INFORMATICA, 2019, Vol. 30, No. 4, 729–748

DOI: http://dx.doi.org/10.15388/Informatica.2019.227

A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions

Remigijus PAULAVIČIUS*, Saulius GRIGAITIS,
Aleksandr IGUMENOV, Ernestas FILATOVAS
Institute of Data Science and Digital Technologies, Vilnius University,
Akademijos str. 4, LT-08412 Vilnius, Lithuania
e-mail: remigijus.paulavicius@mif.vu.lt, saulius.grigaitis@mif.vu.lt,
aleksandr.igumenov@mif.vu.lt, ernestas.filatovas@mif.vu.lt

Received: June 2019; accepted: December 2019

Abstract. In this paper, we present the progress of blockchain technology from the advent of the original publication titled "Bitcoin: A Peer-to-Peer Electronic Cash System," written by the mysterious Satoshi Nakamoto, until the current days. Historical background and a comprehensive overview of the blockchain technology are given. We provide an up-to-date comparison of the most popular blockchain platforms with particular emphasis given to consensus protocols. Additionally, we introduce a `BlockLib`, an extensively growing online library on blockchain platforms collected from the various sources and designed to enable contributions from the blockchain community. Main directions of the current blockchain research, facing challenges as well as the main fields of applications, are summarized. We also layout the possible future lines in the blockchain technology development.

Key words: blockchain, Distributed Ledger Technology (DLT), Bitcoin, blockchain platforms, consensus protocols, cryptocurrencies.

1. Introduction

Blockchain claimed to be one of the most disruptive inventions of the last decade, with the potential to impact almost every industry from finance to manufacturing to education. Blockchain is tamper evident and tamper resistant distributed ledger technology (DLT), implemented in a distributed way (i.e. without a central repository) and traditionally without a central authority (bank, company or government) (Yaga *et al.*, 2018). Bitcoin is the first blockchain application and therefore is considered the technology which invented the term "blockchain". The technology of Bitcoin is based on the whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008) published in 2008 by a person (or group) under the pseudonym of Satoshi Nakamoto. Bitcoin was invented in the aftermath of the 2008 global financial crisis, which was one of the primary motivating factors for Bitcoin creation (Chuen, 2015). The technology became widely known with the establishment of the Bitcoin blockchain network in 2009. Although initially intended to be

*Corresponding author.

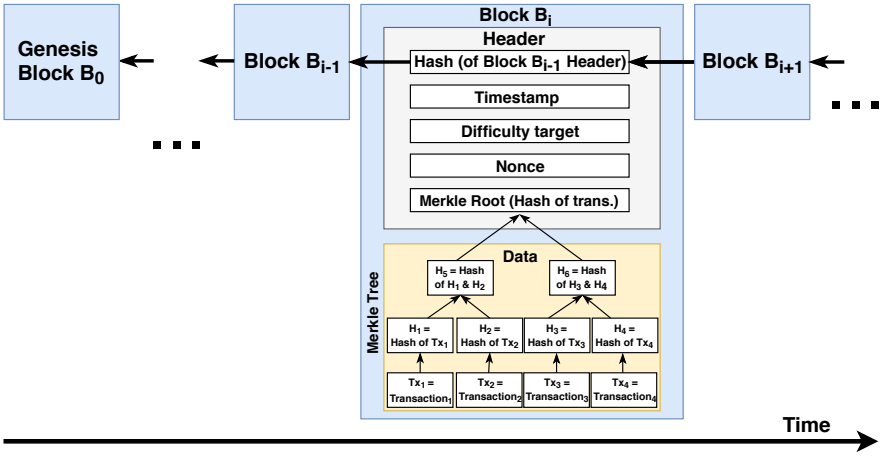


Fig. 1. Chain of blocks and a detailed, yet simplified, Bitcoin block data structure. Bitcoin blockchain could be regarded as a decentralized distributed public ledger, storing all committed transactions in a list of time-stamped data blocks. The newly created block also contains a reference (a cryptographic hash) to the previous block. Such a chain-like structure of blocks (hence "blockchain") grows continuously as new blocks are appended to it.

a decentralized alternative to the traditional centralized financial currency system, Bitcoin was just the first of plethora blockchain applications. While the blockchain technology is still at the stage of active development, the history of the techniques used in blockchain can be traced back several decades ago.

1.1. *A Brief History of Innovations Found in Blockchain*

While the blockchain technology emerged only a decade ago, the core ideas behind the blockchain were proposed in the late 1980s and early 1990s (Narayanan and Clark, 2017). In 1989, Turing Award winner Leslie Lamport developed the Paxos protocol, a consensus model for reaching agreement in a network of computers, where the computers, as well as the network itself, may be unreliable. The paper itself was published almost ten years later (Lamport, 1998).

Next, in a series of papers, written between 1990 and 1997 (Bayer *et al.*, 1993; Haber and Stornetta, 1990, 1997), authors proposed a concept of signed chain of information, forming an electronic ledger. This ledger consisted of digitally signed documents in a way that could be easily shown that none of these signed documents had been tampered with.

To make this data structure more efficient, authors introduced the following improvements: 1) to use faster computable hashes instead of signatures for the document linking; 2) to group documents into blocks instead of handling them individually; 3) within each block, instead of linear document linking, connect them using a binary Merkle tree structure (Merkle, 1980), consisting of transaction hash pointers. These concepts were combined and applied to Bitcoin (Nakamoto, 2008) (see Fig. 1). However, in Bitcoin, transactions take place instead of documents.

Bitcoin borrows the data structure, but redesigns the network security properties with the addition of the Proof-of-Work (PoW) consensus scheme. Proof-of-Work is a cryptographic method created in 1992 by Cynthia Dwork and Moni Naor (Dwork and Naor, 1992) to prevent e-mail spam. The core idea is to include into a email that is being sent a proof that a certain amount of work (hence "proof-of-work") has been done before an email was sent. Usually, the computation of such a proof would take a few seconds, and therefore, this would pose no difficulty for casual users, however, for a spammer, this would take weeks to send million (spam) emails. Moreover, the authors propose that the "proof-of-work" has to be specific to a certain email, and the solution should be trivial to verify for the email recipient. In Bitcoin, this is implemented by looking for a hash value that fulfills certain requirements, i.e. is lower than (or equal to) the target number set by the Bitcoin network.

Many electronic cash schemes existed before Bitcoin, e.g. ecash (Chaum, 1983), b-money (Dai, 1998) or Bit gold (Szabo, 2008), but none of them achieved widespread use. Blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash system, and no single point of failure existed (Yaga *et al.*, 2018). The main benefit of this was the possibility to process direct transactions between users without the need for a trusted third party. Even more, Nakamoto designed a digital currency (Bitcoin) such that the coins are based on digital signatures, therefore assuring the security and integrity of coin transfers by using established cryptographic methods. Moreover, this enabled users to be pseudonymous, while all transactions are publicly visible. In such a way, by using a blockchain and consensus protocols, a self-policing decentralized system (a "trustless" peer-to-peer (P2P) network of nodes) was created. This system automatically ensured that only valid transactions and blocks were added to the blockchain.

1.2. *Basic Structure of Blockchain*

Basically, blockchain is an append-only database maintained in a distributed fashion by the nodes in the P2P network. Figure 2 illustrates the basic hierarchical structure of blockchain consisting of four layers:

- **Network layer:** the bottom layer of computing nodes guarantees that the system is able to work. The P2P network is the key feature ensuring communication among blockchain nodes in a decentralized way.
- **Protocol layer:** the second bottom layer is the protocol layer consisting of fundamental blockchain technologies, such as consensus algorithms and cryptology methods. This layer ensures that the system works properly.
- **Ledger layer:** the third layer from the bottom, global ledger, is responsible for the primary blockchain mission – transmitting transactions (including smart contracts) reliably and securely. This layer assures that the system is functioning correctly.
- **Application layer:** the top layer provides APIs for various applications. This layer is responsible for the interaction with the blockchain when it is needed for the business logic.

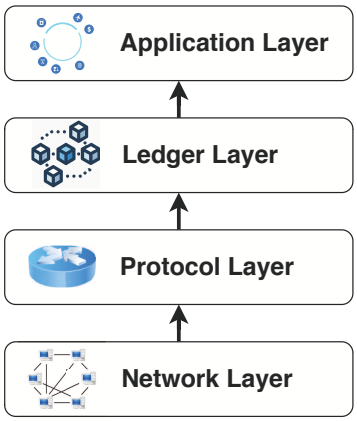


Fig. 2. The basic hierarchical structure of blockchain consisting of four layers.

1.3. *Contribution and Organization*

The blockchain technology is in the early second decade, but already there are lots of research done within this field. We note, that already exist surveys dedicated to the specific blockchain domains, e.g. studies on the security of the blockchain systems (Li *et al.*, 2017; Lin and Liao, 2017), consensus protocols (Bano *et al.*, 2017; Nguyen and Kim, 2018; Xiao *et al.*, 2019), privacy protection (Feng *et al.*, 2019), as well as general blockchain technology surveys (Belotti *et al.*, 2019; Zheng *et al.*, 2017, 2018). In this work, we are not only reviewing the latest advances in the blockchain technology, but also introducing a completely new open-source data collection of the blockchain implementations, platforms, `BlockLib` (Paulavičius *et al.*, 2019). This way, we hope that the `BlockLib` library will contain the largest and the most up-to-date information on blockchain platforms and will be the leading source for the researchers and business industries looking for more detailed information on this topic.

The remainder of the paper is structured as follows. Section 2 presents an aggregated systematic comparison of the 1st and 2nd generation leading blockchain platforms, with particular emphasis given to consensus protocols. Section 3 describes potential of the blockchain applicability. Section 4 summarizes the biggest technological challenges currently facing, and highlights some possible future directions. Finally, Section 5 concludes the paper.

2. A Comparison of Blockchain Platforms

This section focuses on classifying and comparing the various technologies underlying different types of blockchain platforms. The main features of interest include the primal use-case, characteristics of cryptocurrency they include (if any), network type, the data model used, anonymity support, smart contract functionality, hashing algorithm,

throughput measured as the number of transactions per second (tps), and latency (in sec.). Consensus protocols form the basis of any blockchain platform, therefore initially, an overview of the consensus protocols currently used in blockchain platforms is given in Section 2.1. Then, in Section 2.2, we present our comparison of blockchain platforms by distinguishing the following two groups: 1st and 2nd generation platforms. The 1st generation blockchain platforms were initially created to provide a public ledger for financial transactions and thus, have limited support of programmable transactions. Within the 2nd generation blockchain platforms usually a Turing complete programmable infrastructure is available, and public ledger designed to store various computational results (Xu *et al.*, 2016). We note, that 3rd generation blockchain platforms (Yang *et al.*, 2018) are currently under active development (e.g. Ethereum 2.0 (Buterin, 2018; Buterin *et al.*, 2019), Zilliqa (The ZILLIQA Team, 2017), Cardano (Kiayias *et al.*, 2017), EOS (EOS, 2017), etc.). However, there are limited scientific resources about their performance measures, therefore, they are excluded from the comparison provided here. It must be noted that such a classification of blockchain platforms is not strict as most of them are under active development. Finally, in Section 2.3, we introduce an actively growing online data collection of blockchain platforms, `BlockLib` (Paulavičius *et al.*, 2019).

2.1. *Role of Consensus Protocols*

Consensus protocol runs at every node of a blockchain network. It allows to reach a collective agreement on transaction ledger and govern operations of the network: such as message exchange, data replication, encouragement of the participants to behave appropriately. Moreover, consensus must be achieved in conditions of faulty nodes that perform arbitrary or malicious behaviours, i.e. in the situation of Byzantine failures (Castro and Liskov, 2002). Thus, only Byzantine fault-tolerant (BFT) consensus protocol must be used in a case of a public blockchain, as both correct and faulty nodes can join and leave the network without any control. On the other hand, in a private blockchain, nodes need to be authenticated.

Main Types of Consensus Protocols. Nakamoto is the first probabilistic PoW-type (Dwork and Naor, 1992; Back, 1997) consensus protocol used in Bitcoin (Nakamoto, 2008), and many other 1st generation blockchain platforms. The core idea is to allocate the block proposal rights and rewards through the hashing power competition among the network nodes – miners. Lower than or equal to that set by the network difficulty. It is important to note that PoW consensus protocol security is proportional to the number of computing resources in the network. Low amount of resources are very vulnerable. On the other hand, PoW-based protocols are energy inefficient (see Section 4.1). Alternatively, in Proof-of-Stake (PoS) type consensus protocols (King and Nadal, 2012), the PoW mining is replaced with a mechanism where blocks are produced and validated according to the stake value (participants coin holdings on the blockchain). Practical Byzantine Fault Tolerance (PBFT) (Castro and Liskov, 1999) is the first Byzantine fault-tolerant (BFT) protocol, guaranteeing deterministic block finalization. It has laid the foundation for a broad class of BFT-based consensus protocols (Wang *et al.*, 2018).

Comparison of Consensus Protocols. In this comparison, we focus on consensus protocols used in blockchain platforms considered in Section 2.2. The information provided here is gathered and aggregated using a recent comprehensive survey (Xiao *et al.*, 2019), and other related works (Mingxiao *et al.*, 2017; Bach *et al.*, 2018; Chalaemwongwan and Kurutach, 2018; Wang *et al.*, 2018; Nguyen *et al.*, 2019) to which we refer interested readers for a detailed information. The main features of interest include application platform, protocol and type, block proposal (block producing mechanism), block validation (blocks and transactions validity check), block finalization, fault tolerance, throughput (maximal number of transactions per second) and network scalability (ability to process an increasing number of transactions by adding resources to the network) in the same context, as in the study list.

The block finalization is closely related to the fault tolerance (see the fifth and sixth columns in Table 1). In BFT-based consensus protocols, only up to 33% of faulty nodes are tolerated, in contrast to up to 50% in the longest-chain rule, which represents the main chain with the most work put into completing it, or in GHOST rule. In hybrid protocols (as BFT-based PoS), the 33% fault tolerance is also related to the block proposal scheme. The most significant advantage of BFT-based consensus protocols is that a guaranteed deterministic finality, and, as a consequence, a high throughput is provided. On the other hand, protocols developed for public blockchain have higher fault tolerance, and network scalability, but suffer from low throughput (see Table 2 for more information on this).

Finally, let us note that there are a plethora of emerging promising protocols that aim to improve energy consumption, throughput, and scalability issues. Among them, Ouroboros (Kiayias *et al.*, 2017), Tendermint (Kwon, 2014, 2017), Algorand (Gilad *et al.*, 2017), Casper (Buterin and Griffith, 2017), DPoS (Bitshares, 2015), (Popov, 2016), Proof-of-Authority (PoA) (Parity Technologies, 2017), and Proof-of-Importance (PoI) (Nem, 2018) are particularly pressing. However, most of them are out the scope of this comparison, as they are still under an active development together with the 3rd generation blockchain platforms. Interested readers are referred to (Bach *et al.*, 2018; Xiao *et al.*, 2019; Nguyen *et al.*, 2019) for more information on this.

2.2. *The Main Findings of Platform Comparison*

The results presented here are focused on scientific knowledge on blockchain platforms, i.e. the results are combined and aggregated by using mainly scholarly literature (Anh *et al.*, 2018; Belotti *et al.*, 2019; Dinh *et al.*, 2017; Kuo *et al.*, 2019; Valenta and Sandner, 2017) and references therein. Almost all 1st generation blockchain platforms (see Table 2) target the general public, thus the potentially distrustful audience. They typically allow mining for the new coins and include reward mechanisms to incentivize network nodes to actively and fairly participate in the mining process. Whereas 2nd generation blockchain platforms target closed, trustworthy, or at least familiar groups of users (see Table 3). Therefore, these blockchains can use more lightweight consensus mechanisms in private settings compared to public blockchains by relying on a certain level of trust among network participants. This allows 2nd generation blockchain platforms to rebalance efforts for

Table 1
Summary of the blockchain consensus protocol comparison.

Application platform	*Protocol/ Type*	*Block proposal*	*Block validation*	*Block finalization*	*Fault tolerance*	*Throughput*	*Network scalability*
Bitcoin, Litecoin, ZCash	Nakamoto/ PoW	PoW puzzle competition	PoW Check	Longest-chain rule	50% computing power	Low	High
Dash	Nakamoto/ PoW	PoW puzzle competition	PoW Check/ Masternode check	Longest-chain rule	50% computing power	Low	High
PeerCoin	Chain-based PoS	PoS (coin age)	PoS Check	Longest-chain rule	50% deposited stake value	Low	High
Ethereum	Nakamoto-GHOST/PoW	PoW puzzle competition (Ethash)	PoW Check	GHOST rule	50% computing power	Low	High
Ethereum 2.0	Casper-FFG/ BFT-based PoS	PoW puzzle competition	PoW and Checkpoint tree check	BFT (with staked votes)	33% deposited stake value	High	–
Tendermint	Tendermint/ BFT-based PoS	PoS-based round robin	Proposer eligibility check	BFT (adapted DLS protocol)	33% token wealth	High	Medium
Ripple	RCPA (Ripple Consensus Protocol Algorithm)	Any server proposes transactions	UNL membership check	Accepting >80% voted transaction	20% nodes in each UNL	High	Medium
Hyperledger Sawtooth	PoET	PoET within TEE	TEE certificate check	PBFT (agreement on the same state)	50% IDs (33% if BFT used)	High	Low
Hyperledger Fabric	Kafka	–	–	–	no BFT tolerance	High	Low
Quorum	Raft, Istanbul BFT, PoA (Proof of Authority)	–	–	–	depends on the consensus	Medium/ High	Medium/ Low
Corda	Raft, BFT-based	–	–	–	depends on the consensus	Medium/ High	Medium/ Low
Stellar	SCP (Stellar Consensus Protocol)	–	–	–	33%	High	Low

– means that no information was provided in the reviewed sources.

security with initiatives for the much higher throughput and significantly reduced latency. Except for Ripple, Stellar and Monero, public blockchain platforms nowadays ensure a much lower number of transactions per second (tps) throughput and require significantly higher latency time (see Section 4.2 for a brief review of actively developing technologies that address these issues).

Table 2
Summary of the 1st generation blockchain platform comparison.

Characteristics	Bitcoin	Litecoin	Peercoin	Ripple	Stellar	Dash	Monero	Zcash
				General platform characteristics				
Main use-case	Crypto-currency	Crypto-currency	Crypto-currency	Digital assets	Digital assets	Crypto-currency	Crypto-currency	Crypto-currency
Release	2009	2011	2012	2013	2014	2014	2014	2016
Governance	N/A	N/A	N/A	Ripple Labs Inc.	Stellar Development Foundation	N/A	N/A	N/A
Cryptocurrency (symbol)	Bitcoin (BTC)	Litecoin (LTC)	Peercoin (PPC)	Ripple (XRP)	Lumen (XLM)	Dash (DASH)	Monero (XMR)	Zcash (ZEC)
Coin Limit	21 Million	84 Million	2 Billion	100 Billion	>100 Billiona	19 Million	18.3 Million, plus 0.3 XMR per minute afterwards	21 Million
Mining for New Public Coins	✓	✓	✓	✗(Pre-Mining)	✓	✓	✓	✓
				Architectural platform characteristics				
Main Improvement over Bitcoin	N/A	ASIC Resistance (is not applicable anymore)	Long-Term Energy Efficiency	Low-Latency Transaction	Low-Latency Transaction	Privacy-Anonymity	Privacy-Anonymity	Privacy-Anonymity
Network	Permission-less public	Permission-less public	Permission-less public	Semi-permission-less public	Permission-less public	Permission-less public	Permission-less public	Permission-less public
Data model	UTXO	UTXO	UTXO	Account based	Account based	UTXO	UTXO	UTXO
Anonymous payment	✗	✗	✗	✗	✗	✓(Darksend/ PrivateSend)	✓(RingCT/ Stealth Address)	✓(zk-SNARK)
Smart contract execution	Native	Native	Native	✗	Native	Native	✗	Native
Smart contract language	Bitcoin Script	Bitcoin Script	Bitcoin Script	✗	Stellar Smart Contract (SSC) Script	Bitcoin Script	✗	Bitcoin Script
Hash algorithm	SHA-256	Scrypt	SHA-256	ECDSA	Stellar Consensus Protocol (SCP)	X11	CryptoNight	Equihash
Throughput (tps)	7	28	8	1500	1000	∼25	1700	∼25
Latency/block time (sec.)	600	166	480	11	5	158	122	154

[a] New lumens (XLM) are added to the Stellar network at the rate of 1% each year.

Moreover, 2nd generation blockchain platforms are implemented by dividing into modular layers. Such an approach broadens the potential application (see Section 3 for more information on this) of blockchain technology beyond simply exchanging tokens of a single cryptocurrency.

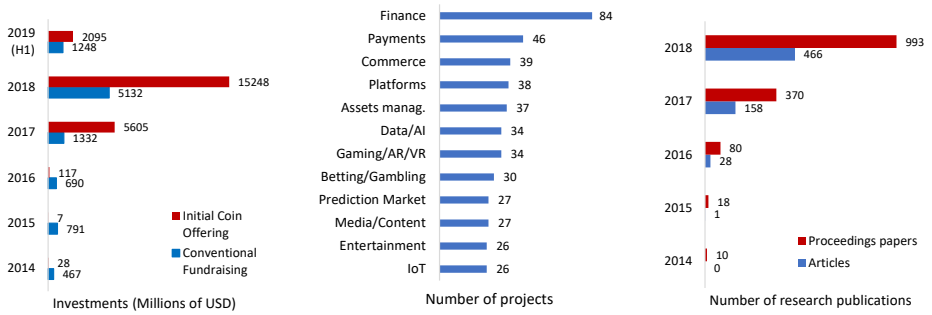
2.3. *BlockLib: A Collection of Blockchain platforms*

The literature on the application of blockchain technology is extensive and grows at a swift pace (see Section 3 for more details on this). There already exist several col-

Table 3
Summary of the 2nd generation blockchain platform comparison.

Characteristics	Ethereum	Hyperledger platforms: Fabric, Sawtooth	Corda	Tendermint	Chain Core	Quorum	MultiChain
			General platform characteristics				
Main use-case	Generic blockchain platform	Modular blockchain platforms	Modular distributed ledger platform for financial industry	Blockchain consensus engine	Multi-assets ledger for assets trading	General application platform	General application platform
Release	2015	2015	2015	2014	2014	2016	2014
Governance	N/A	Linux Foundation	R3	Tendermint developers	Chain, Microsoft, IC3	JPMorgan	Tendermint company
Cryptocurrency (symbol)	Ether (ETH), Tokens via smart contract	Currency and tokens possible via chaincode	✗	Initially, now ✗	✗	✗	✗
Coin Limit	Unlimited	✗	✗	✗	✗	✗	✗
Mining for New Public Coins	✓	✗	✗	✗	✗	✗	✗
			Architectural platform characteristics				
Network	Permission-less public, Permis-sioned private	Permissioned private	Permissioned private	Permission-less public	Permissioned private	Permissioned public or private	Permissioned private
Data model	Account-based	Key-value	UTXO	Various	UTXO	Account-based	UTXO
Smart contract execution	EVM	Fabric: docker; Sawtooth: native	JVM	Various	Chain Virtual Machine (CVM), TxVM	EVM	Native
Smart contract language	Solidity, Serpent, LLL	Fabric: Go, Javascript; Sawtooth: Java, Go, Javascript, Rust, Solidity	Kotlin, Java	Depends on software choice	Written in bytecode instructions for CVM	Go	Javascript
Hash algorithm	Ethash	Fabric: SHA3, SHAKE256; Sawtooth: SHA-256	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256
Throughput (tps)	15–40; in private setup ∼1000	Dozen of thousands	120–1000	Tens of thousands within single data-center	N/A	Dozens to hundreds	Up to 1000
Latency/block time (sec.)	15	<1	N/A	<1	N/A	N/A	<10

lections of blockchain platforms presented in the literature, see e.g. (Anh *et al.*, 2018; Belotti *et al.*, 2019; Dinh *et al.*, 2017; Kuo *et al.*, 2019; Valenta and Sandner, 2017). However, they are limited and focused mainly on special subclasses. Moreover, as far as we are aware, there is no systematic and comprehensive data library available for the evaluation of the broad class existing and actively developed, as well as newly emerging blockchain platforms.



(a) Amount of investment into the blockchain sector

(b) Number of blockchain projects among industries

(c) Number of blockchain research publications

Fig. 3. Investment and research interest into the blockchain technology.

Thus, in this work, we introduce an actively growing online collection of blockchain platforms, `BlockLib` (Paulavičius *et al.*, 2019), gathered from various sources (such as official websites, blogs, wikis, forum posts, source codes, conference proceedings, and journal papers), and devoted to facilitate research on blockchain platforms. `BlockLib` is designed as an open-source library to which other researchers and the blockchain technology community can easily contribute. By doing this, we hope that the blockchain community will help us to fix all errors and inaccuracies, add new data, and in such a way, keep this collection growing and up-to-date. Finally, let us note that the full description of this collection and a detailed analysis of the data provided here is out of this paper's scope.

3. Applications

In this section, we review the current state of blockchain applicability in various industry sectors, specify the level of research already done within this field, and provide some insights about facing limitations. The 1st generation blockchain platforms are designed mainly for monetary transactions, while the most of 2nd generation platforms feature a complete programmable infrastructure. The employment of smart contracts (Szabo, 1994) enabled efficient blockchain incorporation into various industry fields.

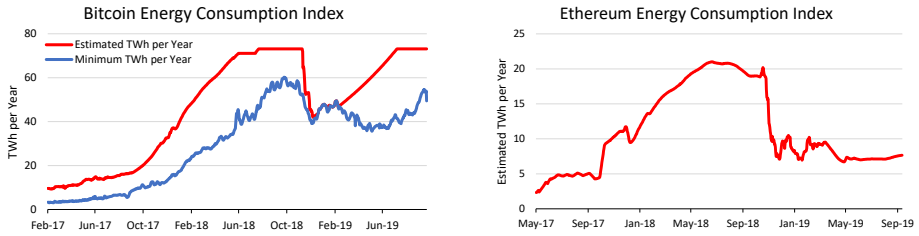
All of this has led to the leading financial organizations, governments, and enterprises actively exploring the applicability of blockchain technology in their domains (IBM, 2018), and providing financial support to the development of these projects. In Fig. 3a worldwide funding into the blockchain sector from 2014 is presented (TeqAtlas, 2019). Note, that after the end of Initial Coin Offering (ICO) hype (during the period of 2017–2018), the value of capital raised via ICO has drastically decreased, however, it is still significant. In Fig. 3b, the blockchain projects are categorized according to their focus to industries (ICO Watch List, 2019). The most popular industries are still related to the financial sector and the development of blockchain platforms. Finally, in Fig. 3, we present the number of research publications on blockchain topic that have been indexed by Web of Science (WoS) from 2014. The interest of the researchers is significantly increasing.

The authors in Risius and Spohrer (2017), Yli-Huumo *et al.* (2016) provide a detailed review and classification of the existing literature dedicated to the blockchain technology. Among existing blockchain surveys, devoted to blockchain applications, the Internet of Things (IoT) (Panarello *et al.*, 2018; Khan and Salah, 2018), Healthcare (Siyal *et al.*, 2019), Energy (Andoni *et al.*, 2019), and Government (Datta, 2019) are the most often investigated areas in the research community (Jaoude and Saade, 2019).

Further, we provide a brief overview of blockchain applications according to the most popular and newly emerging fields:

- **IoT:** IoT applications need trust mechanisms that ensure the integrity of the collected data and the associated interactions as well as their transparency that blockchain can provide (Sicari *et al.*, 2015). The research community puts a lot of interest in the integration of blockchain into of different aspects of IoT – decentralization (Veena *et al.*, 2015), security (Khan and Salah, 2018), anonymity (Christidis and Devetsikiotis, 2016; Huh *et al.*, 2017), identity (Gan, 2017), device management (Samaniego and Deters, 2016).
- **Finance:** the high potential of blockchain application in the finance sector is indisputable. Research works are dedicated to improving transaction processing and performance (Peters and Panayi, 2016), security and data privacy (Singh and Singh, 2016), automatization of financial contracts (Egelund-Müller *et al.*, 2017), corporate finance (Momtaz *et al.*, 2019), etc.
- **Healthcare:** in the field of healthcare, blockchain application has a wide-range applicability and include electronic medical records (EMRs) management (Zhang and Lin, 2018; Gordon and Catalini, 2018), biomedical research (Benchoufi *et al.*, 2017; Mytis-Gkometh *et al.*, 2018), drug supply chain (Tseng *et al.*, 2018), insurance claim (Zhou *et al.*, 2018), etc.
- **Energy:** energy and energy management blockchain-based applications are also becoming mainstream and include electricity market control (Lundqvist *et al.*, 2017), energy trading (Münsing *et al.*, 2017), energy grid security (Bergquist *et al.*, 2017).
- **Government:** in government, blockchain is aimed to be applied for e-government (Batubara *et al.*, 2018; Sullivan and Burger, 2019), digital identity (Dunphy and Petitcolas, 2018), e-voting (Pawlak *et al.*, 2018), value registry (Ramya *et al.*, 2018), etc.
- **AI:** the synergy of blockchain and AI enables tracking the provenance of training models (Sarpatwar *et al.*, 2019), improves the efficiency of transportation systems (Yuan and Wang, 2016), increases robots control (Lopes *et al.*, 2019), supports IoT networks (Singh *et al.*, 2019), etc.
- **Big Data**: in Big Data, blockchain can help to establish a data-sharing platform for interaction of all involved parties (Chen and Xue, 2017), improve data reliability between them (Abdullah *et al.*, 2017), increase data security, and provide timestamping (Karafiloski and Mishev, 2017).

However, it must be noted, the actual current blockchain applicability is still limited, and suffers mainly from the insufficient technical capabilities and poor infrastructure. Most of the blockchain application projects are still in the development phase, and



(a) Bitcoin network (Digiconomist, 2019a) (b) Ethereum network (Digiconomist, 2019b)

Fig. 4. Energy consumption indexes estimated in TWh (terawatt hours of energy) per year.

present blockchain solutions cannot deliver full-fledged support for the most emerging applications. The situation can change essentially when currently actively developed 3rd generation blockchain platforms (see Section 2) will be delivered. They seek to ensure sufficient scalability, interoperability, and sustainability to support the current needs of real-world applications.

4. Challenges and Possible Future Directions

There is no doubt that blockchain is one of the greatest innovations of the 21st century, and has a high potential for applications and direct use in various industries. However, at the current stage, it faces some vital challenges, like very high energy consumption, technological issues, governance problem, and similar. In this section, we review the main blockchain technology challenges and detail possible future directions.

4.1. *Blockchain Energy Consumption Problem*

The high electricity consumption of Bitcoin and some other popular cryptocurrencies (Ethereum, Litecoin, Monero) has been widely reported in the literature (de Vries, 2018; Krause and Tolaymat, 2018; Stoll *et al.*, 2019; Truby, 2018). Bitcoin, like a mineral is extractable and finite, and like traditional mining, cryptomining can be energy-intensive (Krause and Tolaymat, 2018). Currently, the Bitcoin Energy Consumption Index (BECI) (Digiconomist, 2019a) (shown in Fig. 4a), and the Cambridge Bitcoin Electricity Consumption Index (CBECI) (University of Cambridge, 2019) estimates, that the global Bitcoin's annual electricity consumption is equal to around 75 TWh (terawatt-hours of energy), which translates into around 35 $MtCO_2$ annual carbon emissions range. Moreover, recent research claimed that the amount of energy required to mine one dollar's worth of Bitcoin is more than twice that required to mine the same value of copper, gold or platinum (Krause and Tolaymat, 2018). The other popular cryptocurrencies that use PoW consensus protocols seem poorly in this comparison too. Therefore, the virtual mining work that underpins cryptocurrencies is more similar to real mining than anyone actually intended. To summarize, the three main things which drive Bitcoin's vast power usage are

artificial scarcity leading to way too many miners, an increasingly hard competition to mine remaining coins, and PoW approach to network's immutability and validity.

Looking from the opposite perspective, it is worth noting that according to the recent report (CoinShares, 2019) 74.1% of Bitcoin mining is powered by renewable energy. Moreover, blockchain energy consumption can be treated not as a disadvantage, but as an essential feature for dealing with the double-spending problem and security of the public blockchain (Vranken, 2017). In this context, the more energy is consumed, the more secure the network is, as the more costly is to perform the 51% attack. Even more, lots of research has been done to address this. For example, the second largest Ethereum's PoW-based cryptocurrency network annually consumes around 8 TWh electricity (see Fig. 4b), however, Ethereum is about to move to its Casper PoS consensus mechanism (Buterin and Griffith, 2017; Buterin *et al.*, 2019; Buterin, 2018), which will drastically reduce electricity consumption and change the way its blockchain operates. Other 2nd generation blockchain platforms are already using more optimized consensus protocols, such as PoS, PoA with significantly lower electricity costs and carbon emission. Another approach is to effectively exploit computational resources used in PoW, i.e. instead of solving "useless" PoW *math puzzle* replace this process with the solution of computing-intensive important real-world problems, e.g. finding prime numbers (King, 2013) or solving challenging optimization problems (Shibata, 2019).

4.2. *Technological Issues*

Main technological blockchain challenges include scalability, privacy, security, as well as interoperability aspects. Top blockchain platforms, like Bitcoin and Ethereum, are not well adapted to satisfy huge amount of users needs, as they can ensure a way to small maximal number of transactions (see Table 2). Therefore PoS type consensus protocols, sharding technique (Johnson *et al.*, 2019), as well as side-chain and off-chain solutions (Kim *et al.*, 2018) have already shown a high potential to address scalability issues, and are currently under an active development and integration stage, e.g. Lightning Network in Bitcoin (Poon and Dryja, 2016), PoS and sharding technology in Ethereum network (Buterin, 2018).

Privacy is also a sensitive and important topic for blockchain applications. In public blockchains, all the data related to transactions is public accessible, however, transparency in blockchain must be harmonized with personal and sensitive data protection. Private and consortium type blockchains solve this problem, but limit users' access, therefore reducing the degree of decentralization. Thus, an optimal trade-off should be applied for specific use-cases.

Security of blockchains highly depends on the consensus protocol. As a result, they are vulnerable to a 51% attack (or 34% attack if BFT type consensus is used) (Bach *et al.*, 2018). Small blockchains with fewer users are more sensitive to these attacks, while huge blockchains can ensure much higher security, but suffer form hashing and stacking power centralization. Blockchain community works on the development and adaptation of more efficient and secure consensus protocols (see Section 2.1 for more information on this).

Finally, interoperability problem, i.e. the limited ability to share information across different blockchains, is caused by the lack of standardization among various existing platforms, different consensus protocols, privacy mechanisms, data models, and etc. Potential solutions for this, are side-chains, notary schemes, hash locking, as well as standardization. Interoperability-focused projects, like Polkadot (Garvin, 2016) and Cosmos (Kwon and Buchman, 2016) try to solve this with the inter-blockchain communication protocols.

4.3. *The Need for Regulation*

The innovative nature of blockchain creates numerous problems for regulators (Fulmer, 2019): finance-oriented blockchain-based solutions, e.g. cryptocurrencies or various financial services, should be regulated (Cermeño, 2016). However, the current centralized regulation scheme is not acceptable for the blockchain decentralized paradigm, especially for public networks, as territorial regulations constitute a problem (Cermeño, 2016). Smart contracts may also demand different treatments from traditional contracts (Cong and He, 2019). Besides, the immutability of data records in public blockchains must be matched with GDPR in the EU (Finck, 2019). Hence, the close collaboration of regulators and the blockchain industry is required to ensure that compliance with regulation, rules, and policies is achieved. Some countries, including Malta, Estonia, Switzerland, Liechtenstein, Singapore, and Japan, are already preparing blockchain-friendly legislation (Dewey, 2019). However, there is no central administration for each distributed ledger, therefore international standards should be established. EU Parliament has already passed blockchain resolution "Distributed ledger technologies and blockchain: building trust with disintermediation" (European Parliament, 2018). Moreover, on the 3rd of April in 2019, the International Association for Trusted Blockchain Applications (INATBA) was established and united together suppliers and users of blockchain with delegates of governmental and standard-setting organizations from all over the world (INATBA, 2019).

5. Conclusions

Revolutionary blockchain technology is only a decade old, but already showed great potential for transforming the traditional industry with its key features: decentralization, anonymity, persistency, and auditability. While the history of the techniques used in blockchain (P2P network, cryptography, record-keeping database, etc.) can be traced back several decades ago, blockchain combined and introduced them in a completely new manner. To better understand what the current status of the blockchain technology is, we first provided a historical insight into the techniques used in nowadays blockchain architectures. We then provided a comprehensive comparison of blockchain platforms that have gained considerable popularity and potential. Special emphasis was given to review typical consensus protocols that are used in state-of-the-art blockchains and highlighted their main weaknesses and strengths. Furthermore, an actively growing online library of blockchain platforms, `BlockLib`, has been introduced. While most of the research is still devoted to Bitcoin, we showed that the applicability of blockchains is far beyond

Bitcoin. There are a plethora of use-cases in various industry sectors where blockchain could bring more security, trust, transparency, data traceability, and efficiency in general. However, blockchain is not a panacea and the appropriate technical solutions for a particular application use-case should be carefully determined. Furthermore, we reviewed energetic, technological, and regulatory challenges that are currently affecting the still limited adoption of the blockchain technology across the industries. Finally, some possible future blockchain directions were also highlighted.

References

Abdullah, N., Hakansson, A., Moradian, E. (2017). Blockchain based approach to enhance big data authentication in distributed environment. In: *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, pp. 887–892.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A. (2019). Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100, 143–174.

Anh, D.T.T., Zhang, M., Ooi, B.C., Chen, G. (2018). Untangling blockchain: a data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 4347(c), 1.

Bach, L., Mihaljevic, B., Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. In: *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, pp. 1545–1550.

Back, A. (1997). A partial hash collision based postage scheme. http://www. hashcash.org/papers/announce.txt. Accessed: 2019-08-13.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G. (2017). SoK: Consensus in the age of blockchains. arXiv preprint arXiv:1711.03936.

Batubara, F.R., Ubacht, J., Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. In: *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. ACM, p. 76.

Bayer, D., Haber, S., Stornetta, W.S. (1993). Improving the efficiency and reliability of digital time-stamping. In: *Sequences Ii*. Springer, pp. 329–334.

Belotti, M., Bozic, N., Pujolle, G., Secci, S. (2019). A vademecum on blockchain technologies: when, which and how. *IEEE Communications Surveys & Tutorials*, 1–47.

Benchoufi, M., Porcher, R., Ravaud, P. (2017). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research*, 6.

Bergquist, J., Laszka, A., Sturm, M., Dubey, A. (2017). On the design of communication and transaction anonymity in blockchain-based transactive microgrids. In: *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*. ACM, p. 3.

Bitshares (2015). Bitshares 2.0. https://bitshares.org/. Accessed: 2019-09-13.

Buterin, V. (2018). Ethereum 2.0 spec–Casper and sharding. https://github.com/ethereum/eth2.0-specs. Accessed: 2019-09-30.

Buterin, V., Griffith, V. (2017). Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437.

Buterin, V., Reijsbergen, D., Leonardos, S., Piliouras, G. (2019). Incentives in Ethereum's hybrid casper protocol. arXiv preprint arXiv:1903.04205.

Castro, M., Liskov, B. (1999). Practical Byzantine fault tolerance. In: *OSDI*, Vol. 99. pp. 173–186.

Castro, M., Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4), 398–461.

Cermeño, J.S. (2016). Blockchain in financial services: regulatory landscape and future challenges for its commercial application. *BBVA Research Paper*. December (16/20).

Chalaemwongwan, N., Kurutach, W. (2018). State of the art and challenges facing consensus protocols on blockchain. In: *2018 International Conference on Information Networking (ICOIN)*. IEEE, pp. 957–962.

Chaum, D. (1983). Blind signatures for untraceable payments. In: *Advances in Cryptology*. Springer, pp. 199–203.

Chen, J., Xue, Y. (2017). Bootstrapping a blockchain based ecosystem for big data exchange. In: *2017 IEEE International Congress on Big Data (Bigdata Congress)*. IEEE, pp. 460–463.

Christidis, K., Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4, 2292–2303.

Chuen, D.L.K. (2015). *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Academic Press.

CoinShares (2019). The Bitcoin mining network. https://coinsharesgroup.com/research/bitcoin-mining-network-june-2019.

Cong, L.W., He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5), 1754–1797.

Dai, W. (1998). b-money. http://www.weidai.com/bmoney.txt.

Datta, A. (2019). Blockchain in the government technology fabric. arXiv preprint arXiv:1905.08517.

deVries, A. (2018). Bitcoin's growing energy problem. *Joule*, 2(5), 801–805.

Dewey, J. (2019). *Blockchain & Cryptocurrency Regulation*. Global Legal Group Ltd.

Digiconomist (2019a). Bitcoin Energy Consumption Index. https://digiconomist.net/bitcoin-energy-consumption. Accessed: 2019-09-25.

Digiconomist (2019b). Ethereum Energy Consumption Index. https://digiconomist.net/ethereum-energy-consumption. Accessed: 2019-09-26.

Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.L. (2017). Blockbench: a framework for analyzing private blockchains. In: *Proceedings of the 2017 ACM International Conference on Management of Data*. ACM, pp. 1085–1100.

Dunphy, P., Petitcolas, F.A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, 16(4), 20–29.

Dwork, C., Naor, M. (1992). Pricing via processing or combatting junk mail. In: *Annual International Cryptology Conference*. Springer, pp. 139–147.

Egelund-Müller, B., Elsman, M., Henglein, F., Ross, O. (2017). Automated execution of financial contracts on blockchains. *Business & Information Systems Engineering*, 59(6), 457–467.

EOS (2017). EOS. IO technical white paper. https://github.com/EOSIO/Documentation. Accessed: 2019-09-04.

European Parliament (2018). Distributed ledger technologies and blockchains: building trust with disintermediation. http://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.pdf. Accessed: 2019-09-30.

Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126, 45–58.

Finck, M. (2019). *Blockchain and the General Data Protection Regulation*. Tech. rep., Panel for the Future of Science and Technology at European Parliament.

Fulmer, N. (2019). Exploring the Legal Issues of Blockchain Applications. *Akron Law Review*, 52(1), 5.

Gan, S. (2017). *An IoT Simulator in NS3 and a Key-Based Authentication Architecture for IoT Devices Using Blockchain*. Indian Institute of Technology Kanpur.

Garvin, W. (2016). POLKADOT: vision for a heterogeneous multi-chain framework. https://polkadot.network/PolkaDotPaper.pdf. Accessed: 2019-09-26.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., Zeldovich, N. (2017). Algorand: scaling Byzantine agreements for cryptocurrencies. In: *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, pp. 51–68.

Gordon, W.J., Catalini, C. (2018). Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal*, 16, 224–230.

Haber, S., Stornetta, W.S. (1990). How to time-stamp a digital document. In: *Conference on the Theory and Application of Cryptography*. Springer, pp. 437–455.

Haber, S., Stornetta, W.S. (1997). Secure names for bit-strings. In: *Proceedings of the 4th ACM Conference on Computer and Communications Security*. ACM, pp. 28–35.

Huh, S., Cho, S., Kim, S. (2017). Managing IoT devices using blockchain platform. In: *2017 19th International Conference on Advanced Communication Technology (ICACT)*. IEEE, pp. 464–467.

IBM (2018). Blockchain market shares, market strategies, and market forecasts, 2018 to 2024. hhttps://www.ibm.com/downloads/cas/PPRR983X.

ICO Watch List (2019). ICO statistics – by industry. https://icowatchlist.com/statistics/categories. Accessed: 2019-09-29.

INATBA (2019). INATBA: international association for trusted blockchain applications. https://inatba.org. Accessed: 2019-10-01.

Jaoude, J.A., Saade, R.G. (2019). Blockchain applications – usage in different domains. *IEEE Access*, 7, 45360–45381.

Johnson, S., Robinson, P., Brainard, J. (2019). Sidechains and interoperability. arXiv preprint arXiv:1903.04077.

Karafiloski, E., Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In: *IEEE EUROCON 2017-17th International Conference on Smart Technologies*. IEEE, pp. 763–768.

Khan, M.A., Salah, K. (2018). IoT security: review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411.

Kiayias, A., Russell, A., David, B., Oliynykov, R. (2017). Ouroboros: a provably secure proof-of-stake blockchain protocol. In: *Annual International Cryptology Conference*. Springer, pp. 357–388.

Kim, S., Kwon, Y., Cho, S. (2018). A survey of scalability solutions on blockchain. In: *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, pp. 1204–1207.

King, S. (2013). Primecoin: cryptocurrency with prime number proof-of-work. *July 7th*, 1, 6.

King, S., Nadal, S. (2012). PPCoin: peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf.

Krause, M.J., Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*.

Kuo, T.T., Zavaleta Rojas, H., Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. *Journal of the American Medical Informatics Association*, 26(5), 462–478.

Kwon, J. (2014, 2017). Tendermint: Consensus without mining. *Draft v. 0.6, Fall*, 1, 11.

Kwon, J., Buchman, E. (2016). Cosmos: a network of distributed ledgers. https://cosmos.network/cosmos-whitepaper.pdf. Accessed: 2019-09-26.

Lamport, L. (1998). The part-time parliament. *ACM Transactions on Computer Systems*, 16(2), 133–169.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*.

Lin, I.C., Liao, T.C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, 19(5), 653–659.

Lopes, V., Alexandre, L.A., Pereira, N. (2019). Controlling robots using artificial intelligence and a consortium blockchain. arXiv preprint arXiv:1903.00660.

Lundqvist, T., De Blanche, A., Andersson, H.R.H. (2017). Thing-to-thing electricity micro payments using blockchain technology. In: *2017 Global Internet of Things Summit (GIoTS)*. IEEE, pp. 1–6.

Merkle, R.C. (1980). Protocols for public key cryptosystems. In: *1980 IEEE Symposium on Security and Privacy*. IEEE, pp. 122–122.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C. (2017). A review on consensus algorithm of blockchain. In: *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, pp. 2567–2572.

Momtaz, P.P., Rennertseder, K., Schröder, H. (2019). Token offerings: a revolution in corporate finance? Available at SSRN 3346964.

Münsing, E., Mather, J., Moura, S. (2017). Blockchains for decentralized optimization of energy resources in microgrid networks. In: *2017 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE, pp. 2164–2171.

Mytis-Gkometh, P., Drosatos, G., Efraimidis, P., Kaldoudi, E. (2018). Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In: *Precision Medicine Powered by pHealth and Connected Health*. Springer, pp. 69–73.

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, 60(12), 36–45.

Nem (2018). Nem technical reference. https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf. Accessed: 2019-09-28.

Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access*, 7, 85727–85745.

Nguyen, G.T., Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, 14(1).

Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A. (2018). Blockchain and IOT integration: a systematic survey. *Sensors*, 18(8), 2575.

Parity Technologies (2017). Proof of authority chains. https://github.com/paritytech/parity-ethereum. Accessed: 2019-09-13.

Paulavičius, R., Grigaitis, S., Filatovas, E. (2019). BlockLib: a collection of the blockchain platforms. https://github.com/blockchain-group/BlockLib. Accessed: 2019-09-26.

Pawlak, M., Guziur, J., Poniszewska-Marańda, A. (2018). Voting process with blockchain technology: auditable blockchain voting system. In: *International Conference on Intelligent Networking and Collaborative Systems*. Springer, pp. 233–244.

Peters, G.W., Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. In: *Banking Beyond Banks and Money*. Springer, pp. 239–278.

Poon, J., Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf. Accessed: 2019-09-29.

Popov, S. (2016). The tangle. *Cit. on*, 131.

Ramya, U., Sindhuja, P., Atsaya, R., Dharani, B.B., Golla, S.M.V. (2018). Reducing forgery in land registry system using blockchain technology. In: *International Conference on Advanced Informatics for Computing Research*. Springer, pp. 725–734.

Risius, M., Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering*, 59(6), 385–409.

Samaniego, M., Deters, R. (2016). Using blockchain to push software-defined IoT components onto edge hosts. In: *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*. ACM, p. 58.

Sarpatwar, K., Vaculin, R., Min, H., Su, G., Heath, T., Ganapavarapu, G., Dillenberger, D. (2019). Towards enabling trusted artificial intelligence via blockchain. In: *Policy-Based Autonomic Data Governance*. Springer, pp. 137–153.

Shibata, N. (2019). Blockchain consensus formation while solving optimization problems. arXiv preprint arXiv:1908.01915.

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: the road ahead. *Computer Networks*, 76, 146–164.

Singh, S., Singh, N. (2016). Blockchain: future of financial and cyber security. In: *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, pp. 463–467.

Singh, S.K., Rathore, S., Park, J.H. (2019). BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*.

Siyal, A., Junejo, A., Zawish, M., Ahmed, K., Khalil, A., Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. *Cryptography*, 3(1), 3.

Stoll, C., Klaaßen, L., Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule*, 3(7), 1647–1661.

Sullivan, C., Burger, E. (2019). Blockchain, digital identity, E-government. In: *Business Transformation through Blockchain*. Springer, pp. 233–258.

Szabo, N. (1994). Smart Contracts. *Unpublished manuscript*.

Szabo, N. (2008). Bit gold. Unenumerated. https://unenumerated.blogspot.com/2005/12/bit-gold.html.

TeqAtlas (2019). Blockchain investment trends. https://teqatlas.com/analytics-and-research/fs776-blockchain-investment-trends-1h-2019. Accessed: 2019-10-20.

The ZILLIQA Team (2017). The ZILLIQA technical whitepaper. https://docs.zilliqa.com/whitepaper.pdf.

Truby, J. (2018). Decarbonizing Bitcoin: law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Research & Social Science*, 44(June), 399–410.

Tseng, J.H., Liao, Y.C., Chong, B., Liao, S.W. (2018). Governance on the drug supply chain via gcoin blockchain. *International Journal of Environmental Research and Public Health*, 15(6), 1055.

University of Cambridge (2019). Cambridge Bitcoin Electricity Consumption Index. https://www.cbeci.org. Accessed: 2019-09-26.

Valenta, M., Sandner, P. (2017). *Comparison of Ethereum, Hyperledger Fabric and Corda*. FSBC Working Paper.

Veena, P., Panikkar, S., Nair, S., Brody, P. (2015). Empowering the edge-practical insights on a decentralized internet of things. *Empowering the Edge-Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value*, 17.

Vranken, H. (2017). Sustainability of Bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, 28, 1–9.

Wang, W., Hoang, D.T., Xiong, Z., Niyato, D., Wang, P., Hu, P., Wen, Y. (2018). A survey on consensus mechanisms and mining management in blockchain networks. arXiv preprint arXiv:1805.02707, 1–33.

Xiao, Y., Zhang, N., Lou, W., Hou, Y.T. (2019). A survey of distributed consensus protocols for blockchain networks. http://arxiv.org/abs/1904.04098.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A.B., Chen, S. (2016). The blockchain as a software connector. In: *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. IEEE, pp. 182–191.

Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). *Blockchain Technology Overview*. Tech. rep., National Institute of Standards and Technology.

Yang, W., Garg, S., Raza, A., Herbert, D., Kang, B. (2018). Blockchain: trends and future. In: Yoshida, K., Lee, M. (Eds.), *Knowledge Management and Acquisition for Intelligent Systems*, pp. 201–210.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology? – A systematic review. *PLOS ONE*, 11(10), e0163477.

Yuan, Y., Wang, F.Y. (2016). Towards blockchain-based intelligent transportation systems. In: *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, pp. 2663–2668.

Zhang, A., Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, 42(8), 140.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: architecture, consensus, and future trends. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, pp. 557–564.

Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352.

Zhou, L., Wang, L., Sun, Y. (2018). Mistore: a blockchain-based medical insurance storage system. *Journal of medical systems*, 42(8), 149.

R. Paulavičius is a senior researcher and head of the Blockchain Group at the Institute of Data Science and Digital Technologies, Vilnius University, Lithuania. His research interests include blockchain technology, optimization software, parallel computing, development and application of various operation research techniques.

S. Grigaitis is a partnership associate professor at Vilnius University, a member of the Blockchain Group in the Institute of Data Science and Digital Technologies, and an experienced industry professional. His research interests focus on blockchain technologies, large-scale distributed systems and artificial intelligence.

A. Igumenov is a lecturer at the Faculty of Mathematics and Informatics, Vilnius University, Lithuania. Received the doctoral degree in informatics engineering from the Vilnius University in 2012. His main research interests include blockchain technologies, global optimization, high-performance and parallel computing, IoT and internet technologies.

E. Filatovas is a senior researcher and co-founder the Blockchain Group at the Institute of Data Science and Digital Technologies, Vilnius University, Lithuania. His main research interests include blockchain technologies, global and multi-objective optimization, evolutionary algorithms, high-performance computing, artificial intelligence, and image processing.