Computer Communications 169 (2021) 179–201

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research

Abdurrashid Ibrahim Sanka [a,*], Muhammad Irfan [a], Ian Huang [b], Ray C.C. Cheung [a]

[a] Department of Electrical Engineering, City University of Hong Kong, Hong Kong
[b] Digital Transaction Limited, Hong Kong

ARTICLE INFO

Keywords:
Blockchain
Cryptography
Consensus
Breakthrough
Adoptions

ABSTRACT

Blockchain technology gets more attention and adoptions in various countries and companies all over the world. Blockchain is currently bringing a revolution in many enterprises like finance, healthcare, supply chain, insurance, registry, and the internet of things. Many enterprises integrate blockchain with their systems for the benefits of the blockchain. Despite its strength, blockchain has some challenges in security, privacy, scalability, and other few. This paper surveys the breakthrough in blockchain technology, its applications, and challenges. As many blockchain papers focus on cryptocurrencies, IoT, and security, this paper focuses on the overall state of the art of blockchain technology, its recent developments, and adoptions, especially in areas besides cryptocurrencies. We give a comprehensive review of the cryptography behind the blockchain for a better understanding of the technology. We also review quantitative surveys and analysis on both the public and the enterprise blockchains. Finally, we review the future research opportunities and directions on the blockchain technology.

Contents

* Corresponding author.
E-mail addresses: iasanka2-c@my.cityu.edu.hk (A.I. Sanka), m.irfan@my.cityu.edu.hk (M. Irfan), info@digital-transaction.com (I. Huang), r.cheung@cityu.edu.hk (R.C.C. Cheung).

https://doi.org/10.1016/j.comcom.2020.12.028
Received 31 March 2020; Received in revised form 25 September 2020; Accepted 29 December 2020
Available online 30 January 2021

1. Introduction

Blockchain technology is an inspiring emerging technology capable of disrupting many industries and our way of life. Besides cryptocurrencies, blockchain can help many industries to improve inefficiencies and overcome many bottlenecks. For example, using blockchain can speed up transaction settlements, reduce costs, provide transparency, auditability, efficiency, revenue, and security [1–3]. R3 [4], a consortium of globally over 200 financial institutions has been harnessing the benefits of blockchain using their Corda blockchain platform [5]. There are several adoptions of blockchain in various countries like Georgia, Estonia, and Russia as well as in companies such as IBM and Microsoft.

Gartner [6] forecasted the business value of blockchain to be over 176 billion USD and 3.1 trillion USD by 2025 and 2030 respectively. Cisco [7] also predicted that 10% of the global GDP will be on blockchain by 2027 and the blockchain market will be 9.7 billion USD by 2021. More than 40 central banks are experimenting with central bank digital currency (CBDC) [8] while Facebook's digital currency (Libra) was targeted to be launched in 2020 pending approval from the US regulators [9].

Most enterprise blockchain projects are currently in production stage with many already deployed in 2019. The Cambridge center for alternative finance [10] surveyed 67 live blockchain networks that were already in production. According to the Deloitte's 2019 global blockchain survey [11], 86% of 1386 high revenue companies believed that blockchain will finally get mainstream adoption. Many of the respondents (53%) said blockchain is one of their top five critical strategic priorities.

Despite its benefits, blockchain has some challenges of scalability, security, legal regulation, privacy, and a few more. Hence, there is a need to review and survey the state of the art of blockchain to quantify its progress and explore its challenges and future directions for further research.

There are many survey papers on blockchain many of which concentrated on Bitcoin, security, and IoT [12]. Conti [13] presented a detailed survey of the privacy and security issues in Bitcoin. Tschorsch [14] gave a comprehensive survey on Bitcoin. Nofer [15] discussed the applications of blockchain and highlighted how the blockchain could disrupt other industries. Zheng et al. [16] presented a survey of the challenges and opportunities of blockchain technology. Monrat [17] also surveyed blockchain applications and challenges. Firica [18] presented the progress achieved by blockchain in Romans. Vranken [19] looked into the possibility of sustaining Bitcoin system. Wang [3] presented a blockchain survey for IoT. Farouk [1] surveyed blockchain for industrial healthcare while Miglani [20] studied the applicability of blockchain on the internet of energy management. Frizzo-Barker [2] is a systematic review of blockchain for businesses. Kus [21] surveyed the privacy and anonymity in Bitcoin-like payment systems. Sankar [22] and Wang [23] are surveys of blockchain consensus protocols. Other blockchain surveys include [24–30].

However, review of quantitative analysis and surveys of the blockchain is missing in the existing academic blockchain survey papers. The existing survey papers also lack in-depth discussion and review of the cryptography behind the blockchain. In this paper, we survey the breakthrough and the state of the art of blockchain technology covering recent developments in its adoptions, applications, and challenges. We provide a comprehensive review of the cryptography behind the blockchain technology. We also review the recent quantitative analysis and surveys of blockchain as it is missing in the existing blockchain surveys. Finally, we studied the challenges and future research directions on the blockchain. The contributions of this paper are summarized as follows:

- We give a detailed background of blockchain technology citing its benefits and importance.
- We review the blockchain applications and challenges.
- We give a comprehensive review of the cryptography behind blockchain technology.
- We survey the breakthrough of blockchain technology covering its recent developments, adoptions, and use cases.
- We review the recent quantitative analysis and surveys on blockchain technology.
- We review the future research opportunities and directions on blockchain.

The rest of the paper is organized as follows: Section 2 gives the background of blockchain technology. Section 3 gives the details of the cryptography behind blockchain. Section 4 reviews the applications of blockchain while Section 5 discusses the breakthrough and the state of the art of blockchain. Section 6 is the review of the quantitative analysis and surveys of blockchain while the challenges and future research

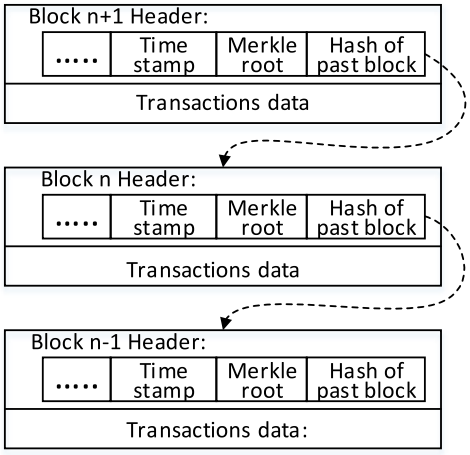

Fig. 1. Blockchain structure.

directions on the blockchain are covered in Section 7. Conclusion is finally made in Section 8.

2. Background

Blockchain was proposed for Bitcoin by Satoshi Nakamoto [31] in his quest to solve the Europe's economic crisis in 2008. The technology underpins cryptocurrencies like the Bitcoin and many other applications. Satoshi proposed Bitcoin as a new payment method that dispenses with central authorities (central banks) using a cryptographically protected chain of data blocks later called as blockchain.

2.1. What is blockchain?

Blockchain is a distributed database (ledger) consisting of interconnected blocks of data protected by cryptographic concepts against tampering. Blockchain works without a central authority and is managed using the consensus of its network participants. Each node in a blockchain network has a copy of the blockchain (full node) or depends on full nodes for the blockchain data (lightweight node). Blockchain data continuously grows as new blocks are added. Once added to the blockchain, the data cannot be deleted unless with the agreement of all or the majority of the network participants (immutability). Each block in blockchain contains the hash of the previous block for tamper-proof protection and data integrity. The hash of the block changes when any data in the block is modified. Any data modification is detected since the new hash is different from the previously stored hash in the next block.

Fig. 1 shows the structure of blockchain. It consists of the block header and the transaction data. The block header consists of several items such as the hash of the previous block, timestamp, Merkle root of transactions, difficulty, and the nonce (depending on the network). The transaction data contains all the transactions in the block. Genesis block is the first block in a blockchain and has no previous block hash. All blocks can be traced to the genesis block for verification.

2.2. Why blockchain is important?

Blockchain possesses good features that make it beneficial. The strength and promising features of blockchain were first observed from the success of Bitcoin whose capital market now reaches 191 billion USD [32]. The UK government office of science reported that blockchain secures data records, reduces operational costs, and provides transparency in transactions [33]. The interesting features, benefits, and importance of blockchain include:

1. **Distributed nature:**
The same blockchain data is stored by different users (nodes) on the blockchain network at the same time. If one node is faulty or lost its data, other nodes on the network still have the copy of the blockchain and keep updating it. The affected node can recopy the blockchain from the other nodes. This feature prevents data loss, record tampering as well as double-spending in cryptocurrencies.
2. **Data integrity and security:**
Blockchain is tamper-proof in the sense that when any data in any block is changed, the change is detected due to the change in the block hash which will differ from the previously stored hash in the next block. For an adversary to be successful, he has to modify the blocks data for all computers on the network which is practically infeasible for a large network. Hence, data is secured on blockchain against tampering in this regard.
3. **Transparency and traceability:**
Since blockchain records are time-stamped and stored on all full nodes on the network, all activities and transactions can be checked and seen by everyone on the network. If the address of a node is known, all its activities and transactions could be traced. This makes blockchain transparent and traceable. It also makes it suitable for fraud detection and a good tool for auditing and public services [29,33].
4. **Decentralized nature:**
Blockchain dispenses with central authorities and intermediaries, thus becoming more suitable for trustless systems. Blockchain allows systems to be autonomous and free from the risks of intermediaries and central authorities. However, private blockchains may be partially or fully centralized but still benefits from the other features of blockchain [15].
5. **Cost saving:**
Using blockchain comes with huge cost savings as costs associated with intermediary systems are saved. About $20 billion per year could be saved by banks when using efficient blockchain [34]. This is one of the reasons why some banks and enterprises want to incorporate blockchain into their systems to reduce costs.
6. **Efficiency:**
Blockchain allows systems to work autonomously with more efficiency resulting from the removal of intermediary subsystems. This is among the benefits many companies and countries are trying to gain from the use of blockchain.
7. **Interoperability:**
Blockchain provides a secure data sharing platform that allows separate parties to share the same data and synchronize their services. For example, companies like banks and insurance companies may share data using blockchain for interoperability and other benefits [35].
8. **Verifiability:**
Due to the cryptography in blockchain, the authenticity of a record can be verified. This may be difficult to achieve in other databases because it requires cryptographic mechanisms like digital signature as used in blockchain.

2.3. Types of blockchain

Due to the diversification of interests in blockchain applications, blockchain is classified into public, private, and consortium blockchains [36]. Table 1 compares the three types of blockchain.

1. **Public blockchain:**
A public blockchain is permissionless, hence anyone can join the network, read or write and participate in its consensus with full right without prior permission. Public blockchains are fully decentralized, however, they are vulnerable to privacy issues, selfish mining, and 51% attack [37,38]. Bitcoin and Ethereum are the most prominent public blockchains.

Table 1
Comparison of blockchain types.

Blockchain	Participation	Members	Security	Centralization	Scalability	Efficiency	Energy spent	Examples
Public	Permissionless	Unknown	Best	Decentralized	Low	Low	Consensus-dependent	Bitcoin, Ethereum
Private	Permissioned	Known	Good	Centralized	High	Higher	Very low	Blockstack, Multichain
Consortium	Permissioned	Known	Better	Partial	Moderate	High	Very low	Hyperledger, Corda

Table 2
Comparison of blockchain Consensus protocols.

Consensus	PoW	POS	DPoS	PBFT	Raft	Tendermint	Ripple
Year	1999	2012	2014	1999	2013	2014	2012
Type	Permissionless	Permissionless	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned
Criteria	solving puzzle	Stake	voting+stake	BFT+voting	voting	voting	voting
Energy waste	Very high	Low	Very low	Very low	Very low	Very low	Very low
Security	More secure	less secure	Secure	Secure	Secure	Secure	Secure
Scalability	Very low	High	Very high	Low	Very high	Very high	High
Latency	Very High	Low	Very low	Low	Very low	Very low	Low
Trust	No	No	No	Semi	Semi	Yes	Yes
Throughput (tps)	< 20	100	100,000	Up to 20,000	$> 10,000$	10,000	1,500
Mining done	Yes	Yes	Yes	No	No	No	No
Record finality	No	No	No	Immediate	Immediate	Immediate	Immediate
Adversary tolerance	$< 50\%$	$< 50\%$	$< 50\%$	$\leq (n-1)/3$	–	$\leq (n-1)/3$	$\leq (n-1)/5$
Crash tolerance	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$	$< 50\%$
Use case	Bitcoin,Ethereum	Peercoin, NVC	Bitshares	Hyperledger	Corda	Tendermint	Ripple

2. **Private blockchain:**
A private blockchain is permissioned, that is, users are required to be authorized to join the network. The authorized users are known and can read or write as well as validate transactions. Normally, a private blockchain is used for business process automation in a single organization with sub-divided departments that can act as blockchain nodes. Even though private blockchain is less secure and centralized, it is more scalable and has no 51% attack, privacy, and selfish mining issues. Multichain and Blockstack are examples of private blockchains [19,37].
3. **Consortium blockchain:**
A consortium blockchain is also permissioned and stands between the public and the private blockchains. Consortium blockchains are used by independent organizations sharing information with little or no trust. Only pre-selected nodes (validators) order transactions and create new blocks. The rest of the nodes can only send transactions, read and verify new blocks. Consortium blockchains are partially centralized. However, they have less privacy and security concerns as well as no 51% attack. Corda and Hyperledger are examples of consortium blockchains [36,38].

2.4. How blockchain system works

Blockchain is used where data is to be shared and there are multiple writers to the ledger having little or no trust. A new record (transaction) is signed using digital signature with the sender's private key for authentication. The signed transaction is then broadcasted to the blockchain peer to peer network for verification and addition into the blockchain. Other nodes verify the transaction and retransmit it through their neighbors. Special nodes (miners/orderers/validators) collect transactions and create a new block containing a large number of transactions depending on the consensus algorithm. Upon successful creation of a block by the miner/validator node, the new block is broadcasted to the network for further verification and acceptance. The rest of the nodes verify the new block and add it to their main blockchain if it is valid. When a fork (existence of two or more chains at the same time) occurs, the longest chain is chosen as the main blockchain while the shorter chain is discarded. Most private blockchains use consensus protocols with finality (having no fork).

2.5. Consensus in blockchain technology

Consensus protocol in blockchain is a general agreement (rules) followed by the blockchain nodes to synchronize the network, maintain and update the blockchain ledger. Consensus protocol describes how new blocks are created. Blockchain generally uses the Byzantine General's problem for its consensus. Table 2 compares some of the popular consensus protocols. Fig. 10 also shows the consensus mechanisms commonly used in enterprise blockchains.

1. **Proof of Work (PoW):**
The idea of PoW was invented in 1993 by Cynthia Dwork and Naor Moni [39]. Markus Jacobson and Ari Juels coined the idea as "proof of work" in 1999 [40]. PoW uses computing power and is used for mining process. In the mining process, some of the network nodes called miners compete in doing computation by solving complex mathematical puzzles to qualify for creating a new block and minting new crypto coins. The miner that gets the required result first is the winner and the one to submit the new block as well as enjoy some new coins as an incentive. Miners repeatedly compute the hash of their proposed block until the hash value is as small as a given difficulty value (nBits) in the block. If the desired value is not obtained, a nonce in the block is incremented for the next hashing trial. In Bitcoin, the difficulty is adjusted over time to maintain the addition of 1 block on average of 10 min for security purpose [41]. PoW secures the network against double-spending and denial of service (DoS) attacks. However, 51% attacks and selfish mining are security concerns in networks using PoW. When a fork occurs, the longest chain is chosen as the main chain. Hence, more confirmations (6 in Bitcoin) are recommended before accepting payments in cryptocurrencies using PoW consensus for security.
There is so much concern on PoW over its enormous energy waste which was estimated in September 2020 as 65.19TWh per year [42]. This energy is equivalent to the energy consumed by countries like Austria and Czech Republic. It is also more than the energy consumed individually by 175–181 countries [43]. However, more energy efficient PoW is used in Primecoin cryptocurrency. Instead of hashing, Primecoin miners compute special prime number sequences (Cunningham and bi-twin chains) which are useful for Cryptography [44].
2. **Proof of Stake (PoS):**
Unlike the PoW, PoS consensus requires no mining computations to save the energy waste in PoW. In PoS, special nodes called validators collect transactions and create new blocks. The chance of a validator to add a new block is related to the amount of the stake (coins/currency) he owns. Validator with a higher stake has higher chance to submit new blocks. The reason behind this is that owners of large stakes are unlikely to harm the network. However, the main issue with POS is the so-called nothing-at-stake problem. Validators lose nothing by building

on both chains when a fork occurs thus, the chances of double-spending attacks increase.

To enhance security and avoid centralization, variant types of proof of stake such as the Delegated Proof of Stake (DPoS) are used in altcoins like Blackcoin and Peercoin [16]. Casper is a project aimed at upgrading Ethereum blockchain to PoS combined with Byzantine Fault Tolerant (BFT) consensus.

3. **Practical Byzantine Fault Tolerance (PBFT):**

PBFT is a voting-based consensus used in private and consortium blockchains. The consensus works securely with f out of n nodes assumed to be malicious, where $n = (3f + 1)$ and $f = (n - 1)/3$. The system is only secure if the malicious nodes (f) are at most $1/3$ of the total nodes n. PBFT involves a large number of messages $O(n^2)$ hence, it works best with a small number of nodes (< 100 for example) [3].

PBFT operated in successive rounds called views. Each view has an elected leader called primary and other nodes (replicas or backups). The primary coordinates the creation of new blocks. Clients send transactions (requests) to the primary of a current view. The primary then starts a three-phase protocol (pre-prepare, prepare, and commit phases) by multicasting the transactions to all the backups. In the pre-prepare phase, the primary assigns a sequence number to each transaction and prepares a new block proposal which is sent to all the backups. The primary also sends a pre-prepare message containing the view number, the primary ID, the block ID, and the block number. If a backup accepts the pre-prepare message, it sends a prepare message to the primary and all other backups as its agreement on the new block to be created. When a backup receives $2f + 1$ prepare messages, it enters the commit phase. In the commit phase, backups verify and validate requests in the proposed block. If all the requests are valid the backup sends a commit message to all other backups. The new block is finally added to the blockchain if a backup receives at least $2f + 1$ matching commit messages i.e. at least $2/3$ of the nodes agree to add the new block. There is no fork in PBFT hence, the newly added block is final [3].

4. **Tendermint:**

Tendermint is also a voting-based consensus protocol. It also has finality and achieves consensus without mining (zero energy waste). In Tendermint also, new blocks are created in rounds. Each round consists of three steps (propose, prevote, and pre-commit) of democratic voting among the block validators. A validator adds (commit) the proposed block to his blockchain if he receives pre-commit messages from $2/3$ of the validators. Validators are punished if found cheating. Tendermint coin uses the Tendermint consensus [17,45].

5. **Other consensus protocols:**

Several other consensus algorithms proposed include the Raft, Ripple, Proof of Burn (PoB), Proof of Activity (PoA), Delegated Proof of Stake (DPoS), Federated Byzantine Fault Tolerance (FBFT), Proof of Publication (PoP), Proof of Capacity (PoC), Proof of Existence (PoE), Proof of Elapsed time (PoET), Proof of Space(PoS), and so on [23,25].

3. Cryptography behind blockchain

The beauty of blockchain technology is how the existing concepts in cryptography are integrated with consensus and incentive mechanisms. Blockchain is supported and protected by cryptographic concepts such as hashing operations, digital signatures, Merkle tree, and Merkle Patricia trie. Cryptographic accumulators, commitments, and zero-knowledge proofs are also used mostly for privacy enhancements [35,46].

3.1. Hashing operations in blockchain

Hashing (hash function) transforms strings of information into a fixed length and scrambled hex string. For use in security applications, hash functions are required to be collision-free and possess one-way property. Collision-free means that no two different inputs to the hash function will generate the same hash output (message digest). Any slight alteration to the input results in a different message digest. The one-way property ensures that the input cannot be obtained (reverse engineered) from the message digest.

Hashing is used in blockchain to provide data integrity (security), create addresses and transactions. Furthermore, hashing is essential in PoW consensus mechanism as well as in digital signature schemes. A Hash function is used to generate the transactions and the block hashes referred to as the Merkle root and block hash respectively.

The security of blockchain, especially that of its consensus protocols can be broken if a hash collision can easily be found. Based on the birthday paradox, it averagely takes $2^{n/2}$ trials using brute force to find a collision for an n-bit output hash function. Thus, a hash function with a small number of output bits (n), is much easier to break. If less than $2^{n/2}$ trials are discovered to be required for collision on a hash function, the hash function is considered broken. In 2004, Wang et al. [47] found several collisions on MD5, MD4, RIPEMD, and Haval-128 hash functions. They later broke the SHA-1 hash function in 2005 with 2^{69} trials which are less than the expected birthday attack (2^{80} trials) [48]. Hence, NIST in 2010 recommended SHA-2 hash functions for applications needing collision resistance. SHA-256 and other approved hash functions are currently very secure. To find collision on SHA-256, an adversary requires 2^{128} trials which is practically infeasible with the currently available computing power. Even with a fast supercomputer, it will take millions of years to break the SHA-256.

Most blockchain applications use the SHA-256 hash function. RIPEMD160 is also used together with the SHA-256 for blockchain addresses as in Bitcoin. Few other hash functions have been created to be memory-hard in order to resist ASIC mining (dominant in Bitcoin) so that more miners can participate using PCs and GPUs. Ethereum (ETH), Ethereum Classic (ETC), Ethereum Fog, Metaverse, DaxxCoin (DAXX), Musicoin (MUSIC), Expanse (EXP), Elementrem (ELE), and Ellaism (ELLA) all use Ethash hash function in mining for its ASIC resistance [49]. Litecoin, Blackcoin, BitConnect, Stratis, and some other altcoins use Scrypt hash function which is also ASIC resistant. Equihash and X11 are other memory-hard hash functions used in Zcash and Dash cryptocurrencies respectively.

3.1.1. SHA-256 hash function

Most blockchains use SHA-256 hash function. SHA-256 is recommended by NIST [50] as a secure hash standard. In fact, double SHA-256 hashing is carried out in Bitcoin for more data integrity. Fig. 2 describes the procedure for SHA-256 hash function. SHA-256 takes in a message of length l bits ($0 < l < 2^{64}$) and outputs a 256-bits message digest $H(M)$. The input message (M) is processed in blocks, each 512-bit wide. After padding, the message is divided into N blocks. Each block is processed by the compression function in sequence. The hash result after processing block i (intermediate hash $H^{(i)}$) is used as the initial hash input for processing the next block. The message digest $H(M)$ is the intermediate hash after processing the last block.

Padding:

Padding is adding extra bits to an input message to make the number of bits of the message multiple of 512 so that the message will have exactly n blocks, 512-bits each.

Initial Hash Value $H^{(0)}$:

The initial hash value is the fractional part (first 32 bits) of the square root of first 8 prime numbers (2–19). It is used as the initial hash value for initializing the working variables in processing the first message block. This value consists of eight 32-bits vectors $H_0^{(0)}$ to $H_7^{(0)}$ shown in (1) [50]:

$$\begin{aligned} H_0^{(0)} &= 6a09e667 & H_1^{(0)} &= bb7ae85 \\ H_2^{(0)} &= 3c6ef372 & H_3^{(0)} &= a54ff53a \\ H_4^{(0)} &= 510e527f & H_5^{(0)} &= 9b05688c \\ H_6^{(0)} &= 1f83d9ab & H_7^{(0)} &= 5be0cd19 \end{aligned} \tag{1}$$

The working variables *a, b, c, d, e, f g, and h*:

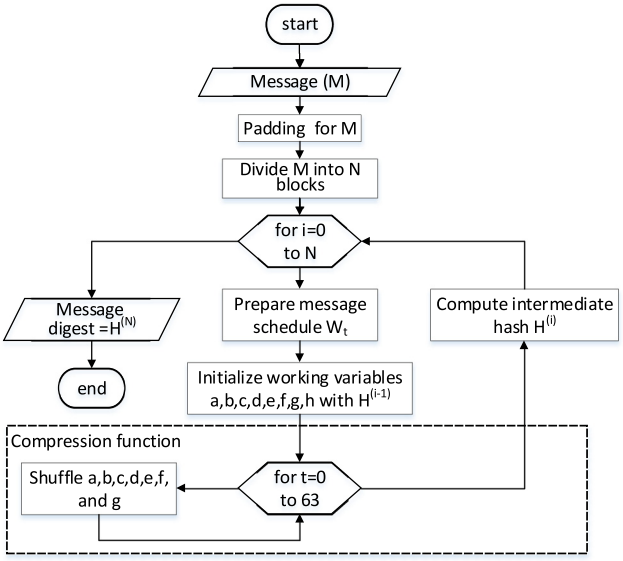

Fig. 2. SHA-256 hash function procedure.

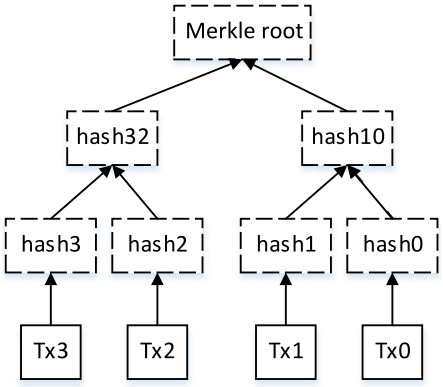

Fig. 3. Merkle tree in blockchain.

The working variables represent the hash of the previous message block $H^{(i-1)}$ which consists of eight 32-bits vectors $H_0^{(i-1)}$ to $H_7^{(i-1)}$. At the beginning of processing each block, the eight working variables are initialized as shown in (2) before used in the compression function [50].

$$\begin{aligned} a &= H_0^{(i-1)} & b &= H_1^{(i-1)} \\ c &= H_2^{(i-1)} & d &= H_3^{(i-1)} \\ e &= H_4^{(i-1)} & f &= H_5^{(i-1)} \\ g &= H_6^{(i-1)} & h &= H_7^{(i-1)} \end{aligned} \tag{2}$$

Message Schedule (W_t):

Each message block (M^i) is expanded into a message schedule (W_t) before processed by the compression function for the actual hashing operations. Each message block consists of 16 words $M_0^{(i)}$ to $M_{15}^{(i)}$ (32 bits each). The block is passed to a message scheduler function which further expands the 16 words of the block to 64 words W_0 to W_{63} (32 bits each) as the message schedule (W_t) for use in the compression function.

The compression function:

The actual hashing takes place in the compression function. The compression function performs 64 rounds of operations on the message schedule and the working variables for each message block. The operations are bitwise XOR, AND, OR, complement, mod 2^{32} addition, rotation, and shifting operations. Before used in the compression function, the working variables are initialized with the hash of previous message block (intermediate hash $H^{(i)}$). The message schedule is also prepared from the current message block. The aim of the compression function is to shuffle as well as compress the working variables with the message block represented by the message schedule. After shuffling of the working variables by the compression function, the intermediate hash vectors $H_0^{(i)}$ to $H_7^{(i)}$ for each message block i are computed as:

$$\begin{aligned} H_0^{(i)} &= a + H_0^{(i-1)} \\ H_1^{(i)} &= b + H_1^{(i-1)} \\ H_2^{(i)} &= c + H_2^{(i-1)} \\ H_3^{(i)} &= d + H_3^{(i-1)} \\ H_4^{(i)} &= e + H_4^{(i-1)} \\ H_5^{(i)} &= f + H_5^{(i-1)} \\ H_6^{(i)} &= g + H_6^{(i-1)} \\ H_7^{(i)} &= h + H_7^{(i-1)} \end{aligned} \tag{3}$$

The intermediate hash value $H^{(i)}$ for each message block is obtained by concatenating the intermediate hash vectors as:

$$H^{(i)} = H_0^{(i)} \parallel H_1^{(i)} \parallel H_2^{(i)} \parallel H_3^{(i)} \parallel H_4^{(i)} \parallel H_5^{(i)} \parallel H_6^{(i)} \parallel H_7^{(i)} \tag{4}$$

After processing all the message blocks ($M^{(0)}$ to $M^{(N)}$), the final hash value (message digest) of the message $H(M)$ is the intermediate hash of the last message block ($H^{(N)}$).

For further reading, the full and more in-depth implementation details of SHA-256 is given by NIST in [50].

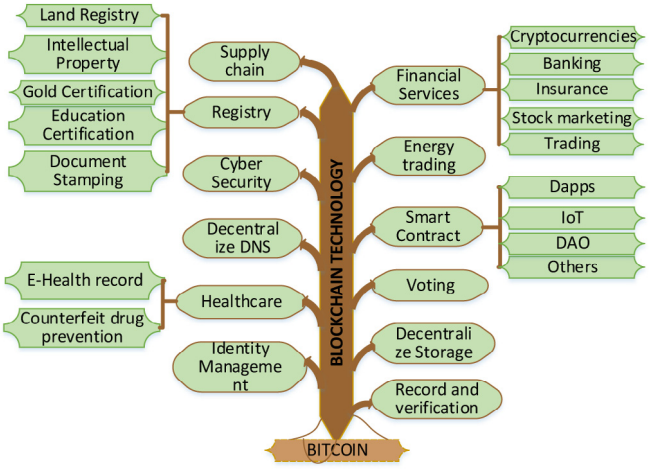

Fig. 4. Blockchain applications tree.

3.2. Merkle root, Merkle tree and Merkle Patricia trie

In blockchain, all transactions in a block are represented by a single hash called the Merkle root which is stored in the block header. The Merkle root is the last hash value of the Merkle tree constructed from the hashes of the transactions in a block. Fig. 3 shows the construction of a Merkle tree from an example block having four transactions even though a block in blockchain may contain a few thousand transactions. To compute the Merkle root, the hashes of the transactions in a block are hashed in pairs. The hash results are continuously paired and hashed again until the Merkle root which is the last hash result is obtained. Modification of any transaction data will be detected since the Merkle root of the modified transactions will be different from the previously stored Merkle root in the block header.

Simplified Payment Verification (SPV) nodes use Merkle root to check whether a claimed payment transaction is in the blockchain or not. SPV node stores only block headers leaving the transactions data. After receiving the payment transaction claim, the SPV node requests the Merkle branches of the transaction hash from a blockchain server. The SPV node then computes the Merkle root from the transaction hash and the Merkle branches received from the server. If the result is the same as the Merkle root already stored in the block header, the transaction is in the blockchain and hence accepted. For example, to verify if Tx0 in Fig. 4 is indeed in the block, the SPV node only requests for $hash1$ and $hash32$ (Merkle branches of $hash0$). Using the $hash0$, $hash1$, and $hash32$, the SPV node computes the Merkle root and compares it with the Merkle root stored in the block header. Therefore, the SPV node can verify if transactions are in the blockchain without needing to download all the block transactions (Tx1, Tx2, and Tx3 in this case).

In Ethereum, every full node stores the network's global state. The global state contains information such as the account balance, gas price, and the gas limit for all the accounts in the network. Ethereum uses Modified Merkle Patricia Trie (MPT) to maintain and store data such as transactions and the global state. MPT is a combination of Merkle tree and Patricia trie optimized for the Ethereum. Patricia trie is a data structure for storing and retrieval of key–value pairs. Therefore, MPT is a cryptographically authenticated persistent data structure for mapping keys to values where the key is the sha3 hash of the value. Unlike in hash table, searching or retrieval of data in MPT requires looking up into a sequence of nodes (key–value pairs) each storing the key of the next node. The last node (leaf node) contains the required value corresponding to the searched key. Any data modification in the tree is detected since the root hash will also change. In Ethereum, the MPTs are stored in leveldb database upon commit of a block.

In addition to data integrity, MPT provides more information such as the state of accounts to Ethereum users. An Ethereum block contains three MPTs, namely, the state, transaction, and receipt tries. The state trie gives the global state, the transaction trie gives the transaction records while the receipt trie gives the outcomes of the executions of all the transactions (e.g. cumulative gas consumed) in a block. For further reading, a detailed specification of MPT is given by Ethereum in [51].

3.3. Digital signature in blockchain

Digital signature is used to authenticate transactions and ensure non-repudiation in blockchain. Elliptic Curve Digital Signature Algorithm (ECDSA) is used in Bitcoin and most blockchain applications to sign and verify transactions [52]. However, Monera and NaiveCoin use the Edwards-curve digital signature algorithm (EdDSA) [53]. RingCoin and some other altcoins use ring signatures for anonymity. One-time ring signature (OTS) [54] and Borromean ring signature (BRS) [55] are used together with ECDSA or EdDSA or rarely alone in some few applications such as Monero. Most blockchains nowadays use multi-signature in addition to the ECDSA or EdDSA for privacy and more security [46]. For brevity, we review Elliptic Curve Cryptography (ECC) and the Elliptic Curve Digital Signature Algorithm (ECDSA).

3.3.1. Elliptic curve cryptography

Blockchain uses asymmetric cryptography where two different keys (public and private keys) are required. These keys are used for encryption, decryption, and digital signatures. Most blockchains use an elliptic curve over prime field for key pair creation and other operations like the digital signature. Elliptic curve cryptography (ECC) shows better implementation efficiency and security than other cryptography schemes like RSA and DSA. It is also more suitable for devices with low power, less memory, and bandwidth capabilities [56]. ECC was invented in 1985 independently by Neal Koblitz [57] and Victor Miller [58]. The security of elliptic curve cryptos is based on the difficulty of their discrete logarithmic problem. This means that, given a point P on an elliptic curve, it is easy to multiply P by a multiplier k to get another point Q. However, it is very much difficult (computationally infeasible with the current computing power) to get the multiplier by just knowing the two points P and Q. Therefore, using ECC it is infeasible to get the private key of someone by just knowing his public key and the curve's generator point.

3.3.2. Definition

An elliptic curve E over the field $\mathbb{F}_p$ is defined by the equation:

$$E : y^2 = x^3 + ax + b \qquad mod\ p \tag{5}$$

where: $a, b \in \mathbb{F}_p : 4a^3 + 27b^2 \neq 0$.

Parameters *a, b, p, G, n, h* are the global domain parameters chosen for a particular elliptic curve to determine the curve's characteristics. The parameter p is usually a large prime number serving as the upper limit for the coordinates x and y. The G is the generator point which is the base point of the curve that is used to generate all other points. The n and h are the order of the curve (determining the number of points on the curve) and the cofactor of the curve ($\#E(\mathbb{F}_p)/n$) respectively. For security purpose, n is usually chosen to be a very large integer value. All parties in the same ECC application must use the same elliptic curve parameters [59].

An Elliptic curve having an order of n, has *n-1* discrete points starting from 1 and including a point at infinity i.e.

$$\langle G \rangle = \{\infty, 1G, 2G, 3G.....(n-1)G\} \tag{6}$$

3.3.3. The elliptic curve used in blockchain

NIST recommended 15 elliptic curves having varying levels of security [60]. Bitcoin and most other cryptocurrencies use the *secp256k1* elliptic curve defined over prime field with the following domain parameters given by Certicom [56]:

$$\begin{aligned}
&a = 0; \qquad b = 7; \qquad h = 01;\\
&p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1\\
&\quad = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF\\
&\qquad FFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFF\\
&\qquad FC2F\\
&G \ \ in \ \ compressed \ \ form:\\
&G = \qquad 0279BE667EF9DCBBAC55A06295CE870B\\
&\qquad 07029BFCDB2DCE28D959F2815B16F81798\\
&G \ \ in \ \ uncompressed \ \ form:\\
&G = \qquad 0479BE667EF9DCBBAC55A06295CE870B\\
&\qquad 07029BFCDB2DCE28D959F2815B16F81798483A\\
&\qquad DA7726A3C4655DA4FBFC0E1108A8FD17B448A\\
&\qquad 68554199C47D08FFB10D4B8\\
&n = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF\\
&\quad FFEBAAEDCE6AF48A03BBFD25E8CD0364141
\end{aligned} \tag{7}$$

Therefore, most blockchain applications including Bitcoin use the elliptic curve: $y^2 = x^3 + 7 \ \ mod\ p$.

3.3.4. Key pair creation with elliptic curve

Algorithm 1 is used to create a key pair in elliptic curve cryptography [61]. The key pair is used for purposes like encryption, decryption, digital signatures, and identities.

3.3.5. Elliptic curve digital signature algorithm (ECDSA) and transaction creation in blockchain

Blockchain transactions have to be signed and verified before added to a block. Signing transaction involves creating the transaction as a message. The message is then hashed and encrypted with the sender's

Algorithm 1 Key Pair Creation with Elliptic Curve

INPUT: Global domain parameters (n, G, p)
OUTPUT: private key d and public key Q

1: Select a unique random or pseudorandom large integer d : $d \in_R [1, n-1]$
2: Compute public key $Q = dG$
3: **return** (d, Q)

Algorithm 2 Generation of ECDSA Signature

INPUT: private key d, public domain parameters (G, n), hash function H, message m
OUTPUT: signature (r, s)

1: choose a unique random or pseudorandom large integer k : $k \in_R [1, n-1]$
2: compute the point $P(x, y) = kG$ mod n and convert x to integer
3: assign $r = x$ goto 1 if $x = 0$
4: compute message hash $e = H(m)$
5: compute $s = k^{-1}(e + dr)$ mod n. If $s = 0$ then goto 1
6: **return** signature as the pair (r, s)

Algorithm 3 Verification of ECDSA digital signature (r, s)

INPUT: public key Q, public domain parameters (G, n), hash function H, signature (r, s), message m
OUTPUT: verification result ($TRUE$ or $FALSE$)

1: **if** $(r, s) \in_R [1, n-1]$, **then**
2: valid signature, proceed to verify
3: **else**
4: invalid signature, terminate
5: **end if**
6: compute message hash $e = H(m)$
7: compute $u_1 = s^{-1}$ mod n
8: compute $u_2 = u_1 e$ mod n, and $v_1 = u_1 r$ mod n
9: compute $P(x, y) = u_2 G + v_1 Q$ mod n,
10: **if** $x = r$ **then**
11: **return true**
12: **else**
13: **return false**
14: **end if**

private key to create the digital signature (s). The sender then broadcasts both the digital signature together with the raw transaction. To verify a particular transaction, the signature is decrypted with the public key of the sender. The result is compared with the hash of the raw transaction. The transaction is valid if they are the same. Scripts are normally used to automate this transaction signing and verification.

Algorithm 2 and algorithm 3 describe the ECDSA which is used for signing and verification of blockchain transactions respectively [61]. ECDSA was proposed as a response to NIST's proposal by Scott Vanstone in 1992 through John Anderson [62]. ECDSA is accepted as an ISO standard (since 1998) as well as ANSI, IEEE, and NIST standard.

3.4. Blockchain address creation

Blockchain uses a scrambled hex string to represent user accounts (addresses) instead of physical identities. In Bitcoin, ECDSA key pair, SHA-256, and RIPEMD160 hash are used to create the Bitcoin addresses. Key pairs and the addresses can independently be created for every transaction and then stored by the wallet software. The address is a 160-bit message digest result of the SHA-256 and RIPEMD160 hashing converted to Base58Check string encoding. The process of Bitcoin address creation is given in algorithm 4.

Algorithm 4 Blockchain Address Creation

INPUT: ECDSA domain parameters (n, G), version number (network ID)
OUTPUT: private key d and Address

1: Create ECDSA key pair (private key d and public key Q)
2: Compute $A_1 = Ripemd160(SHA256(Q))$
3: Append version number(1 byte): $A_2 = version\_no||A_1$
4: Compute $Sum = SHA256(SHA256(A_2))$
5: Assign $Checksum$ =first 4 least significant bytes of Sum
6: Append checksum: $A_3 = version\_no||A_1||checksum$
7: Convert to Base58: Address=Base58Encoding(A_3)
8: **return** (private key, Address)

After the key pair (private and public keys) is created, the public key is hashed using SHA-256 hash function. The 256-bit output is then hashed again using RIPEMD160 hash function (double hashing) which gives a 160-bit output. A 1-byte network ID (0x00 for the main network) version number is appended to this output. To get a checksum, the output is hashed twice again with SHA-256. The checksum is the first 4 least significant bytes of the hashing result. Now with the checksum appended to the right and the version number appended to the left, the result is converted to Base58 using Base58Check encoding to string to get the final Bitcoin address. Scripts are also normally used for this purpose and the addresses are checked for validity before making transactions by the wallet software [63].

4. Applications of blockchain

Blockchain was first used in cryptocurrencies where its success was first seen from Bitcoin. Nowadays, there are many applications of blockchain as summarized in Fig. 4.

1. **Cryptocurrencies:**
Blockchain underpins Bitcoin and many other cryptocurrencies such as Ether. As of September 2020, the market capitals of Bitcoin and Ethereum are $191 billion and $41 billion, while their prices are $10345 and $364, respectively. There are currently around 1200 cryptocurrencies including Bitcoin-cash, Litecoin, Dash, Ripple, Monero, Zcash, and several others [32].
Many companies and vendors accept payments in cryptocurrencies. Bitcoin is accepted by Microsoft, Expedia, Wikipedia, Burger King, KFC, Subway, Norwegian Air, and more. According to HSB's 2020 survey, Bitcoin is accepted by 36% of the small to medium businesses in the US and 56% of the businesses in the US purchase the currency for their own use. Cryptocurrency ATMs and exchanges such as Coinbase and Cex.io are used to change cryptocurrencies into cash and vice-versa. General Bytes sold over 3322 cryptocurrency ATMs across over 63 countries globally [64].
Many countries have been putting effort to create their own central bank digital currencies (CBDCs) to be used mostly for inter-bank and government transactions. China and Facebook have been anticipated to soon release their digital currencies.
There are many papers on cryptocurrencies especially Bitcoin. Bitcoin-NG presented a protocol to scale Bitcoin for high transactions per second. Ciaian [65] studied Bitcoin pricing. Lightning network, Sidechain, sharding approaches were all proposed to speed up cryptocurrency transactions [66].
2. **Smart contract:**
Smart contract originally introduced in 1994 by Szabo [67] is a contract governed and enforced by a computer program without the need of

a third-party such as a lawyer. The program automatically executes the contract agreements fairly when its conditions are satisfied. With the support of blockchain, smart contract is currently secure and convenient. Smart contracts are used on blockchain to provide several services including financial, notary, game, wallet, voting, library, and other services for businesses, governments, organizations, and the general public [68]. Decentralized applications (Dapps) are typically run on blockchains using smart contracts. For example, the decentralized autonomous organization (DAO) in Ethereum, chaincodes in Hyperledger, and the domain name service (DNS) in Namecoin all use smart contracts.

Smart contracts are deployed on blockchain networks in form of new transactions. There are currently over 14 million smart contracts on Ethereum [69]. A transaction can transfer money to smart contract or call its methods. A Smart contract may also transact with other smart contracts. Solidity is a programming language specifically designed for creating smart contracts and is used in Ethereum. However, languages such as Go are also used for smart contracts (chaincode) as in Hyperledger.

Pinna [69] and Bartoletti [68] studied and analyzed smart contracts. Hawk is a framework proposed by Kosba et al. [70] for smart contracts to ensure privacy. Mense and Flatscher [71] studied security vulnerabilities in smart contracts on Ethereum blockchain. In addition, several surveys such as [72] and [73] have been conducted on smart contracts and their applications.

3. **Stock exchange:**

Traditional ways of buying and selling assets and stocks require a lot of undesired costs, trusts, and intermediary involvements. With blockchain technology, these overheads could be overcome. The eminent transformation of stock exchange marketing by blockchain technology was envisaged by Microsoft [74].

Although shares are not directly sold by banks, secondary markets buy and sell shares using blockchain. Bitshares, Augur, NASDAQ, and Coinsetters have been using blockchain for stock marketing and exchanges [75]. The Australian Security Exchange (ASX Ltd) and the London Stock Exchange have all been working on integrating blockchain in their systems [76]. V-Chain [77] is a blockchain based platform proposed to efficiently provide car leasing services.

4. **Healthcare management:**

The current healthcare management system has several issues such as data inconsistency, duplicate records, and the inability of patients to know and manage their own records. Blockchain, when properly used could solve these healthcare challenges. Blockchain is currently used to share and secure data for healthcare management. The records are uploaded on the blockchain to provide sharing, accessibility, security, reduction in cost, and traceability. Different health institutions could interoperate without issues of different databases and individual central authorities. Estonia is the first government to put its healthcare records on blockchain. There are several companies such as Gem, HealthBank that use blockchain for healthcare services including record sharing and fake drug prevention.

Blockchain applications in healthcare were classified into four categories, namely, medical record management, medical insurance, clinical and biomedical research, and applications connecting healthcare providers [78]. Wang et al. [79] proposed a parallel healthcare system based on ACP approach and powered by blockchain. Griggs [80] proposed a blockchain based healthcare system to securely and autonomously monitor patients remotely. Zhang et al. [81] proposed FHIRChain, a blockchain architecture for scalable and secure sharing of clinical data. Healthchain [82] and OmniPHR [83] were proposed for protected healthcare information (PHI) and healthcare data integration respectively. McGhin [84] and Abujamra [85] are surveys of blockchain applications in healthcare.

5. **Insurance:**

There is increasing use of blockchain by insurance companies. Putting the insurance data on blockchain prevents fraud and allows data sharing and interoperability among the insurance companies. This prevents people from claiming the same insurance from more than one companies. Everledger is a company that uses blockchain for diamond certification history. Etherisc, Insurwave, and MedRec are other example use cases of blockchain in insurance [75]. Raikwar et al. [86] designed a secured blockchain framework for insurance services.

6. **Banking and finance:**

Blockchain is capable of disrupting the banking and finance industry. Many banks have been trying blockchain to improve their systems. The first banking transaction with blockchain was carried out in 2016 between Commonwealth Bank of Australia and Wells Fargo [87]. Nofer [15] studied defects in banking system and highlighted solutions using blockchain. Several other financial services like online payments and digital assets are carried out with blockchain [16]. Garrick and Michel discovered that about 63% of central banks experiment with blockchain hoping to integrate it with their system after successful trial [88].

7. **IoT industry:**

Blockchain has got attentions for use in IoT because of the need for the IoT devices to be autonomous, communicate, and share data without human intervention. Example blockchain applications in IoT include the IBM's ADEPT, Filaments, GSF, and Share&Charge. With ADEPT, IoT devices like home appliances can troubleshoot, upgrade, and update themselves [16]. Golden state food (GSF) partnered with IBM for the use of blockchain with IoT sensors to monitor beef conditions across its supply chain. There are several proposals and surveys such as [3,89] for the use of blockchain in the IoT industry.

8. **Blockchain based DNS services:**

Blockchain is also used for domain name service (DNS) to avoid security attacks, censorship, and misuse by the central organizations or governments governing the DNS service for the internet. The DoS attack on *Dyn* DNS provider in October 2016 was a wakeup call for tighter security provisions in DNS service. Blockstack [90] and Namecoin [91] provide DNS services using blockchain while EmerDNS is a blockchain alternative for DNSSec [92]. Karaarslan [93] studied the blockchain based DNS and PKI solutions.

9. **Decentralized data storage:**

One threat of the existing cloud storages provided by companies like Google and dropbox is the security of the data and centralization. Such traditional centralized systems serve as a single source of failure for data security and privacy breach. Hence blockchain is employed to store personal data in a decentralized manner with full control and management by the data owners. Blockchain storage has advantages of speed, security, flexibility, and low cost. Storj is a decentralized cloud storage network using blockchain that is secure, private, and easy to use [94]. Gaia is another blockchain storage of blockstack [93]. Other blockchain based storage networks include Swarm, Sia, IPFS, and SAFA networks [95]. Li et al. [96] proposed a blockchain based data storage for IoT without the use of certificates.

10. **Intellectual properties and document stamping:**

Blockchain is also used to support intellectual properties and document stamping for preventing documents forging. Documents are stored on blockchain after being stamped and digitally signed. Since everyone can access the certified document on the blockchain for verification, forging such documents is more difficult and harder to achieve. Blockchain is used by companies such as Stampery, Ascribe, Block notary, and Microsoft to certify emails, certificates, and documents. Vaultitude, Vechain, and KODAKone are blockchain platforms that provide intellectual properties management and protection. Muzika, Mycelia, and BigchainDB provide blockchain IP for music and entertainment industry.

11. **Voting:**

Many countries especially developing ones are incapable of carrying out free and fair elections. Blockchain could be used to make transparent voting in organizations, meetings, and countries. BitCongress, Remotengrity, and AgoraVoting are projects that provide good architectures for voting with blockchain [97]. Blockchain based e-voting was

tested in sixteen (16) countries to promote free and fair election with a tamper-proof record [98]. Slock.it implemented a blockchain based decentralized digital organization (DDO), Hutten for Siemens to allow voting by their partnering companies [99].

12. **Digital identity management:**

Identity management is one of the recent and effective applications of blockchain considered by some governments and organizations. Traditionally, government bodies and organizations provide identifications for individuals in form of passports, ID cards, certificates, and so on. The traditional identity management is much vulnerable to losses, theft, and fraud. Now with the advent of blockchain, identities could be securely managed autonomously without central authorities. Blockchain in conjunction with zero-knowledge proof supports claiming and verification of identities stored on the blockchain in a secure and private way. A typical use case of blockchain based identity is the e-Identity of Estonia. Many other countries like the USA, Japan, Switzerland, India, and Finland are currently doing blockchain trials for identity [98]. Tykn is a blockchain platform that provides digital identity management and services. United Nation in collaboration with Microsoft and Accenture showcased a prototype of its global refugee identity system based on blockchain during the United Nation ID2020 summit in New York [100].

13. **Cybersecurity:**

Blockchain is used to enhance cybersecurity. Network history, configuration, log files, and other network files are stored on blockchain to provide secure and immutable records against attackers. This concept is used by companies like Guardtime to provide network security services against several network attacks [101,102]. Blockchain based DNS, PKI, and storage secure web services against DDoS and other attacks. CertCoin uses blockchain for public key infrastructure (PKI). REMME is a startup that stores SSL certificates on blockchain to dispense with certificate authorities (CA). CryptoMove protects APIs and apps with blockchain, Hacken provides security tools based on blockchain for professionals in cybersecurity while Gladius protects DDoS using the blockchain. Other companies and startups using blockchain for cybersecurity include openAVN, block armor, Cryptyk, Sentinel Protocol, Megahoot, and AnChain.ai [103].

14. **Asset registry and tokenization:**

Assets are also represented as tokens and then trade or stored on blockchain. Registry of assets can easily be kept on blockchain in a secure way to avoid fraud and asset theft. Blockchain provides secure asset tokenization, land registry, asset marketplaces, and property data standardization. Georgia had its land registry records on blockchain. There are many trials of using blockchain for asset registries in the UK, Sweden, India, and Russia [98]. Codefi Assets platform of Consensys company provides blockchain based asset management services and platform. Securitize, Harbor, AlphaPoint, trustToken, and Polymath provide blockchain based asset tokenization platforms. In addition, Meridio, Blockimmo, Propy, and Imbrex provide real estate investment, marketplace, and registry services on blockchain [104].

15. **Supply chain and trade management:**

Blockchain provides security, transparency, speed, and reduced cost to supply chain and trade. Records of supply of goods and trades could be stored on blockchain for better tracking and verification. At any instant of time, all parties involved in the supply chain will be aware that certain goods are at a particular location or a certain trade occurred. The information is received much faster without relying on central authorities which may act maliciously. Using blockchain may also prevent loss of items and records. TradeLens is a blockchain based supply chain network founded by Maersk and is currently partnered by about half of the global shipping companies [105]. Grainchain uses blockchain for selling, buying, and tracking grains and other agricultural commodities [106]. Mediledger provides blockchain solution such as medicine tracking and payments for pharmaceutical supply chains.

Table 3
Blockchain Applications and use cases.

Application	Example Use cases
Cryptocurrencies	Bitcoin, Ethereum, Libra
Smart contract	DAO, Clause, Namecoin, Agrello
Stock Exchange	Nasdaq, Coinsetters, Augur, Bitshares, V-chain
Healthcare	HealthBank, Gem, Healthchain, MeDShare, FHIRChain, OmniPHR, CoverUS
Insurance	Etherisc, Insurwave, MedRec
Banking and Finance	JPM coin, Wells Fargo coin, MonetaGo, Komgo, Studium, Khokha, Ubin
IoT	ADEPT, Filament, Dorri, GSF, netObjex, Share&Charge
DNS service	Blockstack, Namecoin, EmerDNS, DNSChain, Blockchain-DNS
Decentralize storage	Storj, Gaia, Swarm, Sia, IPFS, SAFA networks
Intellectual Property	Stampery, Ascribe, block notary, Vaultitude, Vechain, KODAKOne
Voting	Bitcongress, AgoraVoting, Siemens Hutten DDO, Kaspersky voting machine
Identity management	Evernym, Verified.me, ID2020, Tykn, Shocard
Cybersecurity	Guardtime KSI,CertCoin, REMME, Gladius, CryptoMove, Hacken,block armor
Asset Registry	Georgia land registry, Codefi Asset, Blockimmo, Meridio, Propy, Imbrex
Supply chain	TradeLens, Grainchain, Waltonchain, Mediledger, Walmart, Circulor
Energy	PowerLedger, Verv, Electron, EWF, Grid+, Ondiflo, Enerchain,

16. **Energy trading and management:**

Energy is another sector that has been disrupted by blockchain technology. Blockchain is currently used to coordinate energy trade on smart microgrid without the central authority [17]. Blockchain could be used for electricity distribution and data management as well as oil and gas exploration, trading, and resource management. PowerLedger is a company based in Australia that provides a blockchain platform for people to sell and buy energy. Electron, Verv, EWF, Grid+, Wepower, Settlemint, Enerchain, and Ondiflo are examples of companies that provide blockchain services in energy sector.

17. **Project management:**

Traditional contract management is inefficient and involves a lot of risks and increased operational costs. There are many companies that now provide blockchain solutions and platforms for contract management. Contractors and their clients use the platforms for tracking and managing their contracts efficiently. The solutions are used in construction and other projects. Currently, Monax, Corda, Oracle, Konfidio, and Icertis all provide efficient blockchain based contract management platforms and solutions.

Other blockchain applications are found in areas including public services, building services, trust management, music industry, and more [107–109]. Table 3 summarizes blockchain applications citing their example use cases.

5. Breakthrough and state of the art of blockchain

This section discusses the journey of blockchain technology from its inception. The breakthrough and the progress of the technology in various industries and countries were also discussed. The emergence of various applications using blockchain and the wider adoption of the blockchain in several countries and companies bring the major breakthrough of the blockchain technology.

5.1. Blockchain journey brief

In 2008, Satoshi Nakamoto brought the idea of blockchain in Bitcoin as a peer to peer electronic cash system that works without central bank and solves double-spending problem. Bitcoin was launched in 2009 supported by the blockchain and started getting more attention

Table 4
Comparison of blockchain platforms.

Platform	Blockchain type	Consensus supported	Currency used	Language	Throughput (T/S)	Usage
Bitcoin	Permissionless	PoW	Bitcoin (BTC)	C++	3–4	Cryptocurrencies
Ethereum	Permissionless	PoW-PoS	Ether (ETC)	Solidity	15–20	Dapps, DAO
Hyperledger Fabric	Permissioned	PBFT,Kafka,Raft	No currency	Go,js,Java	up to 20,000	Business networks
Corda	Permissioned	Raft,BFT-SMaRt	No currency	Kotlin,Java	up to 6300	Business networks
Ripple	Permissioned	Ripple	XRP	C++	1500	Currency exchange
Quorum	Permissioned	Raft,QuorumChain	JPM coin	Solidity	752	Business networks
Multichain	Permissioned	Multichain consensus	No currency	JavaScript	2000–2500	Business networks

around 2012 [31]. Currently, there are around 1200 cryptocurrencies using blockchain technology [32].

In the beginning of Bitcoin, CPU was used for mining and succeeded by GPUs. FPGA was later used to provide higher hash rates than GPU. Currently, ASIC mining hardware dominates the CPU, GPU, and the FPGA for their much higher throughput [19]. The current hash rate of Bitcoin is about 128 million TH/sec [110]. Taylor [111] examined the trend of hardware used for Bitcoin mining from CPU to GPU to FPGA and finally to the ASICs. Some blockchain systems using non-PoW consensus only use CPU or rarely GPUs. To avoid centralization in ASIC and FPGA mining, some PoW cryptocurrencies such as Ethereum, Litecoin, and Zcash developed memory-hard algorithms that are unsuitable for mining with ASICs in order to allow users to use their normal computers or GPUs.

Blockchain transforms from Bitcoin blockchain known as blockchain 1.0 to blockchain 2.0 which consists of smart contracts and Dapps. The next generation blockchain is predicted to be a blockchain of things [29]. More enterprise blockchain networks and platforms have been created to allow enterprises to use blockchain that is more suitable for their requirements.

In 2014, Ethereum platform was invented and formally announced by Vitalik Buterin [112]. Unlike Bitcoin, Ethereum runs distributed applications (Dapps) known as smart contracts using Ether as its currency. Ethereum is used in many public and now enterprise blockchain applications ranging from DAO to IoT using smart contracts. Ethereum is the second largest public blockchain platform after Bitcoin. As of July 2020, Ethereum has over 114 million users (unique addresses) [113].

Hyperledger project hosted by Linux Foundation provides several open source platforms for building enterprise blockchain applications and networks. Hyperledger was officially launched in 2016 with 30 founding corporate members [114]. The most popular Hyperledger platform is Hyperledger Fabric [115] which was contributed by IBM in 2015 and can support over 3500 transactions per second. About 40% of enterprise blockchain networks now use Hyperledger Fabric [10]. Other Hyperledger platforms include the Hyperledger Sawtooth, Iroha, Indy, Burrow, and Besu. Hyperledger Sawtooth allows for both permissioned and permissionless networks while Hyperledger Iroha focuses on mobile applications. Hyperledger Indy provides a platform for distributed identity, Hyperledger Burrow is a permissioned smart contract virtual machine. Finally, the Hyperledger Besu is a Java based Ethereum client [116].

Corda [5] is another consortium blockchain platform provided by R3 [4] in 2016 for financial enterprises. Other blockchain platforms which are mostly consortium include the J.P. Morgan's quorum [117], Enterprise Ethereum Alliance [118], Multichain [119], Kadena [120], Axoni [121], SETL.io [122], Digital Asset Holdings [123], and Clearmatics [124]. Table 4 compares some of the existing popular blockchain platforms.

5.2. Breakthrough in industries and companies

Blockchain has achieved major breakthrough and adoptions in industries especially in 2018 and 2019. The year 2019 was termed as the year of enterprise blockchain adoption. Fig. 5 depicts the forecasted timeline of blockchain adoption in industries from 2014. The ideation stage is the beginning where ideas of using the blockchain in industries started to be generated. Proof of concepts (POC) were created to preliminarily test the generated ideas. Many companies started prototypes and trials in 2016/2017. Many projects entered the pilot stage in 2017/2018 while a large number of them are currently moving to production phase. It was predicted that most blockchain projects will be in production stage around 2022. In the year 2025, blockchain will attain mainstream adoption and be matured [125].

In this section, we discuss some major breakthroughs and adoptions of blockchain classified into five periods of time starting from 2012 since only Bitcoin existed prior to this time.

1. **2012–2014:**
In this period, there were few blockchain activities and use cases in companies. Companies using blockchain at this time mainly used it for cryptocurrencies and their exchanges. Examples of such companies are Coinbase, Coinsetters, and Peercoin which opened in 2012 and 2013 respectively.
2. **2014–2016:**
Some companies started realizing the benefits of blockchain mostly after the launch of Ethereum in 2014. NASDAQ started using blockchain since 2014 for stock exchange. In 2015, NASDAQ unveiled the Nasdaq Linq blockchain for keeping security records. They also collaborated with Citi to develop a blockchain payment solution [126].
In 2015, IBM and Samsung unveiled the Autonomous Decentralized Peer to Peer Telemetry (ADEPT) platform using blockchain as a proof of concept. ADEPT connects IoT devices and allows them to communicate for autonomous maintenance, self-services, upgrades, and updates. Samsung washing machine (W9000) connected to ADEPT ordered for detergent from a retailer when the detergent went low. The washing machine checked its warranty information and even paid bills using smart contract [127].
Gem, Storj, and Augur were founded in this period also. Gem uses blockchain for healthcare, Storj is a decentralized cloud storage, and Augur uses blockchain for market predictions. Bitshares is a Cryptocurrency exchange company that was also founded in 2014.
3. **2016–2018:**
In October 2016, the first blockchain international transaction between banks was made by Wells Fargo and the Commonwealth Bank of Australia through the use of many blockchain applications different from Bitcoin. The transaction was for the shipment of 88 bales of cotton totaling $35,000 from USA to China. It marked a great milestone for blockchain technology adoption in banks [87].
Microsoft in 2017 created an add-in for Microsoft office outlook which uses the so called Stampery API created to stamp and verify documents using the Bitcoin and Ethereum blockchain. The add-in helps customers to certify documents and emails from within the Outlook app without going to the third-party page for certification and authentication. The Stampery API embeds the hash of a document in the blockchain which could later be used for the document certification [128].
IBM and Microsoft in 2017 unveiled their cloud blockchain platforms, that is, the IBM blockchain and Microsoft Coco respectively. IBM blockchain is the first fully managed blockchain cloud service based on Hyperledger technology. It eases application developments, governance, and operation of business networks. The Microsoft Coco framework was revealed later in August 2017. It integrates with several blockchains and distributed ledgers like the R3's Corda, Ethereum,

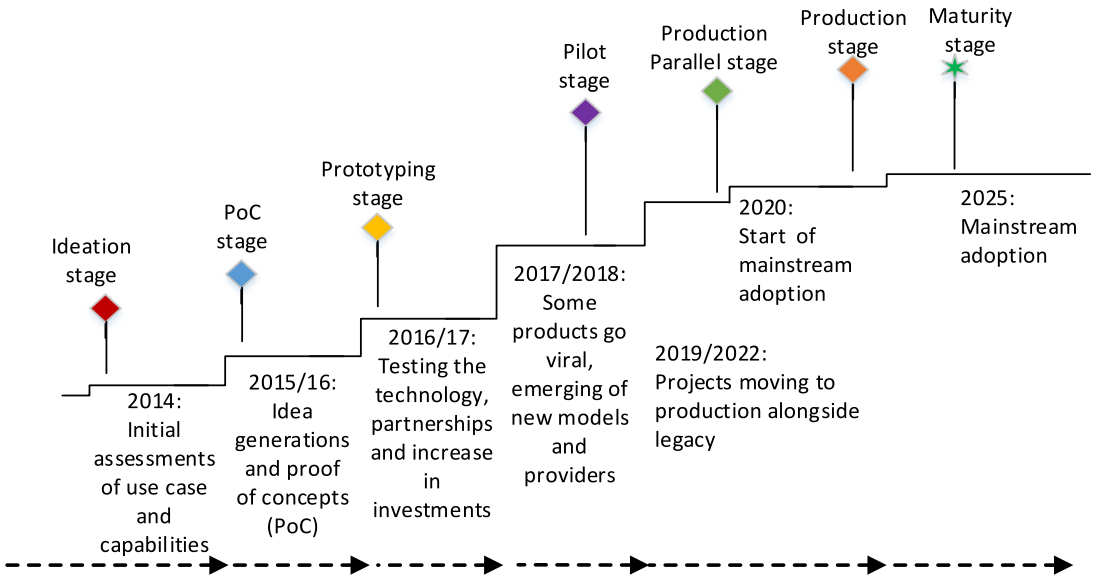

Fig. 5. Timeline for blockchain adoption in industries.

JPMorgan's quorum, and Intel's Sawtooth Lake. Microsoft decided to build this blockchain framework to enable business enterprise networks to realize requirements lacking in the other existing blockchain protocols in terms of performance, governance, desired processing power, and confidentiality [129].

R3 as a consortium consisting of over 200 financial institutions has been using blockchain since 2016 for trading, redeeming, and issuance of fixed income products for adoption. R3 secured the ever highest distributed ledger technology (blockchain) investment of $107m in 2016 from its over 40 member institutions across 15 countries. Corda partners with other companies to provide blockchain solutions. They also provide contract management blockchain solutions for contractors [18].

There was a wider acceptance of cryptocurrencies by companies like World Press, Microsoft, and Dell. More than 100,000 merchants accept Bitcoin worldwide since 2015 [18,130]. Wepower, Settlemint, Enerchain, PowerLedger, and Electrify. Asia are energy trading platforms using blockchain since 2016 and 2017. A Survey made by Cambridge university in 2017 revealed that 67% of central banks were experimenting with blockchain and many of them now reported successful trials [88].

4. **2018–2020:**

In May 2018, the giant automobile companies and largest automakers in the world (BMW, Ford, Renault, and GM) formed a consortium with blockchain developers (Hyperledger and Consensys), IBM, Accenture, and some manufacturers of car parts (ZF and Bosch) for using blockchain in automobile industry. The consortium called the Mobility Open Blockchain Initiative (MOBI) was aimed at using blockchain for payments and data sharing [131].

Oracle unveiled its giant autonomous cloud blockchain platform (OABCS). The company intended to attract small and big firms to use blockchain for business networks. Oracle also provide several blockchain solutions on their cloud platform. They provide contract management solutions for construction companies and other companies [132].

FedEx has been exploring and using blockchain for tracking high-value cargoes. They are currently working to extend the use of blockchain and IoT for their other logistics. In 2018, FedEx institute of technology partnered with Good Shepherd Pharmacy in a project called REMEDI which used blockchain to trace and collect unused cancer medicines to be distributed to poor cancer patients across the world. FedEx joined the Blockchain in Transport Alliance (BiTa) in 2018. BiTa coordinates and promotes the use of blockchain among the transport and freight industries [133].

In October 2018, Healthbank revealed their healthcare blockchain project. Icertis, Monax, and Konfidio currently use blockchain for efficient contract management on the cloud. Securitize, Harbor, Polymath, AlphaPoint, and TrustToken are blockchain based solutions for asset tokenization. Blockpass, Civic, Selfkey, Shocard, and Zamna are blockchain based solutions for validation and digital identities.

The Australian Security Exchange (ASX Ltd) released its new implementation plan for the replacement of its Clearing House Electronic Subregister System (CHESS) with blockchain. However, the commencement date was postponed to March 2021. This will make ASX the first exchange in the world to use blockchain. The decision was made after two years of successful testing with the blockchain in order to reduce costs for their customers in addition to simplicity, increased speed, and efficiency [76].

The shipping giant Maersk and IBM in August 2018 launched a blockchain based supply chain shipping tracking platform *TradeLens*. The platform was aimed at reducing costs, information sharing, and increased efficiency for the global ocean shipment supply chain [134]. TradeLens now supports almost half of the global ocean shipping industry. Over 100 shipping operators including the top global shipping companies (Hapag-Lloyd, MSC, CMA-CGM, and Ocean Network Express) partner and use TradeLens [105].

Towards the middle and the end of 2019, stablecoins took a lot of media attention. Facebook's stablecoin Libra [9] planned to be launched in 2020, took the highest media news coverage. JPMorgan (JPM) proposed its stablecoin JPM coin while Walmart secured a digital currency patent. Walmart together with other nine food industries partnered with IBM for using blockchain in food logistics and supply chain.

Barclays Bank and Swiss bank have been experimenting with blockchain to improve settlement time which could save them 20 billion USD middlemen costs. Barclays in May 2019, invested in a blockchain based peer to peer payment startup, Crowdz. Crowdz works with companies for digital invoice automation and payment collection [135].

The giant bank, Wells Fargo and the communication tech leader, Verizon have all revealed their plans for using blockchain. Wells Fargo has planned to have its own cryptocurrency for use in its internal banking. On the other hand, the Verizon has applied for a patent that will allow it to issue virtual sim card vSIM on blockchain [136].

Recently on 27th February 2020, the cybersecurity company Kaspersky unveiled its blockchain based voting machine prototype built on top

Table 5
Adoption of blockchain in various industries.

Company	Blockchain usage
R3	Corda-blockchain platform for finance
IBM	IBM cloud blockchain platform, ADEPT
Microsoft	COCO — cloud blockchain platform
Oracle	OABCS — cloud blockchain platform
Facebook	Libra coin — Stable coin
Maersk	TradeLens — Shipping network
Walmart	Digital currency patent, food supply chain
Wells Fargo	Internal stablecoin
Verizon	Blockchain virtual SIM patent
LG Uplus	Payment service
J.P Morgan	JPM coin — stable coin
BMW, Ford, Renault	MOBI — blockchain consortium
Healthbank, Gem	Healthcare management
Hyperledger	Enterprise blockchain platforms
Storj	Decentralized cloud storage solution
Grainchain	Blockchain trading solution for farmers
Verv, Grid+, Wepower, EWF, PowerLedger	Peer to peer energy trading and management
Blockstack, Namecoin	Decentralized DNS
BanQu	Cassava farming supply chain and trading
Spring Labs	Global B2B information sharing platform
Vechain, Kodakone	Intellectual property
CoverUS	Blockchain healthcare marketplace
Australian Security Exchange (ASX)	blockchain based clearing and settlement system
Monax, Konfidio, Icertis	Contract management
Kaspersky	blockchain voting platform/machine
Civic, Selfkey, Zamna	Identity management and validation
Digital transaction	ParallelChain solutions for businesses

of its online election system (Polys). Governments, universities, businesses, and political parties can use the voting platform for free and fair elections [137].

5. **ParallelChain and future adoptions:**

In the future, we envisage more adoptions of blockchain. In the Deloitte's 2019 survey, 86% of the respondents believed that blockchain will finally get mainstream adoption. Many trials and projects are expected to get completed in 2020 [11].

ParallelChain is a next generation hybrid private blockchain with very high-performance and scalability. The blockchain can achieve 100,000 transactions per second (tps) which is much higher than the tps of its counterparts like Hyperledger and Corda. ParallelChain is interoperable and possesses both permissioned and permissionless features in a private blockchain in order to improve the shortcomings of the counterpart blockchains such as Bitcoin and Hyperledger. ParallelChain is the only blockchain platform/fabric that offers the feature of "right to be forgotten". In addition, the platform can emulate the smart contracts in Hyperledger and Ethereum and operate them faster. Behind the ParallelChain, is a high-performance parallel computing architecture that runs multiple parallel chains used by multiple applications concurrently.

Digital Transaction Limited (DTL) is a Hong Kong based company and the owner of the ParallelChain. They provide high-performance industry specific blockchain solutions on ParallelChain. Such solutions are typical parallel chain use cases for business applications. DTL provides killer applications namely; ChattleChain, ConstructionChain, and PreventiveChain, partner applications (loyalty program and QR code verification), and custom decentralized applications on their high-performance ParallelChain. ChattleChain is used for fast tokenization and fraud protection while ConstructionChain provides digital records for work inspection and workflow tracking [138].

Table 5 summarizes the major blockchain adoptions by various industries.

5.3. Breakthrough in various countries

Many countries have been experimenting and using blockchain for public services. Singapore's government has been using blockchain to secure banks against invoice fraud. This prevents customers to duplicate invoices as it happened when almost $200 million were lost by the Standard Chartered due to the same act [139].

Georgia is the first government to keep land titles on Bitcoin blockchain. Bitfurry had been working with the government of Georgia since 2016 for building the public land registry using blockchain technology. The project after successful tests was expanded in 2017 to enable other land services like sales, mortgage, new land title, and notary [140]. Another company (Factom) has been aiming to build a blockchain based secure land registry for the Honduras government. The company has been in talks with the government since 2015 [141].

UK Government in September 2017, awarded a contract to a startup company *Electron* for trying blockchain solution in power grid balancing. In January 2018, Japanese giant power company (TEPCO) invested in the Electron for using blockchain in the energy industry [142,143]. Besides Electron, there are many companies and startups currently using blockchain for energy services [144]. UK earlier disclosed that it was testing blockchain for its land registry as Sweden went far on its second phase trial of using blockchain for land registry [98]. The Swedish land registry has started blockchain transactions for land trades after successful testing for two years [145].

In the mid-2018, United Arab Emirate (UAE) launched its 2021 blockchain strategy. It was hoping that by 2021, 50% of the UAE government transactions will be based on blockchain. Therefore, regulations were made for using crypto assets such as cryptocurrencies [146]. Earlier in December 2017, the central bank governor of the UAE disclosed that the UAE was collaborating with the Saudi Arabia government with a view of creating a cryptocurrency for their central banks. The digital currency will be used for efficient cross-border transactions between the banks in the two countries [147].

The Moscow government in August 2018, disclosed its plan to use Ethereum blockchain to upload applications for trading plots allocations by over 20,000 farmers for the farmer's market in Moscow. This is to allow transparency and credibility in the competitive application. Earlier in December 2017, the Russian government integrated blockchain in its Active Citizen e-voting platform to allow citizens to take part in taking decisions on the city management and urban transformation. Russia also planned to extend the use of blockchain for healthcare [148].

Malta is the first country in the world to pass regulatory law supporting cryptocurrencies and other blockchain applications. For this regulation, Malta was referred to as the "first blockchain island". Currently, more blockchain investments are rushing into Malta due to the enacted blockchain regulations.

The governor of Colorado inaugurated the Colorado council for the advancement of blockchain technology in 2018. In July 2019, the council reported the issues they identified on the adoption and regulation of the blockchain technology. They also proposed possible solutions to the identified issues [149].

ID2020 Alliance unveiled its two pilot projects based on blockchain at the September 2018 ID2020 Summit in New York. The first project was a digital identification aimed at recording and verifying the identities of refugees in Thailand using iris recognition. The refugee's digital identities will be used for healthcare services and later be extended to education. The second project was to facilitate the disbursement of subsidy from liquid propane gas (LPG) for Indonesian government using biometric digital wallet and blockchain technology [150].

China's central bank announced in August 2019 that, its cryptocurrency whose development started 5 years ago, was almost ready. It is evident that the digital currency will be released soon possibly in 2020 or 2021. In April 2020, China also launched a national blockchain service network (BSN) in 100 cities. The network was hoped to reduce the costs of businesses using blockchain in China by 80% and become a global standard [151,152].

There are several other developments on the blockchain. Table 6 summarizes some of the blockchain adoptions in various countries across the world.

Table 6
Adoption of blockchain in various countries.

Country	Blockchain usage
Georgia	Land registry
UAE	Bank payments, shareholder proxies, identity
Estonia	Healthcare management, e-identity
Saudi Arabia	Internal bank payments
USA	State archive, stock trade, birth, and land registry, voting, healthcare
UK	Grants distribution, land registry, and energy
Sweden	Estate transactions, land registry
Chile	Energy data tracking
Indonesia, Japan, Switzerland	Identity management
India	Land registry, education certification
South Korea	Banking ecosystem
Russia	Trading plots allocation, e-voting, secure trading, healthcare
Kenya	Education certification
Australia	Stock exchange, voting
Singapore	Trade invoice fraud protection
Mexico	Public contract and bidding
Ghana	Property ownership
Canada	Government funding
Malta	Cryptocurrency, DLT regulatory framework
Japan, South Korea	Voting
China	Digital currency, blockchain service network

Table 7
Quantitative analysis of blockchain adoption (N = 1386).

Survey statement	Response percentage
Blockchain will get mainstream adoption	86%
Blockchain becomes our critical priority (in top 5)	53%
We are planning to replace our record systems	81%
We will lose competitive advantages without blockchain	77%
Our industry will be disrupted by blockchain	56%
Blockchain is overhyped	43%

Table 8
Blockchain use cases survey (N = 1386).

Use case	Response percentage	Use case	Response percentage
Data validation	43%	Asset transfer	24%
Data sharing	40%	Revenue sharing	23%
Identity	39%	Asset backed tokens	22%
Payments	37%	Tokenized equity	21%
Digital currency	36%	Tokenized assets	20%
Trade and trace	32%	Time stamping	19%
Certification	30%	Custody	16%
Access to IP	30%	Not sure/other	2%
Records reconciliation	25%	None	1%

6. Blockchain quantitative surveys and analysis

There are various quantitative surveys and analysis on blockchain conducted by several organizations and departments. The quantitative surveys provide statistical and quantitative data on various aspects of blockchain such as state of adoption of the technology. The data is got from hundreds of participants through questionnaires, interviews, or via emails. This section reviews the quantitative surveys and analysis of blockchain technology.

6.1. The quantitative analysis and surveys sources

The Cambridge Center for Alternative Finance conducted and released in September 2019, its second global benchmarking study on enterprise blockchains. The study contacted and analyzed 67 live and deployed enterprise blockchain networks that were already in production from 25 countries across the world. They also analyzed data collected from over 160 enterprises across 49 countries worldwide. The enterprises include 60 blockchain vendors, 56 blockchain network operators, and 45 public sectors. The survey respondents include start-ups, medium and large enterprises, other public sector institutions (OPSIS), government agencies, and central banks. The data collection method used is a direct survey through invitation by email, social networks, and contact via R3 and Hyperledger companies [10].

In their investigation of finding out the ways (use cases) blockchain is used, the Stanford university center for social innovation surveyed 110 organizations through phone interviews and digital surveys. They reported findings based on six (6) sectors where blockchain is used. The sectors are agriculture, finance, environment, governance, digital identity, and finally the health sectors [153].

The giant fintech company, Deloitte interviewed 1386 top executives of high revenue companies in 12 countries for their 2019 global blockchain survey. They also surveyed a group of 31 firms that had an interest in investment in blockchain technology [11].

PWC in its 2018 global blockchain, surveyed 600 respondents who were executives in big business companies across 15 regions globally. Most of the respondents were carrying out blockchain projects with 32% of the projects were under development and 15% already in production [154].

Ipsos is a leading market research company. In 2018 and 2019, Ipsos conducted a global research on internet security and trust including blockchain technology for the Center for International Governance Innovation (CIGI). Over 10,000 people from 25 countries were surveyed through an online interview and face to face interview for approximately 10 and 20 min respectively [155].

The other blockchain statistical analysis studied include [6,7,156–161].

6.2. The quantitative surveys findings

The findings of the survey sources are discussed here. We use the term N to refer to the total number of respondents (sample size) of a survey. Likewise, the percentage (%) in this analysis refers to the percentage of the total number of the respondents (N). For some of the surveys presented, the sum of the percentages is more than 100% because some of the respondents had more than one valid responses (answers). For example, in the survey of blockchain use cases (Table 8), some respondents used the blockchain for more than one use cases such as data sharing and payments. Likewise, in the survey of blockchain consensus protocols (Fig. 10), some of the blockchain platforms (respondents) supported more than one consensus. For example, PBFT and Raft consensus supported by Hyperledger Fabric platform.

6.2.1. Analysis of the current state of blockchain adoption

According to the survey findings, blockchain gets more adoptions with increasing use cases in 2019. At the end of 2019, many enterprise blockchain projects were completed and are already in production. Table 7 shows the result of the Deloitte's 2019 survey on the adoption of blockchain technology [11]. The number of respondents (N) in the survey was 1386. The survey revealed so much hope for greater blockchain adoption in the future. The Majority (86%) of the respondents believed that blockchain will finally get mainstream adoption and is widely scalable. An earlier survey by PWC [154] also showed that 86% of 600 respondents were actively engaged with blockchain. Fig. 6 shows the analysis of the state of deployment of new enterprise blockchain networks based on the Cambridge university's survey of 67 live enterprise blockchain networks [10].

6.2.2. Survey of blockchain platforms in use

Generally speaking, Ethereum is the most widely used platform among the general (both the permission and permissionless) blockchains [153]. On the other hand, Hyperledger Fabric is the most used blockchain platform among the enterprise blockchain networks. Fig. 7 shows the survey analysis of blockchain platforms. The general

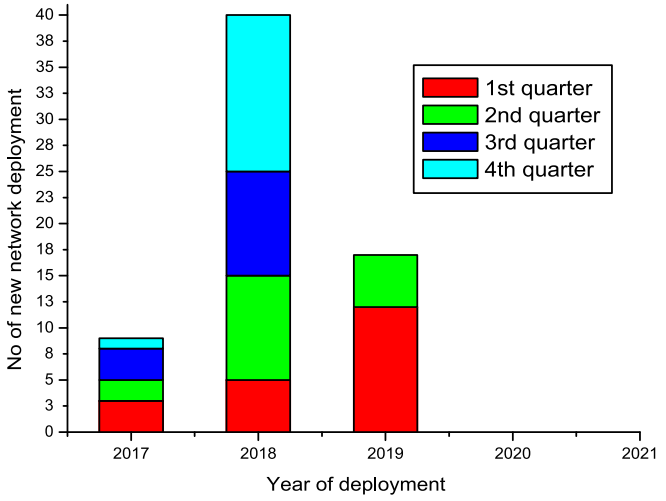

Fig. 6. Survey of enterprise blockchain deployment (N=67). Quarter refers to the quarter of the year.

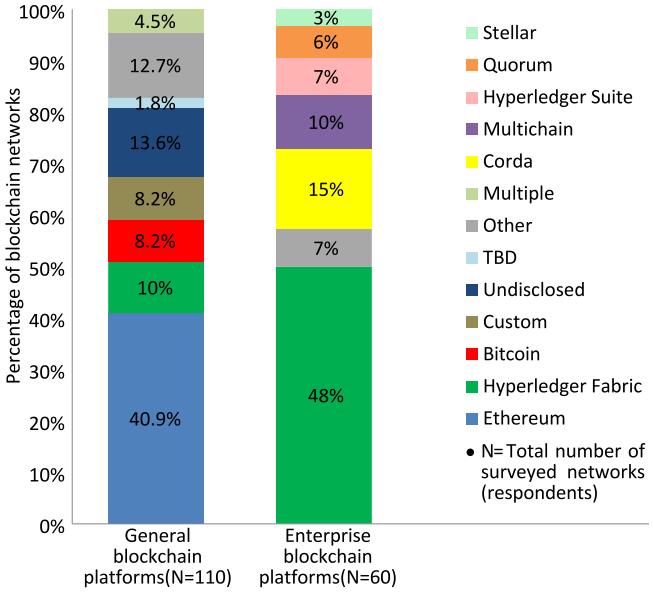

Fig. 7. Analysis of blockchain platforms used.

blockchains analysis in Fig. 7 was based on Stanford university's survey with 110 respondents [153]. On the other hand, the enterprise blockchain analysis was based on the Cambridge university's survey with 60 respondents [10]. In addition, PWC's survey [154] showed that 40% of the 389 respondents use permissioned blockchains such as the Hyperledger and Corda while 34% use permissionless blockchain. The rest 26% use hybrid blockchain (having both permissioned and permissionless features).

6.2.3. Multi-party blockchain vs blockchain meme networks

Multi-party blockchain networks run blockchain as a fully distributed ledger technology (DLT) with multi-party consensus and shared record keeping. On the other hand, blockchain meme networks only implement some of the components of the DLT such as the cryptographic mechanisms without multi-party consensus. Many blockchain memes have the goal of becoming full multi-party blockchain systems in the future. Findings by [10] revealed that most, live blockchain networks (77% of 67 surveyed) were blockchain memes while 20% were considered potential multiparty DLTs. Only the remaining 3% were fully multi-party DLT networks.

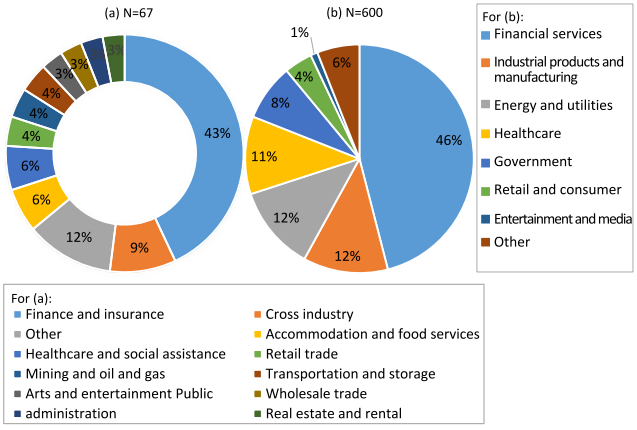

Fig. 8. Survey of sectors using blockchain.

6.2.4. Analysis of sectors using blockchain

Finance and insurance industries are the dominant sectors where blockchain is being used. They host most of the live enterprise blockchain networks as well as the public blockchain networks [10, 154]. Fig. 8(a) and (b) show the surveys of sectors where blockchain technology is being currently used based on the findings of [10] and [154] respectively.

6.2.5. Analysis of blockchain use cases

Generally speaking, record verification and validation is the most common use case of blockchain. However, in the enterprise blockchain atmosphere, supply chain tracking is the most widely used use case. Among the 67 live networks surveyed in [10], 19% use blockchain for supply chain. Fig. 9(a) and (b) show the surveys of the blockchain use cases based on the findings of [153] and [10] respectively. Furthermore, Table 8 summarizes the blockchain use cases survey analysis based on the findings of [11].

6.2.6. Analysis of the smart contract languages use

Most blockchain platforms (69% of 60 vendors surveyed by [10]) use the existing general-purpose smart contract languages such as Java and solidity for smart contract. The rest (56%) and (12%) of the 60 respondents use new general-purpose and fixed-purpose smart contracting languages respectively [10].

6.2.7. Enterprise blockchain consensus algorithms analysis

As enterprise blockchain aimed for high scalability and performance, PoW is undesirable. Currently, the Practical Byzantine Fault Tolerance (PBFT) consensus is the most widely used consensus among the enterprise blockchain networks. Fig. 10 shows the analysis of consensus algorithms used in the enterprise blockchain platforms based on the survey of 60 blockchain vendors by [10]. The vendors provide blockchain platforms and services for enterprises. Some platforms support more than one consensus protocols depending on the choice of the enterprise. For example, Hyperledger Fabric supports PBFT and Raft consensus which are pluggable.

6.2.8. Analysis of privacy and confidentiality methods used in enterprise blockchains

Privacy in blockchain refers to hiding the true identity of users (e.g. names) and sometimes the transaction data (e.g. amount) from unauthorized access and the public. Enterprises fear revealing their customer data in public and consortium blockchains. Blockchain uses addresses (hex string) as a user's identity for privacy. In addition to the

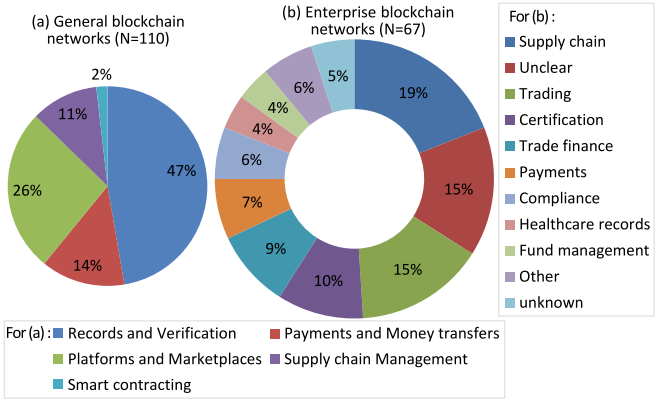

Fig. 9. Blockchain use cases analysis.

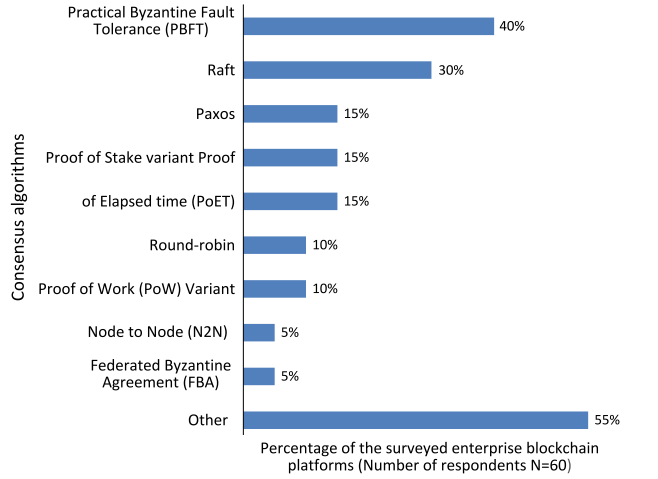

Fig. 10. Consensus algorithms in enterprise blockchain platforms.

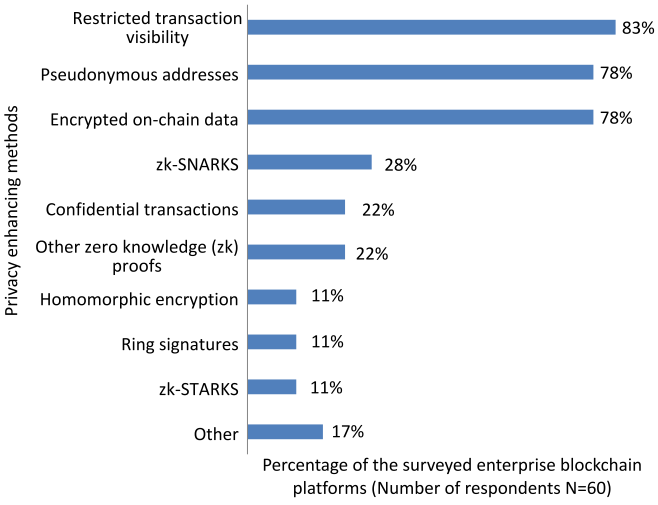

Fig. 11. Privacy methods in enterprise blockchain platforms.

addresses, different privacy-preserving methods are also used in some blockchains for better privacy. We discuss privacy in more detail under *privacy issues* in Section 7.1.

Fig. 11 shows a survey of privacy-enhancing methods used in enterprise blockchain platforms [10]. The survey responses were obtained from 60 blockchain vendors who provide blockchain platforms and other services to enterprises. Some vendors provide more than one privacy-enhancing method options for enterprises. The survey revealed that zero-knowledge proof (ZK) privacy method is still in the experimental state and not used by many platforms. Restricted transaction visibility and the pseudonymous addresses are the most widely used privacy methods in enterprise blockchain networks.

Table 9
Key Motivation of Enterprise Blockchains (N = 56).

Motivation	Response percentage
New revenue generation	69%
Efficiency improvement across boundaries	62%
Transparency improvement	62%
Cost savings	55%
Efficiency improvement within boundaries	26%
Competitive advantages	14%
Assets trading	10%
Moral hazards reduction	5%
Other	10%

Table 10
Blockchain project discontinuation survey 1 (N = 600).

Cause of project discontinuation	Response percentage
Cost	51%
Unsure how to start	45%
Lack of governance	45%
Users did not realize benefits	10%
No executive buy-in	9%
Compliance/Audit demands	7%
Regular discomforts	6%

Table 11
Blockchain project discontinuation Survey 2 (N = 56).

Cause of project discontinuation	Response percentage
Failed to realize tangible benefits	62%
Privacy and confidentiality concerns	38%
Not suitable for business case	25%
Technical issues	19%
Funding issues	12%
No executive buy-in	12%
Market competition	6%
Other	31%

Table 12
Blockchain platform selection criteria (56).

Criteria	Response percentage	Criteria	Response percentage
Vendor maturity	52%	Security	20%
Scalability/Performance	44%	Privacy/Confidentiality	24%
Use case compatibility	24%	Interoperability/extensibility	16
Costs	12%	Open source	8%
Unique features	8%	Other	8%

Table 13
Survey of blockchain adoption inhibitors 1 (N = 1386).

Adoption inhibitor	Response percentage
Regulatory issue	30%
Replacing/adapting existing legacy systems	30%
Possible security threat	29%
Uncertain benefit/return	28%
Lack of understanding and skills	28%
Fear of competitive information sensitivity	25%
Lack of compelling application	23%
Consortium formation challenges	22%
Blockchain is unproven	20%
Insufficient funding	20%
Not our business priority	17%
No. barrier to adoption	8%

Table 14
Survey of blockchain adoption inhibitors 2 (N = 600).

Adoption inhibitor	Response percentage
Regulatory uncertainty	48%
Users not trusting each other	45%
Ability to integrate network	44%
Interoperability	41%
Scalability issues	29%
Concerns for intellectual property	30%
Concerns for Audit/compliance	20%

6.2.9. Key motivation of enterprise blockchain networks

Most existing enterprise blockchain networks currently target cost reduction [10,159]. The Survey of 67 live blockchain networks by [10] shows that 72% of the respondents used blockchain for cost reduction, 8% for new market models, 6% for revenue generation, and 14% for both revenue generation and cost reduction. In the analysis of 90 use cases surveyed by [159], cost reduction was the immediate value targeted by 70% of the use cases. Table 9 shows a survey of 56 blockchain network operators also by [10]. The survey finding shows that new revenue generation is the ultimate future goal and motivation for most of the companies (69% of the 56 companies surveyed).

6.2.10. Causes of blockchain project discontinuation

The PWC's 2018 survey of 600 respondents shown in Table 10 [154], revealed that costs and lack of know-how were the major reasons for discontinuing blockchain projects. However, in the more recent survey of 56 respondents [10] shown in Table 11, failure of companies to realize significant benefits was the major reason for discontinuing blockchain projects. The failure is contributed by obstacles such as lack of law regulations on blockchain as well as lack of understanding of the technology.

6.2.11. Overall satisfaction of existing blockchains

Most organizations using blockchain are satisfied with the results of their blockchain projects. A survey of 56 organizations running blockchain projects showed that the majority (66%) of the respondents are satisfied with their projects [10].

6.2.12. Duration of blockchain project completion

It roughly takes 25 months on average to complete a blockchain project up to production. This duration includes the time taken for the initial background study, the creation of the proof of concept (PoC), pilot trial, and the final production. The Majority (about 2/3) of the time is spent in the PoC and the pilot trial state [10]. According to the Deloitte's survey of 1386 [11], many industries (47% of the respondents) expect 1–3 years to get a measurable return from investment in blockchain. The other (30%), (14%), and (6%) of the respondents expected 3–5 years, less than a year, and greater than 5 years respectively.

6.2.13. Analysis of blockchain platform selection criteria

Vendor maturity is the criteria mostly used for selecting an enterprise blockchain platform. Choosing a suitable and mature platform is very essential for getting the desired benefits of blockchain technology. Table 12 shows the survey of the criteria used for selecting blockchain platform based on the response got from 56 blockchain companies by [10].

6.2.14. Survey of obstacles impeding wider blockchain adoptions

Regulatory issues and lack of understanding are the biggest obstacles inhibiting the wider adoption of blockchain technology. Central banks and OPSIs consider blockchain hype as one of its adoption inhibitors due to the fear of unrealistic expectations. Other inhibitors listed by the central banks include the lack of compelling use cases, vendor immaturity, lack of standardization, and shortage of skilled blockchain developers. On the other hand, OPSIs mentioned the reluctance of companies to change their current systems and shortage of skilled blockchain developers among other blockchain inhibitors. In addition, the low scalability of blockchain inhibits its full adoption in some sectors [11,154]. Tables 13 and 14 summarize the survey of blockchain adoption inhibitors based on the survey of 1386 respondents by [11] and the survey of 600 respondents by [154] respectively.

6.2.15. Other key survey findings

Table 15 gives a summary of the other major quantitative survey findings [6,155–160].

7. Challenges and future research directions on blockchain

Despite its strength and successes, blockchain technology has some challenges that hinder its full adoption in some areas [12,25]. These challenges include:

7.1. Technical challenges

1. **Scalability Issues:**

Scalability issues mostly found in public blockchains are one of the biggest challenges of blockchain. The major blockchain scalability issues are its low throughput (tps) and large storage data (more than 299GB for Bitcoin) [110]. The low throughput of blockchain is caused by the long block interval and the small block size. There is a tradeoff between the block interval and the block size for getting the optimal throughput. There is also a tradeoff between the scalability, decentralization, and security of blockchain (blockchain trilemma). On the other hand, the huge blockchain storage size discourages running full nodes especially, by IoT devices since they cannot store all the blockchain data due to their small memory.

Blockchain applications lag much behind their non-blockchain counterparts in terms of throughput. For example, Bitcoin and Ethereum handle 3–4 and 20 tps respectively. In comparison, Visa and PayPal handle 24,000 and 193 transactions respectively [162]. The huge size of the blockchain data also affects the read performance of blockchain data requests. Blockchain servers such as Blockcypher perform less when compared to non-blockchain servers like Google. For example, Blockcypher supports 3 requests per second while Google on the other hand support 85,830 searches per second [163].

Several approaches such as Segregated Witness (SegWit), sharding, lightning network, sidechains, DAG, compact block relay, Jidar, and improved consensus algorithms were proposed for blockchain scalability improvements [164].

2. **Security related issues:**

Some security threats and vulnerabilities have been found in blockchain applications especially public blockchains (mostly cryptocurrencies) despite the security of the blockchain technology. Private and consortium blockchains are more secure due to their restricted access. Scams, malware attacks, denial of service (DoS), Sybil attacks, application, and network vulnerabilities are the commonly reported security issues. Loss of private keys due to the attacks, accidents, or recklessness also causes huge security breaches [3,24,165]. Cryptocurrencies worth $2 billion have been stolen mostly from exchanges since 2017 [166]. LedgerOPS in its 2018 blockchain security threat report [167], estimated such cryptocurrency losses as $1.604 billion in 2018 alone.

There were reports of attacks on Bitcoin, Ethereum, and other altcoins with the famous ones on MtGox and DAO causing the loss of 450 million USD and 60 million USD respectively. Bitfinnex exchange in Hong Kong suffered a $72 million loss and a DoS attack in 2016 and 2017 respectively. Money could also be stolen from cryptocurrencies through Border Gateway Protocol (BGP) attacks. About 83,000 USD was estimated to be lost from BGP attacks within just two months [24]. Blockchains using PoW consensus have the vulnerability of 51% attack. The networks can be attacked when a node or mining pool possesses

Table 15
Summary of the other key quantitative survey findings.

SN	Other survey findings
1.	Blockchain is more secure than the existing IT systems according to 71% of 1386 respondents surveyed [11].
2.	Based on the survey of 56 respondents, 50% of blockchain vendor platforms are open source [10].
3.	Efficiency, risk, revenue, time, and cost savings are the main metrics used for measuring results of blockchain projects [11].
4.	Based on a survey of 25,229 people, about 22% of the people in the world are somewhat familiar with blockchain [155].
5.	Out of 1386 organizations surveyed, 43% deployed blockchain as a new technology stack [11].
6.	Majority (71% of 67 respondents) of enterprise blockchain networks are founded by single organizations [10].
7.	Approximately 68% of 10,960 people surveyed believe that blockchain technology will affect all economic sectors [155].
8.	Blockchain should be used in national elections, according to 60% of 10,960 people surveyed globally [155].
9.	In a survey of 740 respondents, 48% agree that blockchain will likely disrupt their businesses in the next 3 years [156].
10.	Many companies (41% of 740 respondents) opined that they will likely implement blockchain in the next 3 years [156].
11.	Global blockchain device market was forecasted to grow from $218 million to $1,285 million between 2019 and 2024 [158].
12.	Business value added by blockchain will reach more than $176 billion by 2025 and $3.1 trillion by 2030 [6].
13.	Most (70% of 63) central banks are or will start experimenting with CBDC [157].
14.	More than 40% of 1871 respondents are very confident of blockchain industry [161].
15	Blockchain is not trusted by 68% of 576 Asia-pacific companies (excluding china) due to its lack of understanding [160].

51% of the network's computing power. With this immense power, the attacker can overcome the remaining nodes and successfully add false blocks that get into the main blockchain. The 51% attacker could censor transactions and carry out other forms of attacks such as double-spending, DoS, and eclipse attacks. GHash.IO Bitcoin mining pool once got 54% of the Bitcoin network computing power in July 2014. Due to public concerns, GHash.IO had to reduce its computing power before shutting down in 2016 [13,107,168]. In early 2019, Ethereum classic also experienced a 51% attack where $1.1 million was suspected to be stolen. Furthermore, Gate.io confirmed losing $200,000 which about half was later returned after few days from the attack [166]. In 2018 alone, several cryptocurrencies such as ZenCash, Monacoin, Verge, and Bitcoin Gold encountered 51% attack causing them to lose over $20 million [169].

Selfish mining is another security concern in blockchain. Miners with bad intentions and high computing power may refuse to publish their mined valid blocks until they aggregate a very long chain of blocks without competitors. By publishing their blocks, the new chain having their mined blocks becomes the longest chain and subsequently gets accepted as the main chain. As a result, the other valid blocks mined before the selfish mined blocks by the honest miners get rejected. Selfish mining discourages honest miners from mining and causes them to incur losses. Hence the scalability and security of the network get affected with the fewer miners and many selfish miners [170].

Vulnerabilities sometimes exist in blockchain programming and smart contracts. Such vulnerabilities lead to attacks such as the over $60 million Ethereum DAO's attack (The DAO) in 2016 causing the hard fork on the Ethereum network. Out of 19,366 Ethereum smart contracts, 8,833 were found to be vulnerable to potential security bugs [171].

Other forms of attacks possible on blockchain include the double-spending, eclipse attacks, DNS hijacking, consensus delay, liveness, and balance attacks [172]. Marcus [165] uncovered eclipse attack threats on Ethereum similar to the eclipse attacks found on Bitcoin. Li [172] extensively surveyed the security of blockchain systems. Conti [13] presented a detailed survey of the privacy and security issues in Bitcoin. Atzei [171] surveyed the vulnerabilities and attacks on Ethereum while Saad [24] further explored the attacks on blockchain. In addition, several proposals were made to curtail the security issues in blockchain. Trustchain [173] was proposed as a Sybil resistant and scalable blockchain. SmartPool was proposed to prevent 51% attack in mining pools [174].

3. **Privacy issues:**

Even though blockchain is pseudonymous, the physical identity of a user could be revealed over critical analysis of the transactions from a particular node or by the analysis of the network activities and the blockchain data [12,175]. Alternatively, the user's IP addresses could be extracted and linked with the user's wallet thus, breaking their privacy [3,176]. Goldfeder [177] demonstrated how web cookies (third-party trackers) could be used to uncover user's original identity upon online payments with cryptocurrencies.

Various methods of solving the privacy issues on blockchain have been proposed. An intermediary entity is used to provide an exchange of the identity with another identification such as a voucher to evade privacy detection [96,178,179]. Some researchers propose methods to enhance the existing privacy methods while some other researches propose new methods for the privacy provision in blockchain [180,181].

Zero-Knowledge proofs such as the Zero-Knowledge Succinct Non-interactive Argument of Knowledge (ZK-SNARKs), Idemix, and AZTEC are cryptographic protocols for enhancing privacy in blockchain. They allow blockchain transactions to be verified without revealing the transaction details (addresses and data) [182]. Conti [13] is a survey of privacy issues on Bitcoin while Merve [21] gives a comprehensive survey of privacy and anonymity in Bitcoin-like cryptocurrencies.

Zcash and some cryptocurrencies use the zk-SNARKs to guarantee privacy [182]. Vitalik Buterin proposed the use of the ZK-SNARKs to scale asset transfer on Ethereum up to 500 transactions per second [183]. A privacy solution API on Ethereum (AZTEC) uses zk protocol [184]. Hyperledger Fabric and Indy also use a zk variant protocol known as the identity mixer (Idemix) for privacy [185].

4. **Usability:**

Swan [186] opined that blockchain APIs are difficult to use from the developer's perspective even though some software can parse and extract information from the blockchain. There is a need to further simplify the blockchain APIs for developers.

5. **Quantum computing threat:**

There are many researches and projects on quantum computing. Some companies like Google, Rigetti, IBM, and Microsoft have been working to create commercial quantum computers whose speed much outperform the speed of the current computers. In October 2019, Google announced that it achieved quantum supremacy by doing in 200 s, a task that would take supercomputers 10,000 years to achieve. However, a viable commercial quantum computer is still far from being ready [187,188].

Most blockchains use the elliptic curve digital signature (ECDSA) which can be broken with quantum computers using a modified Shor's algorithm [188]. Kiktenko et al. [189] claimed that blockchain signatures are vulnerable to attacks using quantum computers and will be broken in the future. Hence, they proposed a post-quantum digital signature whose security is theoretical and rather unproven.

7.2. Regulatory issues

Lack of regulations is one of the greatest issues that impede blockchain adoptions worldwide especially by central banks. According to the PWC's survey of 600 respondents, 48% of the respondents chose regulatory issues as the major setback for blockchain adoption [154]. Most governments are skeptical of legalizing blockchain activities especially cryptocurrencies due to the fear of illegal activities and the impact of the cryptocurrencies on their national currencies. For this reason, many countries are considering creating their digital currencies.

7.3. Lack of understanding of blockchain

Another major setback for blockchain adoption is the lack of understanding of the blockchain technology. Many people find it difficult to understand blockchain technology or do not trust it thinking that the technology is used for illegal activities. A survey of 576 Asia-pacific (excluding China) companies revealed that 68% of the companies do not trust blockchain because they lack understanding of the technology [160]. According to the Deloitte's 2019 survey of 1386 executives, 28% of the executives counted the lack of understanding of blockchain as a major barrier for its greater adoption [11].

7.4. Reluctance to change current systems

It is natural to get reluctance when moving to a new system until the new system is well matured. Blockchain too suffers from this reluctance phenomenon. Many companies are reluctant to replace or modify their existing systems with blockchain. Out of the 1386 executives surveyed by Deloitte, 30% opined that reluctance to replace the existing system is the greatest barrier to blockchain adoption [11].

7.5. Future research direction on blockchain technology

There are many research opportunities in blockchain for improving the technology to make it more efficient, mature, and beneficial.

1. **Scalability:**
The scalability of blockchain is a big issue but less researched compared to other blockchain aspects like security [12]. There is a big opportunity to conduct researches on how to make blockchain more scalable. The throughput and latency issues of blockchain need to be further improved. Efficient ways to surmount the huge increasing size of the blockchain data should be studied and proposed.
2. **Big Data Analytics:**
The large data contained in blockchain create space for big data analytics of the blockchain. Other forms of big data storage (tensor computing for example) could also be enhanced to efficiently store and process the blockchain data for space, faster accessibility, and other benefits.
3. **Blockchain Verification:**
With the advent of several blockchains created by different companies and communities, there is a need to verify the blockchains for their authenticity to avoid fake blockchain creations [25]. Efficient and secure systems for blockchain authenticity verification are hence required.
4. **Blockchain Interoperability:**
Interoperability of blockchain is also an area to look into. Many of the different blockchain platforms may interoperate to enhance their security, operability, and efficiencies. Blockchain should also be able to complement some compatible existing systems. Many companies want to adopt blockchain but do not like to abandon their existing systems without big problems. There is a need to research the best way how the blockchain will work with the existing systems in a company. It is also pertinent to research how different blockchain systems can effectively interoperate for mutual benefits.
5. **Efficient and Secure Consensus Protocols:**
There are many consensus algorithms for blockchain trying to replace the PoW consensus due to its huge energy waste. However, these alternative protocols come with new security issues or may be infeasible to implement in reality [190]. There is a research opportunity within the blockchain consensus protocols. Stronger and realizable protocols that are more secure than PoW and having the least energy consumption are the quest for future researches. More work needs to be done to ensure the right protocol is used in the right applications [13].
6. **Post-quantum blockchain cryptosystems:**
With the threat of quantum computers to blockchain security, there is a demand for an efficient and well-proven post-quantum digital signature schemes and other relevant studies to protect the blockchain against all kind of threats of quantum computers. Having quantum computers affordable is a welcome development, however, there is a need to protect systems like blockchain whose security could be breached by the quantum computers.
There are other cryptographic systems (post-quantum cryptos) apart from ECDSA, RSA, and DSA that have not been discovered to be affected by quantum computers. Such systems exist in hash-based cryptography (e.g. Merkle signature system), code-based cryptography (e.g. McEliece public key system), and symmetric key cryptography (e.g. AES). The Other post-quantum cryptosystems are the lattice-based cryptography (e.g. NTRU public key cryptosystem) and the multivariate quadratic public key systems. There are still research opportunities for improving the usability (key size), efficiency, and the confidence of such post-quantum cryptosystems for their use in blockchain against the quantum computer threats [191]. There is also a need for more study on quantum channels as well as the development of efficient post-quantum consensus algorithms [189].
7. **Integrating blockchain with other technologies:**
Artificial intelligence (AI), IoT, and cloud computing are nowadays other big directions that draw the attention of several researchers. There is a research opportunity to study what and how blockchain could be efficiently integrated with other technologies. Integrating blockchain with the appropriate AI, cloud computing and IoT systems may enhance the efficiency, security, and the autonomy of the systems. The IBM's ADEPT is a suitable example use case where IoT devices use blockchain to achieve autonomous transactions (for auto repair and update), better privacy, and security [29].

8. Conclusion

Blockchain is a promising technology with immense benefits such as data security, cost savings, anonymity, speed, transparency, traceability, and most importantly the eviction of intermediaries and central authorities. Blockchain is bringing digital revolution by disrupting many industries. Currently, there are many applications of blockchain besides cryptocurrencies as well as several adoptions from many countries and companies. We envisage more adoptions as the technology matures and many trials reveal successful results. It is believed that blockchain will finally get mainstream adoption across the globe. In this paper, we surveyed the breakthrough and the state of the art of blockchain technology covering recent developments in its adoptions, applications, and challenges. We also gave a comprehensive review of the cryptography behind the blockchain technology. In addition, we reviewed the quantitative surveys and analysis of blockchain technology and finally outlined the future research directions of the blockchain technology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Farouk, A. Alahmadi, S. Ghose, A. Mashatan, Blockchain platform for industrial healthcare: Vision and future opportunities, Comput. Commun. 154 (2020) 223–235, http://dx.doi.org/10.1016/j.comcom.2020.02.058.
[2] J. Frizzo-Barker, P.A. Chow-White, P.R. Adams, J. Mentanko, D. Ha, S. Green, Blockchain as a disruptive technology for business: A systematic review, Int. J. Inf. Manage. 51 (2020) 102029, http://dx.doi.org/10.1016/j.ijinfomgt.2019.10.014.
[3] X. Wang, X. Zha, W. Ni, P. Liu, Y.G. Jay, X. Niu, K. Zheng, Survey on blockchain for Internet of Things, Comput. Commun. 136 (2019) 10–29, http://dx.doi.org/10.1016/j.comcom.2019.01.006.
[4] R3, The R3 story, 2018, About R3, URL https://www.r3.com/about/.
[5] R.G. Brown, The corda platform: An introduction, Corda platform White Paper, 2018, pp. 1–21, URL https://www.corda.net/wp-content/uploads/2018/05/corda-platform-whitepaper.pdf.

[6] D. Furlonger, R. Valdes, Practical blockchain: a gartner trend insight report, 2017, URL https://blockcointoday.com/wp-content/uploads/2018/04/Practical-Blockchain_-A-Gartner-Trend-Insight-Report.pdf.

[7] Cisco, Blockchain by Cisco - Build trust-based business networks for digital transformation, Cisco Blockchain White paper, 2018.

[8] A. Lannquist, How are Central Banks Exploring Blockchain Today? World Economic Forum White Paper, 2019, URL http://www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf.

[9] L. Association, Libra White Paper, 2019, URL https://libra.org/en-US/white-paper/.

[10] M. Rauchs, A. Blandin, K. Bear, S.B. McKeon, 2nd global enterprise blockchain benchmarking study, 2019, Cambridge Centre for Alternative Finance Available at SSRN, URL https://ssrn.com/abstract=3461765.

[11] L. Pawczuk, R. Massey, J. Holdowsky, Deloitte 2019 global blockchain survey - blockchain gets down to business, 2019, Deloitte insights, URL https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.

[12] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on Blockchain technology? - A systematic review, PLoS One 11 (10) (2016) 1–27, http://dx.doi.org/10.1371/journal.pone.0163477.

[13] M. Conti, E. Sandeep Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3416–3452, http://dx.doi.org/10.1109/comst.2018.2842460.

[14] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2084–2123, http://dx.doi.org/10.1109/COMST.2016.2535718.

[15] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inf. Syst. Eng. 59 (3) (2017) 183–187, http://dx.doi.org/10.1007/s12599-017-0467-3.

[16] Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. (2017) 1–24, http://dx.doi.org/10.1504/IJWGS.2018.095647.

[17] A.A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151.

[18] O. Firica, Blockchain technology: Promises and realities of the year 2017, Quality - Access Success 18 (October) (2017) 51–58.

[19] H. Vranken, Sustainability of bitcoin and blockchains, Curr. Opin. Environ. Sustain. 28 (2017) 1–9, http://dx.doi.org/10.1016/j.cosust.2017.04.011.

[20] A. Miglani, N. Kumar, V. Chamola, S. Zeadally, Blockchain for internet of energy management: Review, solutions, and challenges, Comput. Commun. 151 (2020) 395–418, http://dx.doi.org/10.1016/j.comcom.2020.01.014.

[21] M.C. Kus Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2543–2585, http://dx.doi.org/10.1109/COMST.2018.2818623.

[22] L.S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS, 2017, pp. 1–5, http://dx.doi.org/10.1109/ICACCS.2017.8014672.

[23] W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370, http://dx.doi.org/10.1109/ACCESS.2019.2896108.

[24] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, A. Mohaisen, Exploring the attack surface of blockchain: A systematic overview, 2019, arXiv:1904.03487, CoRR abs/1904.03487, URL http://arxiv.org/abs/1904.03487.

[25] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017 (2017) 557–564, http://dx.doi.org/10.1109/BigDataCongress.2017.85.

[26] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the Internet of Things: Research issues and challenges, IEEE Internet Things J. 6 (2) (2019) 2188–2204, http://dx.doi.org/10.1109/JIOT.2018.2882794.

[27] D. Romano, G. Schmid, D. Romano, G. Schmid, Beyond bitcoin: A critical look at blockchain-based systems, Cryptography 1 (2) (2017) 15, http://dx.doi.org/10.3390/cryptography1020015.

[28] K. Salah, M.H.U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: Review and open research challenges, IEEE Access 7 (2019) 10127–10149, http://dx.doi.org/10.1109/ACCESS.2018.2890507.

[29] L. Yang, The blockchain: State-of-the-art and research challenges, J. Ind. Inf. Integr. 15 (2019) 80–90, http://dx.doi.org/10.1016/j.jii.2019.04.002.

[30] M. Belotti, N. Božić, G. Pujolle, S. Secci, A vademecum on blockchain technologies: When, which, and how, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3796–3838, http://dx.doi.org/10.1109/COMST.2019.2928178.

[31] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, p. 9, http://dx.doi.org/10.1007/s10838-008-9062-0, arXiv:43543534534v343453, www.bitcoin.org.

[32] Cryptoreport, Live crypto prices and trading, 2020, URL https://cryptoreport.com/all.

[33] Government Office for Science, Distributed ledger technology: beyond block chain, in: A Report by the UK Government Chief Scientific Adviser, Tech. Rep., 2016, p. 88, URL https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain.

[34] H. Van Steenis, B.L. Graseck, F. Simpson, J.E. Faucette, Global insight: Blockchain in banking: Disruptive threat or tool? Morgan Stanley Res. (2016) 1–31, URL http://www.ameda.org.eg/files/Morgan-Stanley-blockchain-report.pdf.

[35] A. Narayanan, J. Clark, Bitcoin's academic pedigree, Commun. ACM 60 (12) (2017) 36–45, http://dx.doi.org/10.1145/3132259.

[36] V. Buterin, On public and private blockchains, 2015, URL https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[37] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, Int. J. Netw. Secur. 1919 (55) (2017) 653–659, http://dx.doi.org/10.6633/IJNS.201709.19(5).01.

[38] C. Cachin, M. Vukolić, Blockchain consensus protocols in the wild, 2017, http://dx.doi.org/10.4230/LIPIcs.DISC.2017.1, arXiv:1707.01873, arXiv preprint arXiv:1707.01873.

[39] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in: E.F. Brickell (Ed.), Advances in Cryptology — CRYPTO' 92, Springer Berlin Heidelberg, Berlin, Heidelberg, 1993, pp. 139–147.

[40] M. Jakobsson, A. Juels, Proofs of work and bread pudding protocols(extended abstract), in: Secure Information Networks: Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20–21, 1999, Leuven, Belgium, Springer US, Boston, MA, 1999, pp. 258–272, http://dx.doi.org/10.1007/978-0-387-35568-9_18.

[41] Z. Zheng, Z. Chen, Pool strategies selection in pow-based analysis, IEEE Access PP (c) (2018) 1, http://dx.doi.org/10.1109/ACCESS.2018.2890391.

[42] C.C. for Alternative Finance, Live Bitcoin network power updated every 30 seconds, 2020, Cambridge Bitcoin Electricity Consumption Index, URL https://www.cbeci.org/.

[43] Powercompare, Countries that consume more or less electricity than bitcoin mining in late 2018, 2020, Power Compare, URL https://powercompare.co.uk/bitcoin-mining-electricity-map/.

[44] S. King, Primecoin: Cryptocurrency with prime number proof-of-work, King, Sunny 4 (2) (2013) 6, URL https://bravenewcoin.com/assets/Whitepapers/primecoin-paper.pdf.

[45] J. Kwon, TenderMint: Consensus without mining, 6, 2014, pp. 1–10, the-Blockchain.Com, URL tendermint.com/docs/tendermint.pdf.

[46] L. Wang, X. Shen, J. Li, J. Shao, Y. Yang, Cryptographic primitives in blockchains, J. Netw. Comput. Appl. 127 (2019) 43–58, http://dx.doi.org/10.1016/j.jnca.2018.11.003.

[47] X. Wang, D. Feng, X. Lai, H. Yu, Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD, IACR Cryptol. ePrint Arch. 2004 (2004).

[48] B. Schneier, SHA-1 broken, Schneier on Security (2005) URL https://www.schneier.com/blog/archives/2005/02/sha1_broken.html.

[49] Coinguides, What is ethash? A list of all ethash coins – ethash PoW algorithm, 2018, CoinGuides, URL https://coinguides.org/ethash-coins/.

[50] NIST, Secure Hash Standard (SHS), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION CATEGORY: (FIPS PUB 180-4), 2015, http://dx.doi.org/10.6028/NIST.FIPS.180-4.

[51] C. Ward, Modified merkle patricia trie specification (also merkle patricia tree), 2020, Ethereum Wiki, URL https://eth.wiki/fundamentals/patricia-tree.

[52] J.W. Bos, J.A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow, Elliptic curve cryptography in practice, IACR Cryptol. (2014) 157–175, http://dx.doi.org/10.1007/978-3-662-45472-5_11.

[53] S. Josefsson, I. Liusvaara, Edwards-curve digital signature algorithm (EdDSA), in: Internet Research Task Force, Crypto Forum Research Group, RFC, Vol. 8032, 2017.

[54] L. Lamport, Constructing Digital Signatures from a One-Way Function, Technical Report CSL-98, SRI International, 1979.

[55] G. Maxwell, A. Poelstra, Borromean ring signatures, 2019, (Accessed 8 June 2015).

[56] Certicom, Standards for efficient cryptography 2 (SEC 2): Recommended elliptic curve domain parameters, Stand. Efficient Cryptogr. 2 (Sec 2) (2010) 37, URL http://www.secg.org/sec2-v2.pdf.

[57] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (177) (1987) 203, http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5.

[58] V.S. Miller, Use of Elliptic Curves in Cryptography, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 218 LNCS, 1986, pp. 417–426, http://dx.doi.org/10.1007/3-540-39799-X_31.

[59] S. William, Cryptography and Network Security: Principles and Practice, sixth ed., Pearson Education, Inc., New York, 2014.

[60] NIST, FIPS 186–2: Digital signature standard (DSS), 2000, FIPS PUB 186–2 2 (category: Computer Security).

[61] A. ANSI, X9. 62–1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, ECDSA, American National Standards Institute (ANSI), Washington, DC, 1998.

[62] R.L. Rivest, M. Hellman, J. Anderson, J. Lyons, Responses to NIST's proposal, Commun. ACM 35 (7) (1992) 50–52, http://dx.doi.org/10.1145/129902.129905.

[63] D. Lee Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, first ed., Elsevier Inc., Amsterdam, 2015, p. 588, URL https://www.sciencedirect.com/science/book/9780128021170.

[64] O. Beigel, Who accepts bitcoin as payment? 2020, URL https://99bitcoins.com/bitcoin/who-accepts/.

[65] P. Ciaian, M. Rajcaniova, d. Kancs, The economics of Bitcoin price formation, Appl. Econ. 48 (19) (2016) 1799–1815.

[66] A.I. Sanka, R.C. Cheung, Efficient high performance FPGA based NoSQL caching system for blockchain scalability and throughput improvement, in: 2018 26th International Conference on Systems Engineering, ICSEng 2018, Australia, IEEE, 2018, pp. 1–8, http://dx.doi.org/10.1109/ICSENG.2018.8638204.

[67] N. Szabo, Formalizing and securing relationships on public networks, First Monday 2 (9) (1997) http://dx.doi.org/10.5210/fm.v2i9.548.

[68] M. Bartoletti, L. Pompianu, An empirical analysis of smart contracts: platforms, applications, and design patterns, 2017, CoRR abs/1703.06322, URL http://arxiv.org/abs/1703.06322.

[69] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, M. Marchesi, A massive analysis of ethereum smart contracts empirical study and code metrics, IEEE Access 7 (2019) 78194–78213, http://dx.doi.org/10.1109/ACCESS.2019.2921936.

[70] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: 2016 IEEE Symposium on Security and Privacy, SP, IEEE, 2016, pp. 839–858, http://dx.doi.org/10.1109/SP.2016.55.

[71] A. Mense, M. Flatscher, Security vulnerabilities in ethereum smart contracts, in: Proceedings of the 20th International Conference on Information Integration and Web-Based Applications and Services, iiWAS2018, Association for Computing Machinery, New York, NY, USA, 2018, pp. 375–380, http://dx.doi.org/10.1145/3282373.3282419.

[72] S. Rouhani, R. Deters, Security, performance, and applications of smart contracts: A systematic survey, IEEE Access 7 (2019) 50759–50779, http://dx.doi.org/10.1109/ACCESS.2019.2911031.

[73] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: Architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. A 49 (11) (2019) 2266–2277, http://dx.doi.org/10.1109/TSMC.2019.2895123.

[74] N. Biedrzycki, Will Blockchain Transform the Stock Market? Data driven investor, 2019, URL https://www.datadriveninvestor.com/2019/04/09/will-blockchain-transform-the-stock-market/.

[75] M. Crosby, Blockchain technology: Beyond bitcoin, Appl. Innov. Rev. Issue (2) (2016).

[76] ASX, CHESS Replacement: ASX is replacing CHESS with distributed ledger technology (DLT) developed by digital asset, 2020, ASX services, URL https://www.asx.com.au/services/chess-replacement.htm.

[77] K.O. Obour Agyekum, Q. Xia, E. Boateng Sifah, S. Amofa, K. Nketia Acheampong, J. Gao, R. Chen, H. Xia, J.C. Gee, X. Du, M. Guizani, V-chain: a blockchain-based car lease platform, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1317–1325, http://dx.doi.org/10.1109/Cybermatics_2018.2018.00228.

[78] A.A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S.Z. Abdul Rasid, M.F. Yusof, Scalability challenges in healthcare blockchain system—A systematic review, IEEE Access 8 (2020) 23663–23673, http://dx.doi.org/10.1109/ACCESS.2020.2969230.

[79] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F. Wang, Blockchain-powered parallel healthcare systems based on the ACP approach, IEEE Trans. Comput. Soc. Syst. 5 (4) (2018) 942–950, http://dx.doi.org/10.1109/TCSS.2018.2865526.

[80] K. Griggs, O. Ossipova, C. Kohlios, A. Baccarini, E. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018) 1–7.

[81] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: Applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278, http://dx.doi.org/10.1016/j.csbj.2018.07.004.

[82] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technology Engineering Management Conference, TEMSCON, 2017, pp. 137–141, http://dx.doi.org/10.1109/TEMSCON.2017.7998367.

[83] A. Roehrs, C.A. Da Costa, R. Da Rosa Righi, OmniPHR: A distributed architecture model to integrate personal health records, J. Biomed. Inform. 71 (2017) 70–81.

[84] T. McGhin, K.-K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, J. Netw. Comput. Appl. 135 (2019) 62–75, http://dx.doi.org/10.1016/j.jnca.2019.02.027.

[85] R. Abujamra, D. Randall, Chapter Five - Blockchain applications in healthcare and the opportunities and the advancements due to the new information technology framework, in: S. Kim, G.C. Deka, P. Zhang (Eds.), Role of Blockchain Technology in IoT Applications, in: Advances in Computers, vol. 115, Elsevier, 2019, pp. 141–154, http://dx.doi.org/10.1016/bs.adcom.2018.12.002.

[86] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, K.Y. Lam, A blockchain framework for insurance processes, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings 2018-January, 2018, pp. 1–4, http://dx.doi.org/10.1109/NTMS.2018.8328731.

[87] Reuters, Commonwealth and wells fargo mark 1st international blockchain trade | fortune, 2016, URL http://fortune.com/2016/10/24/commonwealth-bank-well-fargo-blockchain/.

[88] G. Hileman, M. Rauchs, 2017 global cryptocurrency benchmarking study, SSRN Electron. J. 44 (0) (2017) http://dx.doi.org/10.2139/ssrn.2965436.

[89] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, R. Sirdey, Towards better availability and accountability for IoT updates by means of a blockchain, in: 2017 IEEE European Symposium on Security and Privacy Workshops, EuroS PW, 2017, pp. 50–58, http://dx.doi.org/10.1109/EuroSPW.2017.50.

[90] M. Ali, R. Shea, M.J. Freedman, Blockstack: A new decentralized internet, Whitepaper, (Version 1.0.1) (2017) 1–22, URL https://blockstack.org/blockstack{_}whitepaper.pdf.

[91] Namecoin, Decentralize all the things, 2018, URL https://namecoin.org/.

[92] Emercoin, EmerDNS, 2020, URL https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction.

[93] E. Karaarslan, E. Adiguzel, Blockchain based DNS and PKI solutions, IEEE Commun. Stand. Mag. 2 (3) (2018) 52–57, http://dx.doi.org/10.1109/MCOMSTD.2018.1800023.

[94] S.L. Inc., Decentralized cloud object storage that is affordable, easy to use, private, and secure, 2019, URL https://storj.io/.

[95] V. Saini, StoragePedia: An encyclopedia of 5 blockchain storage platforms, 2018, StoragePedia, URL https://hackernoon.com/storagepedia-an-encyclopedia-of-5-blockchain-storage-platform-8aa13c630ace.

[96] R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, Blockchain for large-scale Internet of Things data storage and protection, IEEE Trans. Serv. Comput. 12 (5) (2019) 762–771, http://dx.doi.org/10.1109/TSC.2018.2853167.

[97] G. Foroglou, A.L. Tsilidou, Further applications of the blockchain, in: Conference: 12th Student Conference on Managerial Science and Technology, At Athens, 2015, pp. 0–8, http://dx.doi.org/10.13140/RG.2.1.2350.8568.

[98] A. Third, K. Quick, M. Bachler, P. John, Government services and digital identity, in: European Union Blockchain Observatory and Forum, 2018, pp. 1–52.

[99] Slock.it, Governance (voting/DAO), 2019, use cases, URL https://slock.it/use-cases/.

[100] Fortune, Microsoft and accenture unveil global ID system for refugees, 2018, URL http://fortune.com/2017/06/19/id2020-blockchain-microsoft/.

[101] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. (2018) 1, http://dx.doi.org/10.1109/COMST.2018.2863956.

[102] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (10) (2017) http://dx.doi.org/10.1016/j.telpol.2017.09.003.

[103] S. Mire, Blockchain in cybersecurity: 11 startups to watch in 2019, 2019, Disruptor Daily, URL https://www.disruptordaily.com/blockchain-startups-cybersecurity/.

[104] B. Don, b. AG, S. Rajah, Dharma Ott, K. Fromm, Enterprise ethereum alliance –real estate special interest Group1Real estate use casesfor blockchain technology, 2019, Enterprise Ethereum Alliance-Volume 1, 2019, URL https://entethalliance.org/wp-content/uploads/2019/05/EEA-Real-Estate-SIG-Use-Cases-May-2019.pdf.

[105] Maersk, Tradelens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers Hapag-Lloyd and Ocean Network Express, 2020, URL https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens. (Accessed January 2020).

[106] Grainchain, Revolutionary blockchain platform for the agricultural business ecosystem fast and secured transactions for real commodities, 2019, URL https://www.grainchain.io/.

[107] D. Romano, G. Schmid, Beyond bitcoin: A critical look at blockchain-based systems, Cryptography 1 (2) (2017) 15, http://dx.doi.org/10.3390/cryptography1020015.

[108] Ž. Turk, R. Klinc, Potentials of blockchain technology for construction management, Procedia Eng. 196 (June) (2017) 638–645, http://dx.doi.org/10.1016/j.proeng.2017.08.052.

[109] H. Hyvärinen, M. Risius, G. Friis, A blockchain-based approach towards overcoming financial fraud in public sector services, Bus. Inf. Syst. Eng. 59 (6) (2017) 441–456, http://dx.doi.org/10.1007/s12599-017-0502-4.

[110] Blockchain.com, Blockchain size (mb), 2020, URL https://www.blockchain.com/charts/blocks-size.

[111] M.B. Taylor, Bitcoin and the age of bespoke silicon, in: 2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems, CASES 2013, 2013, http://dx.doi.org/10.1109/CASES.2013.6662520.
[112] V. Buterin, A next-generation smart contract and decentralized application platform, Etherum White paper (2014) 1–36, http://dx.doi.org/10.5663/aps.v1i1.10138.
[113] Etherscan, Ethereum unique address chart, 2020, URL https://etherscan.io/chart/address. (Accessed September 2020).
[114] T.L. Foundation, About hyperledger, 2018, URL https://www.hyperledger.org/about. (Accessed January 2020).
[115] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: A distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, EuroSys '18, Association for Computing Machinery, New York, NY, USA, 2018, p. 15, http://dx.doi.org/10.1145/3190508.3190538.
[116] T.L. Foundation, About hyperledger, 2018, URL https://www.hyperledger.org/. (Accessed January 2020).
[117] Quorum, Evolve with Quorum. The proven blockchain solution for business, 2019, Quorum, URL https://www.goquorum.com/.
[118] E.E. Alliance, About the eea, 2020, URL https://entethalliance.org/. (Accessed January 2020).
[119] MultiChain, Enterprise blockchain. That actually works, 2020, URL https://www.multichain.com/. (Accessed January 2020).
[120] L.L.C. Kadena, Kadena's feature set is the industry's future roadmap, 2019, URL https://www.kadena.io/. (Accessed January 2020).
[121] I. Schvey, Axoni's distributed ledger technology provides secure, multi-party data infrastructure with unparalleled performance, 2020, Technology, URL https://axoni.com/technology/.
[122] N. Pennington, An introduction to SETL blockchain, 2019, SETL Blog, URL https://setl.io/blog/an-introduction-to-setl-blockchain/.
[123] L. Digital Asset Holdings, Digital asset transforming the way multi-party applications are built and deployed, 2020, URL https://digitalasset.com/.
[124] C.T. LTD, Building the Decentralised Financial Market Infrastructure (dFMI) of the Future, Clearmatics, 2020, URL https://www.clearmatics.com/about/.
[125] C. Brennan, B. Zelnick, M. Yates, W. Lunn, Blockchain 2.0, 2018, Credit Suisse: Global Equity Research Technology.
[126] P. Bajpai, How stock exchanges are experimenting with blockchain technology, 2018, URL https://www.nasdaq.com/articles/how-stock-exchanges-are-experimenting-blockchain-technology-2017-06-12.
[127] S. Panikkar, S. Nair, P. Brody, V. Pureswaran, ADEPT: An IoT practitioner perspective, 2015, pp. 1–20, URL http://ibm.biz/devicedemocracy.
[128] Microsoft, Stampery blockchain add-in for microsoft office - developer blog, 2017, URL https://www.microsoft.com/developerblog/2017/04/10/stampery-blockchain-add-microsoft-office/.
[129] R. Mark, Announcing the CoCo framework for enterprise blockchain networks: Microsoft Azure, 2017, URL https://azure.microsoft.com/sv-se/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks/.
[130] Bitpay, Bitcoin: A new global economy, 2018, URL https://blog.bitpay.com/bitcoin-a-new-global-economy/.
[131] I. Allison, BMW, ford, GM: World's largest automakers form blockchain coalition - CoinDesk, 2018, URL https://www.coindesk.com/bmw-ford-gm-worlds-largest-automakers-form-blockchain-coalition/.
[132] Oracle, Autonomous blockchain cloud service: Oracle cloud, 2018, URL https://cloud.oracle.com/en{_}US/blockchain.
[133] R. Florea, How FedEx is benefiting from blockchain technology, 2020, URL https://blockchainflashnews.com/how-fedex-is-benefiting-from-blockchain/.
[134] Tradelens, About tradelens, 2020, URL https://www.tradelens.com/about/. (Accessed January 2020).
[135] cbinsight, Banking is only the beginning: 55 big industries blockchain could transform, 2019, Research Portal, URL https://www.cbinsights.com/research/industries-disrupted-blockchain/.
[136] D. Moadel, Verizon and Wells Fargo are Getting on the Blockchain, Market Realist, 2020, URL https://articles2.marketrealist.com/2019/09/verizon-wells-fargo-getting-on-blockchain/.
[137] E. Daniel, Kaspersky Unveils Blockchain-Based Voting Machine, Verdict Media Limited UK, 2020, URL https://www.verdict.co.uk/kaspersky-blockchain-voting/.
[138] D.T. Limited, Digital transaction, 2020, URL https://www.digital-transaction.com/.
[139] Basu Medha, Singapore Government builds blockchain system to protect banks, 2016, URL https://govinsider.asia/smart-gov/singapore-government-builds-blockchain-system-to-protect-banks/.
[140] L. Shin, The first government to secure land titles on the bitcoin blockchain expands project, 2017, URL https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/{#}67aee1a04dcd.
[141] Reason Foundation, Can blockchain technology reduce third-world poverty? - hit & run: Reason.com, 2016, URL http://reason.com/blog/2016/04/30/bitfury-desoto-blockchain-land-registry.
[142] De Nikhilesh, TEPCO Invests in blockchain startup in bid to decentralize systems - CoinDesk, 2018, URL https://www.coindesk.com/tepco-buys-stake-uk-blockchain-startup-bid-decentralized-systems/.
[143] Finextra, Electron wins uk government award to advance blockchain in balancing electricity markets, 2017, URL https://www.finextra.com/pressarticle/70874/electron-wins-uk-government-award-to-advance-blockchain-in-balancing-electricity-markets.
[144] SolarPlaza, Comprehensive guide to companies involved in blockchian and energy, 2018, p. 44, Blockchain Business, URL http://ipci.io/wp-content/uploads/2017/12/Energy-Blockchain-Report.compressed.pdf.
[145] M.J. Zuckerman, Swedish government land registry soon to conduct first blockchain property transaction, 2018, URL https://cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction.
[146] A. Shafi, K. Patel, Cryptocurrency laws and regulations in UAE 2018, Asia Bus. Law J. (2018) URL https://www.vantageasia.com/cryptocurrency-law-uae/.
[147] S. Carvalho, UPDATE 1-UAE, Saudi working on digital currency for cross-border deals, 2017, URL https://www.reuters.com/article/emirates-saudi-currency/update-1-uae-saudi-working-on-digital-currency-for-cross-border-deals-idUSL8N1OD2LP.
[148] M. Custodio, Moscow plans to use ethereum blockchain to increase commerce efficiency, 2018, URL https://blocktribune.com/moscow-plans-to-use-ethereum-blockchain-to-increase-commerce-efficiency/.
[149] C.B. Council, Blockchain council report to the community: Colorado office of economic development and international trade, 2019, URL https://choosecolorado.com/blockchain/.
[150] ID2020 Alliance, ID2020 Alliance launches inaugural pilots, welcomes new partners at annual summit, 2018, URL https://www.prnewswire.com/news-releases/id2020-alliance-launches-inaugural-pilots-welcomes-new-partners-at-annual-summit-300713089.html?tc=eml{_}cleartime.
[151] Reuters, China's sovereign digital currency is 'almost ready': PBOC official, 2020, URL https://www.reuters.com/article/us-china-cryptocurrency-cenbank/chinas-sovereign-digital-currency-is-almost-ready-pboc-official-idUSKCN1V20RD.
[152] N. Stockton, China launches national blockchain network in 100 cities, IEEE Spectr. (2020) URL https://spectrum.ieee.org/computing/software/china-launches-national-blockchain-network-100-cities.
[153] D.J. Galen, A. Abdualiyev, W. Chong, S. Iyer, R. Kim, J. Ma, D. Mann, E. Owen, G. Park, Junhyung (Edward), O. Portelance, N. Seideman, Thakur, U. of Oregon Blockchain Club, Blockchain for Social Impact 2019, Centre for social innovation Stanford Graduate School of Business, 2019, URL https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/csi-report-2019-blockchain-social-impact.pdf.
[154] P. China, PwC global blockchain survey 2018 - blockchain is here. What's your next move? Res. Insights (2018) URL www.pwccn.com/global-blockchain-survey-2018.
[155] F.O. Hampson, E. Jardine, CIGI-IPSOS global survey on internet seurity and trust 2019 part 5: Cryptocurrencies, blockchain, bark web, product certification, 2019, Ipsos public affairs, URL https://www.cigionline.org/internet-survey-2019.
[156] K. LLP, KPMG technology industry innovation survey: Blockchain, 2019, URL https://assets.kpmg/content/dam/kpmg/us/pdf/2019/02/blockchain-tech-survey-2019-infographic.pdf.
[157] C. Barontini, H. Holden, Proceeding with caution –a survey on central bank digital currency, 2019, Bank for International Settlements (BIS) Papers No 101, URL https://www.bis.org/publ/bppdf/bispap101.pdf.
[158] R. Markets, Blockchain devices market by type, connectivity, application, and geography - global forecast to 2024, 2019, URL https://www.marketsandmarkets.com/Market-Reports/blockchain-device-market-177053178.html.
[159] B. Carson, G. Romanelli, P. Walsh, A. Zhumaev, Blockchain beyond the hype: What is the strategic business value? McKinsey Q. (2018) 118–127, URL https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.
[160] M. Huillet, EY: Blockchain not understood by almost 70% of firms in Asia-Pacific, 2019, https://cointelegraph.com/news/ey-blockchain-not-understood-by-almost-70-of-firms-in-asia-pacific.
[161] A. Leong, Global STO, regtech blockchain industry survey and sentiment analysis ("Dipstick Study"), World Economic Forum White Paper, 2019, URL https://secureservercdn.net/198.71.233.195/1a6.6ba.myftpupload.com/wp-content/uploads/2019/09/STO-REGTECH-BLOCKCHAIN-INDUSTRY-SURVEY.pdf.
[162] Visa, Security and reliability (visa speed), 2018, URL https://usa.visa.com/run-your-business/small-business-tools/retail.html.

[163] I. live stats, Google searches in 1 second - internet live stats, 2020, URL http://www.internetlivestats.com/one-second/{#}google-band.
[164] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: A survey, IEEE Access 8 (2020) 16440–16455.
[165] Y. Marcus, E. Heilman, S. Goldberg, Low-resource eclipse attacks on ethereum's peer-to-peer network, 2018, p. 15, URL https://www.cs.bu.edu/%7Egoldbe/projects/eclipseEth.pdf.
[166] M. Orcutt, Once hailed as unhackable, blockchains are now getting hacked, 2019, URL https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.
[167] LedgerOPS, Blockchain security threat report: 2018 review, 2018, URL https://documentcloud.adobe.com/link/track?uri=urn:aaid:scds:US:eae0e5e7-d798-4854-b3fa-4dae1686eb3f.
[168] C. Farivar, Bitcoin pool GHash.io commits to 40 breach, ARS Tecnica (2014) http://dx.doi.org/10.1109/comst.2018.2842460.
[169] C. Ajay, Top five blockchain security issues in 2019, 2019, URL https://ledgerops.com/blog/2019/03/28/top-five-blockchain-security-issues-in-2019.
[170] C. Grunspan, R. Pérez-Marco, On profitability of selfish mining, 2018, arXiv:1805.08281, CoRR abs/1805.08281, URL http://arxiv.org/abs/1805.08281.
[171] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (SoK), in: M. Maffei, M. Ryan (Eds.), Principles of Security and Trust, Springer Berlin Heidelberg, Berlin, Heidelberg, 2017, pp. 164–186.
[172] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017) http://dx.doi.org/10.1016/j.future.2017.08.020, arXiv:arXiv:1011.1669v3.
[173] P. Otte, M. de Vos, J. Poulwelse, TrustChain: A sybil-resistant scalable blockchain, Future Gener. Comput. Syst. 29 (5) (2017) 333–335, http://dx.doi.org/10.1016/j.future.2017.08.048.
[174] L. Luu, Y. Velner, J. Teutsch, P. Saxena, SmartPool: Practical decentralized pooled mining, in: 26th USENIX Security Symposium, USENIX Security 17, USENIX Association, Vancouver, BC, 2017, pp. 1409–1426, URL https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/luu.
[175] A. Biryukov, D. Khovratovich, I. Pustogarov, Deanonymisation of clients in bitcoin p2p network, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, CCS '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 15–29, http://dx.doi.org/10.1145/2660267.2660379.
[176] M.A. Harlev, H. Sun Yin, K.C. Langenheldt, R. Mukkamala, R. Vatrapu, Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning, in: Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, URL http://hdl.handle.net/10125/50331.
[177] S. Goldfeder, H. Kalodner, D. Reisman, A. Narayanan, When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies, Proc. Priv. Enhancing Technol. 2018 (4) (2018) 179–199.
[178] M. Green, I. Miers, Bolt: Anonymous payment channels for decentralized currencies, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, Association for Computing Machinery, New York, NY, USA, 2017, pp. 473–489, http://dx.doi.org/10.1145/3133956.3134093.
[179] J. Camenisch, M. Drijvers, M. Dubovitskaya, Practical UC-secure delegatable credentials with attributes and their application to blockchain, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 683–699.
[180] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A comprehensive survey of blockchain: From theory to IoT applications and beyond, IEEE Internet Things J. 6 (5) (2019) 8114–8154.
[181] T. Ruffing, P. Moreno-Sanchez, A. Kate, P2p mixing and unlinkable bitcoin transactions, in: NDSS, 2017, URL https://eprint.iacr.org/2016/824.pdf.
[182] E. coin company, What are zk-snarks? 2019, URL https://z.cash/technology/zksnarks/.
[183] V. Buterin, On-chain scaling to potentially 500 tx/sec through mass tx validation, 2018, Research, URL https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477.
[184] S.H. Ltd, The privacy engine on Ethereum, 2020, URL https://www.aztecprotocol.com/.
[185] Hyperledger, MSP implementation with identity mixer, 2017, URL https://hyperledger-fabric.readthedocs.io/en/release-1.2/idemix.html. (Accessed December 2019).
[186] M. Swan, Blockchain: Blueprint for a New Economy, first ed., O'Reilly Media, Incorporated, Cambridge, 2015, p. 129, URL https://ebookcentral.proquest.com/lib/cityuhk/detail.action?docID=1929181.
[187] D. Castelvecchi, Quantum computers ready to leap out of the lab in 2017, Nature 541 (7635) (2017) 9–10, http://dx.doi.org/10.1038/541009a.
[188] A. Bouguera, How will quantum computing affect blockchain? 2019, Consensys-Blockchain Development, URL https://consensys.net/blog/blockchain-development/how-will-quantum-supremacy-affect-blockchain/.
[189] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A. Lvovsky, A. Fedorov, Quantum-secured blockchain, Quantum Sci. Technol. 3 (3) (2018) 035004.
[190] A. Shoker, Brief announcement: Sustainable blockchains through proof of eXercise, in: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, 2018, pp. 269–271, http://dx.doi.org/10.1145/3212734.3212781.
[191] D.J. Bernstein, Introduction to post-quantum cryptography, in: Post-Quantum Cryptography, Springer, 2009, pp. 1–14.

Abdurrashid Ibrahim Sanka received B.Eng. Electrical from Bayero University Kano, Nigeria in 2011. He got MSc. in Embedded Microelectronics and Wireless Systems from Coventry University, United Kingdom, in 2014. He has been working with the Bayero University, Kano as a lecturer since 2012. Currently, he is working towards Ph.D. degree with the department of Electrical Engineering, City University of Hong Kong. His research interests include blockchain technology, digital systems design, network computing and information security.

Muhammad Irfan received the B.Sc. degree in Electrical Engineering from University of Engineering and Technology, Pakistan, in 2013 and the M.S. degree in Electrical Engineering from Lahore University of Management Sciences, Pakistan, in 2016, respectively. He worked as a Lecturer in Electrical Engineering department at CECOS University of IT and Emerging Sciences, Pakistan. He has joined City University of Hong Kong as a Ph.D. student in the Electronic Engineering department in 2018. His research interests include designing/optimization of digital systems; and specifically CAM/TCAM on reconfigurable hardware.

Mr. Ian Huang is a serial entrepreneur, a serial technology investor, and a former US global communication engineering executive. Ian holds a BS in Electrical & Computer Engineering and an MS in Computer Science, both from Carnegie Mellon University, and an MS in Electrical Engineering from the University of Portland. He is a graduate of the AMP program at Harvard Business School. Ian was the first Visiting Chief Architect at the Singapore National Science and Technology Board (renamed as Agency for Science, Technology and Research A*STAR). He is listed in Who's Who in Technology and Who's Who in Outstanding American. Ian has been an adviser to MIT Technology Review (EMTECH Emerging Technology) since 2015. In 2018, Ian founded Digital Transaction Limited offering high performance and high scalable blockchain solutions for industrial applications.

Ray C.C. Cheung received B.Eng. and MPhil degrees in computing engineering from CUHK in 1999 and 2001 respectively. He received his Ph.D. degree in computing from Imperial College London (IC) in 2007. He received the Hong Kong Croucher Foundation Fellowship for postdoctoral and doctoral research work at UCLA and IC. In 2009, he visited Princeton University as a visiting research fellow. He is currently an associate professor in the department of Electrical Engineering, City University of Hong Kong. His current research interests include blockchain technology, cryptographic hardware design; rapid prototyping trusted computing platforms and high-performance biomedical VLSI designs.