Computer Science and Engineering 2018, 8(2): 23-29
DOI: 10.5923/j.computer.20180802.02

Understanding Blockchain Technology

Simanta Shekhar Sarmah

Business Intelligence Architect, Alpha Clinical Systems, USA

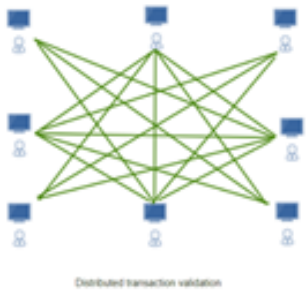
Abstract Blockchain is one of the most important technical invention in the recent years. Blockchain is a transparent money exchange system that has transformed the way a business is conducted. Companies and tech giants have started investing significantly in the blockchain market and it is expected to be net worth of more than 3 trillion dollars in next 5 years. It has become growing popular because of its irrefutable security and ability to provide complete solution to digital identity issues. It is a digital ledger in a peer to peer network. This paper provides a background on Blockchain technology, history, it's architecture, how it works, advantages and disadvantages and its application in different industries.

Keywords Blockchain, Cryptocurrency, Bitcoin, Peer-to-Peer Network, Decentralized Ledger, Nodes, Token

1. What is Blockchain

Blockchain technology is normally associated with cryptocurrencies such as Bitcoin. It is a database of record of transactions which is distributed, and which is validated and maintained by a network of computers around the world. Instead of a single central authority such as a bank, the records are supervised by a large community and no individual person has control over it and no one can go back and change or erase a transaction history. As compared to a conventional centralized database, the information cannot be manipulated due to blockchain's built in distributed nature of structure and confirmed guarantees by the peers. In another words, when a normal centralized database is located on an individual server, blockchain is distributed among the users of a software. Blockchain allows anyone on the network to access everyone else's entries which makes it impossible for one central entity to gain control of the network. Whenever someone performs a transaction, it goes to the network and computer algorithms determine the authenticity of the transaction. Once the transaction is verified, this new transaction is linked with the previous transaction forming a chain of transactions. This chain is called the blockchain.

Blockchain technology is based on decentralized network meaning it operates as a peer to peer network.



Distributed transaction validation

One of the most popular blockchain technology is Bitcoin which hosts a digital ledger. Bitcoin provides the platform to mine, store and trade bitcoins via a complex computer algorithm which is tied to a distributed network. Blockchains can be not only used for transactions but it can be considered as registry and inventory for all assets.

2. History of Blockchain

In the year 1976, a paper was released on "New Directions in Cryptography" discussed the concept of distributed ledger. With the advancement in the field of Cryptography, another paper entitled as "Hot to Time-Stamp a Digital Document" by Stuart Haber and Scott Stornetta which laid out the concept to timestamp the data instead of the medium. Another important concept called as "Electronic cash" or "Digital Currency" which came into existence based on a model proposed by David Chaum also contributed towards the development of the concept of Blockchain which was followed by Protocols such as e-cash schemes that introduced double spending detection.

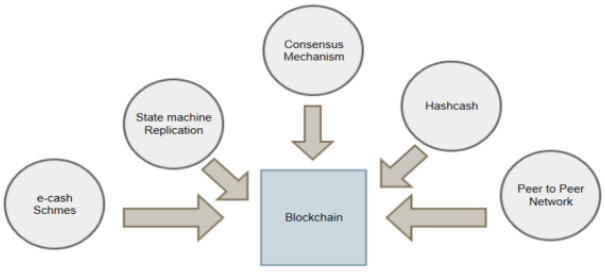
In 1997, Adam Back introduced another concept called "hashcash" which offered a solution to control spam emails. This lead to the concept of creating money called as "b-money" by Wei Dai based on peer to peer network.

* Corresponding author:
sarmah.simanta@gmail.com (Simanta Shekhar Sarmah)
Published online at http://journal.sapub.org/computer

Satoshi Nakamoto is considered as the inventor of blockchain technology when he published a paper on bitcoin in 2008 as "Bitcoin: A Peer-to-Peer Electronic Cash System,". The abstract of the paper was on the direct online payment from one source to another source without relying on a third-party source. The paper described an electronic payment system based on the concept of cryptography. Nakamoto's paper provided a solution to the double spending where a digital currency cannot be duplicated, and no one can spend it more than once. The paper stated the concept of public ledger where an electronic coin transaction history can be traced and confirmed if the coin has not been spent before and to prevent double spending issue.

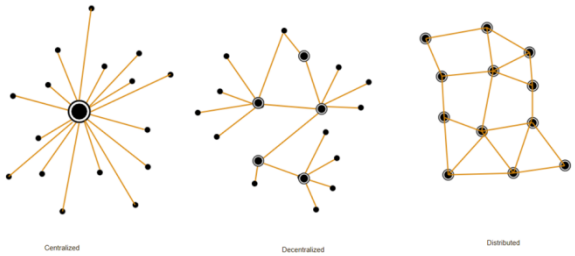
An open source program to implement bitcoin system was released just after a few months later and first bitcoin network was begun in early 2009 when Satoshi Nakamoto created the first bitcoins. Although the inventor of the bitcoins remains unanimous, bitcoins continued to be created and marketized and a large community was there to support and address various issues with the code.

There are hundreds of different cryptocurrencies such as Litecoin, Dogecoin etc., but bitcoins hold the lion share of the market it has become the most popular cryptocurrency among the others. It was able to draw the attention of the users due to its ability to keep its users unanimous, but it became real popular due its transparency. Bitcoin started to flourish since then and by the year 2013, investors started to pour funds on the start-ups related to Bitcoin. Bitcoins can be exchanged for regular currency, for any service or products. With the use of wallet software, users can electronically transfer bitcoins using a computer, mobile or a web application. In 2015, Ethereum platform was launched which enabled blockchain to work with loans and contacts. It was based on an algorithm called smart contract ensuring the implementation of an action between the two parties. Due to Ethereum's ability to offer a faster, safer and efficient environment, the technology became widely popular.



3. Blockchain Architecture

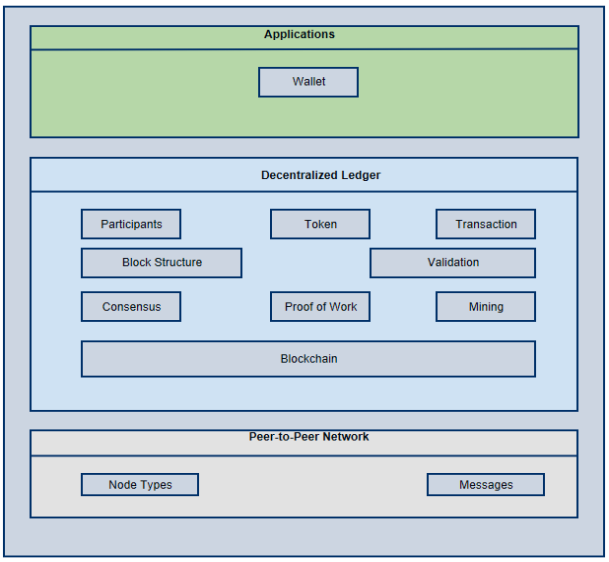
Blockchain technology works on the concept of decentralized database where these databases exist in multiple computers and every copy of these database are identical.



Organizations maintain their data in centralized database which makes them an easy target for the hackers whereas due to decentralized structure of blockchain, it has made the blockchain as a temper proof technology. Blockchain can be considered as a peer to peer network that run on the top of the internet.

Blockchain architecture can be mainly divided in three layers which are Applications, Decentralized Ledger and Peer-to-Peer Network. Applications is the top layer pf the network which is followed by the Decentralized Ledger and the bottom layer is the Peer-to-Peer Network.

Application layer contains the application software of the Blockchain. For example, Bitcoin wallet software creates and stores private and public keys enabling users to keep control over the unspent bitcoins. Application layer provides a human readable interface where users can keep track of their transactions.



Decentralized Ledger is the middle layer in a blockchain architecture that confirms a consistent and temper-proof global ledger. In this layer, transactions can be grouped into blocks which are cryptographically linked to one another. Transactions can be defined as the exchange of tokens between two participants and every transaction goes through validation process before it is considered as a legitimate transaction. Mining is the process of grouping transactions into a block that is added to the end of the current blockchain. Blockchain uses a proof-of-work algorithm to decide the

chain that has required the most cumulative effort to build and to assure consensus among all the nodes to determine the blockchain's legit. The bottom layer in the blockchain architecture is the Peer-to-Peer Network where Node types play different roles and various messages are exchanged to main the Decentralized Ledger.

3.1. Applications

It provides application interfaces on top of the blockchain and used for keeping the cryptocurrencies secure. This software can be installed on your computer or mobile devices or also can be hosted on a third-party platform.

3.2. Decentralized Ledger

A decentralized ledger is a shared and replicated database which is synchronized among the members of the network. It maintains the records of transactions among the participants in the network. The ledger is responsible for keeping records of transactions among the participants. Blockchain has a property of a database except the fact that it stores the information in the header and data is stored in the form of a token or a cryptocurrency.

It is required to group the newly validated transactions into block as the first step of recording transactions in the ledger. Any participant in the blockchain can gather new transactions create blocks that can be appended to the blockchain. A block mainly consists of transactions and the has pointer, timestamps and the nonce.

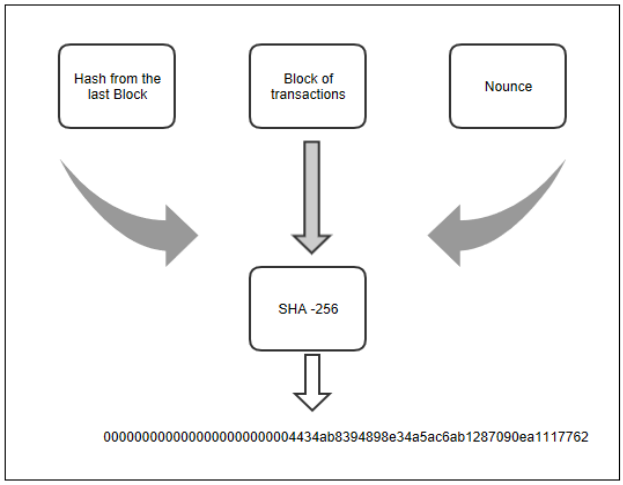
Nodes perform various functions depending on its role in the blockchain network. A node can be called a miner when it proposes and validates transactions and perform mining to provide consensus to secure the blockchain. It can perform functions such as simple payment verification etc., and functions depending on the blockchain used.

Proof of work is defined as a consensus algorithm that verifies the accuracy of data. For example, Bitcoin uses hashcash as a proof of work for bitcoin transactions. Miners are required to complete a proof of work to verify the transactions in the block so that it can be accepted by the network.

Proof of work ensures security and consensus in the blockchain network. During the verification, a block receives a hash (id). To verify the next block, this hash is added to the current block of transactions. In the next step, add a nonce-which is defined as a random number that can be used only once, to the end of next block. Hash function is used to change this random number to generate a string that contains number of zeros in front of it.

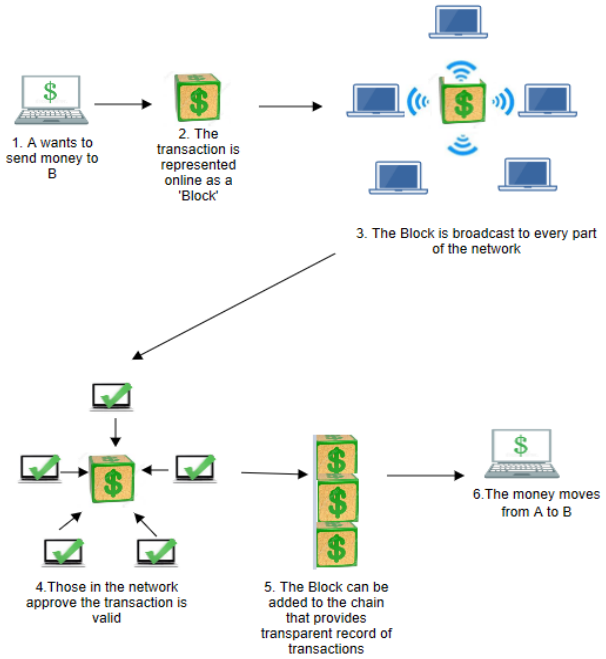
Proof of work is costly to maintain, and it can have future scalability and security issues as it always relies on the miners' incentives. There is an advanced solution called as "proof-of-stake," which is lucrative to enforce, and it identifies who gets to update the consensus and defers unwanted forking of the underlying blockchain.

No confidential information is transferred in a blockchain network and all the transactions are visible to every node in the network. This peer to peer network does not require any additional protection and can be built on any physical infrastructure.



4. How Blockchain Works

Following picture depicts how Blockchain works



5. Tiers of Blockchain

Following three tiers of blockchain technology were originally described in the book 'Blockchain, Blueprint for a new Economy' by Melaine Swan based on the applications in each category.

5.1. Blockchain 1.0

This Blockchain is basically used for cryptocurrencies and it was introduced with the invention of bitcoin. All the

alternative coins as well as bitcoin fall into this tier of blockchain. It also includes core applications as well.

5.2. Blockchain 2.0

Blockchain 2.0 is used in financial services and industries which includes financial assets, options, swamps and bonds etc. Smart Contracts was first introduced in Blockchain 2.0 that can be defined as the way to verify if the products and services are sent by the supplier during a transaction process between two parties.

5.3. Blockchain 3.0

Blockchain 3.0 offers more security as compared to Blockchain 1.0 and 2.0 and it is highly scalable and adaptable and provides sustainability. It is used in various industries such as arts, health, justice, media and in many government institutions.

5.4. Generation X

This vision the concept of singularity where this blockchain service will be available for anyone. This blockchain will be open to all and would be operated by autonomous agents.

6. Types of Blockchain

Blockchain has evolved greatly in the last few years and based on its different attributes, they can be divided in multiple types.

6.1. Public Blockchains

Public blockchains are open to the public and any individual can involve in the decision-making process by becoming a node, but users may or may not be benefited for their involvement in the decision-making process. No one in the network has ownership of the ledgers and are publicly open to anyone participated in the network. The users in the blockchain use a distributed consensus mechanism to reach on a decision and maintain a copy of the ledger on their local nodes.

6.2. Private Blockchains

These types of blockchains are not open to the public and are open to only a group of people or organizations and the ledger is shared to its participated members only.

6.3. Semi-private Blockchains

In a semi-private blockchain, some part of the blockchain is private and controlled by a group or organizations and the rest is open to the public for anyone to participate.

6.4. Sidechains

These blockchains are also known as pegged sidechains where coins can be moved from blockchain to another blockchain. There are two types of sidechains naming one-way pegged sidechain and two-way pegged sidechain. One-way pegged sidechain allows movement from one sidechain to another whereas two-way pegged sidechain allows movement on both sides of two sidechain.

6.5. Permissioned Ledger

In this type of blockchain, the participants are known and already trusted. In permissioned ledger, an agreement protocol is used to maintain a shared version of the truth rather than a consensus mechanism.

6.6. Distributed Ledger

In a distributed ledger blockchain, the ledger is distributed among all the participants in the blockchain and it can spread across multiple organizations. In distributed ledger, records are stored contiguously instead sorted block and they can be both private or public.

6.7. Shared Ledger

Shared ledger can be an application or a database that is shared by public or an organization.

6.8. Fully Private of Proprietary Blockchains

These types of Blockchains are not a part of any mainstream applications and differ the idea of decentralization. These type of blockchains come in handy when it is required to shared data within an organization and provide authenticity of the data. Government organizations use private of proprietary Blockchains to share data between various departments.

6.9. Tokenized Blockchains

These are standard blockchains which generate cryptocurrencies through consensus process using mining or initial distribution.

6.10. Tokenless Blockchains

These blockchains are not real blockchains as they do not have the ability to transfer values, but they can be useful when it is not required to transfer value between nodes and there is only the need to transfer data among already trusted parties.

7. Advantages of Blockchain

a. One of the biggest advantages of Blockchain is Dissemination which allows a database to be shared without a central body or entity. Because of the decentralized nature of the blockchain, it is almost impossible to temper the data as compared to conventional database.
b. Users are empowered to control their information and transaction.
c. Blockchains provide complete, consistent and up to date data without accuracy.

d. Since blockchain does not have any central point of failure due to its decentralized network, it can withstand any security attack.
e. As no central authority is required, users can be assured that a transaction will be executed as protocol commands.
f. Blockchains provide transparency and immutability to the transactions as all the transactions cannot be altered or deleted.
g. Blockchain's peer-to-peer connections help to identify fraud activities in the network and distributed consensus. It is almost impossible to invade a network as attacker can impact the network only when they get control of 51% of the nodes.
h. By using blockchain, sensitive business data can be protected using end to end encryption.
i. Users in a blockchain can easily trace the history of any transaction as all the transactions a blockchain are digitally stamped.
j. Blockchain are resilient to cyber-attacks due to peer-to-peer nature and network would operate even when some of the nodes are offline or under security attack.
k. Multiple copies of the data can be stored in the blockchain and hence users can avoid storing sensitive data in one place.
l. Customers tend to trust more in the blockchain system due to its enhanced security.

8. Disadvantages of Blockchain

a. Blockchains are expensive and resource intensive as every node in the blockchain repeats a task to reach consensus.
b. In blockchain, users verify a transaction based on certificate authentication, land titles, cryptocurrencies, etc. But there is no way to reverse a transaction even if both the parties involved in the transaction are ready to do so or if the transaction go sour due to some reason.
c. A transaction in the blockchain is settled only when all the nodes in the blockchain successfully verifies the transaction. This could be a very slow process as the block inserted needs to be verified to mark the transaction as authentic by all the nodes. A new concept called as lightening network where transaction can be verified immediately could be good solution to this issue.
d. The size of blockchain grows with an addition of a block. A node needs to store the entire history of the blockchain to be a participant in validating transactions, causing the blockchain to grow continuously. Blockchain will grow faster if it has large blocks and thereby would separate the miners and this would impact the health of the blockchain as the health is dependent on the number of nodes in the network.
e. One of the disadvantage of blockchain is its complexity and complicacy to understand for a general human being. Blockchain is full of complex concepts and processes which is not yet refined so that common man can easily digest and consume the information on how to use it and hence it's not yet ready for mainstream use.
f. In blockchain, all the transaction related information is available publicly which can become a great liability when distributed ledgers are used in sensitive environments such as dealing with government data or patients medical data. The ledgers need to be altered and access should be limited with proper clearance only.

9. Blockchain's Industrial Use

Blockchain's transparent and decentralized platform has attracted various industries and organizations are inclining more and more towards using blockchain for various business purpose.

Bank and Payment systems have started using blockchain to make their operations smoother, efficient and secure. Funds can be efficiently and safely transferred with the decentralization technology.

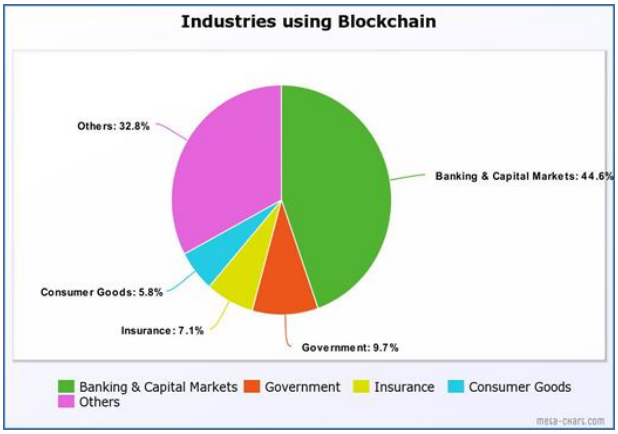
Blockchain has become increasingly popular in healthcare industries as it is able to restore the lost trust between the customers and healthcare provides. With the help of blockchain, authorization and identification of people have become easier and frauds and records loss can be avoided.

Due it blockchain's ability to store and verify documents efficiently, the legal industries have started using blockchain to verify records and documents securely. Blockchain can significantly reduce the court cases and battles by providing an authentic medium to verify and confirm truthfulness of legal documents.

Rigging of election results can be avoided with an effective use of blockchain. Voter registration and validation can be done using blockchain and ensure the legitimacy of votes by creating a publicly available ledger of recorded votes.

Industries such as Insurance, Education, Private transport and Ride sharing, government and public benefits, retail, real estate etc. have started implementing blockchain to reduce costs, to increase transparency and to build trust.

Top market analysts predicts that industries such as Banking and Capital Markets, Government, Insurance, Consumers would grow rapidly by 2020 and various other industries such as retail, health, pharmaceutical, travel and transport would also start to use blockchains heavily in their respective domains.



10. Practical Implementation of Blockchain in Organizations

For an organization, the best area to start implementing Blockchain is a single use independent application where no coordination is required among different applications and third parties.

An easy approach to implement blockchain would be to introduce bitcoin as a payment system since bitcon has already has solid and proven architecture and also it has a growing market.

Another safe and effective approach would be introducing blockchain as a database technology for managing and maintaining digital transaction records. Testing out these single use independent applications would give an organization the idea to implement blockchain as scaled projects.

As the next step, organizations can focus on the localized applications such as Financial Service companies where setting up private networks for transactions among the counterparts would help the organizations to save huge transaction costs. It is always a challenge to change the existing solutions and implement a new and better solution which requires thorough planning and execution. A good approach would be without effecting the end users but by providing cost effective and efficient solutions which should be easily adaptive.

Though Transformative applications are still futuristic, it's important to evaluate their possibilities and start developing them which can unlock new future for companies. Public identity systems or algorithm driven decision making systems can be benefitted by the transformative applications and new ecosystems will be governed efficiently with the support of these applications.

11. Conclusions

Blockchain is a revolutionary concept as it has been successfully able to bring the transparency among the users and has become a game changer for many industries. Blockchain encourages entrepreneurship by destroying corruption and breaking down the walls of bureaucracy and establish the ownership of common mass. This peer-to-peer technology has opened the door to new possibilities and has provided a personal ground for economic empowerment. It is too early to say what lies ahead, but the future of blockchain looks promising and it can be concluded that blockchain technology is here to stay.

REFERENCES

[1] Pilkington, Marc. "11 Blockchain Technol-Ogy: Principles and Applications." Re-Search Handbook On Digital Transfor-Mations (2016): 225.

[2] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Tech-Nology: Beyond Bitcoin. Applied Innova-Tion, 2, 6-10.

[3] Atzori, Marcella. "Blockchain Technology And Decentralized Governance: Is The State Still Necessary?" (2015).

[4] Zheng, Zibin, Et Al. "An Overview of Block-Chain Technology: Architecture, Consen-Sus, And Future Trends." Big Data (Bigdata Congress), 2017 Ieee International Congress On. Ieee, 2017.

[5] Malinova, Katya, and Andreas Park. "Market Design with Blockchain Technology." (2017).

[6] Nguyen, Quoc Khanh. "Blockchain-a financial technology for future sustainable development." Green Technology and Sustainable Development (GTSD), International Conference on. IEEE, 2016.

[7] Ammous, Saifedean. "Blockchain Technology: What is it good for?." (2016).

[8] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Vol. 310. 2016.

[9] Condos, James, William H. Sorrell, and Susan L. Donegan. "Blockchain technology: Opportunities and risks." Vermont, January 15 (2016).

[10] Pilkington, Marc. "Blockchain technology: principles and applications. Research handbook on digital transformations, edited by f. xavier olleros and majlinda zhegu." (2016).

[11] Subash Thota, 2017. Analytics – Life Cycle. International Journal of Multidisciplinary Research and Development, pp. 117-126. http://www.allsubjectjournal.com/archives/2017/vol4/issue12/4-12-33.

[12] Nofer, Michael, et al. "Blockchain." Business & Information Systems Engineering 59.3 (2017): 183-187.

[13] De Filippi, Primavera, and Samer Hassan. "Blockchain technology as a regulatory technology: From code is law to law is code." arXiv preprint arXiv:1801.02507 (2018).

[14] Ahram, Tareq, et al. "Blockchain technology innovations." Technology & Engineering Management Conference (TEMSCON), 2017 IEEE. IEEE, 2017.

[15] Boucher, Philip. "What if blockchain technology revolutionised voting." Unpublished manuscript, European Parliament (2016).

[16] Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): 118-127.

[17] Sarmah, Simanta Shekhar. "Data Migration." Science and Technology 8.1 (2018): 1-10.

[18] Foroglou, George, and Anna-Lali Tsilidou. "Further applications of the blockchain." Columbia University PhD in Sustainable Development 10 (2015).

[19] Mougayar, William. The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons, 2016.

[20] Bashir, Imran. Mastering Blockchain. Packt Publishing Ltd, 2017.

[21] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118-127.