Cryptographic Technology Blockchain and Its Applications

Andriy Luntovskyy[1](✉) and Dietbert Guetter[2](✉)

[1] BA Dresden University of Cooperative Education (Saxon Study Academy),
Hans-Grundig-Str. 25, 01307 Dresden, Germany
Andriy.Luntovskyy@ba-dresden.de

[2] Dresden University of Technology,
Noethnitzer Str. 46, 01187 Dresden, Germany
Dietbert.Guetter@tu-dresden.de

Abstract. The use of modern cryptotechnology “Blockchain” for acceleration, transparency and decentralization of financial transactions and as a promising digital payment instruments and cryptocurrencies (e.g. Bitcoin, Monero, and Ethereum) has become an important trend since approximately 2000.

This article focuses the problem of using blockchain technologies and their networked cryptographic applications and apps.

The influencing factors and sources of Blockchain cryptotechnology were discussed, the comparison of centralized bank systems vs. decentralized systems was carried out, the mining process for cryptographic currencies, the concept of a public ledger, the validation principles PoW and PoS are represented, and profitability of cryptographic currencies was analyzed. Furthermore, important applications of Blockchain cryptotechnology were shown (such as Smart Contracting, Bletchley) as well as the accompanying risks, their advantages and disadvantages were discussed. In addition, the malicious applications were discussed such as the ransomware (extortion Trojans).

Finally, the potential and future perspectives of Blockchain cryptotechnology for real business applications were assessed.

Keywords: Blockchain · Cryptocurrency · Electronic payments · Decentralized payment system · Mining · Energy efficiency · Bitcoin · Ethereum · Monero · Smart Contracting · Ransomware · Profitability

1 Motivation: Payment Instruments in Past and Future

Blockchain is a cryptographically distributed computer network application supporting a decentralized payment system and decentralized financial online transactions in the peer-to-peer (P2P) concept. However, the economic success of this cryptotechnology will be evident in the next 10 up to 20 years.

Figure 1(a, b) depicts the historical development of the payment instruments from archaic shells and early coins to e-cash and cryptocurrencies, which can accelerate financial transactions and significantly reduce the cash mass. The important milestones of Blockchain technology are as follows [1, 2, 5, 11, 12]:

M. Ilchenko et al. (Eds.): UKRMICO 2018, LNEE 560, pp. 14–33, 2019.
https://doi.org/10.1007/978-3-030-16770-7_2

- 1991 – The basic principles from S. Haber and W. Scott: cryptografically secured chaining of individual blocks
- 2000 – Theory for cryptographic blockchaining of Stefan Konst as well as some implementation solutions
- 2008 – White Paper "Bitcoin: A Peer-to-Peer Electronic Cash System" for the conception of a distributed database system BTC created by so-called "Satoshi Nakamoto" (a pseudo of the known developing group as well as a lot of numerous speculations about the developer name, i.a. Elon Musk was mentioned, the founder, CEO and CTO of the companies like PayPal, SpaceX and Tesla)
- 2009 – Launch of the first publicly distributed worldwide Blockchain.

Additionally, an important question on the edge: who did actually invent and create Bitcoin?

Assumption:

Bitcoin was combined by the names of the prominent companies Samsung, Toshiba, Nakamichi and Motorola, i.e.

Satoshi = Samsung + Toshiba
Nakamoto = Nakamichi + Motorola.

A graphical comparison of the decentralized chaining of the secured blocks with a centralized banking system can be seen in Fig. 2 (a, b).

Early coins
Metal coins
Seashells
Banknotes
Debentures
a) Central system: issuing authorities, states, banking
bitcoin
Cryptocurrency
b) Decentralized Blockchain system

Fig. 1. Payment instruments in past and future

The deployment of Blockchain technology speaks mainly for a decentralized financial system. The advantages of such a solution are obvious:

- Sustainability, general transparency and commitment
- Accelerated economic workflows and digitization processes (so-called IT in the digital age)
- Blockchain cryptotechnology is also well-suited to supporting current cryptocurrencies (such as Bitcoin, Monero, Ethereum).

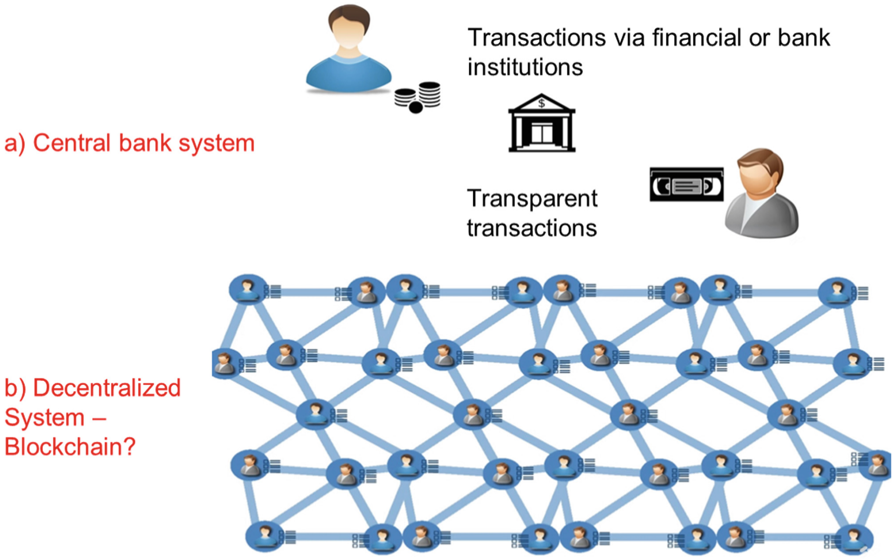

Transactions via financial or bank institutions
a) Central bank system
Transparent transactions
b) Decentralized System – Blockchain?

Fig. 2. Decentralized chaining of blocks instead of a central bank system.

2 Blockchain Architecture

Decentralized, cryptographically secured and unified blocks, their chains and transactions are grouped under a general, global public ledger (account), the structure of which is as follows (Fig. 3).

The Blockchain, as a networked Public Ledger, consists of participating nodes that represent an efficient P2P communication model. Typical features of the Blockchain are as follows:

- Redundancy and synchronization
- Cryptographic hash procedures for integrity assurance and attack safety
- Decentralized management and control of the Blockchain
- Network subscribers are also referred to as Nodes (Full-Nodes, Miners, Validators) and run redundantly with mutual synchronization

In addition, large block volumina can cause the “Big Data” problem.

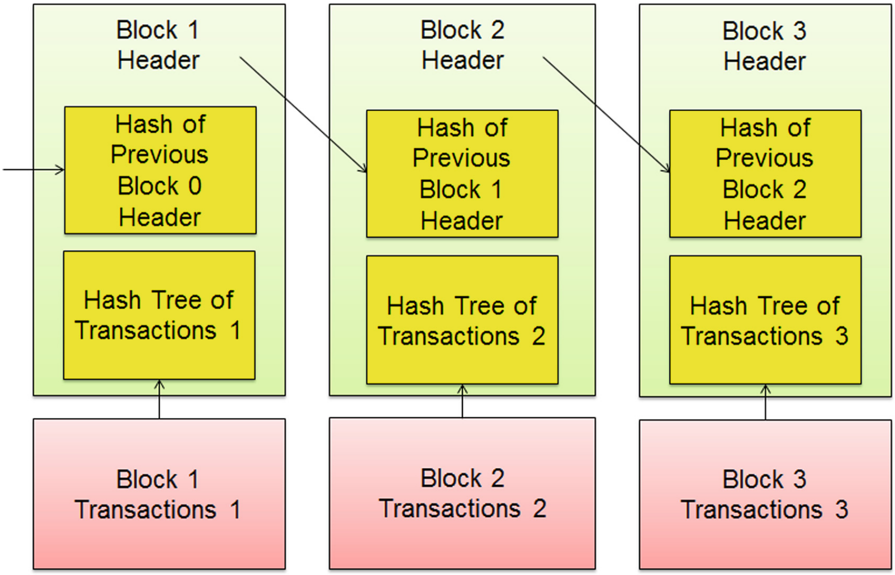

Block 1 Header
Hash of Previous Block 0 Header
Hash Tree of Transactions 1
Block 2 Header
Hash of Previous Block 1 Header
Hash Tree of Transactions 2
Block 3 Header
Hash of Previous Block 2 Header
Hash Tree of Transactions 3
Block 1 Transactions 1
Block 2 Transactions 2
Block 3 Transactions 3

Fig. 3. Block chaining (headers and blocks within a hash tree)

Figure 4 depicts the structure for an exemplary block chain.

- The defining block chain (yellow color) consists of the longest sequence of secured blocks from the origin to the current block (blue).
- Alternative chains (pink color) became orphan as soon as they are shorter than another chain.

Within the Blockchain architecture between the following basic components can be distinguished: the simple Nodes, the Full-Nodes, and Miner/Validator:

1. **Nodes**:
   Each Blockchain participant (computer, smartphones, tablets, or even clusters) is qualified as Node, if he has installed the corresponding software, which runs based on the Bitcoin protocol or the program code of Bitcoin.
2. **Full-Nodes:**
   - A Node with full local copy of the Blockchain
   - Checking for so-called “consensus rules”
3. **Miner/Validator**
   - The individual participants or mining pool (high resource requirements regarding hardware and energy consumption)
   - Finalising of blocks (Miner – block generation, Validator – proving)
   - Externally they act each like a large participant, but in fact many small blocks are generated for payment in fractions of the cryptocurrency units.

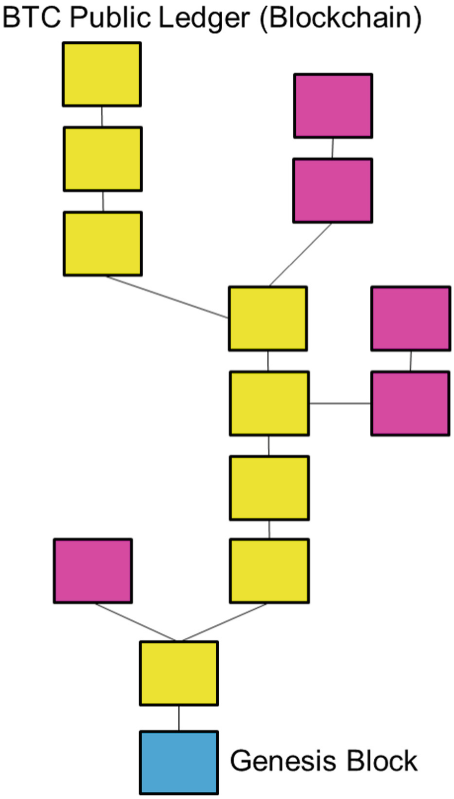


Fig. 4. Distributed digital public ledger

However, the following problems occur during the Blockchain operation:

- Enormous energy consumption due to "mining" of cryptocurrencies (processing of the hash blocks via its algorithmic complexity).
- Exponential memory growth (including capacity migration between USB media, smartphones, PC, storage media such as SAN/NAS, as well as cloud storages)
- Cryptographic data security is guaranteed, but privacy issues may arise. One way out is as follows: no processing the complete Blockchain with all the transactions, but only use of excerpts of the Blockchain without a prehistory.

3 Cryptographic Technology Blockchain and Cryptocurrencies

A cryptocurrency is a digital payment instrument under use of cryptographic methods to realize a decentralized and secure payment system. The following questions can occur for describing of the discussed functionality:

- How is new money created? – Create a new block
- How can the transactions be stored? – Creator of a block selects certain transactions
- How does the respective credit balance come about? – A credit is the sum of all procressed transactions of a user.

Example 1

The examples of the cryptocurrencies: Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin. One of them, the cryptocurrency Monero (XMR), has the following properties:

Proof-of-Work with CryptoNight

Memory intensive, but relatively low computational effort

Supported WebAssembly and Coinhive (Coinhive.com) with JavaScript-Mining for Monero-Blockchain

The users can run the miner directly in their browsers and "mine" the XMR for an ad-free experience!

Table 1 contains an overview of current cryptocurrencies.

Table 1. Overview of cryptocurrencies and market growth (sources: [3, 4, 13], https://coinmarketcap.com/)

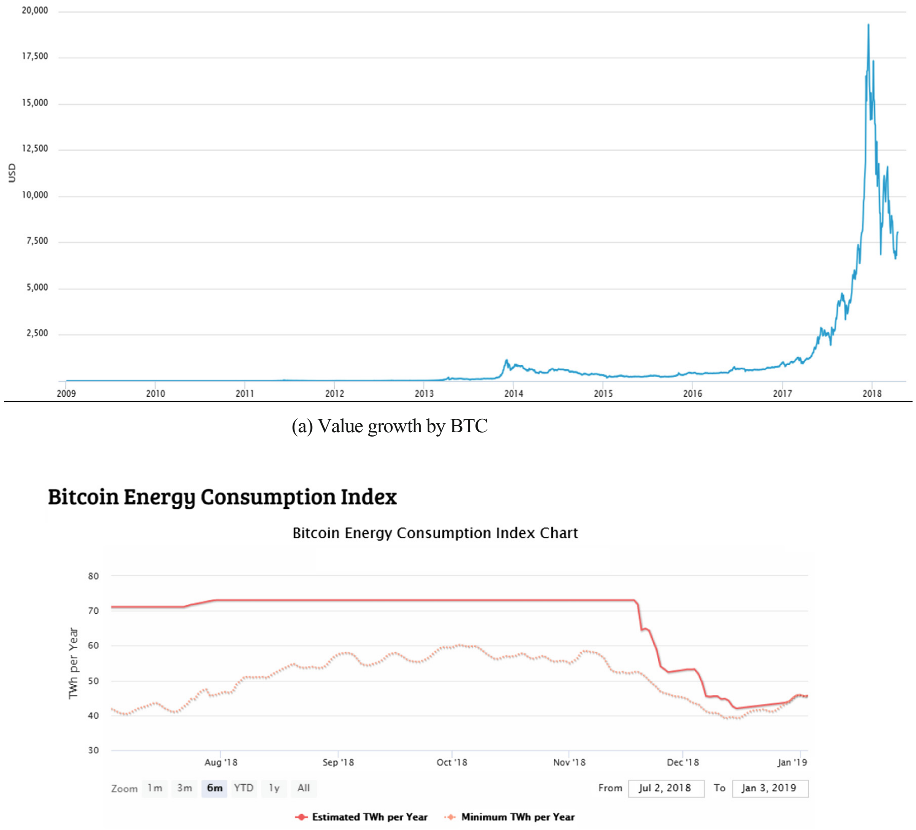
#	Currency	Shorthand symbol	Launch	Mining available	Percentage	Emission
1	Bitcoin	BTC	2009	yes, SHA-256	84,2%	3,9% per anno
2	Ethereum	ETH	2015	yes, Ethash	6,4%	14% per anno
3	Ripple	XRP	2013	no	2,1%	4,1% per anno
4	Litecoin	LTC	2011	yes, Scrypt	1,4%	11% per anno
5	Ethereum classic	ETC	2016	yes, Ethash	0,5%	14% per anno
6	Monero	XMR	2014	yes, CryptoNight	0,5%	20% per anno
7	Dash (formerly darkcoin)	DASH	2014	yes, X11	0,4%	11% per anno

Digital payment instruments under use of cryptographic principles, which built a fast growing market nowadays, are often created via deployment of the hash algorithms titled SHA256 (FIPS NIST 2008). Such algorithms (refer Table 2) were introduced since 2002. The first representant was titled SHA-1. The successor was SHA-2 (including the further modifications like SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256). The hash size is variable between 224, 256, 384 and 512 bits by the parametrized round number 64 or 80.

Table 2. Overview of NIST hash algorithms [17]

Hash algorithm	Message size (bits)	Block size (bits)	Word size (bits)	Message digest Size (bits)
SHA-1	$<2^{64}$	512	32	160
SHA-224	$<2^{64}$	512	32	224
SHA-256 (blockchain)	**$<2^{64}$**	**512**	**32**	**256**
SHA-384	$<2^{128}$	1024	64	384
SHA-512	$<2^{128}$	1024	64	512

The cryptoapplication Bitcoin (founded in 2009 and based on the Blockchain) is today considered as one of the most important cryptocurrencies (shorthand symbol BTC). The value growth as well as energy consumption by BTC was depicted in the given diagram (refer Fig. 5a, b).



(a) Value growth by BTC

(b) Energy consumption by BTC

Legend (b):
- Estimated energy consumption per anno (upper curve),
- Minimum energy consumption per anno (lower curve as a dash-dot line)

Fig. 5. Hype period for the cryptocurrency Bitcoin (Sources: http://www.heise.de/forum/, http://www.statista.de/, https://digiconomist.net/bitcoin-energy-consumption)

However, there is also criticism ([7, 9, 15, 16], http://www.heise.de/forum/):

- Blockchain is itself the biggest problem for Bitcoin (due to energy and memory consumption).
- Bitcoin was primarily intended as a decentralized payment system. But due to the exponential growth (storage requirements) of the Blockchain, anyone can still hold the blocks on its local HDD or other storage device. On the smartphones or other mobile devices, the retrieving is also unthinkable anyway. This may affect i.a. the obligation and traceability of transactions.
- Due to critical requirements on ever-growing memory for the Blockchain the users hold the blocks on centralized servers and cloud services and then access it with their online clients. This leads to a certain centralization and is again depending on the central Blockchain servers offered by bank-analog financial institutions and stock markets. The original advantage of decentralization and thus security against manipulation and server failures is no longer available!

4 Profitability of Bitcoin Is Questionable?

As it was shown the cryptocurrency Bitcoin is one of the most popular cryptocurrency examples. Equation (1) describes the profit of cryptocurrency generation. Equation (2) describes the complexity of the mining process via Blockchain [1]:

$$profit = revenue - \left(cost_{electricity} + cost_{difficulty}\right) \tag{1}$$

$$cost_{difficulty} = \frac{\max imum - difficulty}{current - difficulty} \times \frac{2^{32}}{hashrate} \tag{2}$$

The good profitability of BTC production is difficult to consider or predict due to enormous algorithmic complexity and rising energy prices (Fig. 6).

Example 2

On January 4, 2019 the cryptocurrencies Bitcoin (shorthand symbol BTC) and Monero (shorthand symbol XMR) stood by an exchange price of (refer https://de.coinmill.com/):

- Cryptocurrency Bitcoin obtains the value: 3364 EUR = 1 BTC
- Cryptocurrency Monero obtains the value: 43 EUR = 1 XMR.

It should be noted that the variable exchange rates of these cryptocurrencies are not related to the realities of the world industry and trade, so investments in these domains is highly risky. Table 3 contains the most important questions regarding modern cryptocurrencies:

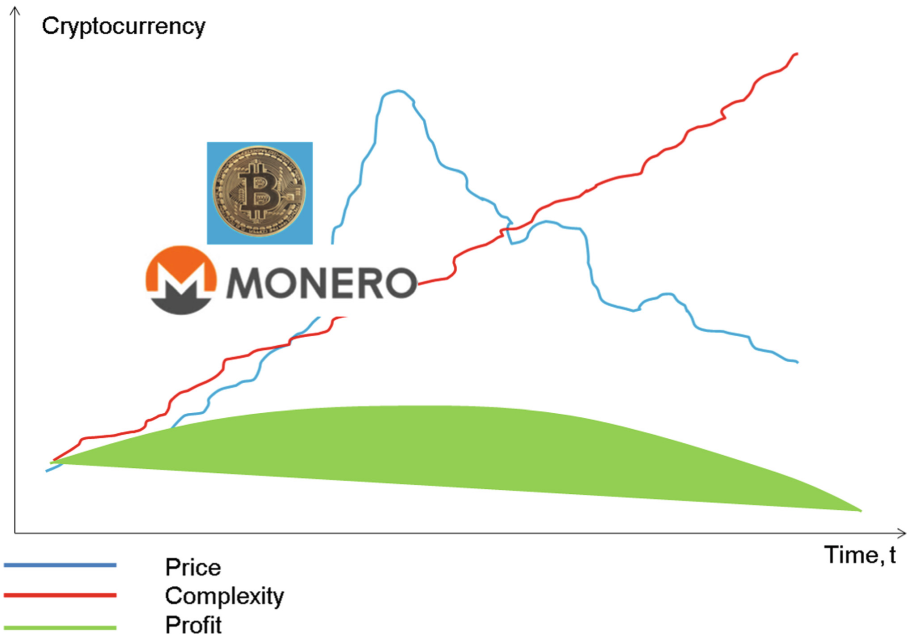


Fig. 6. Profit evaluation for Bitcoin [1, 15]

Table 3. FAQ regarding modern cryptocurrencies

Question	Answer
1. How does it operate?	See above
2. How is new currency generated?	You have to generate a new block for the Blockchain system
3. How can I save transactions?	The blocker chooses certain transactions
4. How is the loan balance provided?	Credit is the sum of all user transactions

5 Operation and Validation of Blockchain

The formation of a transaction block is depiected in Fig. 7. During the Blockchain operation the transaction block is generated accompanied by the both validation processes (Fig. 8):

- PoW, Proof of Work
- PoS, Proof of Stake.

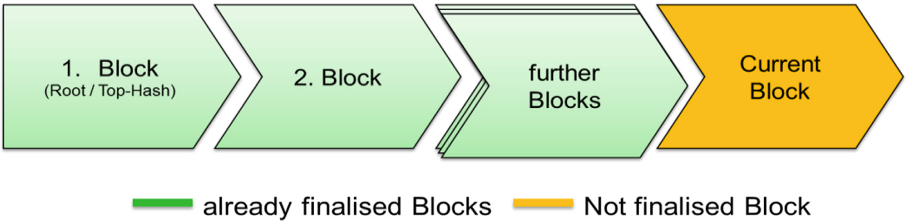


Fig. 7. Blockchain operation: block construction

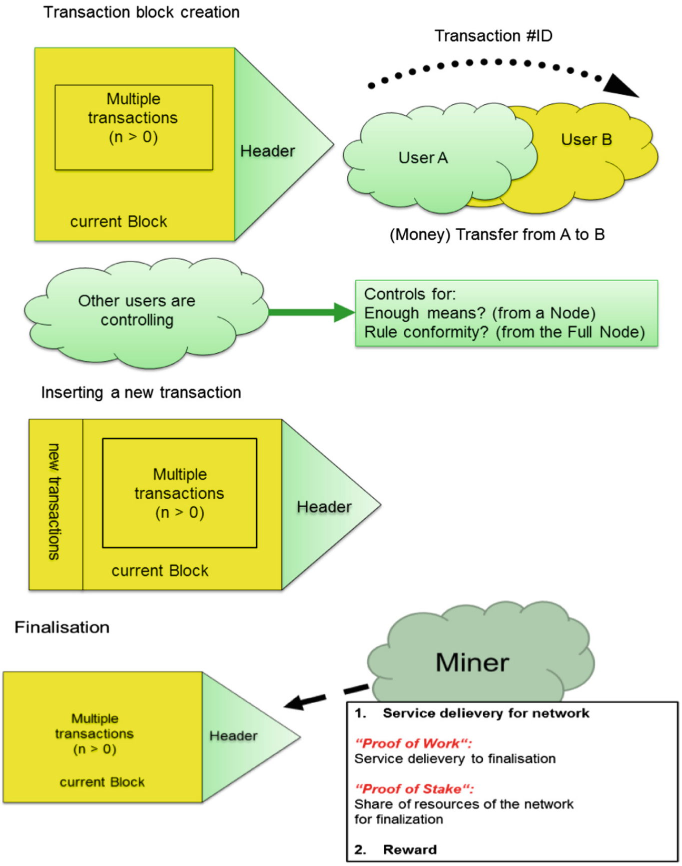

Transaction block creation
Multiple transactions (n > 0)
current Block
Header
Transaction #ID
User A
User B
(Money) Transfer from A to B
Other users are controlling
Controls for:
Enough means? (from a Node)
Rule conformity? (from the Full Node)
Inserting a new transaction
new transactions
Multiple transactions (n > 0)
current Block
Header
Finalisation
Multiple transactions (n > 0)
current Block
Header
Miner
1. Service delievery for network
"Proof of Work":
Service delievery to finalisation
"Proof of Stake":
Share of resources of the network for finalization
2. Reward

Fig. 8. Blockchain operation: generation of a transaction block

The complete tracking of the chain begins from the first own transaction (refer Fig. 9).

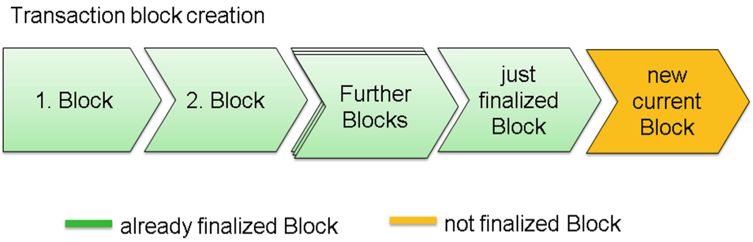
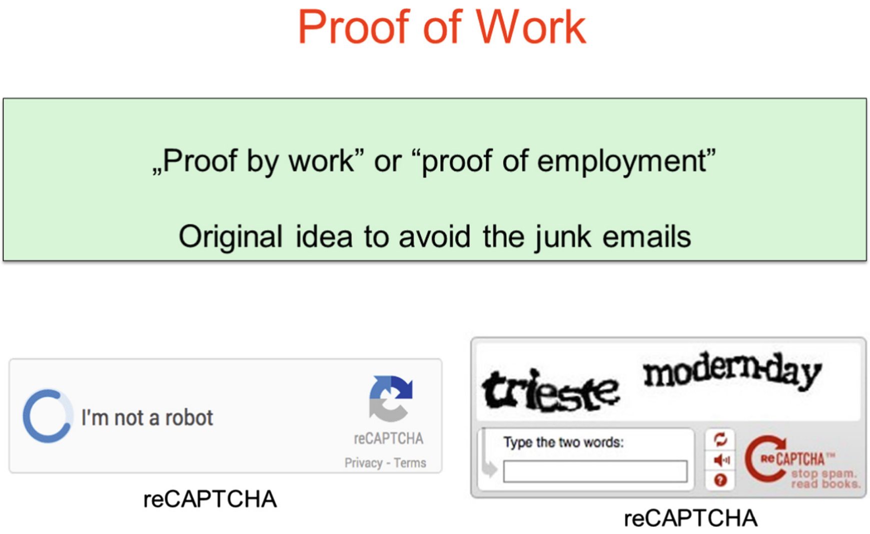


Fig. 9. Blockchain operation: complete tracking of the chain from the first own transaction

What is understood in the frame of the Blockchain technology under the validation processes titled PoW (Proof of Work) and PoS (Proof of Stake) respectively

1. Proof of Work, PoW

PoW is the cryptographic puzzle to confirm the complexity of a particular task and service functions. This demonstrates an overuse of this service, such as a Denial-of-Service-Attack on an Internet host, or a spamming e-mail chain to an SMTP server. PoW should prevent such excessive use of the considered service (Fig. 10).


Proof of Work

„Proof by work" or "proof of employment"

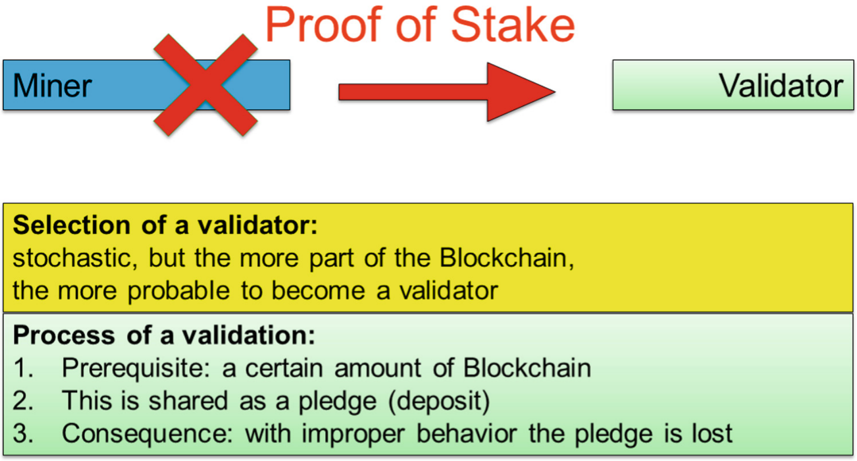
Original idea to avoid the junk emails

Fig. 10. Blockchain operation: PoW

2. Proof of Stake, PoS

Under PoS is understood a complete or partial proofing method which can create so-called “consensus”: it means which party (which participant) of the Blockchain is allowed to generate the next block (Fig. 11). In this case, a weighted random selection is made, in which weightings are determined for each participant, depending on the duration of the participant’s participation and/or his “assets” (stake). Unlike the PoW, which uses cryptocurrencies Bitcoin and Ethereum, PoS does not consume time or energy like mining processing, nor can the network be “intercepted” because it has a single processing power (“51% attack”) (see Figs. 10 and 11). Instead of a miner, a validator is used whose selection is stochastic.

The best selection options have the validators that stay in the system the longest. A specific part of the Blockchain system is reserved for verification. Such a reserved deposit or “pledge” is distributed and a check is made. In the presence of injuries/offenses, the custody is definitely lost.



Selection of a validator:
stochastic, but the more part of the Blockchain, the more probable to become a validator

Process of a validation:

1. Prerequisite: a certain amount of Blockchain
2. This is shared as a pledge (deposit)
3. Consequence: with improper behavior the pledge is lost

Fig. 11. Blockchain operation: PoS

6 Practical Blockchain Applications

6.1 Framework MS Bletchley

In July 2016 the framework MS Bletchley was launched as a specific service BaaS (Blockchain as a Service) and as a part of the Azure cloud platform. The main goal of the framework introduction [6, 8, 14] was the acceleration of the development of the practical Blockchain applications aimed to financial institutions, manufacturing, retail, healthcare, public sector, media on a common platform. The above mentioned platform contains three following layers (Fig. 12):

1. Base platform tier
2. Middleware (MW) tier
3. Industrial solutions layer.

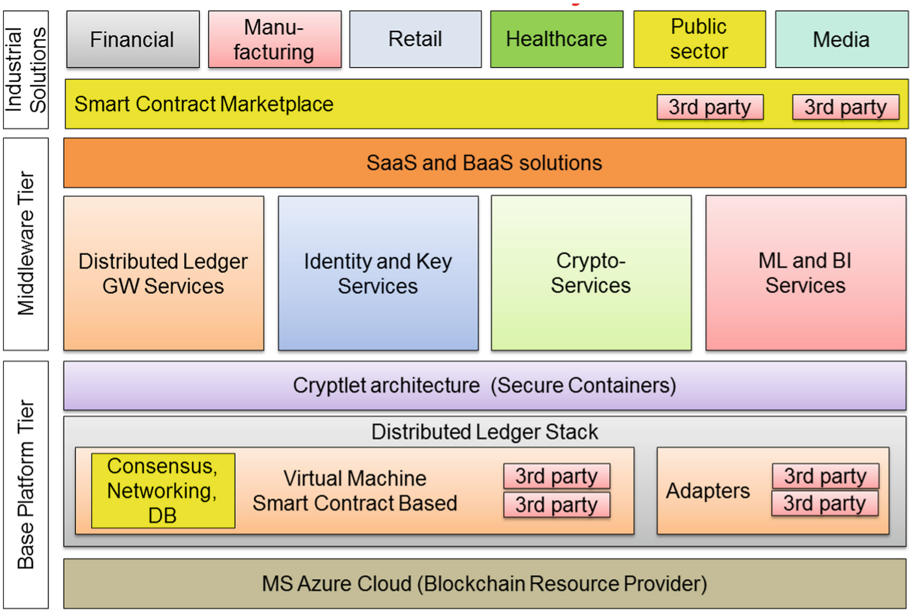


Fig. 12. Blockchain platform MS Bletchley (based on: http://www.microsoft.com)

The framework MS Bletchley introduces two new concepts: Blockchain middleware (MW) with so-called cryptlets. To SaaS and BaaS belong i.a. so-called ML and BI functionality (Machine Learning and Business Intelligence). The Blockchain MW components support the core features of services in the clouds, such as identity management, analytics, or machine learning.

Based on the Azure cloud, these components can work with different Blockchain-based technologies aimed to creaton of the practical applications. The cryptlets are the building blocks for the Blockchain technology. They are designed to ensure secure communication between the Azure cloud, the MW ecosystem and each specific customer's technology. The interoperability of the applications with Azure cloud and Azure stack is secured, as well as with the 3rd parties, the clouds like AWS, Google and further private clouds.

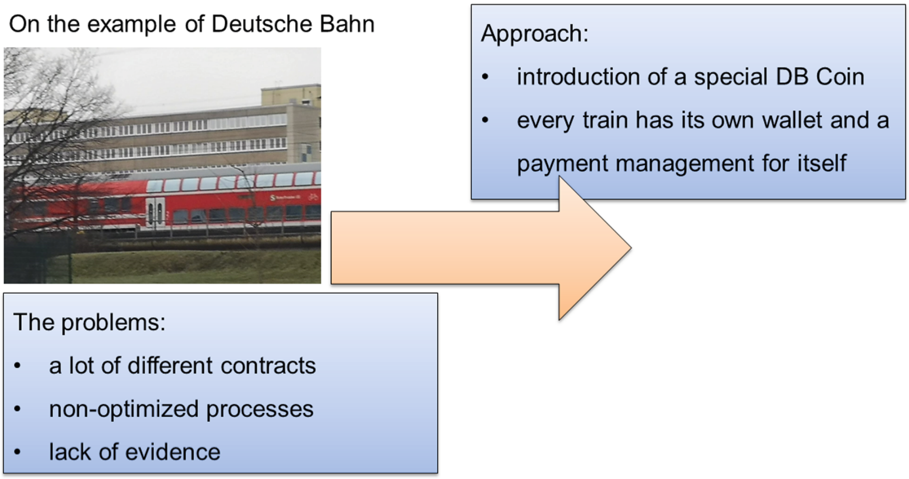
6.2 Smart Contracting

Further Blockchain applications are so-called Smart Contracts [7, 20–22]. A "smart" contract is a software-based agreement that allows and can contain a variety of contract terms. In the course of the usual contract processing (transactioning), certain linked actions can be executed automatically if there is a corresponding trigger. The contracts are offered and signed within and via the Blockchain. The evident advantages of the discussed approach are as follows:

- Digitality and legal openness of the platform
- Transparency and time savings.

Example 3

An example of a Smart Contracting application for DB.de [7, 20–22] is given in Fig. 13.



On the example of Deutsche Bahn

Approach:

- introduction of a special DB Coin
- every train has its own wallet and a payment management for itself

The problems:

- a lot of different contracts
- non-optimized processes
- lack of evidence

Fig. 13. Smart Contracting on the example of DB.de [7, 20–22]

Furthermore, the Blockchain is used for Smart Contracting applications for the following world-wide leading companies deployed:

- Walmart, Maersk, Alibaba, CartaSense, Kuehne + Nagel (aimed to logistics, sea freight, stock exchanges, marking of containers)
- Nestlé, Tyson Foods, Unilever (aimed to food delivery)
- Everledger (the registers for diamond certification) and so on.

7 Risks and Hacking

Despite of advances in modern cryptography, viruses and Trojans are however an important threat to the Blockchain technology [18, 19]. Sure, even the Blockchain can also store any data that is often different from financial transactions, transactions and contracts. Such malicious messages can be written to the source transaction addresses using the scripting language OP_Return. Therefore, the Blockchain can also block the extremistic or pornographic contents.

As an example of such manipulation of the contents of the Blockchain, the Cryptograffiti.info website may be viewed for read and write accesses.

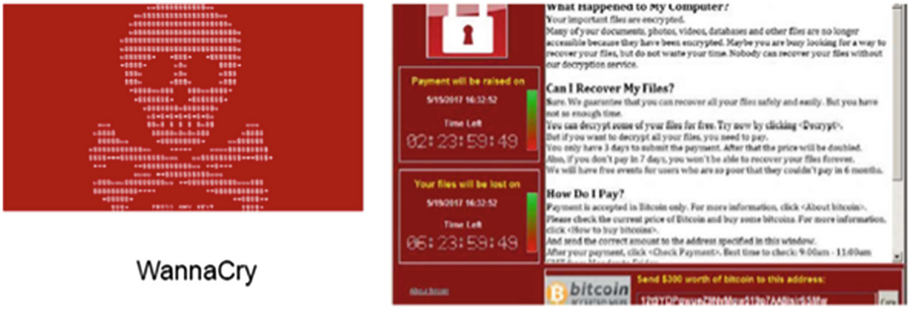
7.1 Ransomware

The next important topic is so-called Ransomware as a dangerous malware type with a blackmail background and the following features:

- Dangerous malware with extortionate action
- Virus-like operation
- Get through prepared attachments to emails
- Exploiting the vulnerabilities of web browsers
- Encryption of passwords and/or files on the hard disk with a powerful 2048-bit-long RSA key
- Prevented or completely blocked encrypted access by the victim to their own data.

Example 4

The ransomware prevents access to the initially encrypted user data. The victim is required to pay a ransom in cryptocurrency units (frequently in bitcoins), about the equivalent of $ 300–500. The source of the attack or the recipient of the repayment is difficult to track through the use of cryptography. Some examples of this type of Blockchain apps have been listed in Fig. 14.



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

Fig. 14. Ransomware (screenshots)

One of the well-known examples of ransomware was crypto-trojan WannaCry (approx. 300.000 PCs in 150 countries were affected) as well as Wcrypt, WCRY, WannaCrypt, Wana Decrypt0r 2.0 etc. Many international companies have suffered from these harmful applications.

The GandCrab Ransomware belongs to one of the latest recent risks. The effect of the GandCrab ransomware can be seen in the above figure. An exemplary workflow for the "careless users" was depicted (Fig. 15). Additionally this includes the use of the no-name and well-unstudied development tools (kits). The ransomware also searches for vulnerabilities in Java, IE, Adobe plugins etc.

Unfortunately, the well-known antimalware like ESET, Avira or Kaspersky do not currently have any antidotes.

Example 5

A Windows host receives an e-mail. The subject of the e-mail is titled “Application form to the advertised position – Nadine Bachert/Sarah Summer/Viktoria Hagen/Caroline Smith/Margareth Williams” etc. The application form contains a cover letter, a photo and a CV. The spam filters can classify these as a non-harmful. The malware is packaged as an attachment in a ZIP file. The file contains an executable file. If this file is executed by the user, a symmetric encryption procedure starts. For the key to restore the encrypted host data a ransom is asked. For each user, a unique URL on an anonymizer gate for hidden service is generated. Behind the gate, within the anonymized network the ransom amount and the instructions for payment can be viewed. The amount will be mostly adjusted to the victim.

What is the average case, how do companies solve the problem? The distribution of primary actions for the victims is as follows:

- 78% restore the system simply with a backup
- 20% pay even blackmail money (ransom) to avoid reputation losses
- 2% even try to decrypt themselves.

The advanced firewall systems [1, 23] such as Cisco Umbrella and Check Point R80 contain Anti-Ransomware and can efficiently detect and prevent unauthorized access to the desktop systems, the clouds, the corporate data centers and networks under use of so-called Intrusion Detection/Prevention Systems (IDS/IPS).

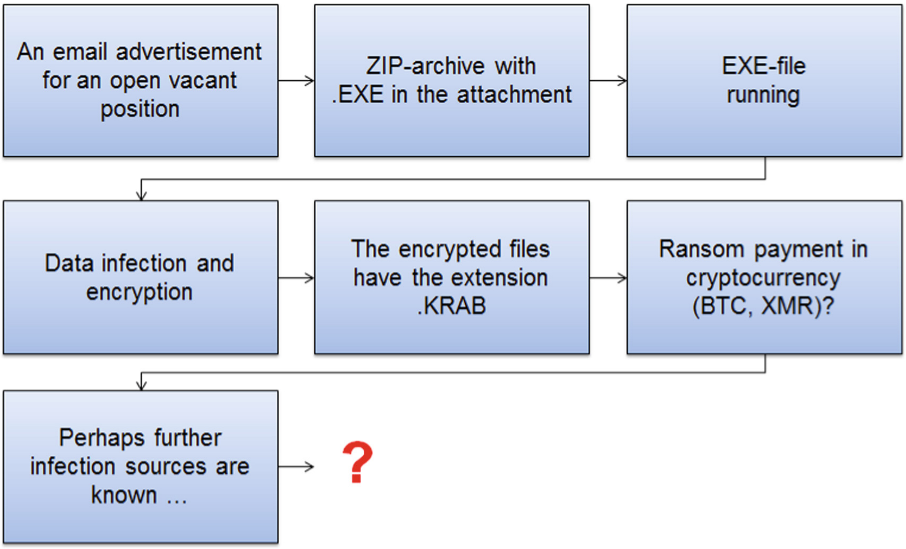

An email advertisement for an open vacant position
ZIP-archive with .EXE in the attachment
EXE-file running
Data infection and encryption
The encrypted files have the extension .KRAB
Ransom payment in cryptocurrency (BTC, XMR)?
Perhaps further infection sources are known …
?

Fig. 15. GandCrab Ransomware: exemplary procedure for “careless users” [19]

7.2 Cryptocurrency Fraud

Some cases of large-scale cryptocurrency fraud in billion amounts became known to the public last time. Cybercriminals use for the robbery the anonymous Internet (so-called Darknet), which can potentially arise through a MIX cascading [1, 23] and is therefore untraceable. This fact effectively ruins the reputation of such MIX networks as Tor, Onion, JAP which are aimed to guarantee primarily the anonymity and privacy for the users. The anonymous Internet is accessible through special software and cannot be generally fully monitored by security analysts.

The attackers can remain anonymous for longer periods. However, the average price for mentioned malware is only $ 224, with the market value for blockchain-oriented malware now as high as $ 6.7 million with potential for growth. The attacks on the growing crypto-exchange market now account for up to 25% of all Internet server attacks (according to Computer Forensic experts).

Example 6

According to the statistics for 2018, the following cyber currencies are recognized as the most common targets of fraudsters [18, 19]:

- Monero, XMR (2014) – 44% of hacker quota
- Ethereum, ETH (2015) – 11% of hacker quota
- Bitcoin, BTC (2009) – 10% of hacker quota.

The theft of cryptographic means of payment can be carried out by organized crime cartels or smaller criminal groups. However, it is often about highly skilled professionals looking for an additional criminal source of revenue on the anonymous internet. Most of these incidents related to the theft of the cryptocurrency have been unfortunately recorded in USA (24), China (10) and UK (8).

8 Analysis: What's Stopping the Development of Blockchain?

Despite optimistic forecasts and Blockchain perspectives, development and deployment of the technology is not so fast as the optimists would like to. Certain restrictions prevent this, for example [7, 15, 18]:

1. Control and management

Although the banks and financial institutions recognize the revolutionary character of the Blockchain applications, they also recognize the primary con: when everything is registered on the financial transactions, there is no more banking security and confidentiality! In the case of decentralized transaction processing, the lack of supervisory authorities means i.a. that even weapons and drugs can also be traded using the blocks and cryptocurrencies.

As conclusion:

In some countries – Romania, Kyrgizstan – a simple way was taken: the Blockchain transactions are prohibited.

The first steps towards the Blockchain regulation were undertaken within the EU. So since May 2018 the General Data Protection Regulation (GDPR, in German: DSGVO) came into force, which restricts the storage and processing of (personal and privacy) information. The Blockchain has to adhere to these restrictions – at least for EU citizens.

2. Mass character

Despite the apparent increase in cryptocurrency popularity, it should take several years for the cryptocurrency to become fully established. However, insufficient training of the population, skeptical citizens and certain unsuccessful or even criminal inset experiments (e.g. financial pyramid transactions) do not allow the Blockchain to conquer the market immediately.

There is also negative propaganda from some financial institutions and entire states, such as India and China, where the government creates a negative image of the Blockchain and calls every transaction a criminal offense.

3. Costs

The main algorithm for the blockchain is SHA-256. All operations are checked and executed according to this hash algorithm [17]. However, these are very energy intensive processes. By comparison, global hashing exceeded 2018 the level for the power consumption of Cyprus! And these resource requirements will increase even more with a higher number of transactions [3, 4, 13, 20].

9 Conclusions

1. Advantages:

- Blockchain is developing dynamically
- Large IT companies and financial institutions are becoming increasingly involved
- Blockchain is manipulation-proven and theoretically infinitely traceable
- Multiple applications: cryptocurrencies, Smart Contracting and middle-term automation of the domains where an intermediary (confident) is required.

2. Disadvantages:

- Complete replacement of the existing centralized banking system in middle-term is rather hopeless and fantastic; therefore rather niche business as an alternative to centralized banking system and stock exchanges
- Profitability of the Bitcoin and other cryptocurrencies is questionable!
- One thing is evident nowadays:
- The solution to the above listed problems may be too complex and resource-intensive, long-term mass data retrieving ("Big Data"), mass validity tests, prevention of criminal activities (ransomware, fraud)
- So, it is still unclear what way the Blockchain technology will take in the future?

Acknowledgment. Authors' acknowledgements to the BA Dresden students and scientific fellows (M. Stoll, E. Zumpe, F. Franke, Prof. Dr. L. Zipfel, Prof. Dr. E. Jahn), the colleagues and friends (Prof. Dr. L. Globa from NTUU "Igor Sikorsky KPI" Kyiv, Dr. habil. J. Spillner from ZHAW Zurich) for technical support, inspiration and challenges by fulfilling of this work.

References

1. Luntovskyy, A., Spillner, J.: Architectural Transformations in Network Services and Distributed Systems: Service Vision. Springer, Heidelberg (2017). Case Studies, XXIV, 344p., 238 pict., (ISBN: 9-783-6581-484-09)
2. Staples, M., Chen, S., et al.: Risks and opportunities for systems using blockchain and smart contracts
3. XMR: Was ist Monero? Kryptowährungen und Coins einfach erklärt. https://www.cryptolist.de/monero/
4. Monero – Secure, private, untraceable. https://getmonero.org/
5. Münzwelt: die Geschichte des Geldes, MDM; Abrufdatum. https://www.mdm.de/muenzwelt/einfuehrung-ins-muenzensammeln/geschichte-des-geldes/. Accessed 20 Sept 2017
6. Gray, M.: Projekt Bletchley Whitepaper, MS Worldwide Partner Conference Toronto, July 2016
7. Liesenjohann, M., et al.: Blockchain#Banking: Ein Leitfaden zum Ansatz des Distributed Ledger und Anwendungsszenarien, Bitkom 2016 (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.), 66 S. https://www.bitkom.org/noindex/Publikationen/2016/Leitfaden/Blockchain/161104-LF-Blockchain-final.pdf
8. Rixecker, K.: Modulares Blockchain-Framework von Microsoft: Das steckt hinter Project Bletchley. http://www.t3n.de/news/checked-c-microsoft-716063/
9. Malborn Wolff: Blockchain als Open Source: das Hyperledger-Projekt. https://www.maibornwolff.de/blog/blockchain-als-open-source-das-hyperledger-projekt
10. Blockexplorer. https://btc.com/3fb5f4fd6d1129b9797d66be1750b208a10ac2d551125990305211834be94cd9
11. Bundesanstalt für Finanzdienstleistungsaufsicht: Artikel: Blockchain Technologie; Abrufdatum. https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html. Accessed 1 Oct 2017
12. Welt-Bruttosozialprodukt, Bundeszentrale für Politische Bildung. https://www.bpb.de/nachschlagen/zahlen-und fakten/globalisierung/52655/welt-bruttoinlandsprodukt
13. Malmo, C.: Bitcoin hat ein großes Problem: Die Krypto-Währung ist einfach nicht nachhaltig. https://motherboard.vice.com/de/article/4xa9ed/das-oeko-problem-von-bitcoin-darum-ist-die-krypto-waehrung-nicht-nachhaltig-3920
14. Oberndorfer, E.: Blockchain as a Service: Microsoft baut einen Blockchain-Marktplatz. http://www.t3n.de/news/microsoft-blockchain-marktplatz-680639/
15. Giese, P., Kops, M., Wagenknecht, S., de Boer, D., Preus, M.: Die Bitcoin Bibel – Das Buch zur digitalen Währung. Verlag BTC-Echo (2016)
16. Simon Hülsbömer. Was ist Blockchain? https://www.computerwoche.de/a/blockchain-was-ist-das
17. Secure Hash Standards (Algorithms – SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), Federal Information Processing Standards, National Institute of Standards and Technology, 33 p. http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4. Accessed October 2008
18. Vishik, C., et al. (ed.): Blockchain: Perspectives on Research, Technology and Policy. https://pdfs.semanticscholar.org/405a/da981be3a49a78c3e5b281c539938c286001.pdf
19. Ransomware GandCrab. https://www.searchsecurity.de/news/252448017/Ransomware-GandCrab-kommt-als-Bewerbung-getarnt
20. Struckmeier, J.: Cloud and Heat Datacenter for AI, AR and Big Data: secure, scalable and sustainable, Workshop “Energieeffizientes Rechnen und Green IT”, BA Dresden, 59 p, 26 October 2018

21. Karzel, D., Klinger, P.: Prototyping einer Blockchain-Anwedung. In: Stal, M. (ed.) Magazin "Java mit Integrationsspektrum" für professionelle Entwicklung und Integration von Enterprise-Systemen, EAN 4194-156107907, pp. 37–40
22. Jansing, M., Tilkov, S.: Kluge Kontrakte auf Basis von Ethereum. In: Stal, M. (ed.) Magazin "Java mit Integrationsspektrum" für professionelle Entwicklung und Integration von Enterprise-Systemen, EAN 4194-156107907, pp. 41–45
23. Luntovskyy, A., Klymash, M.: Examination of modern concepts for firewalls and collaborative intrusion detection. Int. Res. J. Telecommun. Sci. (2), 44–49 (2016). Issue 14, Kiev (Registration Certificate KB No. 15064-3636P, ISSN 2219-9454, UDC 621.39)