a full blockchain and are unable to guarantee complete verification of the transaction contents. They are forced to trust the miner and are consequently not as secure as full nodes [67]. Both the PoW and PoS concepts are vulnerable to the 51 Percent Attack.

Such an attack will likely mean a great expense for the Bitcom system. According to BTCECHO, this type of attack can cost around 375.2 million euros a day [37]. Profit-oriented attackers thus prefer a cheaper alternative.

In the Bitcoin system, mining pools have the largest share of computing capacity 2.21).

[53] For more information on this topic see [139].

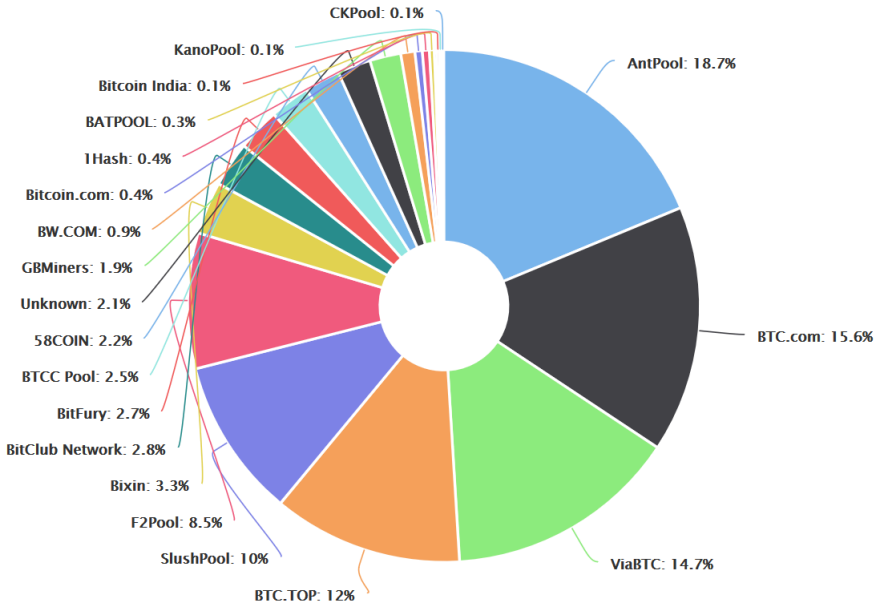


Figure 2.21: Market share of largest bitcoin mining pools, as of 1 Dec. 2017 [69]

In July 2014, the Ghash.io mining pool achieved more than 50 percent of the computing capacity of the Bitcoin network. The Bitcoin community reacted by introducing specific restrictions. Currently, an agreement exists between the mining pools of not exceeding the 39.95 percent limit. A supervisory committee was also set up to oversee the computing capacity of the mining pools. It consists of mining pool representatives, Bitcoin company representatives, and other specialists from the field [108].

Nevertheless, the possibility still remains of attack being carried out in the whole network with less than 50 percent computing capacity. The success rate is correspondingly low [139].

2.4.4 Sybil Attack

The name of this attack method comes from the main character of the book[54] by Flora Rheta Schreiber, wherein the author describes a woman with a multiple personality disorder named Sybil. Similar to the case in the book, the attacker creates several fake "identities" (nodes, servers) in a distributed network with the intent of manipulating or disturbing network communication [17].

In the case of a blockchain network, such attackers generally forward only selected blocks and transactions thereby shutting off other users from using the network.

The Bitcoin system tries to get around this kind of attack by restricting outgoing connections (see section 2.1.3).

[54] Sybil – Flora Rheta Schreiber, 1973.

2.4.5 Tracing the Transactions

Tracing the transaction between senders and recipients is one of the most common problems in a blockchain network. Despite the use of pseudonyms (P2PKH addresses[55], see section 2.1.2), which can be specially generated for every new transaction, and despite the use of the TOR network, transactions can be traced to end users. The 2014 scientific work by Biryukov and Pustogarov describes a method for the de-anonymization of bitcoin users, whereby the bitcoin address and the sender's IP address are linked. This method also works if users have a firewall or use the TOR network. Changes have been made in other bitcoin versions based on this information [132].

It should also be noted that the IP addresses of many full nodes are public. This makes it easier to match transactions to IP address.

Mixing services (see section 2.1) offers more anonymity; however it also assumes trust in the service provider.

2.4.6 Gaining Unauthorized Access to the Private Key

In spite of the innovative and secure architecture of blockchain technology, and despite numerous safety procedures against many attacks, the bulk of security measures are ultimately left to the end user. The values in a blockchain (e.g., bitcoins) can only then be "issued" to a new user if the corresponding private key is available. With little effort and using standard tools, attackers can gain unauthorized access to the private key of a user if it is not adequately protected.

For this reason it is recommended that bitcoin users, for instance, forego the use of online services providing online wallets. Recently such services have suffered security vulnerabilities that made it possible for attackers to steal users' bitcoins [60].

Applications that are locally installed at the user's computer promise more security regarding private key storage. Many of them provide wallet encryption and regular backups.

A two-factor authentication makes private key protection even more secure. The identity of the user is checked by proving two components – for example, a combination of hardware wallet and the PIN or password.

The private keys are stored at an external data medium that requires a PIN or password for unlocking, and which is immune to viruses. The private key never leaves the storage medium. Transactions are handled at the data carrier. They are then signed using the corresponding private key. The signed transactions are then transferred to the application on the user's computer [63].

[55] Pay To Public Key Hash Address.

2.5 Scalability – Problem or Feature

Scalability is among the most important characteristics of distributed networks. It shows how performance varies with the change of the system's size and whether the system can grow loss-free.

2.5.1 System Growth – New Users

Because all transactions that were ever carried out in the system are recorded, the size of the blockchain grows continuously. In December 2017 the size of the bitcoin blockchain was 147 GB. A full node needs a complete copy of the blockchain to verify a received transaction.

One of the most important rules regarding the validity of a transaction is that the values contained therein (e.g. bitcoins) have not been "issued" before. In this regard, the full node verifies all earlier transactions in the blockchain up to the transaction where the values were last "assigned" [55].

As it is not in the interest of all users to provide great storage capacity and computing power, lightweight nodes are widespread in the bitcoin system. They save the block header and the information that affects their transactions. Based on the information contained in the header (Merkle tree), the user can verify whether the transaction has been included in a block and, if so, how many blocks are following this block. As lightweight nodes do not save any block contents (transactions), they must trust the full nodes in determining that the blocks and transactions are compliant and do not contain any double spent transactions. This means that the security of the system rests on the full nodes.

Currently, an estimated 13 times as many lightweight nodes as full nodes exist in the bitcoin system [116]. Both numbers are increasing at an uneven rate. Some full nodes operate mining. Many of them bundle their computing capacity with that of others and together they form mining pools. Those whose members come from countries with cheaper electricity, profit the most from this arrangement (e.g., China). Through mining-pools increases the risk of centralized mining [43].

For systems with higher data volumes, such as cloud storage and identity management, or for systems with lower storage and computing capacity, such as the Internet of Things (IoT), the possibility exists to implement blockchain only for logging changes in the system (logs). This is, for example, the solution of the company Blockstack (see figure 2.14), which offers an identity system and also adds additional components for the management and the storage of data to the blockchain.

In a consortium, or private blockchain, the role of full node can be taken over by the company. The customers then only have lightweight applications (more in section 3.1). Thus the problem of security and scalability can be solved. However, in this case the system is no longer completely decentralized as mining is centralized within the company.

2.5.2 System Growth – Greater Transaction Volume

In accordance with fixed rules, bitcoin transactions are summarized every ten minutes by miners into 1 MB large blocks. Generally, there are about 2,500 transactions in a block. As the miners want to earn as many bitcoins as possible, transactions with higher fees are prioritized. Users who pay little or no fees must therefore wait longer until their transactions are included in a block (at this time about an hour). This is an unfavorable situation for users who want to exchange smaller amounts of currency.

Disadvantages of this kind are intended to be remedied by off-chain transactions. Here, the transactions are exchanged outside the network (off-chain) via so-called micropayment channels and then summarized into one transaction. Only then are they sent to the network. In the third quarter of 2014, the micropayment technology was already being implemented in bitcoinj[56] version 0.10.

The idea of micropayment channels was pursued by Joseph Poon and Thaddeus Dryvja in Bitcoin Lightning Network technology. This technology allows scalable and immediately executable off-chain transactions.

Temporary micropayment channels are set up between users. As long as the channel is open, users can exchange transactions in large quantities and at high speed. After the agreed time, they can release these transactions (or a total transaction) to the blockchain.

The lightning network concept has the following advantages:

- Bidirectional Payment Channels. Two users open a "micropayment channel" by creating a so-called funding transaction. Hereby, they transfer a certain amount of digital coins to an address created in the context of the micropayment channel (2-of-2 multisignature address[57]). They have agreed beforehand on the sum to be transferred (for example: Bob and Charlie agree on 1.0 BTC and each transfers 0.5 BTC, thereby "financing the transaction"). In the case that there is no exchange of digital coins, but only one of the two users wants to carry our several small transfers, just this user's coins are sent to the address (e.g., Alice transfers 0.8 BTC to the 2-of-2 multisignature address with the intent of sending Charlie digital coins later in several transactions). After the financial transaction is created, several small transactions (commitment transactions) can be carried out from the address agreed upon by both users. The small transactions are used for updating the "balance" of both users in the channel. After the first small transaction between both users is exchanged, they are assured of getting their money back and release the financial transaction to the blockchain (with the input, consisting of the contributions of both users, and the output, consisting of the 2-of-2 multisignature script). As long as small transactions between users are exchanged, the micropayment channel is open. To end the transaction exchange, the last small transaction is sent to the blockchain [135].

[56] Bitcoinj is a Java library for working with the bitcoin protocol [31].
[57] 2-of-2 multisignature address, is also called 2-of-2 multisignature script or 2-of-2 output.

- Ability to revoke transactions (Revocable Sequence Maturity Contract - RSCMS).
- Possibility of either of the two users to close the channel.
- Transfer of only the last current transaction to the blockchain.
- Large network of micropayment channels. In the Lightning Network a secure transaction exchange is also possible between two users who have no mutual open micropayment channel. This becomes a path carried out over multiple network nodes (users) (similar to routing in the Internet, through several hops). The technology that allows this means of transaction is called Hashed Timelock Contracts (HTLC). For example, Alice has an open channel with Charlie, and Charlie with Bob. Alice and Bob want to exchange off-chain transactions. Alice then requests a hash from Bob and counts the nodes (users) between them. Depending on the number of nodes (between Alice and Bob there is only one node – Charlie) she sets a HTLC expiration time of two days. Charlie sets the HTLC expiration time with Bob for 1 day. Bob shares the hash value with Charlie and they thus reach an agreement on exchanging small transactions. Charlie and Alice undertake the same steps (see figure 2.22) [135].
- Reduced load on the blockchain. Only the opening transaction (financing transaction) and the closing transaction (last commitment transaction) are released to the blockchain. This allows Lightning Network users to exchange fast transactions without overloading the blockchain [29].
- Low fees for bidirectional channels. The substantially low fees in the Lightning Network are paid between the two communicating users in the channel.

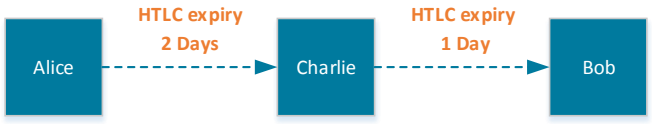


Figure 2.22: Network of the micropayment channels

After White Paper by Poon and Dryvia (January 2016) two blockchain startups, The Bitfury Group and ACINQ, started working with the Lightning Network technology. In July 2016, The Bitfury Group developed a hybrid algorithm called Flare[58], which can be used for payment routing in Lightning Networks. The French

[58] White Paper [136].

startup ACINQ conducted successful tests of the Lightning Network and of the Flare algorithm in September 2016.

The blockchain giants Bitcoin and Ethereum are also now working to implement the Lightning Network.[59] The framework for implementation in Ethereum is called Plasma [134].

2.6 The Right Application Promises Success

The use of a new technology in an existing system must bring distinct benefits (e.g., increase efficiency or lower costs). The cost-benefit ratio should be clear before the decision is made for blockchain technology and the objective clearly defined. It is always necessary to consider both the possibilities and the challenges of blockchain technology.

Blockchain technology allows value exchange in a decentralized system without the need of trust between the parties. The intelligence lies with the users and not with a central instance. The values, which are included in the block chain history, are unchangeable and irrevocable. Through its transparent nature, the history provides proof of when and by whom a value was owned.

A company can opt for a consortium blockchain if, for example, the responsibility for the consensus finding needs to remain in-house. It can decide on a private blockchain if the user is only to be granted certain permissions (for more on this subject, see section 3.1).

Blockchain technology also allows a value exchange with "if-then" conditions. This is possible by means of so-called "smart contracts" (see section 3.3).

The fact that blockchain technology is still relatively young and is developing quickly, means it is still missing the uniform standards needed by developers. Currently, developers focus on the Bitcoin, Ethereum and Hyperledger systems, which serve as the foundation for many blockchain applications.

A clear indication of the difficulties in practice is shown by the consulting company Gartner. Their studies have shown, most blockchain projects fail in the first 18–24 months [83].

Due to a lack of uniform standards, interoperability[60] between the various block chain applications cannot be ensured [83]. Currently, many researchers and developers are working on achieving and guaranteeing a balance between scalability and security.

If, after a critical analysis, blockchain technology is determined to be beneficial in achieving the objectives of a project, it is necessary to give attention to its technical realization and usage examples (see sections 3 and 4).

[59] More on this subject in [58, 71, 104, 74].

[60] Cross-platform compatibility.

3 How to Implement a Blockchain?

As soon as you have clearly defined what you want to achieve by implementing blockchain technology – and your goal corresponds to the possibilities and challenges of the technology – it is necessary to decide how to use the technology in the most efficient way.

Regardless of the goal or extent to which blockchain technology is to be introduced, it is crucial to have a clear understanding of its structure and operation.

The following aspects need to be considered:

- The values must be defined that are to be exchanged between the nodes (e.g., users or IoT devices) in the new system. In the normal case, these can be derived from the predefined use case[61] (see section 4).
- The user's authorization must be determined: Should all users have the same rights and thus form a decentralized system? Should only a part of the users – as determined by the company – be able to see the history of the blockchain and be involved in the consensus-finding process (e.g., updating the blockchain)? A distinction is thereby made between a public, consortium, and private blockchain (see section 3.1).
- On this basis it is determined whether an already existing blockchain (e.g., Bitcoin or Ethereum) is to be the foundation for a new system or if a new blockchain is to be developed (see section 3.2).

Because Bitcoin and many other blockchain projects are open source projects, systems with different consensus algorithms are available for duplication and modification. The term "fork" is important in this context. Any modification of an existing blockchain software that leads to changes in fixed rules (consensus protocol) is called "forking" (e.g., a bitcoin fork). When the blockchain branches off, the two branches that result have the same starting block (genesis block) and the same predecessor blocks.

There are two types of blockchain forking: the hard and the soft fork. In the case of the hard fork, the software changes must be accepted by all nodes (such as a change in the architecture of the blockchain e.g., an increase of block size from 1 MB to 2 MB). Several hard forks have already been implemented in the Ethereum blockchain. The first hard fork was implemented on July 20, 2016 and came about as the consequence of an attack one month earlier. The attacker had found an error in "The DAO"[62] framework, which resulted in the theft of 3.6 million worth of

[61] Cryptocurrency, record of ownership or complex systems with smart contracts.

[62] Decentralized Autonomous Organization realized at the Ethereum blockchain (see section 4.2 for more information).

Ether[63] (65 millions euro). The Ethereum developers tracked the error and decided on a hard fork update in order to recover the stolen Ether.

A soft fork affects changes in the blockchain such as new or updated functionalities that need to be accepted only by the miners and users who want to use them. In contrast to a hard fork, a soft fork is backwards-compatible. This creates many new application that use (for example) a bitcoin blockchain, whereby some functionalities are changed or added.

3.1 Private and Public Blockchains

The great interest of many companies in the blockchain and its implementation for different applications has resulted in numerous attempts to tailor the technology to fit one's own needs. A distinction is therefore made between public, private, and consortium blockchain.

In a public blockchain all users can send and receive transactions, see the history, as well as take part in blockchain updating (mining, minting, etc.). In cases where limitations are made in user authorization, one speaks of a consortium or private blockchain. The blockchain system is thus no longer completely decentralized.

In a consortium blockchain, the authorization to participate in the consensus finding process is limited to a group of users. The possibility to view the blockchain history can either be granted to all users or to just a specific group [20].

The private blockchain leads to further restrictions in user authorization. There is no longer a transparency of history – this is only possible for predefined users (e.g., in the realm of one company or distributed among multiple companies). The authorization to update the blockchain and create transactions is limited to one group of users.

Changes in the software are simpler and faster to carry out in private blockchains. Those users who are allowed to update and verify the blockchain are already known. However, the risk of a 51 Percent Attack still exists, even if modified. Users who are chosen in advance for the update of the blockchain and participation in the consensus-finding process can still be manipulated by possible attackers [106].

Every type of blockchain has its own advantages and disadvantages, which have a stronger or weaker affect depending on the application area.

3.2 Blockchain: Types of Application

Based on information such as desired blockchain application, value transfer, user authorization, or possible/planned expenses, a decision can be made concerning the desired implementation of blockchain technology. Numerous projects and providers on the market support companies who are using blockchain for the first time. A company must ultimately decide whether it is seeking to develop its

[63] Ether – Cryptocurrency of Ethereum.

own blockchain solution or if it can use an existing blockchain (e.g., Bitcoin or Ethereum).

In principle, the possibility exists of either having one's own miners or operating merged mining. Merged mining is the process whereby a miner operates a blockchain for several systems simultaneously [76]. This means that miners of one blockchain generate blocks for several other blockchains. For example, the blocks of the "Namecoin" blockchain are built by the bitcoin miner. Each blockchain has its own "difficulty".

Here are the best known methods.

3.2.1 Colored Coins

The "colored coins" method is the simplest way of using blockchain technology. The method's principle is that it builds on an existing blockchain[64] and additional information (metadata) is then added to the existing values (more precisely, to the UTXO[65]). The original digital coins (e.g. bitcoins) are therefore linked ("colored") with other information and thereby get another semantics/usage. For example, after additional information is added to the bitcoins, these can have new values such as a certificate, stock share, movie ticket, a rented apartment or a digital key for a house or a car [85].

The nodes that exchange the colored coins use a colored coin application and know the coins' value or property. The blockchain miners or minters, however, cannot recognize the "color" of the digital coins and view all incoming transactions as standard transactions. For this reason, the added information (metadata) should be verified by users on their own.

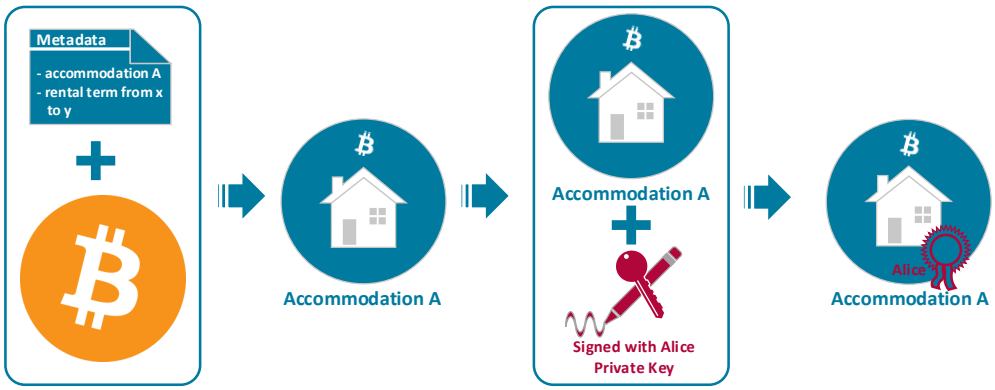


Figure 3.1: Colored coins method based on the Bitcoin blockchain with a new value (apartment for rent)

[64] The most commonly used blockchain for the colored coin method is the Bitcoin blockchain.

[65] Unspent Transaction Output (UTXO).

Coinprism is a well-known provider of "colored coin wallets".

Since December 2015, the largest US stock exchange platform NASDAQ[66] has used colored coins in its platform LINQ. The LINQ platform offers a service for secure private transactions, and through blockchain technology allows an overview of all previous owners. The colored coins are exchanged between private investors and/or banks and linked to securities.

Colu, an Israeli provider of blockchain-based technologies, relies on colored coins in connection with Lightning Networks. This allows a decentralized value transfer with a minimum verification time, as well as a high rate of transactions per second and low fees [48].

3.2.2 Meta Coins

Because the miners of the Bitcoin blockchain do not recognize the "color" of the colored coins and see all incoming transactions as standard transactions, the added information (metadata) needs to be verified by the colored coin users on their own. Meta coins offer an improvement over the colored coins protocol. Like colored coins, meta coins can also represent arbitrary values and are created in an existing blockchain. The difference between these two methods is found in a middleware[67] layer in the form of dedicated servers (which verify the colored coin transactions) [125]. These will be built on the existing blockchain. The meta coins method allows more functionality when compared to colored coins.

3.2.3 Alternative Chain

Alternative chain, or "altchain", is a separate and independent blockchain that is not built on an already existing chain (e.g., Bitcoin). Since Bitcoin and many other blockchain projects are open-source projects, the source code of blockchain is available with different consensus algorithms for duplication and modification.

In an altchain, the blockchain units[68] can have arbitrary values from different application areas. For example, these could be digital coins (altcoins). The blockchain rules can be adjusted: more data can be transferred, the block size changed, the speed of block creation increased and a matching consensus algorithm selected.

While benefits can be achieved through these changes – such as a higher number of transactions per second – weaknesses in security can also occur.

3.2.4 Sidechain

The intention of developing new blockchain system, and designing them for novel application has led to more and more changes and adjustments in the original

[66] NASDAQ – National Association of Securities Dealers Automated Quotations.

[67] According to the Duden dictionary, middleware is a software for data exchange between application programs that work under different operating systems or in a heterogeneous networks.

[68] Also called scarce tokens or ledger assets.

Bitcoin code and allowed the creation of many altchain projects. Besides security issues, altchain developers encounter further complications in the area of "interaction between the blockchains", such as interoperability (every altchain implements the technology in its own way) or the fluctuating exchange rates of a new cryptocurrency (altcoin) [114].

The authors of "Enabling Blockchain Innovations with Pegged Sidechains" [114] describe a new mechanism that allows the easy development and use of an interoperable altchain. Using this mechanism, the units of a blockchain can be transferred to another blockchain – the "sidechain". A sidechain is a blockchain that can recognizes and check data from other blockchains [114].

The idea of interconnected blockchains (also called cross-chains or inter-chain transfer) already existed before this study [114]. The procedure[69], known as an "atomic swap" or "atomic exchange" was familiar to blockchain developers as early as 2012. Tier Nolan developed it further in 2013 (see appendix 6.5).

The sidechain technology was introduced by Adam Back in 2014 [114]. The core idea lies in so-called "pegged sidechains". In contrast to the sidechain, a pegged sidechain is able to transmit back the data received from another blockchain. This mechanism is called the "two way peg" and allows a transfer of blockchain units between sidechains in both directions – at a fixed exchange rate. Thus without directly acquiring new blockchain units, the user can test a new blockchain through the "transformation" of existing units.

The two-way peg mechanism is separated into two types:

- symmetrical and
- asymmetrical.

The difference is found in transaction verification. The symmetrical two-way peg mechanism supports SPV[70] verification at both blockchains – "parent"blokchain and sidechain. This means the two blockchains "know" each other. In the asymmetric procedure, SPV verification is done only on the parentchain. The parentchain does not "know" the sidechain and must make a SPV verification of the sidechain data. Whereas users of the sidechain are completely knowledgeable about the parentchain and need no SPV evidence of the parentchain's data.

For example: Alice has bitcoins and wants to have a different cryptocurrency or certain values from another blockchain (in our case, a sidechain). She uses the symmetrical procedure to do this. She creates a transaction whose output has a certain address in her parentchain (in this case a bitcoin blockchain), where her bitcoins are blocked initially for a confirmation period(1-2 days). After the confirmation period has expired, a transaction is created at the sidechain that refers to the output from the bitcoin blockchain and supports a SPV proof. Using a

[69] Contracts with a Secret-exchange and Lock-Time-Parameter have been used for this procedure.

[70] SPV – Simplified Payment Verification Proof gives users the possibility to verify transactions without downloading entire blockchain (e.g., using block headers). Before a transaction is added to the wallet, the user checks whether the transaction is in the block and whether the block is in the main chain.

fixed conversion rate, the bitcoins are calculated in sidechain values/units. Then the units are blocked for another one to two days in the sidechain for a "contest period", which is intended to prevent double spending. After the contest period, the sidechain values/units are available to Alice (see figure 3.2). They contain information about her parentchain (bitcoin) and can be transferred back in the same way (also with blocked output, confirmation and contest periods as well as SPV proof).

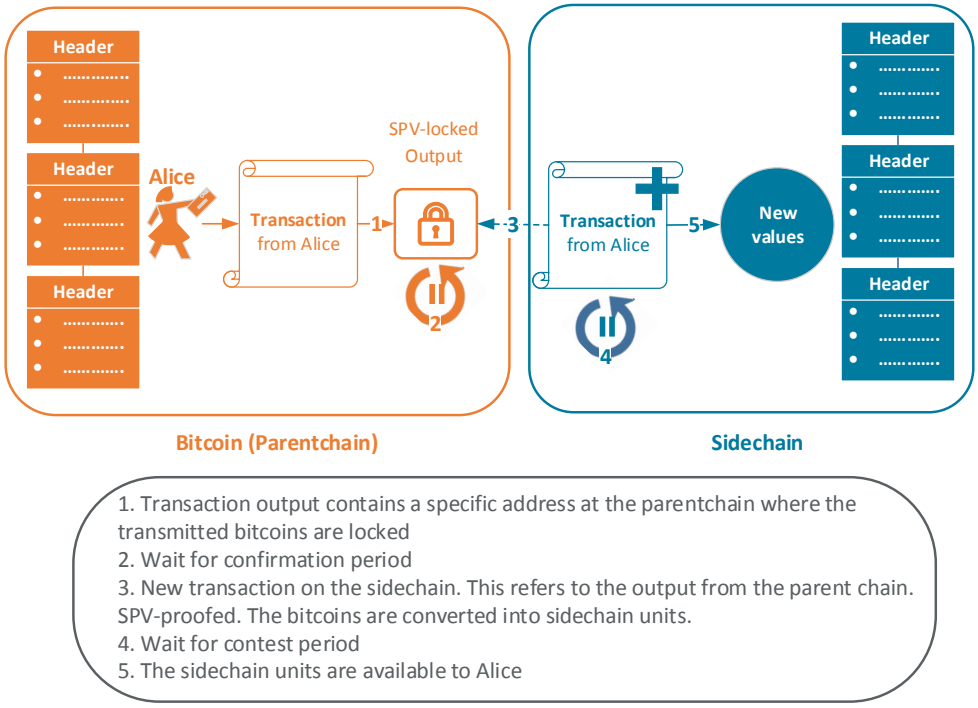


Figure 3.2: Conversion of bitcoins into sidechain units

Security is an important factor in the transfer of blockchain units to the sidechains. The receiver chain must be able to recognize that the units of the sender chain are correctly locked.

Generally every blockchain can be tailored to interact with sidechains. The blockchain units can be transferred between several sidechains and back to the parentchain. To be able to use Bitcoin as a parentchain, an extension (soft fork) must be implemented in the Bitcoin system in order to recognize and validate SPV proofs.

The disadvantages of the sidechain technology have already been clearly described by its developers:

- Complexity,
- Risks of fraudulent transmissions,

- Risks of the centralization of mining and
- Risks of the soft fork (any change to the existing system can result in security problems) [114].

In the publication year of the sidechain papers, the authors founded the company Blockstream to advance the technology and develop sidechains for different projects.

A project that started in 2015 called Rootstock[71] uses sidechain technology and offers a platform for smart contracts. The Rootstock sidechain has a two-way peg connection to the bitcoin parentchain, does not have its own cryptocurrency, and passes on the transaction fees for merged mining to the bitcoin miner. The blocks in the Rootstock sidechain are generated every ten seconds.

3.3 Smart Contracts

Smart contract technology is among the recent blockchain developments. Its use is not limited to cryptocurrency, but the technology is often employed as a programmable decentralized trust infrastructure [27].

Ethereum is one of these Blockchain 2.0 applications and has the most commonly used and strongest blockchain after Bitcoin. Ethereum uses a programming language[72] for the creation of so-called "smart contracts" and decentralized applications (called "dapps" for short). It allows for the implementation of arbitrary rules, transaction formats and functionalities [81].

Ethereum developers compare smart contracts to cryptographic "boxes" containing fixed values. These values can only be unlocked when specific conditions are met.

Smart contracts are complex autonomous applications[73] that run specific parts of the source code with "if-then" conditions according to specific instructions[74]. For example, if a potential tenant has paid the money for a rental apartment and the first day of rental arrives, a digital key is sent to the tenant to unlock the apartment [34].

Smart contracts have control over their content and components, for example over the contained values, conditions, and cryptocurrency, which can be used for system-dependent fees. Smart contracts are written in a high-level programming language and subsequently translated into a bytecode [103]. The result is added to a transaction. Just as users do, smart contracts have their own addresses (so-called "accounts"). They can be contacted by other contracts through special messages or by users through transactions. Accordingly, this means that both the user address and the smart contract address can be specified as the destination of a transaction.

[71] White Paper [128].
[72] High-level programming languages like Solidity, Serpent, LLL etc. [42].
[73] Smart contract applications contain script instructions such as contracts and time locks.
[74] Messages received from other contracts or transactions from other users [81].

A virtual machine (EVM) is run on the computer of every Ethereum user that allows the reading and writing of data and code from and in the blockchain as well as the verification of digital signatures. The EVM only runs the code from the smart contract if it contains a signed message and if the information from the blockchain history confirms the execution [77].

The concept of smart contracts existed long before the development of blockchain technology. As early as 1997, the term "smart contract" was defined in Nick Szabo's work "Formalizing and Securing Relationships on Public Networks" [141]. The author describes smart contracts as a combination of protocols and user interfaces for ensuring the legally and cryptographically secured relationships between nodes in a computer network. According to Szabo, the contracts automatically executed by the computer should substantially reduce processing costs – in contrast to their paper-based predecessors.

A well-known example for the use of smart contracts is car rental or car purchase on credit. The car is provided to the renter or purchaser based on the conditions stated in the smart contract. If the purchaser does not pay off a credit rate punctually or if the rental period has expired, the car can be blocked for the user.

An advantage of Ethereum, in comparison to Bitcoin, is its multi-signature method ("multsig"), which allows more flexibility. In the Bitcoin system, users can, for example, unlock a credit balance with three of the five private keys. In contrast, by virtue of the smart contract the Ethereum user has the possibility to access the entire balance with four of the five private keys and ten percent of the balance per day with three of five keys and 0.5 percent per day with two of five keys per day. Ethereum users can sign a transaction independent of each other. In this way, the transaction will be automatically sent out after the last signature [81].

It is important to note that when only one private key is used, there is also only one weak spot [94]. On July 19, 2017 a failure was found in Ethereum's multi-signature wallet and exploited by attackers. A group of white hat hackers were enlisted to protect other wallets from possible attacks [80].

Increased flexibility in smart contracts is provided by so-called "oracles". Oracles serve as a bridge to the "real world", making its information available to smart contracts [70]. For example, for the exchange of US dollars into BTC, an oracle for conversion with the respective, current exchange rate is included in the smart contract [81]. The London startup Oraclize offers a service for the connection of blockchain data with external information from the Internet (see figure 3.3). One of the projects from Oraclize is "Proof-of-Identity" [98], whereby an Ethereum address is connected with an Estonian digital identification number (Digi-ID).

In summary, smart contracts can be considered special programs that are created and verified in a decentralized way by users with the help of provided software. The most important challenges faced by smart contracts are their legally binding nature, liability and data protection. Who bears the responsibility when an error slips into the smart contract code? Or, how can the legality of a smart contract be proven in the real world?

A solution for the problem of legal liability in smart contracts, as discussed in section 2.1.5, is presented by a company called Agrello [57]. With a user-friendly interface (see figure 2.13), Agrello's product provides support during the creation of a legally binding contract. The contract created with the help of this solution

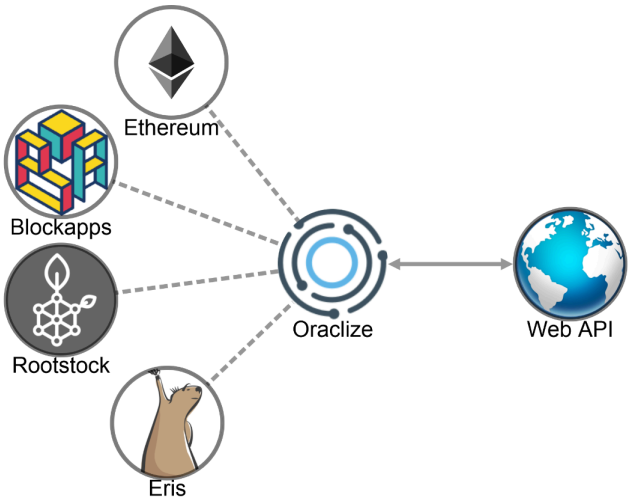


Figure 3.3: Oraclize – Data "courier" for decentralized application

is converted into a smart contract and stored in a blockchain. At the same time, a legally-binding contract in natural language is drawn up and digitally signed [57]. During contract creation, the user is supported by an AI[75] agent.

Smart contracts offer a wide range of application possibilities – from token-based systems[76] to decentralized autonomous organizations (DAOs). The tokens can represent different values such as currency, possessions, events, or properties [81].

"The DAO" is the name of an application that was implemented as a smart contract on the Ethereum blockchain [52]. It had no central management institution and was based on the fixed rules recorded in the code – for all means and purposes a company without employees. "The DAO" was essentially an investment company that carried out crowdfunding solely through a voting process. Following a July 2016 attack, which exploited an error discovered in the code, "The DAO" was discontinued.

The company Ripple has recently planned to offer its own decentralized application on the basis of smart contracts and "oracles" [16].

[75] AI – Artificial Intelligence.

[76] A token is a tool for the synchronization of parallel processes – whoever has the token can access the resources. When a user releases the token, the resource is then available to another user [112].

4 Projects and Application Areas of Blockchain Technology

It is amazing how fast blockchain technology has spread. The many tests and projects show us that there is virtually no application area with decentralized infrastructure where an attempt has not been made to introduce blockchain. Science, medicine, identity management, cloud computing, the Internet of Things, banking, insurance, logistics, retail, energy provision – these and other areas have been benefitted from blockchain technology. A large number of startups were founded offering blockchain as the total or partial solution, using thereby either an existing blockchain (e.g., Bitcoin or Ethereum) or developing their own. But also companies with developed infrastructures and established products and services, such as IBM, Microsoft, Samsung, SAP, Intel and others, have been experimenting for a long time with the technology and launching new projects.

For example, OpenBazaar uses blockchain technology for P2P online trade. Each node can act as a buyer or seller and pay for the purchased goods in bitcoins. The procedure, signing of transactions to confirm ownership of objects, and implementation of smart contracts are also suitable for other areas of application for example:

- The fine arts: For the purchase and sale of paintings at auctions it is easy to verify the origin, previous owners and current owner (when, where, and from whom the item was purchased).
- Booking and renting private accommodations as well as cars and bicycles: Providers such as Airbnb and Uber can especially particularly benefit from use of blockchain technology.
- Voting systems: In collaboration with BitShares, FollowMyVote offers a voting platform on the basis of blockchain technology. The system provides a secure guarantee that cast votes cannot be changed by third parties, in addition to transparency and flexibility. The voting process can now be carried out from mobile devices anywhere.
- Medicine: The use of blockchain technology in the medical field offers more than just a digitized patient file. New technologies, such as wearable devices like fitness wristbands or smart watches, generate more and more new health data. Therefore, the importance of secure and digitized patient data storage with the right of limited accessibility for certain data cannot be underestimated. A smart profile can give patients the option of deciding whether to share and release their personal data. Moreover, via blockchain it is also possible to share anonymized data with researchers (Public Research Repository), learn more about one's own illness, communicate with others who are also

affected, operate donor acquisitions or crowd funding, and get an overview of prescriptions and billing [18]. In May 2017, at the blockchain technology meeting "Consensus 2017" in New York, the Los Angeles-based startup Gem presented the first blockchain product for the management of health data (see figure 4.1) [84].

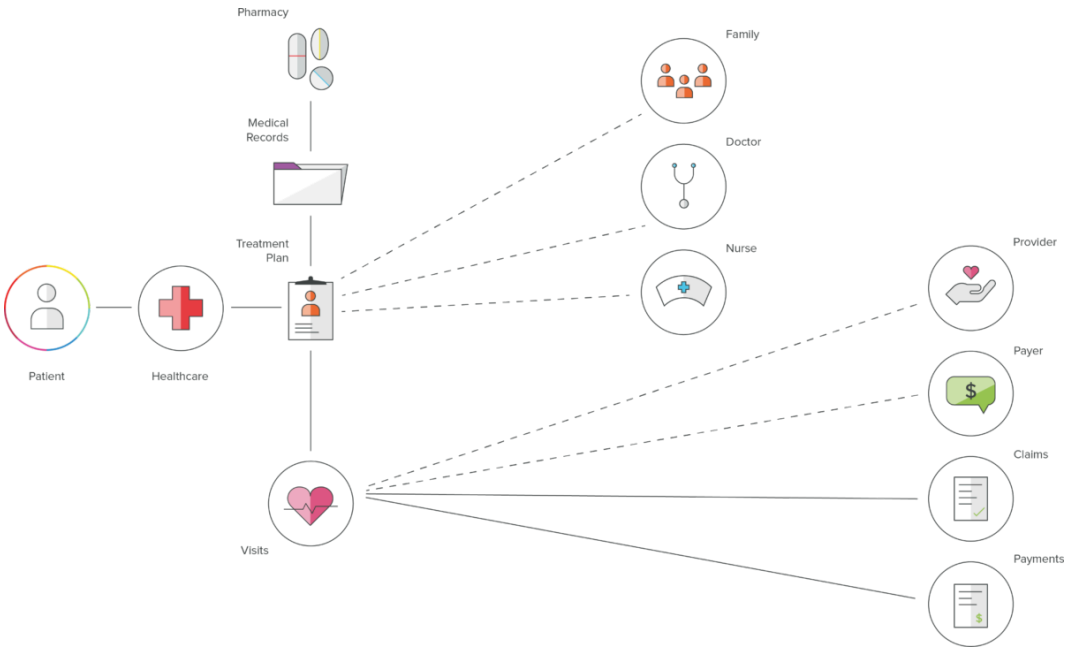


Figure 4.1: Gem – blockchain for health data [84]

The company Encrypgen offered secure access to anonymized genome data with its Gene-Chain.

Social networks and the free press also benefit from blockchain technology. Steemit is a blockchain-based social media platform where users publish their contents (e.g., messages) and are rewarded by other users in the platform's own cryptocurrency. Steemit also inspired another project called Publicism whose goal is to enable freedom of expression and to provide journalists a platform for anonymous and secure publication. Journalists are rewarded with micro-payments, collected from donations and crowdfunding. Thanks to blockchain technology, censorship from a central instance can be eliminated [99]. One of the challenges in the project is the absolute anonymity of its users (e.g., journalists).

Another blockchain solution is not only directed at a particular target audience, but sees itself as a "person layer" in a decentralized protocol stack. In this sense, the Colony company offers an infrastructure for the development of open organizations. The Colony protocol is an Ethereum smart contract. It allows developers to integrate decentralized and self-regulating work allocation, decision making and financial management in their applications. This means that the Colony solution allows the creation of anonymous and decentralized organizations whose employees come

together from all over the world digitally for one or more projects and are rewarded according to their engagement [75].

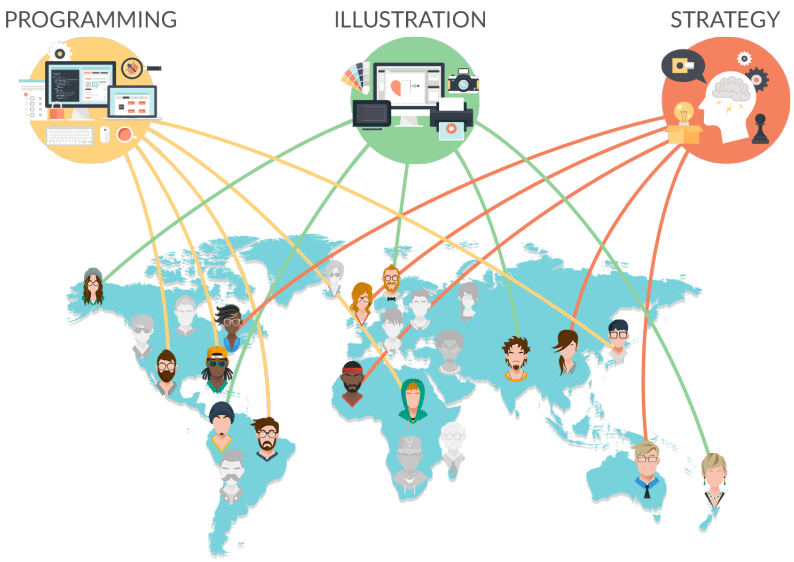


Figure 4.2: Colony approach [1]

The company Peerism, on the other hand, focuses on the competencies and skills of individuals, adding so-called "skill tokens" to them, with the aim of bringing people together with jobs. The beta version of the Peerism solution is presented in the first half of 2018. It is based on an Ethereum smart contract [95] and can compete with another business networks such as LinkedIn or Xing.

With new blockchain solutions, developers are continually striving to make existing processes more efficient. Thanks to the rapid progress of technology, the currently existing blockchains will continue to undergo further development.

One such example is Gridcoin [86], whose developers offer an alternative to the one of the biggest points of criticism of the Bitcoin system – energy consumption. Their cryptocurrency is used for a worthy cause, as Gridcoin's consensus algorithm was originally designed to support scientific projects in the BOINC[77] framework. The algorithm DPoR (Distributed Proof-of-Research) links the Proof-of-BOINC (PoB) and the Proof-of-Stake (POSv2) algorithms. PoB is similar to the Proof-of-Work algorithm. Instead of just calculating a hash – and consequently expending a large amount of energy for nothing – the computing capacity is made available for scientific purposes. Miners are named within the framework of the PoB researchers and use their computing capacity (CPU, GPU, etc.) to solve tasks from BOINC projects in different areas (physics, mathematics, medicine, etc.).

[77] BOINC (Berkeley Open Infrastructure for Network Computing) is one of the opensource frameworks developed by the University of California, Berkeley for various distributed computing projects [50].

Compared internationally, the biggest hot spots on the blockchain startup scene are the US and UK, followed by Canada, the Netherlands and China [121] (see figure 4.3). For example, the US company Ripple has been active in the financial sector since 2013 and offers a blockchain-based real-time money transfer service. It supports various "fiat"[78] and cryptocurrencies (dollar, euro, yen, bitcoin, etc.). Chain is another US startup from the area of finance and was founded in 2014. It offers a blockchain platform for financial services.

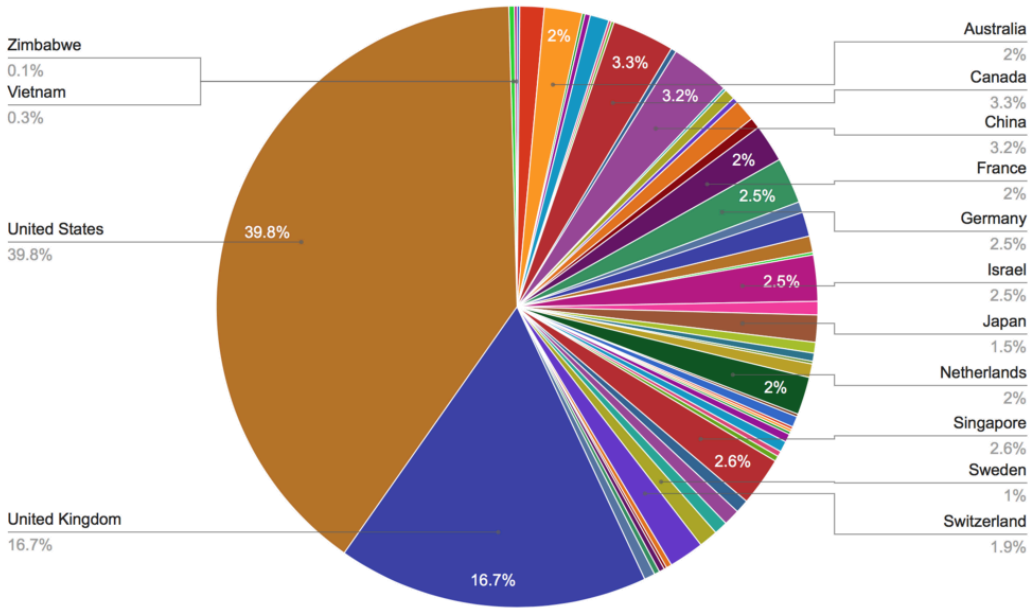


Figure 4.3: Breakdown of blockchain startups by country [49]

Eris Industries is a well-known startup that began in the UK (from October 2016 known as Monax Industries and headquartered in the US). Eris provides a platform for the development, testing and operation of blockchain-based applications.

Numerous applications either have their own blockchain as a foundation, or use already existing and widespread blockchains such as Bitcoin or Ethereum.

The pursuit of blockchain is not just carried out by individual companies; several countries are also dedicated to the topic on a national level. In the report "Backing Australian FinTech", Australia's government welcomed a 2016 initiative by the Australian Securities Exchange (ASX[79]), who introduced blockchain technology for its clearing and settlement processes.

[78] Fiat currency, or fiat money, is money that is not covered by assets. It is used as a medium of exchange but has no value of its own. Today's systems of currency are usually not covered by raw material. For example, money issued from a central bank, such as the dollar or euro is called fiat money.

[79] ASX is the Australian Stock Exchange, based in Sydney.

> "The Government welcomes the announcement by the ASX that it is exploring Blockchain technology for a new post-trade solution for the Australian equity market. While it is in the early stages of development, the technology has the potential to radically simplify the way our market operates end-to-end, with significant benefits to investors, participants, regulators and government agencies." [123]

In addition, the International Organization for Standardization (ISO) is planning to support Australia in the development of new international standard for blockchain technology. Australia's finance minister Scott Morrison said on the subject: "Establishing standards around this emerging technology will provide a common language for industry, policy makers, regulators and technology developers. This will provide a basis for ensuring interoperability as this technology becomes more widely used [130]."

In Europe, Estonia is among the pioneers in the field and has deservedly earned the name "e-Estonia". As early as 1999, the Estonian cabinet has been working paperless [56] (see figure 4.4). Since the advent of blockchain technology in 2008, the Estonian government has been experimenting with it, and it has been used in Estonian registries since 2012. Blockchain has been introduced, for instance, in the health care sector, in the parliamentary and judicial spheres, and in the field of security. Estonia uses its own blockchain called KSI Blockchain (see appendix 6.6). The technology is also used by NATO, the US Department of Dense, and the EU Information System for Cyber Security [79].

"In fact, blockchain has the power to transform almost every aspect of our lives – improving democracy and providing greater opportunities – but it may only be possible to unleash this full potential with the support and co-operation of governments," said the managing director of the digital Estonian registry e-Residency, Kasper Korjus, in an article entitled, "Welcome to the blockchain nation". Here he explains how the government can contribute to exploiting the full potential of blockchain technology [96].

In Germany, a Blockchain Federal Association was established in Berlin on June 29, 2017, with more than 20 working groups involved. In October a position paper was published with recommendations for making Germany a global player in the worldwide blockchain ecosystem [72].

Among other nations, Sweden has expressed its interest in blockchain technology. The government in Stockholm plans to introduce a blockchain-based title registry. The city of Arnhem in the Netherlands calls itself Bitcoin City. And it is in fact possible to pay there with bitcoins in many shops, cafes and bars.

In the following, the application areas and projects where blockchain technology is used most often are explained in detail.

4.1 Finance

The very first and most important application of blockchain technology is finance. A variety of cryptocurrencies have been created since the introduction of bitcoin;

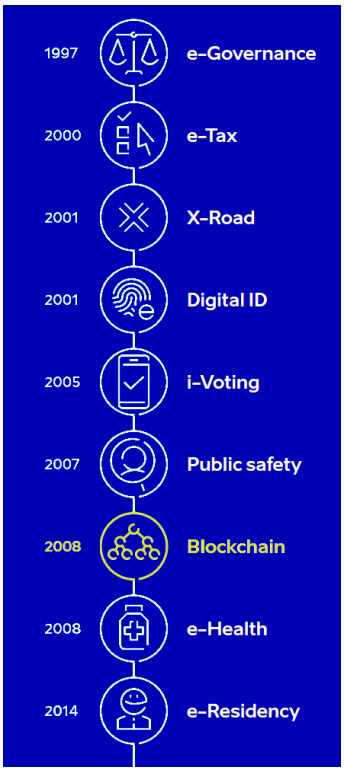


Figure 4.4: Estonia's path of digitization [79]

however, but not all of them have been able to survive. The best known and most widespread cryptocurrencies are:

- Litecoin (2011, PoW),
- Namecoin (2011, PoW),
- Peercoin (2012, PoW und PoS),
- Primecoin (2013, PoW),
- XRP von Ripple (2013, RPCA[80]),
- Nxt (founded in 2013, PoS),
- BlackCoin (2014, PoS).

Besides NASDAQ[81] in the US and ASX[82] in Australia, many financial companies are already using blockchain technology. A number of so-called blockchain consortia have emerged whose participants are financial companies. The Japanese

[80] Ripple Protocol Consensus Algorithm.
[81] NASDAQ – National Association of Securities Dealers Automated Quotations.
[82] ASX is the Australian Stock Exchange, based in Sydney.

blockchain consortium BCCC has already over 100 members [36]. The blockchain consortium R3, with its headquarters in New York, already numbers over 70 members. In Taiwan a consortium is being started that is supported by Microsoft [47]. Currently a large number of banks (e.g., Deutsche Bank, Santander, UBS, Barclays Bank) are experimenting with the technology [46].

The majority of financial service companies are primarily interested in blockchain technology for the possibility of transaction exchange with each other. Some banks, however, also use blockchain in customer-oriented solutions.

Blockchain solutions in the finance sector are mainly applications using smart contracts. Companies such as Starbase and WeiFund operate blockchain-based crowdfunding for startups and projects. In 2016, BNP Paribas Securities Services started a blockchain-based pilot project with France's leading crowdfunding platform provider – SmartAngels [35].

A company called Circle enables blockchain-based P2P money transfer, thus offering an easy way to carry out transactions in current money currencies (fiat money). The Clearmatics company offers a new, clearing platform based on blockchain technology for the OTC stock market (markets in over-the-counter trade) [39]. Financial companies provide the startup chain with blockchain-based solutions that allow the creation, signing, and validation of transactions in milliseconds [38].

Eris from the Monax company is a further platform that offers the development and operation of blockchain-based applications for business ecosystems.

Numerous companies are also springing up around the Bitcoin system and providing services for the trade and the use of its cryptocurrency, for example itBit and XAPO.

4.2 Decentralized Autonomous Organization

As described, blockchain technology makes possible the realization of so-called decentralized autonomous organizations (DAO). This means an organization functioning without a managing director or central management body, or a headquarters, but instead relying on a decentralized structure with automated decision-finding according to fixed rules. These rules are set up based on the majority decisions of the involved members and developed constantly [41]. DAO is realized through an open source software (the code is freely viewable). The consensus protocol is based on a set of rules that make it possible to achieve unity between participants (e.g., in the case of a forking chain), and to ensure security in the face of attackers, as well as to operate and further develop the blockchain (create new blocks, expand software).

DAOs buy products and services in agreement with their smart contracts from third parties – so-called contractors. Payment is made in cryptocurrency. The products and services are produced by contractors according to specifications and, in turn, used or marketed by the DAO. Through the marketing of these products and services, the DAO earns money that can be reinvested or divided among its shareholders [9].

The first decentralized autonomous organization was called "The DAO". Because of an error in the code it could be manipulated and, as a result, lasted less than a

year. After a number of software updates, which were designed to attempt to fix the bug and the consequences of the attack, "The DAO" was dismantled.

4.3 Hyperledger

Hyperledger is an open source consortium. It was founded in December 2015 by the Linux Foundation to advance cross-industry blockchain applications. In 2017, there were about 170 members. Hyperledger is a worldwide cooperation, consisting of leading companies in the areas of finance, banking, the Internet of Things, supply chains, manufacturing and technology as well as over 400 programmers. The Hyperledger consortium is one of Linux Foundation's fastest growing cooperation projects. Hyperledger supports various projects in different application fields to ensure the interoperability of various blockchain business solutions. At the present time, the consortium provides five open source blockchain frameworks[83] and four open source blockchain tools with smart contracts, client libraries, graphic interfaces and sample applications. Using these frameworks and tools, companies can implement blockchain-based applications and services for their business areas [90].

4.4 Cloud

In some sources, blockchain technology is considered a distributed database. This designation alludes to the property of distributed data stored at multiple machines. As blockchain technology needs no central instance for data storage and data management, every full user has a complete and identical copy of the blockchain at his machine. The protection against manipulation of the contained data makes the technology attractive for distributed cloud solutions. At the same time, the question of data protection and privacy is raised, as blockchain technology ensures the transparency of its contents.

A company called Storj offers a solution to this problem. Storj is a provider of P2P cloud storage with client-side encryption. Users who make their storage space available are called "farmers" and are rewarded with Storj coins (Storj's own cryptocurrency). The data set to be kept is first encrypted and then disassembled into multiple parts called "shards" before being stored in the Storj cloud. A so-called "salt"[84] is added to each shard and a hash value generated. This value is referred to as a pre-leaf in a Merkle tree. Finally, hash values are generated from pre-leaves, which are referred to as the leaves of the Merkle tree. From the leaves, first branches and then a Merkle root are calculated (see figure 4.5).

The root, salts and depth of the Merkle tree are stored at the owner of the file to be sent. The leaves of the Merkle tree are sent to the farmers along with the shards. The owner of the data set can decide how it is to be split into shards and where

[83] A framework is not yet a finished program, but provides the structure in which the programmer creates an application. The design pattern used in the framework, among other things, affects the structure of the individual application [107].

[84] Salt is a random string added to a given plaintext before a hash function is used [111].

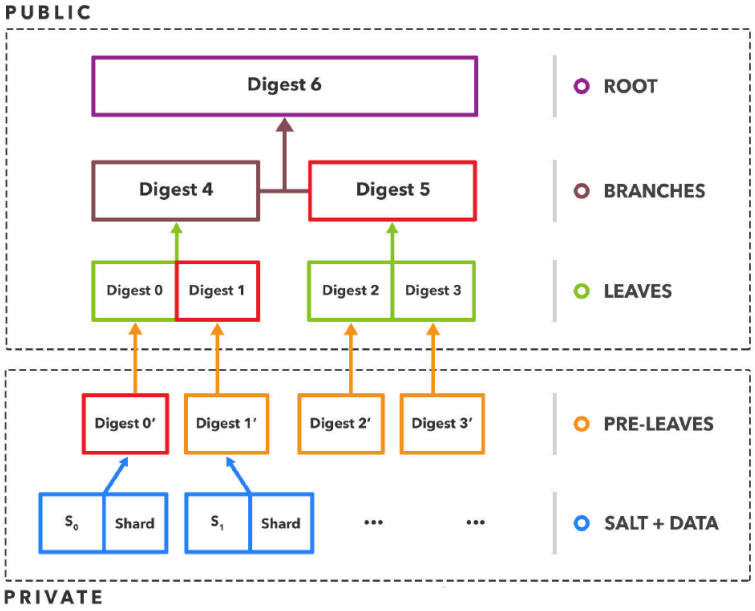


Figure 4.5: Storj Merkle tree [143]

the shards are to be saved in the network. Users should thereby be aware of the possibility of redundancy[85] [143].

Microsoft's Azure[86] offers several blockchain based solutions as part of its blockchain-as-a service concept. IBM also has a blockchain-cloud service, which is available via the Blumix platform.

Acronis, a provider of hybrid cloud data protection and storage solutions, also relies on blockchain technology. On October 20, 2016, the company announced a new product called "Acronis Storage". The solution is designed for heterogeneous standard hardware and includes Acronis CloudRAID and Acronis Notary with blockchain, which provide controllable redundancy and secure proof to ensure that stored objects have not been modified [26].

4.5 Identity Management

Due to the ever increasing number of digital services in the Internet, and the associated amount of registration data, digital identity management is becoming increasingly important. Despite prevailing user-friendly standards, it is essential that a secure infrastructure can be guaranteed. In the future, digital identities can, and are likely to, replace physical identification.

The biggest weaknesses of current identity management are:

[85] For example, simple mirroring or "K-of-M erasure coding" can be used. "Reed-Solomon erasure coding" is planned to be used in the future [143].

[86] Collection of integrated cloud services.

- Security defects,
- The necessity of an individual digital identity for each web service. It is much easier to give a partial authorization for specific data of single digital identity to the various services, than to create a new identity for every new service,
- Password management.

Following the Zookos Dreieck[87], a namespace[88] in a computer network can have only two of the following three properties at the same time:

- Decentralization – there is not a central trustworthy instance managing names,
- Security – authenticity must be guaranteed (if possible with a cryptographic key pair),
- Meaningfulness – human-readable names that can be chosen by people, rather than automatically generated as random strings [113].

Indeed, most of the current name systems support only two of the three properties. The blockchain-based Namecoin system, on the other hand, is the first name system to offer all three characteristics. The original application case of Namecoin was a blockchain-based domain name system. In registering names in the Namecoin system, a two-step confirmation method is used. First a hash of the name is requested, and subsequently the user data is registered. Namecoin allows user data to be updated [113].

In 2013, the project NameID was born. It connects both concepts, Namecoin and OpenID. The Namecoin identity is linked to an OpenID provider. Users who have the Namecoin identity can log in at every website that supports the OpenID service without problems using the same registration data.

Namecoin was also the foundation for another blockchain-based identity system: Blockstack ID, which had the second largest namespace at Namecoin. After Blockstack ID founders determined that a single mining pool had more than 51 percent of the computing power of the entire Namecoin system, Blockstack switched from Namecoin to Bitcoin.

Currently, the Blockstack system is the biggest application built on the Bitcoin blockchain (based on the number of transactions) outside of the finance sector. Blockstack already counts over 68,465 registered identities from every country in the world.

The Blockstack system developers have tried to get around the disadvantages of blockchain technology with a new, complex architecture. These include limited capacity for data storage and block size, low speed in confirming transactions,

[87] The Zookos Triangle is a trilemma of three properties that are desired in network name assignment.

[88] The term namespace originates in programming. In a namespace, every object (e.g., an address or other value) is linked uniquely with a name. One name may be assigned to different objects in multiple namespaces.

as well as the constantly growing blockchain size. The blockchain must be downloaded and validated by every new user – an undertaking that can take up to three days. Therefore, the Blockstack architecture consists of four layers. The first two (blockchain layer and virtualchain layer) are located at the control plane and the other two (routing layer and storage layer) at the data plane (see figure 4.6).

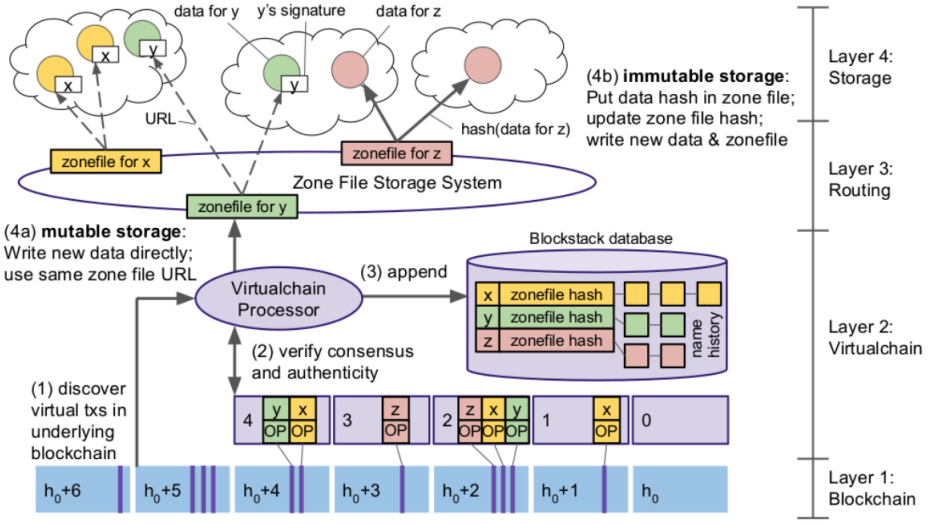


Figure 4.6: Architecture of the Blockstack system [113]

The underlying blockchain serves as a communication channel for announcing changes of state (if user data is altered). Human-readable names are registered at the control plane, and the name-hash connections and connections to the cryptographic key pairs are created. The data plane is responsible for data storage as well as data availability [113].

Blockstack offers several options for identity management. One of these is Onename (founded in March 2014, as of May 16, 2016 Blockstack Inc.). Built on the Blockstack foundation, it provides a simple service for the registration and management of digital identities. These identities are called Blockchain IDs. In May 2015, the possibilities of the Blockchain ID were expanded.

The basic idea of the Blockchain ID is to provide a digital form of identity and access control that can initially replace passwords and then in the future also physical forms of identification, such as passports, driver's licenses as well as house and office keys [24]. Blockchain IDs use the Blockchain Auth for a decentralized single-sign-on system to remove passwords and third-party providers from the user authentication process [21]. The Blockchain ID profile contains the following information fields:

- Name – user name,
- Bio – a short description of the user,

- Location – where the user is situated,
- Website – the user's website,
- Bitcoin – the user's bitcoin address,
- Avatar – a photo of the user,
- Cover – background image that gives the profile a personal flair,
- PGP – information about the public PGP key of the user,
- E-mail – user's email address,
- Twitter – Twitter account information,
- Facebook – Facebook account information,
- Github – Github account information [21].

Users can embed their blockchain ID at their website or blog, or they can use it as a digital business card.

According to Gartner Inc., digital identities can become portable and flexible on the basis of blockchain technology. The goal of successful identity management strives to have only one point of access for all services and thereby preserve security and user-friendliness. Thus, users can dispense with the tiresome creation of user accounts for individual services, such as Facebook, Amazon, and Spotify [40].

A blockchain application from SAP, called TrueRec, provides a solution for the management of official documents that prove the identity attributes of a real person. The documents themselves are not stored in the blockchain, but only the digital fingerprint (hash) of the data is written in the blockchain. When a new document is created using TrueRec, the document user receives the document as a special TRU-file. It can then be viewed in the TrueRec app and then shared with other institutions or people. The validity of the documents can be checked immediately with the blockchain [100].

One of the projects from Hyperledger called Iroha provides the possibility of joint management of the KYC data (Know Your Customer) for multiple companies [90].

4.6 Internet of Things

Despite its rapid development and dissemination, the Internet of Things still has challenges to overcome. According to an IoT study by IBM, these are:

- High costs (high infrastructure and maintenance costs due to cloud systems, server farming and service costs of intermediaries),
- Security (security models must be transparent and not obfuscated, therefore open source is the appropriate solution),

- Lack of future certainty (e.g., in the area of smart home, the user expects a long device life. The smart device should be able to receive updates for several years and, in contrast to a smart phone, be seldom in need of replacement),
- Lack of smartness (not enough meaningful added value; meaningful functionality should be inherent in linking devices),
- Lack of sustainable and profitable business models.

Additionally, the IoT systems use different cloud infrastructures and there is no common platform for connecting all smart devices, making area-wide P2P communication all that more difficult [53].

To master these challenges, each decentralized IoT solution must support a secure P2P data transfer and a robust and scalable form of device management [137]. As described in the IBM study, blockchain technology provides an elegant solution here (see figure 4.7).

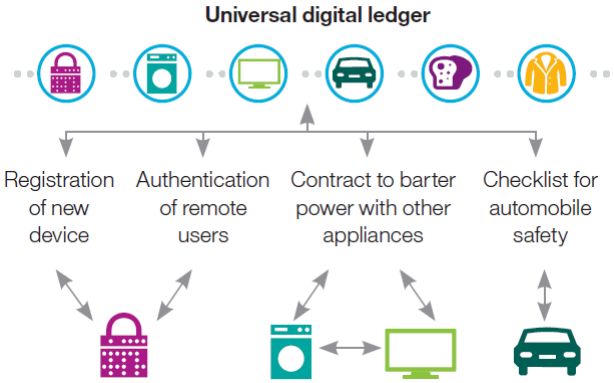


Figure 4.7: Blockchain technology allows different types of IoT transactions between devices [137]

Blockchain solutions for the IoT sector are offered by, for example, the German startup Slock.it, which uses smart contracts and the Ethereum blockchain. The company's first product was an intelligent door lock that could be opened with a smartphone app. Companies such as Airbnb can profit from such a solution in the future. Together with Siemens and Canonical, Slock.it plans to build an Ethereum computer that functions as a smart hub[89] and with which smart devices can be controlled [30]. In a project with RWE called Blockcharge, the startup will facilitate easy and secure payment for charging electric cars. Based on the concepts of Slock.it and RWE, in the future charging will be carried out wirelessly by induction while

[89] In data communication, a hub is a coupling element that receives data from one or more directions and from there forwards it in several directions [25]. A hub receives a data packet and sends it to all other ports [2].

standing at a red light. With drones the situation will be similar. Charging will be carried out at designated stations [51] with payment executed automatically.

The Filament company also uses blockchain technology for IoT solutions. Its focus is on the industrial application of IoT [45]. For this purpose, proprietary secure hardware is developed that supports the expanded cryptographic functions and is physically protected. Cryptographic keys are securely managed on the devices. Communication runs completely encrypted, for which the Telehash protocol is employed [82]. Such Filament solutions can be used, for example, for the optimization of value creation and the supply chain (see figure 4.8).

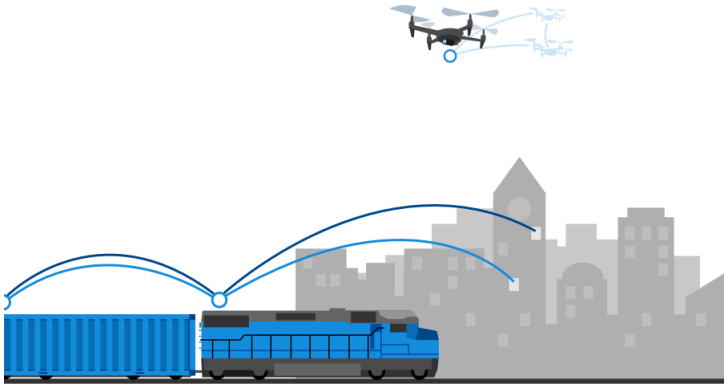


Figure 4.8: Filament – improvement of value-added chain and supply chain

The IBM solution for this application area is called the Watson IoT platform. It enables transferring data, sent by the IoT devices, to a private blockchain, and thus addressing the data to blockchain tokens (see figure 4.9) [92].

In spite of the advantages of blockchain technology for the Internet of Things, some challenges still need to be tackled. For example, the computing power required for the validation of transactions as well as the storage capacity needed by the nodes. These and other challenges can be solved by different concepts [117].

In December 2016 several well-known large companies and blockchain startups came together for a blockchain and IoT summit[90]. Together they sought to form a basis that would allow IoT providers core functions that could be used with different blockchains [102].

A consortium called "Chain of Things" supports the collaborative development of open source standards for blockchain technology in the area of the IoT. Three projects have already been developed on this basis:

[90] Bosch, Cisco, Gemalto, Foxconn, Ambisafe, BitSE, Chronicled, ConsenSys, Distributed, Filament, Hashed Health, Ledger, Skuchain and Slock.it.

- Chain of Security (secure IoT applications),
- Chain of Solar (connects IoT and blockchain technology for use in the solar energy sector),
- Chain of Shipping (IoT and blockchain technology in the context of trade, shipping and transport).

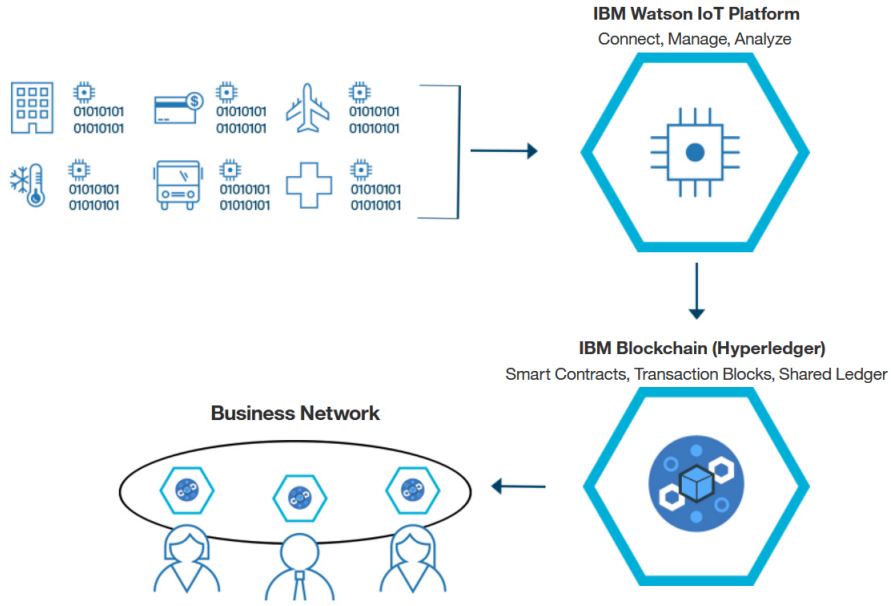


Figure 4.9: Watson IoT with blockchain [92]

4.7 Energy

The energy sector offers a promising scope for blockchain technology, whereby a blockchain value/token can, for example, be coupled with a unit of energy.

The energy company RWE and the German blockchain startup Slock.it plan to modernize how electric cars are charged using blockchain technology. The project, called "Blockcharge", will allow electric car owners to easily pay for recharging via an app. Ethereum smart contracts make this possible. In the future the car will already have an integrated cryptocurrency wallet to automatically facilitate the payment process with the charging station [30].

In 2016, companies from the consortium "Chain of Things" launched the project ElectriCChain. The project has set the goal of linking the seven million solar power facilities around the world currently and sending the real-time usage data to a blockchain. This will give scientists the opportunity to review and analyze the

solar power generation data, among other things. In the context of this project, the development of open standards and tools for the writing and reading of power-generation data in and by blockchain is supported.

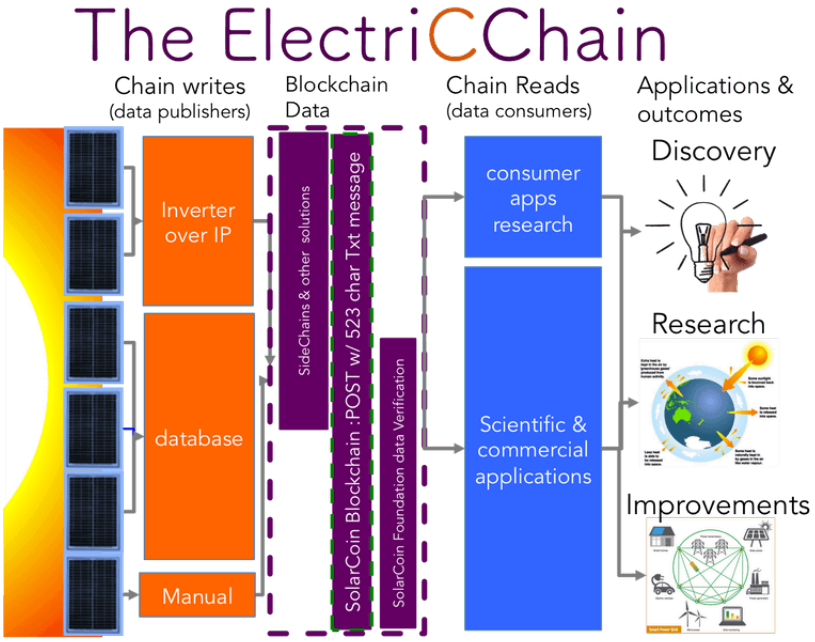


Figure 4.10: ElectriCChain project

The data is transferred from solar cells to data loggers. It is then checked and passed to the nodes of the SolarCoin blockchain, whereby it is linked with SolarCoins (see figure 4.11).

One SolarCoin represents 1 MWh of generated solar energy. Verified solar energy producers can get SolarCoins free of charge. In order to do this, they must chose a suitable wallet (for Windows, Mac OS, etc.) and register the solar system.

Because local producers of renewable energy are also affected when conventional networks fail [88], microgrids[91] are necessary to operate local energy trading. A joint venture[92] between "LO3 Energy" and "Consensys", called "Transactive Grid," introduced a microgrid in conjunction with blockchain and IoT technology. Initially, the system was established for several households in New York's Brooklyn district. Thereby, any surplus electricity produced will be registered in the blockchain (an energy unit becomes a blockchain value) and is traded between neighbors on the basis of smart contracts (see figure 4.12).

[91] Microgrid is a power grid that incorporates electricity producers and electricity consumers in one network or subnetwork, which can be operated independently [11].
[92] A joint venture is a subsidiary that is founded and run by two companies that are independent of one another [6].

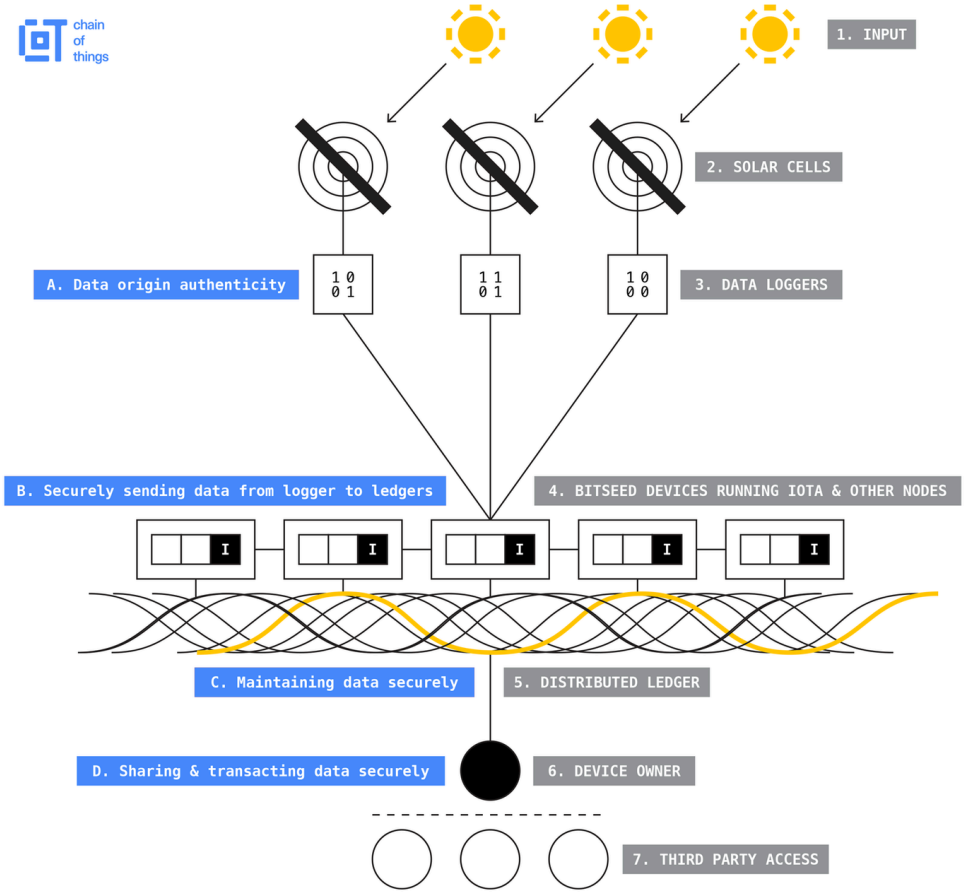


Figure 4.11: Chain of Things – ElectriCChain Project – Conversion of solar energy into blockchain values

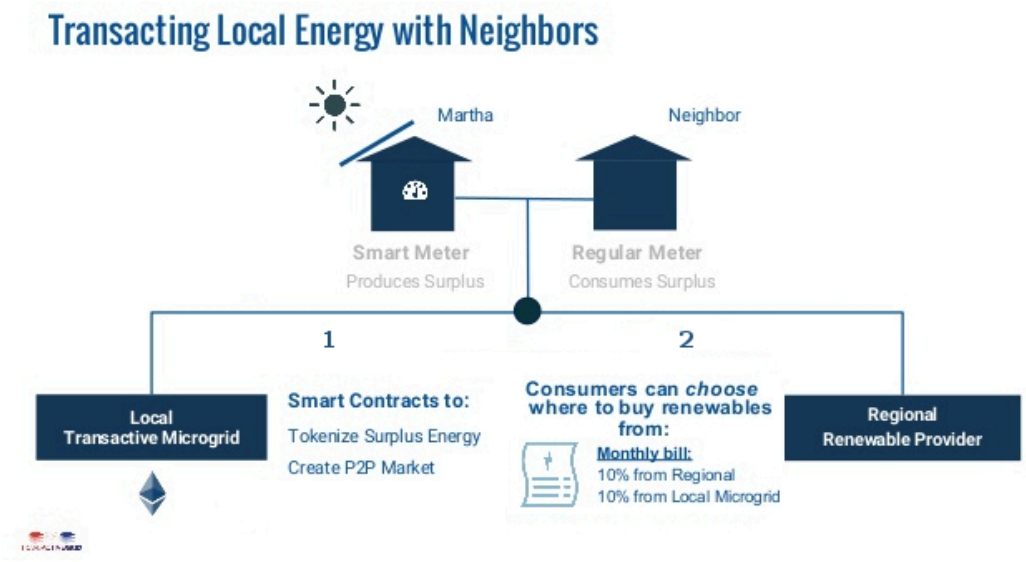


Figure 4.12: Transactive Grid

The Brooklyn project has provided impetus for an undertaking in Germany. The Landau Microgrid Project (LAMP) is a pilot and research project of the Karlsruhe Institute of Technology (KIT), in cooperation with the energy supplier Energie Südwest AG and the hardware and software company LO3 Energy. Within the framework of the project, blockchain is used for the local trade of electricity products. Twenty households are provided with a blockchain-based trading platform. There, locally produced "green" electricity can be traded between households. Via an app, participants have access to the data, that shows how much electricity they have consumed and generated, and can set their price expectations for locally produced energy from renewable sources [93].

4.8 Logistics

Logistics affects several areas of a company's business and generates huge amounts of information between those involved in the flow of goods. The goal is to guarantee the availability of the right goods, in the right amount and condition – and that the goods reach the right customer, at the right time and for the right price [4]. Besides the physical activities, the accompanying order processing and the cash flow processes are necessary considerations.

Supply chain management builds integrated logistic chains (material and information flows) across the entire value creation process and manages them from raw material extraction up to the end user. With successful management and paperless data exchange, procurement, production and business planning can complement each other at various levels. Companies can react directly to any disruptions with planning changes [5].

Participants involved in supply chain management have different access permissions to the information and tasks. Nowadays, supply chains are very complex and include a great number of participants from all over the whole world. Thus keeping track of costs, efficiency and quality is more important than ever.

A company can benefit significantly from blockchain-based supply chain management (see figure 4.13). In this respect, the following qualities of blockchain technology are of primary importance:

- Cryptographic proof replaces trust – thus the possibility of simple access authorization and user management.
- Reliability, traceability and protection against counterfeiting, guaranteed by secure data logging and transparency of data contents.
- Replacement of multiple middlemen with a decentralized user network, smart contracts and oracles. When certain destinations along the supply chain are passed, fixed conditions in the smart contract can be verified. If necessary, further tasks/functions are then activated (e.g., paying for the service if all conditions have been fulfilled).

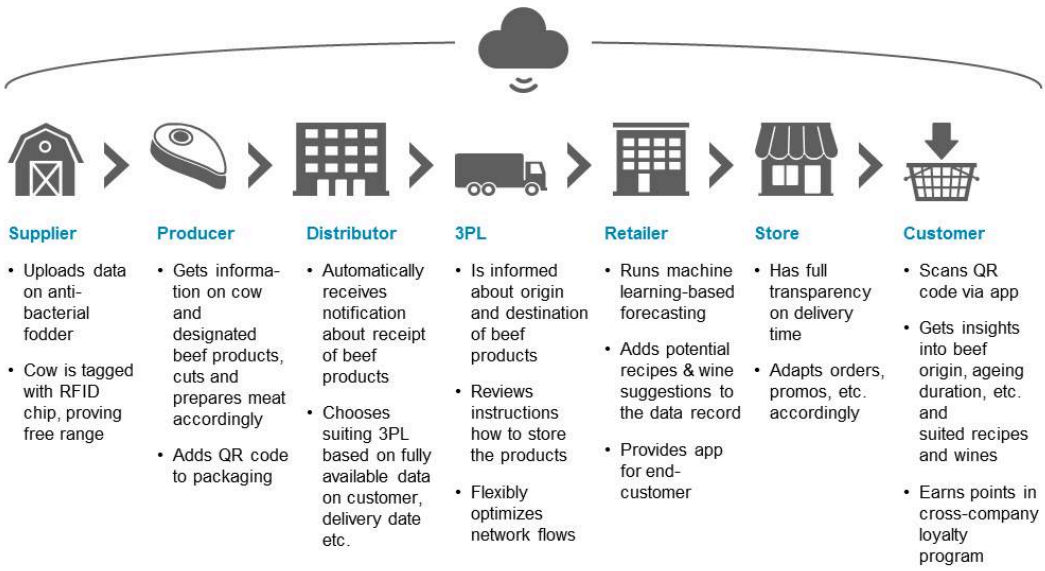


Figure 4.13: End-to-end blockchain-based supply chain [10]

In connection with IoT technology, several application options exist in logistics. Particularly sensitive goods can be provided with sensor-equipped IoT devices, which can forward the collected information to the blockchain. The company Modum.io offers a solution for the traceability of information about the storage status (temperature, humidity) of medicine throughout the supply chain.

IBM and Maersk[93] are developing a solution based on the Hyperledger framework "Fabric" for the shipping and logistics industry. It allows an exchange of events and documents in real time along the whole supply chain with the help of a digital infrastructure. Sustainable transportation is supported through a clear overview of all processes involved and secure access to certain data for certain users [91].

Foxconn, one of the world's largest manufacturers of electronic and computer parts, plans a blockchain-based supply chain financial platform with the Chinese online credit company Dianrong. The project, which will initially focus on the automobile, electronics and apparel industries, aims to make payment and transactions in the supply chain more transparent, more manageable, and easier to authenticate. By virtue of blockchain technology, the entire supply chain will become more efficient and costs will be lowered by eliminating third parties. The whole supply chain, and not just its financial flows, will be processed on the basis of blockchain technology. If all supply chain transactions become easier to validate, the efficiency of the whole eco-system increases [101].

[93] The world's largest container shipping company.

5 Fears and Risks or Success and Increased Efficiency?

Any new technology promising high yields, cost savings and increased efficiency should be viewed with caution. The hype surrounding blockchain creates the impression of an all-purpose weapon whose use is limited to a select few corporate giants and their innovation labs.

If we ignore the hype, we end up with a promising, albeit not yet fully developed, technology that with the right implementation can make business processes leaner and more efficient. As with every innovation, risks are involved because standards and interoperability between systems have not yet been fully established.

Blockchain's innovation lies in its successful composition of already existing approaches: decentralized network, cryptography, and consensus model. The innovative concept enables a value exchange in a decentralized system. Trust between the nodes (e.g., users) is no longer required, with intelligence located at the nodes and not at a central instance. Values are added to the blockchain history – immutably and irreversibly. The history is transparent and, as such, provides proof of when a value was owned and by whom. A value exchange with complex when-if conditions is possible (smart contracts).

Blockchain technology can guarantee a decentralized and secure system where different subsystems interact with each other (e.g., identity management, Internet of Things, cloud storage). Soon to be possible use cases, based on a uniform technology that supports secure P2P communication, include: shopping with only a blockchain wallet, unlocking the door of the home or office, registering to vote and casting a ballot, making specific information from one's own patient file available to a doctor, and opening a car and starting it without a physical key.

Many implementation options are available to interested companies. Over the past three years numerous consortia and projects have sprung up offering "Blockchain–as-a-Service". They support other companies in development, testing and application. Blockchain technology has already conquered many fields of application, and more and more companies are offering ready-made solutions adapted to specific areas.

However, any company that wants to jump on the blockchain bandwagon first needs to seriously examine the cost-benefit ratio before deciding on implementation. The goal hoped to be achieved by the use of the technology must be clearly defined from the beginning. It is important to bear in mind the possibilities and limitations of blockchain technology.

The Bitcoin, Ethereum, and Hyperledger frameworks have evolved as standards on the blockchain scene and serve as the basis for many other applications. Bitcoin is still considered the strongest and safest blockchain system. Despite the high volatility of cryptocurrency and the sinking mining rewards, the system continues

to grow rapidly. The main criticism of the bitcoin system centers on its application in anonymous business dealings and high electricity consumption. In order to cover the costs of its high energy use, transaction fees must be raised accordingly so it continues to be worthwhile for miners to operate.

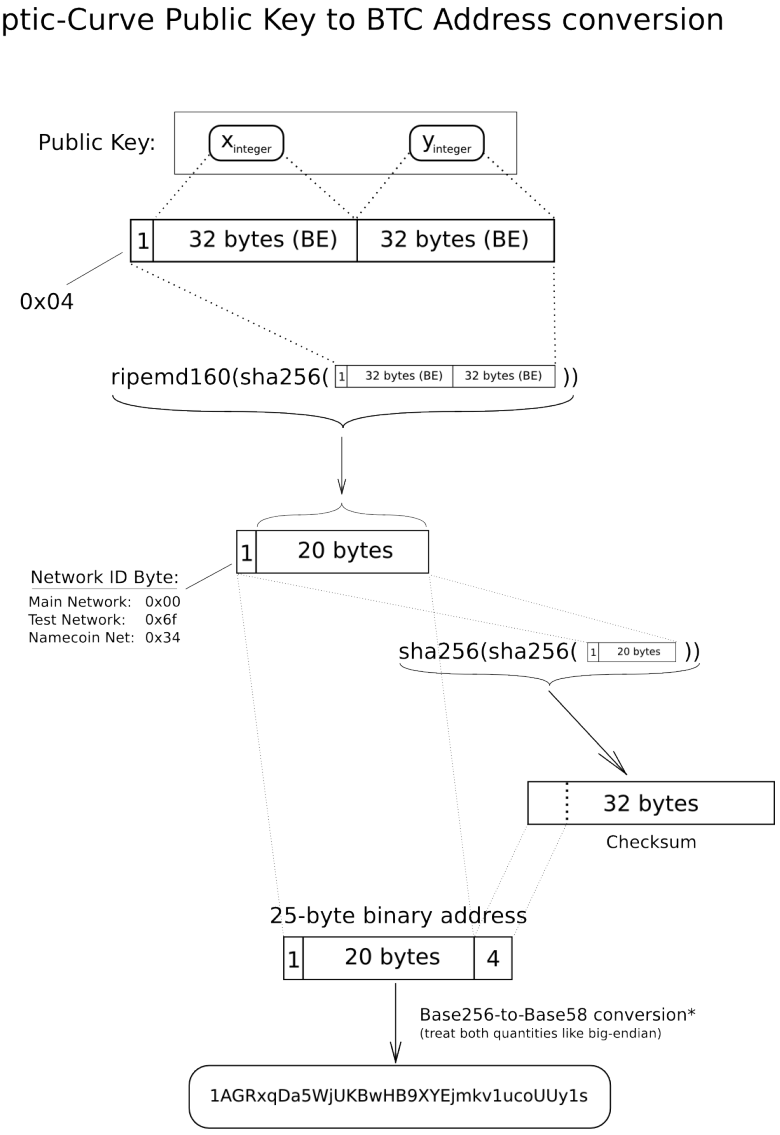
New blockchains run the risk of inadequate security, as changes to the already existing technologies could potentially lead to protection gaps and deficiencies. These can then be exploited, for example, in the so-called 51 Percent Attack. Here a miner, or mining pool, has control of more than half of the entire computing capacity (hash rate) in the network and can thus create new blocks and manipulate them. We can see the exploitation of a weak spot in the code in the attack on the decentralized autonomous organisation known as "The DAO," which is now defunct.

Large companies as well as startups have joined forces for quite a while in attempting to improve blockchain technology and continuing to develop its standards. Through this support, as well as efforts on a national level, there is the very real chance that blockchain will progress beyond hype and securely establish itself as a cross-cutting and sustainable technology.

6 Appendix

6.1 Conversion from ECDSA Public Key to Bitcoin Address

Source [62].



*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

6.2 Automatic Use of TOR Hidden Services

Source: `https://bitcoin.org/en/release/v0.12.0`

Starting with Tor version 0.2.7.1 it is possible, through Tor's control socket API, to create and destroy "ephemeral" hidden services programmatically. Bitcoin Core has been updated to make use of this. This means that if Tor is running (and proper authorization is available), Bitcoin Core automatically creates a hidden service to listen on, without manual configuration. Bitcoin Core will also use Tor automatically to connect to other .onion nodes if the control socket can be successfully opened. This will positively affect the number of available .onion nodes and their usage.

This new feature is enabled by default if Bitcoin Core is listening, and a connection to Tor can be made. It can be configured with the `-listenonion`, `-torcontrol` and `-torpassword` settings. To show verbose debugging information, pass `-debug=tor`.

6.3 Transaction Verification in the Bitcoin System

Source: [13]

1. Check syntactic correctness.
2. Make sure neither in or out lists are empty.
3. Size in bytes $<$ MAX_BLOCK_SIZE.
4. Each output value, as well as the total, must be in legal money range.
5. Make sure none of the inputs have hash $= 0$, $n = -1$ (coinbase transactions).
6. Check that nLockTime $<= INT\_MAX$, size in bytes $>= 100$, and sig opcount $<= 2$.
7. Reject 'nonstandard' transactions: scriptSig doing anything other than pushing numbers on the stack, or scriptPubkey not matching the two usual forms.
8. Reject if we already have matching tx in the pool, or in a block in the main branch.
9. For each input, if the referenced output exists in any other tx in the pool, reject this transaction.
10. For each input, look in the main branch and the transaction pool to find the referenced output transaction. If the output transaction is missing for any input, this will be an orphan transaction. Add to the orphan transactions, if a matching transaction is not in there already.
11. For each input, if the referenced output transaction is coinbase (i.e. only 1 input, with hash $= 0$, $n = -1$), it must have at least COINBASE_MATURITY (100) confirmations; else reject this transaction.

12. For each input, if the referenced output does not exist (e.g. never existed or has already been spent), reject this transaction.
13. Using the referenced output transactions to get input values, check that each input value, as well as the sum, are in legal money range.
14. Reject if the sum of input values $<$ sum of output values.
15. Reject if transaction fee (defined as sum of input values minus sum of output values) would be too low to get into an empty block.
16. Verify the scriptPubKey accepts for each input; reject if any are bad.
17. Add to transaction pool.
18. Add to wallet if mine.
19. Relay transaction to peers.
20. For each orphan transaction that uses this one as one of its inputs, run all these steps (including this one) recursively on that orphan.

6.4 The Byzantine Generals Problem

Source: Leslie Lamport, Robert Shostak and Marshall Pease – The Byzantine Generals Problem, July 1982

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that

1. all loyal generals decide upon the same plan of action. The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition A regardless of what the traitors do. The loyal generals should not only reach agreement, but should agree upon a reasonable plan. We therefore also want to insure that
2. a small number of traitors cannot cause the loyal generals to adopt a bad plan.

6.5 Atomic Cross-Chain Trading

Source: [14]

A and B are two Nodes, that hold Units (coins) on different blockchains.

A picks a random number x

A creates TX1: “Pay w BTC to <B’s public key> if (x for H(x) known and signed by B) or (signed by A & B)”
A creates TX2: “Pay w BTC from TX1 to <A’s public key>, locked 48 hours in the future”
A sends TX2 to B
B signs TX2 and returns to A

1. A submits TX1 to the network

   B creates TX3: “Pay v alt-coins to <A-public-key> if (x for H(x) known and signed by A) or (signed by A & B)”

   B creates TX4: “Pay v alt-coins from TX3 to <B’s public key>, locked 24 hours in the future”

   B sends TX4 to A

   A signs TX4 and sends back to B

2. B submits TX3 to the network

3. A spends TX3 giving x

4. B spends TX1 using x

This is atomic (with timeout). If the process is halted, it can be reversed no matter when it is stopped.
Before 1: Nothing public has been broadcast, so nothing happens
Between 1 & 2: A can use refund transaction after 48 hours to get his money back
Between 2 & 3: B can get refund after 24 hours. A has 24 more hours to get his refund
After 3: Transaction is completed by 2

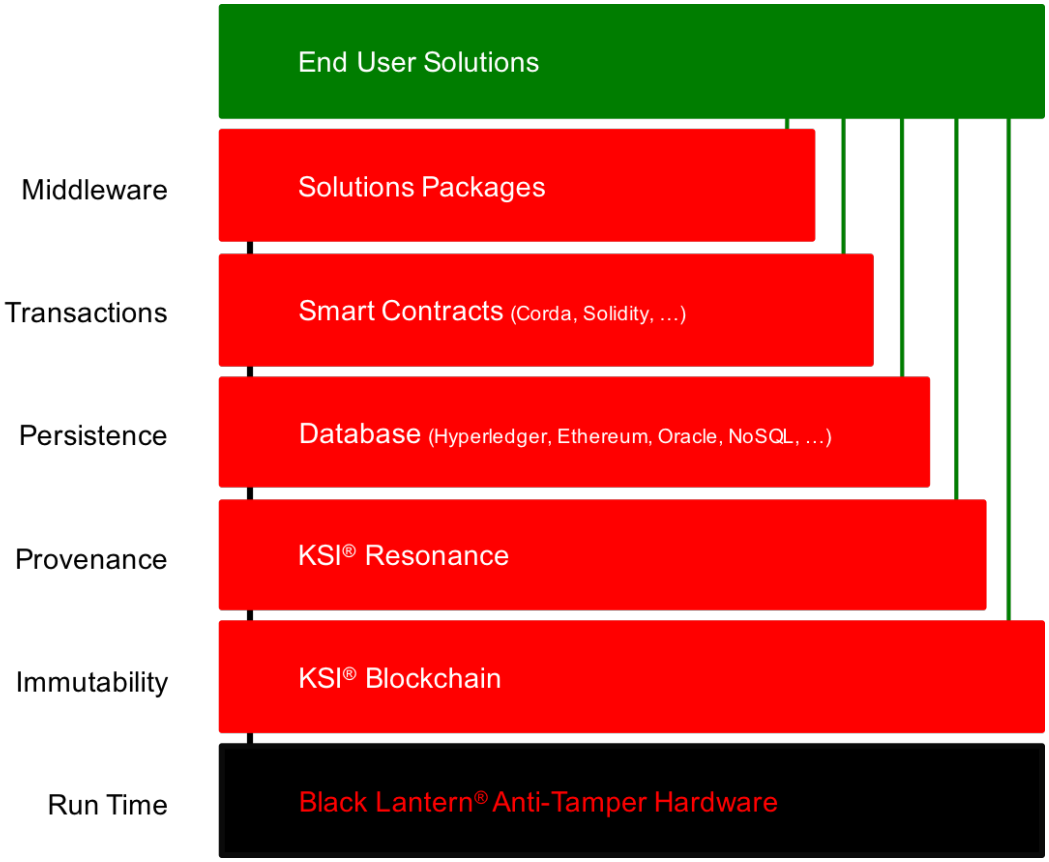
- A must spend his new coin within 24 hours or B can claim the refund and keep his coins

- B must spend his new coin within 48 hours or A can claim the refund and keep his coins

For safety, both should complete the process with lots of time until the deadlines.

6.6 Guardtime Technology Stack

Guardtime's KSI® Technology Stack [87]



References

[1] Colony-Picture. URL: https://wallscover.com/images/colony-7.jpg. Last visited on 11.10.2017.

[2] Elektronik Kompendium – Hub. URL: https://www.elektronik-kompendium.de/sites/net/1405161.htm. Last visited on 23.10.2017.

[3] Gabler Wirtschaftslexikon – Kryptowährung. URL: http://wirtschaftslexikon.gabler.de/Definition/kryptowaehrung.html. Last visited on 08.11.2017.

[4] Gabler Wirtschaftslexikon – Logistik. URL: http://wirtschaftslexikon.gabler.de/Definition/logistik.html. Last visited on 08.11.2017.

[5] Gabler Wirtschaftslexikon – Supply Chain Management (SCM). URL: http://wirtschaftslexikon.gabler.de/Definition/supply-chain-management-scm.html. Last visited on 08.11.2017.

[6] Gründer Szene Lexikon – Joint-Venture. URL: https://www.gruenderszene.de/lexikon/begriffe/joint-venture. Last visited on 09.11.2017.

[7] JuraForum – Analogieverbot. URL: https://www.juraforum.de/lexikon/analogieverbot. Last visited on 12.09.2017.

[8] Kryptografie.de. URL: http://kryptografie.de/kryptografie/index.htm. Last visited on 15.06.2017.

[9] LEADVISE Reply – DAO – Dezentrale Autonome Organisationen. URL: http://www.leadvise.de/latest-thinking/blockchain/dao-dezentrale-autonome-organisationen/. Last visited on 20.10.2017.

[10] Oliver Wyman – Blockchain: The Backbone Of Digital Supply Chains. URL: http://www.oliverwyman.com/our-expertise/insights/2017/jun/blockchain-the-backbone-of-digital-supply-chains.html. Last visited on 08.11.2017.

[11] Zhaw – Was ist der Unterschied zwischen Microgrids und Smart Grids? URL: https://www.zhaw.ch/de/lsfm/institute-zentren/iunr/ecological-engineering/erneuerbare-energien/microgrids/unterscheidung/. Last visited on 06.11.2017.

[12] Bitcoin Wiki – Hauptseite. URL: https://de.bitcoin.it/wiki/Hauptseite, 2011. Last visited on 13.04.2016.

[13] Bitcoin Wiki – Protocol rules. URL: https://en.bitcoin.it/wiki/Protocol_rules, 2011. Last visited on 21.06.2016.

[14] Bitcointalk.org. URL: https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949, 2013. Last visited on 02.12.2016.

[15] ITWissen.info – Peer-to-Peer-Netz. URL: http://www.itwissen.info/Peer-to-Peer-Netz-peer-to-peer-network-P2P.html, 2014. Last visited on 06.09.2017.

[16] Bitcoin Magazin – Ripple Discontinues Smart Contract Platform Codius, Citing Small Market. URL: https://bitcoinmagazine.com/articles/ripple-discontinues-smart-contract-platform-codius-citing-small-market-1435182153, 2015. Last visited on 23.12.2016.

[17] BitcoinBlog.de – Ein Startup, Sybils Angriff und die Privatsphäre. URL: https://bitcoinblog.de/2015/03/19/ein-startup-sybils-angriff-und-die-privatsphare/, 2015. Last visited on 06.10.2017.

[18] CoinDesk – How Bitcoin's Technology Could Reshape Our Medical Experiences. URL: http://www.coindesk.com/bitcoin-technology-could-reshape-medical-experiences/, 2015. Last visited on 17.11.2016.

[19] Coinwelt – Hardware-Wallet Trezor. URL: http://coinwelt.de/wp-content/uploads/2015/09/trezor_transparent.png, 2015. Last visited on 14.04.2017.

[20] Ethereum Blog – On Public and Private Blockchains. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, 2015. Last visited on 22.10.2017.

[21] Github.com – blockstack. URL: https://github.com/blockstack/blockchain-id/wiki, 2015. Last visited on 15.01.2017.

[22] Learn me a bitcoin – Difficulty. URL: http://learnmeabitcoin.com/guide/difficulty, 2015. Last visited on 12.07.2017.

[23] Ledgerwallet – Hardware-Wallet Ledger. URL: https://www.ledgerwallet.com/images/products/lwn/ledger-nano-solo-large.png, 2015. Last visited on 14.04.2017.

[24] Onename.com – Introducing a Blockchain-based Digital Identity. URL: http://blog.onename.com/blockchain-id/, 2015. Last visited on 15.01.2017.

[25] TechTarget – Hub. URL: http://www.searchnetworking.de/definition/Hub, 2015. Last visited on 23.10.2017.

[26] Acronis – Acronis integriert Acronis Notary mit Blockchain und CloudRAID in seine Software-Defined Storage Lösung Acronis Storage. URL: https://www.acronis.com/de-de/pr/2016/10/20-09-39.html, 2016. Last visited on 17.10.2017.

[27] Bird&Bird – Blockchain 2.0, smart contracts and challenges. URL: https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges, 2016. Last visited on 28.10.2017.

[28] Bitcoin Wiki – Address. URL: https://en.bitcoin.it/wiki/Address, 2016. Last visited on 18.04.2017.

[29] Bitcoin Wiki – Lightning Network. URL: https://en.bitcoin.it/wiki/Lightning_Network, 2016. Last visited on 24.02.2017.

[30] BitcoinBlog.de – RWE und slock.it wollen Ethereum für Elektroautos nutzen. URL: https://bitcoinblog.de/2016/02/26/rwe-und-slock-it-wollen-ethereum-fuer-elektroautos-nutzen/, 2016. Last visited on 03.01.2017.

[31] Bitcoinj – What is bitcoinj? URL: https://bitcoinj.github.io/, 2016. Last visited on 14.12.2016.

[32] Bitcoinpaperwallet – Paper-Wallet. URL: https://bitcoinpaperwallet.com/images/front-back-sample-big.jpg, 2016. Last visited on 14.04.2017.

[33] Blockchain.info – Hashwert. URL: https://blockchain.info/de/charts/hash-rate, 2016. Last visited on 11.08.2016.

[34] Blockgeeks – Smart Contracts: The Blockchain Technology That Will Replace Lawyers. URL: https://blockgeeks.com/guides/smart-contracts/, 2016. Last visited on 26.10.2017.

[35] Brave Newcoin – BNP Paribas and SmartAngels blockchain pilot targets Europe's growing crowdfunding sector. URL: https://bravenewcoin.com/news/bnp-paribas-and-smartangels-blockchain-pilot-targets-europes-growing-crowdfunding-sector/, 2016. Last visited on 20.12.2016.

[36] BTC-ECHO – Ein auf Blockchain ausgerichtetes Consortium in Japan berichtet jetzt von einer wachsenden Mitgliederzahl von über 100 Unternehmen. URL: https://www.btc-echo.de/japanisches-blockchain-

consortium-zaehlt-nun-ueber-100-mitglieder/, 2016. Last visited on 19.12.2016.

[37] BTC-ECHO – So viel Geld benötigst du für eine Bitcoin 51 Prozent Attacke. URL: https://www.btc-echo.de/so-viel-geld-benoetigst-du-fuer-eine-bitcoin-51-attacke/, 2016. Last visited on 20.12.2016.

[38] Chain Core. URL: https://chain.com/technology/, 2016. Last visited on 20.12.2016.

[39] Clearmatics. URL: http://www.clearmatics.com/, 2016. Last visited on 20.12.2016.

[40] Computerwoche – Identitäten verwalten mit Blockchain. URL: https://www.computerwoche.de/a/identitaeten-verwalten-mit-blockchain,3316591, 2016. Last visited on 01.11.2017.

[41] Datarella – Eine Dezentrale Autonome Organisation DAO – Was ist das? URL: http://datarella.de/dezentrale-autonome-organisation-dao-was-ist-das/, 2016. Last visited on 20.10.2017.

[42] Ethereum Homestead Documentation – Contracts. URL: http://ethdocs.org/en/latest/contracts-and-transactions/contracts.html, 2016. Last visited on 30.10.2017.

[43] Gartner – The CIO's Guide to Blockchain. URL: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/, 2016. Last visited on 11.10.2017.

[44] Hochschule Niederrhein, Fachbereich Elektrotechnik und Informatik – Verteilte Algorithmen. URL: https://lionel.kr.hs-niederrhein.de/~rethmann/shs06/shs05.pdf, 2016. Last visited on 12.07.2017.

[45] International Business Times – Filament evolving entire IoT space using Bitcoin blockchain. URL: http://www.ibtimes.co.uk/filament-evolving-

entire-iot-space-underwhelming-use-blockchain-1579096, 2016. Last visited on 03.01.2017.

[46] Let's Talk Payments – Know more about Blockchain: Overview, Technology, Application Areas and Use Cases. URL: https://letstalkpayments.com/an-overview-of-blockchain-technology/, 2016. Last visited on 20.12.2016.

[47] Microsoft News – Microsoft and AMIS announce Asia's first blockchain consortium. URL: https://news.microsoft.com/apac/2016/12/12/microsoft-and-amis-announce-asias-first-blockchain-consortium/, 2016. Last visited on 19.12.2016.

[48] Nasdaq – Colu Announces Colored Coins and Lightning Network Integration. URL: http://www.nasdaq.com/article/colu-announces-colored-coins-and-lightning-network-integration-cm710111, 2016. Last visited on 23.10.2017.

[49] Outlier Ventures – 5 Things We Learned From Analysing the Location of 950+ Blockchain Startups. URL: https://medium.com/outlier-ventures-io/5-things-we-learned-from-analysing-the-location-of-950-blockchain-startups-96daa788560c#.78ofyxve8, 2016. Last visited on 21.11.2016.

[50] Rechenkraft.net – BOINC. URL: https://www.rechenkraft.net/wiki/BOINC, 2016. Last visited on 21.11.2016.

[51] Slock.it – Solutions. URL: https://slock.it/solutions.html, 2016. Last visited on 03.01.2017.

[52] StackExchange. URL: http://ethereum.stackexchange.com/questions/3336/what-is-the-difference-between-a-smart-contract-and-a-dao/4240, 2016. Last visited on 21.12.2016.

[53] TechCrunch – Decentralizing IoT networks through blockchain. URL: https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/, 2016. Last visited on 04.01.2017.

[54] 3sat – Bitcoin, der Wert der digitalen Währung schwankt extrem. URL: http://www.3sat.de/page/?source=/nano/glossar/bitcoin.html, 2017. Last visited on 14.09.2017.

[55] Academic library – Full vs. Simplified Payment Verification. URL: https://academlib.com/7951/education/full_simplified_payment_verification, 2017. Last visited on 12.10.2017.

[56] Adobe Blog – Wie Estland zum Digital Government-Vorreiter in Europa wurde. URL: https://blogs.adobe.com/digitaleurope/de/governmental-affairs/wie-estland-zum-digital-government-vorreiter-in-europa-wurde/, 2017. Last visited on 14.10.2017.

[57] Agrello. URL: https://www.agrello.org/how-it-works, 2017. Last visited on 12.09.2017.

[58] Altcointoday – Ethereum Lightning Network Moves into Test Phase. URL: http://www.altcointoday.com/ethereum-lightning-network-moves-into-test-phase/, 2017. Last visited on 12.10.2017.

[59] Bitcoin – Schützen Sie ihre Privatsphäre. URL: https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere, 2017. Last visited on 17.04.2017.

[60] Bitcoin – Sichern Sie Ihre Wallet. URL: https://bitcoin.org/de/sichern-sie-ihre-wallet, 2017. Last visited on 10.10.2017.

[61] Bitcoin Wiki – Common Vulnerabilities and Exposures. URL: https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures, 2017. Last visited on 17.09.2017.

[62] Bitcoin Wiki – Elliptic-Curve Public Key to BTC Address conversion. URL: https://en.bitcoin.it/w/images/en/9/9b/PubKeyToAddr.png, 2017. Last visited on 11.05.2016.

[63] Bitcoin Wiki – Hardware wallet. URL: https://en.bitcoin.it/wiki/Hardware_wallet, 2017. Last visited on 11.10.2017.

[64] Bitcoin Wiki – Mining. URL: https://en.bitcoin.it/wiki/Mining, 2017. Last visited on 15.09.2017.

[65] Bitcoin Wiki – Multisignature. URL: https://en.bitcoin.it/wiki/Multisignature, 2017. Last visited on 18.04.2017.

[66] Bitcoin Wiki – Setting up a Tor hidden service. URL: https://en.bitcoin.it/wiki/Setting_up_a_Tor_hidden_service, 2017. Last visited on 10.09.2017.

[67] Bitcoin Wiki – Weaknesses. URL: https://en.bitcoin.it/wiki/Weaknesses, 2017. Last visited on 15.09.2017.

[68] BitcoinBlog.de – Adressen bei Kryptowährungen: eine Einführung. URL: https://bitcoinblog.de/2017/06/12/adressen-bei-kryptowaehrungen-eine-einfuehrung/, 2017. Last visited on 17.04.2017.

[69] Blockchain.info – Mining Pools. URL: https://blockchain.info/de/pools?timespan=4days, 2017. Last visited on 01.12.2017.

[70] Blockgeeks – Blockchain Glossary: From A-Z. URL: https://blockgeeks.com/guides/blockchain-glossary-from-a-z/, 2017. Last visited on 26.10.2017.

[71] Brave Newcoin – Ethereum scaling solution, Plasma, could facilitate "billions of transactions per second". URL: https://bravenewcoin.com/news/ethereum-scaling-solution-plasma-could-facilitate-billions-of-transactions-per-second/, 2017. Last visited on 14.10.2017.

[72] Bundesblock – Blockchain Bundesverband. URL: http://bundesblock.de/2017/10/17/bundesverband-veroeffentlicht-positionspapier/, 2017. Last visited on 25.10.2017.

[73] ClearKarma. URL: http://www.clearkarma.com/, 2017. Last visited on 09.09.2017.

[74] CoinDesk – Bitcoin's Lightning Network Moves Closer to Compatibility. URL: https://www.coindesk.com/bitcoins-lightning-network-moves-closer-compatibility-standard/, 2017. Last visited on 21.10.2017.

[75] Colony. URL: https://colony.io/, 2017. Last visited on 11.10.2017.

[76] CryptoCompare – What is merged mining – Bitcoin & Namecoin – Litecoin & Dogecoin? URL: https://www.cryptocompare.com/mining/guides/what-is-merged-mining-bitcoin-namecoin-litecoin-dogecoin/, 2017. Last visited on 24.10.2017.

[77] Dapps for beginners – Introduction to development on Ethereum. URL: https://dappsforbeginners.wordpress.com/tutorials/introduction-to-development-on-ethereum/, 2017. Last visited on 11.10.2017.

[78] Deloitte – Die Blockchain aus Sicht des Datenschutzrechts. URL: https://www2.deloitte.com/dl/de/pages/legal/articles/blockchain-datenschutzrecht.html, 2017. Last visited on 12.09.2017.

[79] E-Estonia. URL: https://e-estonia.com/, 2017. Last visited on 14.10.2017.

[80] Ethcore Blog – The Multi-sig Hack: A Postmortem. URL: https://blog.ethcore.io/the-multi-sig-hack-a-postmortem/, 2017. Last visited on 11.10.2017.

[81] Ethereum White Paper – A Next-Generation Smart Contract and Decentralized Application Platform. URL: https://github.com/ethereum/wiki/wiki/White-Paper, 2017. Last visited on 28.10.2017.

[82] Filament – Security Overview. URL: https://filament.com/assets/downloads/Filament%20Security.pdf, 2017. Last visited on 14.10.2017.

[83] Gartner – Top 10 Mistakes in Enterprise Blockchain Projects. URL: https://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/, 2017. Last visited on 11.10.2017.

[84] Gem – Health. URL: https://gem.co/health/, 2017. Last visited on 11.10.2017.

[85] Github – Colored Coins Protocol Specification. URL: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Introduction, 2017. Last visited on 23.10.2017.

[86] Gridcoin. URL: http://gridcoin.us/, 2017. Last visited on 23.06.2017.

[87] Guardtime – Our Technology. URL: https://guardtime.com/technology, 2017. Last visited on 14.10.2017.

[88] Handelsblatt – Strom aus der Nachbarschaft. URL: http://www.handelsblatt.com/technik/energie-umwelt/circular-economy/transactive-grid-mikronetzwerk-fuer-zehn-haeuserblocks/14793648-2.html, 2017. Last visited on 06.11.2017.

[89] Heise Security – Sicherheit der Verschlüsselung. URL: https://m.heise.de/security/artikel/Kryptographie-in-der-IT-Empfehlungen-zu-Verschluesselung-und-Verfahren-3221002.html?artikelseite=all, 2017. Last visited on 17.09.2017.

[90] Hyperledger – Frameworks. URL: https://www.hyperledger.org/, 2017. Last visited on 31.10.2017.

[91] IBM – Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain. URL: http://www-03.ibm.com/press/us/en/pressrelease/51712.wss, 2017. Last visited on 09.11.2017.

[92] IBM – Watson Internet of Things. URL: http://www.ibm.com/internet-of-things/iot-news/announcements/private-blockchain/, 2017. Last visited on 04.01.2017.

[93] Landau Microgrid Project. URL: https://im.iism.kit.edu/1093_2058.php, 2017. Last visited on 06.11.2017.

[94] Medium – Exploring Simpler Ethereum Multisig Contracts. URL: https://medium.com/@ChrisLundkvist/exploring-simpler-ethereum-multisig-contracts-b71020c19037, 2017. Last visited on 11.10.2017.

[95] Medium – Introducing Peerism: the Skill Token Economy for Post-Capitalism. URL: https://medium.com/peerism/introducing-peerism-the-skill-token-economy-for-post-capitalism-6d3a8a893ccc, 2017. Last visited on 14.10.2017.

[96] Medium – Welcome to the blockchain nation. URL: https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4, 2017. Last visited on 14.10.2017.

[97] Modum.io. URL: https://modum.io/, 2017. Last visited on 09.09.2017.

[98] Oraclize.it – Ethereum Proof of Identity. URL: http://dapps.oraclize.it/proof-of-identity/, 2017. Last visited on 14.10.2017.

[99] Publicism – Could Blockchain Technology help free press? URL: https://medium.com/publicism/could-blockchain-technology-help-photographers-free-press-129a7fec4f9, 2017. Last visited on 11.10.2017.

[100] SAP – Die SAP stellt TrueRec vor: Basierend auf der Blockchain-Technologie lassen sich mit der Lösung zuverlässig digitale Zeugnisse und Zertifikate verwalten. URL: https://news.sap.com/germany/truerec-blockchain/?source=email-de-newscenter-newsletter-20170920&lf1=2531622534d194024351450e79609376, 2017. Last visited on 01.11.2017.

[101] SCF Briefing – Foxconn uses blockchain for new SCF platform after 6,5 million dollar pilot. URL: http://www.scfbriefing.com/foxconn-launches-scf-blockchain-platform/, 2017. Last visited on 10.11.2017.

[102] Silicon – Neue Initiative will IoT mit Blockchain sicherer machen. URL: http://www.silicon.de/41639843/neue-initiative-will-iot-mit-blockchain-sicherer-machen/?inf_by=59799667671db810758b4634, 2017. Last visited on 15.10.2017.

[103] Stackoverflow – Where do smart contracts reside in blockchain (Ethereum or Hyperledger). URL: https://stackoverflow.com/questions/42081194/where-do-smart-contracts-reside-in-blockchain-ethereum-or-hyperledger, 2017. Last visited on 31.10.2017.

[104] The Cointelegraph – Lightning Network Will Come to Bitcoin "From Tomorrow": Reports. URL: https://cointelegraph.com/news/lightning-network-will-come-to-bitcoin-from-tomorrow-reports, 2017. Last visited on 14.10.2017.

[105] Tor Project – Tor: Hidden Service Protocol. URL: https://www.torproject.org/docs/hidden-services.html.en, 2017. Last visited on 11.09.2017.

[106] Wikipedia – Blockchain. URL: https://en.wikipedia.org/wiki/Blockchain, 2017. Last visited on 22.10.2017.

[107] Wikipedia – Framework. URL: https://de.wikipedia.org/wiki/Framework, 2017. Last visited on 31.10.2017.

[108] Wikipedia – Ghash.io. URL: https://en.wikipedia.org/wiki/Ghash.io, 2017. Last visited on 20.09.2016.

[109] Wikipedia – Nonce. URL: https://de.wikipedia.org/wiki/Nonce, 2017. Last visited on 13.09.2016.

[110] Wikipedia – Paxos (Informatik). URL: https://de.wikipedia.org/wiki/Paxos_(Informatik), 2017. Last visited on 19.12.2016.

[111] Wikipedia – Salt (Kryptologie). URL: https://de.wikipedia.org/wiki/Salt_(Kryptologie), 2017. Last visited on 04.01.2017.

[112] Wikipedia – Token, Rechnernetz. URL: https://de.wikipedia.org/wiki/Token_(Rechnernetz), 2017. Last visited on 31.10.2017.

[113] Muneeb Ali, Jude Nelson, Ryan Shea, and Michael J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *2016 USENIX Annual Technical Conference (USENIX ATC 16)*, pages 181–194. USENIX Association, 2016.

[114] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. Enabling blockchain innovations with pegged sidechains. *URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 2014.

[115] Martijn Bastiaan. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. *URL: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-of-two-phase-proof-of-work-in-bitcoin.pdf*, 2015.

[116] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. Deanonymisation of clients in bitcoin p2p network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 15–29. ACM, 2014.

[117] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

[118] Bernd Eylert and Dorothee Eylert. Ausgewählte Verschlüsselungsverfahren. In *Sicherheit in der Informationstechnik*, pages 67–83. News & Media, 2012.

[119] Bernd Eylert and Janett Mohnke. Signaturverfahren. In *Sicherheit in der Informationstechnik*, pages 84–90. News & Media, Berlin, 2012.

[120] Pedro Franco. *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons, 2014.

[121] Maximilian Friedlmaier, Andranik Tumasjan, and Isabell M Welpe. Disrupting Industries With Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures. 2016.

[122] Tatiana Gayvoronskaya and Bernd Eylert. Smartcard-Einsatz für sicheren, personaliesierten Dateitransfer im Automotive Bereich. In *Wildau, TH, Masterarbeit, A2013/0201*, page 109. Wildau, TH, 2012.

[123] The Australian Government. Backing Australian FinTech, 2016.

[124] BitFury Group. Proof of Stake versus Proof of Work. In *White Paper, Sep 13, 2015 (Version 1.0)*, pages 1–26. BitFury Group, 2015.

[125] BitFury Group. Digital Assets on Public Blockchains. *White paper*, 2016.

[126] Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Kryptowährung mit Proof-of-Stake. *peercoin.net*, 2012.

[127] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[128] Sergio Demian Lerner. Rootstock – Bitcoin powered Smart Contracts. *theblockchain.com*, 2015.

[129] David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.

[130] Scott Morrison. Australia leading international blockchain standards. URL: `http://sjm.ministers.treasury.gov.au/media-release/097-2016/`, 2016. Last visited on 23.11.2016.

[131] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[132] Giuseppe Pappalardo, Tiziana Di Matteo, Guido Caldarelli, and Tomaso Aste. Blockchain Inefficiency in the Bitcoin Peers Network. *arXiv preprint arXiv:1704.01414*, 2017.

[133] Paulina Pesch and Rainer Böhme. Datenschutz trotz öffentlicher Blockchain? *Datenschutz und Datensicherheit-DuD*, 41(2):93–98, 2017.

[134] Joseph Poon and Vitalik Buterin. Plasma: Scalable Autonomous Smart Contracts. *White paper*, 2017.

[135] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2015.

[136] Pavel Prihodko, Slava Zhigulin, Mykola Sahno, Aleksei Ostrovskiy, and Olaoluwa Osuntokun. Flare: An Approach to Routing in Lightning Network. *bitfury.com*, 2016.

[137] Veena Pureswaran and Paul Brody. Device democracy: Saving the future of the Internet of Things. *IBM Corporation*, 2015.

[138] Hans P. Reiser and Rüdiger Kapitza. Verteilte Algorithmen. In *Verteilte Algorithmen*, pages 1–16. Universität Erlangen-Nürnberg, 2003.

[139] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

[140] David Schwartz, Noah Youngs, and Arthur Britto. The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 5, 2014.

[141] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[142] David M. Toth. *The Byzantine Agreement Protocol Applied to Security*. PhD thesis, WORCESTER POLYTECHNIC INSTITUTE, 2004.

[143] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. Storj a peer-to-peer cloud storage network. 2014.

Aktuelle Technische Berichte des Hasso-Plattner-Instituts

Band	ISBN	Titel	Autoren / Redaktion
123	978-3-86956-433-3	**Metric Temporal Graph Logic over Typed Attributed Graphs**	Holger Giese, Maria Maximova, Lucas Sakizloglou, Sven Schneider
122	978-3-86956-432-6	**Proceedings of the Fifth HPI Cloud Symposium "Operating the Cloud" 2017**	Estee van der Walt, Isaac Odun-Ayo, Matthias Bastian, Mohamed Esam Eldin Elsaid
121	978-3-86956-430-2	**Towards version control in object-based systems**	Jakob Reschke, Marcel Taeumel, Tobias Pape, Fabio Niephaus, Robert Hirschfeld
120	978-3-86956-422-7	**Squimera : a live, Smalltalk-based IDE for dynamic programming languages**	Fabio Niephaus, Tim Felgentreff, Robert Hirschfeld
119	978-3-86956-406-7	**k-Inductive invariant Checking for Graph Transformation Systems**	Johannes Dyck, Holger Giese
118	978-3-86956-405-0	**Probabilistic timed graph transformation systems**	Maria Maximova, Holger Giese, Christian Krause
117	978-3-86956-401-2	**Proceedings of the Fourth HPI Cloud Symposium "Operating the Cloud" 2016**	Stefan Klauck, Fabian Maschler, Karsten Tausche
116	978-3-86956-397-8	**Die Cloud für Schulen in Deutschland : Konzept und Pilotierung der Schul-Cloud**	Jan Renz, Catrina Grella, Nils Karn, Christiane Hagedorn, Christoph Meinel
115	978-3-86956-396-1	**Symbolic model generation for graph properties**	Sven Schneider, Leen Lambers, Fernando Orejas
114	978-3-86956-395-4	**Management Digitaler Identitäten : aktueller Status und zukünftige Trends**	Christian Tietz, Chris Pelchen, Christoph Meinel, Maxim Schnjakin
113	978-3-86956-394-7	**Blockchain : Technologie, Funktionen, Einsatzbereiche**	Tatiana Gayvoronskaya, Christoph Meinel, Maxim Schnjakin
112	978-3-86956-391-6	**Automatic verification of behavior preservation at the transformation level for relational model transformation**	Johannes Dyck, Holger Giese, Leen Lambers
111	978-3-86956-390-9	**Proceedings of the 10th Ph.D. retreat of the HPI research school on service-oriented systems engineering**	Christoph Meinel, Hasso Plattner, Mathias Weske, Andreas Polze, Robert Hirschfeld, Felix Naumann, Holger Giese, Patrick Baudisch, Tobias Friedrich, Emmanuel Müller

ISBN 978-3-86956-441-8
ISSN 1613-5652