SN Computer Science (2020) 1:114
https://doi.org/10.1007/s42979-020-00123-0

SURVEY ARTICLE

A Survey on Blockchain Technology Concepts, Applications, and Issues

H. T. M. Gamage[1] · **H. D. Weerasinghe**[1] · **N. G. J. Dias**[1]

Received: 4 December 2019 / Accepted: 18 March 2020 / Published online: 6 April 2020

Abstract
The blockchain technology first emerged with the Bitcoin whitepaper, which was the first successful proposal to implement a decentralized digital currency with ability to execute completely non-reversible transactions without a trusted and centralized third party. Blockchain concept provided an inherent part of this decentralization together with hash-based proof-of-work, public key cryptography, and peer-to-peer network. Even though blockchain technology was introduced to solve the double-spending problem of electronic money without relying on a trusted third party, this particular concept is being researched and already used to solve problems in many other areas. This paper captures concepts of blockchain, its applications, issues, and suggested improvements referring to blockchain-related subsequent publications.

Keywords Blockchain · Decentralization · Cryptocurrency · Blockchain concepts · Blockchain types · Blockchain issues

Introduction

Blockchain concept was introduced with the Bitcoin whitepaper to solve the double-spending problem, when executing a transaction over a communication medium without relying on a trusted third party like a financial institution or a bank [1]. First public blockchain behind Bitcoin was developed with a specific set of functionality in mind, namely decentralized currency and peer-to-peer electronic cash applications. Therefore, Bitcoin blockchain was practically difficult to customize and had very low programmable support using a scripting system called Script for other purposes. Vitalik Buterin noticed this difficulty and introduced Ethereum blockchain platform with a built-in turing complete programming language, allowing anyone to write programs called smart contracts and run decentralized applications. Protocols like currencies, identity systems, and reputation systems can be implemented with a minimal number of code to be run on Ethereum platform [2]. With the introduction of Ethereum platform, people further started to realize the real virtue of blockchain applications and researched on building alternative applications on top of blockchain technology. In addition to building alternative applications on existing blockchains, new blockchains and software stacks to build new blockchain technologies emerged to expand the success of blockchain. The technology has grown rapidly with wide adoption and investments, whereas much of the created value captured on its protocol layer, unlike in the internet era where value captured in application layer. Therefore, we believe that blockchain technology requires a formal definition and categorization of types for academic and industrial purposes. The increasing popularity of blockchain-based cryptocurrencies has made scalability a primary and urgent concern [3]. Scaling the volume of transactions processed at a given point of time is a key factor for scaling blockchain, and this low transaction throughput for blockchain is a known issue, but fixes for the issue introduce another problem—each transaction block takes a certain amount of storage space in the nodes in the network; when the number of transactions increases rapidly, the storage space required in each node also increases, resulting in a gradual decrease in number of full nodes. When addressing issues in blockchain such factors need thorough consideration, making it even more tricky to scale blockchain in order to match high transaction processing speeds of Visa.

✉ H. T. M. Gamage
2017_tharindu@kln.ac.lk

H. D. Weerasinghe
hesiri@kln.ac.lk

N. G. J. Dias
ngjdias@kln.ac.lk

[1] Department of Computer Systems Engineering, Faculty of Computing and Technology, University of Kelaniya, Kelaniya 11600, Sri Lanka

The objective of this paper is to explore deep into blockchain concepts, types, its applications, issues, and improvements studying the published work found in the literature such as academic journals, technical reports, and conferences. Survey paper aims to provide a comprehensive and detailed reference for blockchain-related future preliminary technology studies. In this survey, we aggregate all the core concepts of blockchain technologies for future researchers and readers who are initiating their studies in the particular technology. Once we started researching this technology, many of the concepts were scattered on different sources such as academic journals, technical reports, books, and research papers. With this paper, we believe that we save quite a lot of time for future readers by presenting blockchain technological terms together within a single survey with heaps of useful technical details. We also come up with formal standard categorizations of blockchain types combining different types of blockchain variations currently available. Blockchain applications we present within the paper are useful for readers to imagine the possibilities beyond decentralized currencies. Issues and improvements are also discussed finally within the paper so that readers would be aware of the platform issues and can come up with improved solutions on top of blockchain.

The remainder of the paper is organized as follows. In "History" section, we provide details about the history of blockchain and cryptocurrencies. In "Blockchain Concepts" section, we present blockchain concepts in detail that are useful to understand the rest of the paper. In "Consensus Algorithms" section, we discuss different consensus algorithms used in popular blockchains to achieve agreement among its nodes. Then, we discuss two main types of blockchains we have categorized and its variations in "Blockchain Types" section. Blockchain applications as well as fat protocols and thin applications concept are discussed in "Applications of Blockchain" section, while main issues of blockchain and its improvements are presented in "Issues and Improvements" section. We conclude the paper in "Conclusion" section.

History

Protocols for decentralized digital currencies and decentralized applications were rumored since 1980s, but the concept of blockchain and first successful decentralized digital currency emerged with the Bitcoin whitepaper in late 2008. Early e-cash protocols were mostly reliant on a cryptographic primitive known as Blind Signature, which was introduced by David Chaum [4]. In 1990 Chaum founded the first digital currency called Digicash through Digicash Inc. to commercialize his research idea. Digicash failed to gain traction due to their reliance on a centralized third party, and the company went bankrupt by 1998. E-gold was another centralized digital currency which was established in 1996 and became successful to scale up to 5 million users within 13 years, until transfers were suspended due to legal reasons [5]. Even though E-gold was suspended due to hackers and fraudulent companies using the platform for illegal activities, centralized aspect of the currency made it possible to close the entire system. Wei Dai's b-money became the first proposal to introduce the idea of creating money through solving computational puzzles and decentralized consensus, but the proposal did not include sufficient information on how to implement decentralized consensus [6]. Hal Finney introduced a concept of reusable proof-of-work [7] to create cryptocurrency using ideas from b-money together with solving Adam Back's computationally difficult Hashcash puzzles [8], but yet again failed to succeed with its reliance on trusted computing as a backend.

The first successful cryptocurrency and blockchain application was released in 2009, combining concepts of public key cryptography with a consensus algorithm known as proof-of-work [1]. Satoshi Nakamoto invited Hal Finney, who originated reusable proofs-of-work concept, to test his implementation and the first successful bitcoin transaction happened between these two users. Namecoin was the first fork to Bitcoin in order to implement a decentralized domain name service using Bitcoin's blockchain. Thereafter, several cryptocurrencies created out of Bitcoin forks and many failed due to less public attraction and pre-mining. A currency called Litecoin was introduced in late 2011 from a fork of Bitcoin code, basically the concept was almost similar but with faster transaction confirmation time by reducing block processing time from 10 to 2.5 min using scrypt-based proof-of-work. The Ethereum whitepaper [2] and yellow paper [9] introduced a built-in turing complete programming language to write and execute smart contracts and decentralized applications easily on top of Ethereum Virtual Machine and Ethereum blockchain; this customizable support was minimal with the Bitcoin blockchain implementation. Ethereum community proposed ERC standards, in other words application level standards for creating tokens, name registries, library formats, and many more. Out of these accepted standards, ERC-20 token standard became hugely popular among blockchain users due to its simplicity to create tokens. Initial Coin Offerings are public offers of new cryptocurrencies in exchange of existing ones, aimed to finance projects in the blockchain development arena [10]. ICOs are managed through smart contracts running on decentralized blockchains. ERC-20 tokens became the de facto standard of Initial Coin Offerings and crowdfunding for Ethereum blockchain-based decentralized applications due to its simplicity.

Cryptocurrency history has been colored by its association with crime [11], which is also a black mark on the sound

technology behind it. Silk Road used to be a popular online anonymous marketplace operated from 2011, which used Bitcoin as the exchange currency [12], but seized and shut down by the FBI in 2014 due to the selling of controlled substances and narcotics. In the early days of Bitcoin mining, compromised PCs have been used to mine Bitcoin [13]. The impact for organizations can be disastrous as the mining process drains processing resources from infected hosts. For the botnets owners, the gains are significant as thousands of dollars in cryptocurrency can be generated easily. Monero has been mined massively exploiting security vulnerabilities in Windows PCs similarly [14]. Over 27 million US dollars were extorted from victims during 2014 using CryptoLocker ransomware trojan. Computer files of the victims were encrypted and hackers demanded a ransom—in the form of bitcoins or a prepaid voucher, which makes tracing the payments more difficult—to decrypt the files and make them accessible again [15]. It is also reported that many cryptocurrency exchanges have collapsed and disappeared during the past, with customer account balances often wiped out [16].

Blockchain Concepts

Blockchain can be defined as an immutable distributed digital ledger, which is secured using advanced cryptography, replicated among the peer nodes in the peer-to-peer network, and uses consensus mechanism to agree upon the transaction log, whereas control is decentralized. With this definition, paper identifies following concepts as the core concepts to unwrap the meaning of blockchain—immutable, distributed, digital ledger, cryptography, peer-to-peer network, consensus mechanism, decentralization.

In accounting, a ledger is a place to record and store all the transactions with regard to an entity. A digital ledger could be a computer file, or database, or even distributed database like blockchain, where transactions are recorded electronically. Blockchain transaction ledger is pretty unique to other ledgers in a manner, which ensures that transaction log is computationally impractical to change, as long as honest nodes in the network control the majority of CPU power, thus making it immutable. The origins of ledger can be traced back to over 5000 years ago in Mesopotamia. The Earliest and simplest form of recording transactions is called single entry accounting, which enters transactions into a list to keep track of adding or deducting assets. The single entry accounting was managed by owners or family members, as this kind of recordings are error-prone as well as difficult to track down, when recorded fraudulently. Double entry accounting added a clear strategy to identify and remove errors, where there are two entries recorded against each transaction, so that the ledger is balanced all the time. Grigg proposed triple entry accounting in 2005, an alternative to traditional double entry accounting, which secures transactions using cryptography in order to make it difficult to change [17]. Blockchain implements triple entry accounting concept to permanently store transactions in blockchain, ensuring that the sender has authority to execute non-reversible transactions using public-key cryptography.

Cryptography can be defined as techniques used for secure communication to protect confidential information, in the presence of adversaries. Blockchain uses concepts from public key cryptosystems to verify the authority of the user to execute transactions, and cryptographic hash functions to achieve consensus between network nodes on blockchain data. The use of public key cryptosystems to provide digital signatures was suggested by Diffie and Hellman [18]. Digital signatures, whether based on public key cryptosystems, conventional encryption functions, on probabilistic computations, or other techniques share several important properties in common—such as an easier way for the sender to generate the personal digital signature, convenient way for receiver to verify the sender of the message, but must be impossible to generate someone else's digital signature by others. In public key cryptography, there exists two keys called public and private and a function or cypher algorithm to encrypt the original text into a ciphertext using the private encryption key. Sender or owner generates the public–private key pair and keeps the private key as the confidential key to encrypt information; public key is distributed to anyone to verify that the information is digitally signed by the original owner. This public key cryptography technique is used in blockchain to verify the ownership of coins or tokens, whenever transferring coins or tokens. One another important concept used in blockchain to secure its data integrity is *cryptographic hash function*—a one-way function that maps strings of arbitrary size into a bit string of fixed size called hash using a mathematical algorithm. An algorithm required for blockchain hash functions has three main properties—same input should always result in with the same output hash, given the hash no algorithm could produce the original input, small changes in input results in completely different output hash. Bitcoin uses SHA-256 hash function, whereas Ethereum uses Ethash, and Litecoin uses Scrypt when hashing its block data.

Every blockchain implements a consensus mechanism to agree upon the correctness of the data between nodes; the most common algorithm is the proof-of-work consensus mechanism. Peer-to-peer network of nodes hold the replicated data of the blockchain, messages are broadcast on a best effort basis, nodes can leave and join the network at will, accepting the longest proof-of-work chain as proof of what happened when nodes were offline [1]. Nodes in the network collect new broadcast transactions and form a tree like data structure of hashed transactions into a block

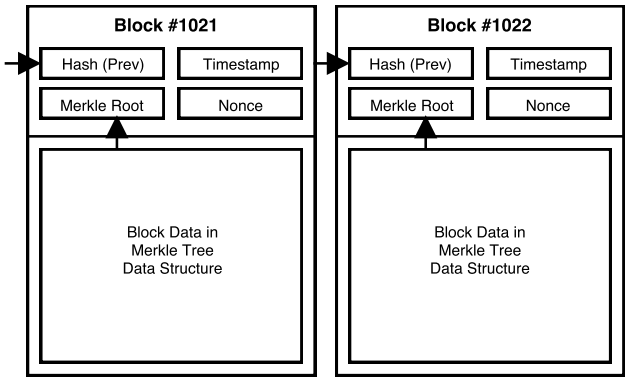

Fig. 1 General block structure in blockchain

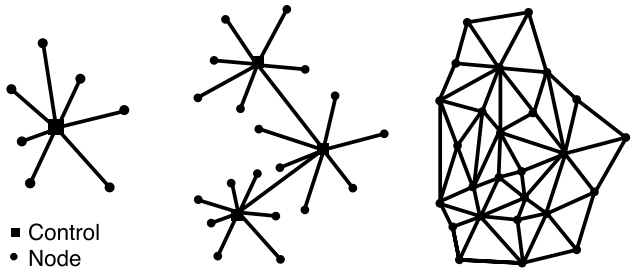

Fig. 2 Centralized, decentralized, and distributed networks

and then compete with each other to solve a difficult hash-based proof-of-work. First node, who solves the proof-of-work, broadcasts the block with answer for others to verify and append into their existing blockchain. Nodes accept the block only if all transactions are valid and not already spent; acceptance is expressed by working on creating the next block with hash of the accepted block as previous hash. Miner of the block, who solved the difficult proof-of-work, receives freshly minted coins as reward for contributing their computing resources for solving the function.

A block contains a header and transaction data similar to Fig. 1. The block header has four pieces of information, namely hash of the previous block, time stamp, nonce, and hash of the Merkle tree root. Merkle tree root hash is a unique identifier for all the transactions combined inside the block. Once a block with transactions is confirmed into the blockchain, changing, deleting, or altering data becomes computationally impossible. Changing transaction data in a block changes the root hash of the Merkle tree stored in block header; thus data will be rejected by other nodes in the network. Replacing a complete block from a random position is impossible as blocks are chained together using hash of the previous block. Presenting a different block in the chain will also result in a mismatch of data between other nodes in the network; as long as the majority of CPU power is controlled by honest nodes, it is not possible to force a fraudulent block into the chain, making the blockchain immutable.

Bitcoin's blockchain is a decentralized technology for executing e-cash transactions, but it is also an example for distributed ledger technology. In order to understand this, we have to consider the differences between three terms—centralized, decentralized, and distributed as illustrated in Fig. 2. Centralization and decentralization refer to control levels, whereas distribution refers to physical location. In a centralized system, control is handled by a single entity, but in a decentralized system control is handled by different independent entities. A non-distributed system resides in a single location, whereas distributed system resides in multiple physical locations. A distributed system can either be centralized or decentralized. A cloud service provider offering data storage would have storage facilities around the globe to have greater uptime and easier access, but its control access is centralized. Public blockchains like Bitcoin and Ethereum are examples of distributed and decentralized systems. Bitcoin and Ethereum blockchain systems cannot be altered by a single entity, thus making it's control decentralized, as well as blockchain data replicated and shared on a peer-to-peer network of independent nodes in different locations around the globe, making it distributed.

Tree Authentication was first proposed as a way to reduce storage requirements and quickly authenticate a randomly chosen value's presence with lesser memory requirement [19]. Merkle trees are a fundamental part of what makes blockchains tick. Although it is definitely theoretically possible to make a blockchain without Merkle trees, simply by creating giant block headers that directly contain every transaction, doing so poses large scalability challenges that arguably puts the ability to trustlessly use blockchains out of the reach of all but the most powerful computers in the long term [20]. A Merkle tree composed of a set of nodes with large number of leaf nodes at the bottom containing the underlying data, a set of intermediate nodes where each node is hash of its two children, and finally a single root node from hash of its two children. The Merkle tree in bitcoin is constructed by recursively hashing pairs of transaction data until a root hash is reached called the Merkle Root, which is then stored in the block header as a pointer to the transaction data in block. As stated in the below diagram, hashes propagate upward with transaction data at the bottom of the data structure, changing any transaction at bottom results in a different hash and subsequently not matching the other hashes and resulting in a new data structure with a completely different root hash. Such malicious blocks will be rejected by honest nodes in the network, as long as the majority of the control is among the honest nodes. In Bitcoin network proof-of-work algorithm, it is one-CPU-one-vote, thus can outpace attacker nodes with the majority of faster computing honest nodes. Similar to proof-of-work

algorithm different blockchains occupy different consensus algorithms as discussed in the next section to achieve agreement between nodes.

Merkle tree as in Fig. 3 is a very efficient data structure to verify the existence of a particular data within the tree. Even when a tree consists of a large number of child nodes at bottom, by comparing hashes from only the relevant part of the tree, the existence of a particular data within the tree can be verified. This relevant part of the tree is called authentication path for the value and can be calculated using the algorithm proposed by Ralph Merkle [19]. Merkle tree is essential for the long term sustainability of the network, when blockchain grows over time full nodes take huge gigabytes of data storage making it difficult to run full nodes within personal computers. Simplified Payment Verification nodes could be setup by storing only the block headers of the longest chain, and obtain only the Merkle branch linking the transaction to the block it is timestamped in from a full node to verify the transaction.

Consensus Algorithms

Consensus algorithms are the mechanisms in which nodes in the blockchain network achieve agreement on the validity and authenticity of transaction or data blocks. Since the blockchain transaction ledger is decentralized, consensus mechanism is the core process, which verifies and secures block of transactions by doing two things. The consensus algorithm first ensures that the next added block is the one and only version of the truth. Secondly algorithm prevents any adversaries from successfully derailing the chain. Any decentralized system including currencies need to solve the problem called Byzantine generals problem to achieve a consensus when the system expects adversaries to attack its expected behavior.

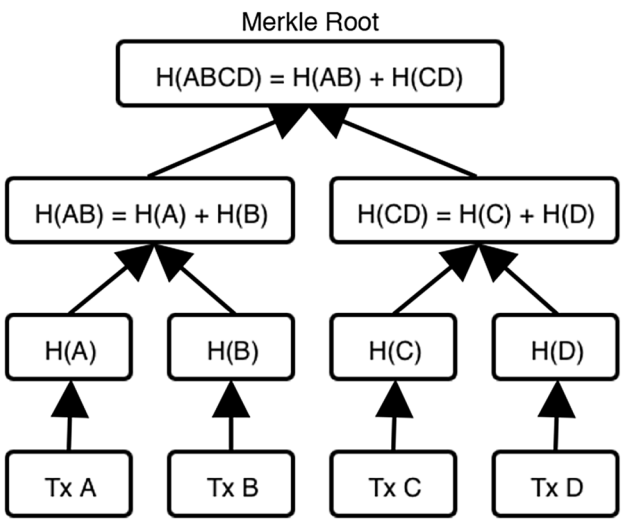

Fig. 3 Simplified version of Merkle tree data structure

In Byzantine generals problem, a set of generals need to organize a coordinated attack against an enemy city. But the generals are far apart so that commanding general needs to send a message to all other lieutenant generals using a messenger about the time for the attack. But during this setup there can be one or more traitors who would confuse others by sending conflicting information [21]. In order to achieve consensus, the commander and lieutenants must agree on the same decision either to attack or retreat, even when the commander can be a traitor. Lamport, Shostak, and Pease argue that there is no solution for Byzantine generals problem when there are three generals with one possible traitor. The paper proves that there should be at least $3m + 1$ or more generals to cope with m possible traitors. In other words, consensus could not be reached if there are more than one third of traitors. It is believed that Byzantine faults are difficult to deal with no assumptions about the behavior of its nodes in the network. Blockchains are decentralized ledgers with no central authority, thus potential to be attacked by malicious nodes for huge economic incentives. Therefore, Byzantine fault tolerance is much needed in the blockchain and consensus algorithm on blockchain solves the Byzantine problem.

The initial algorithm to the Byzantine problem proposed by Lamport, Shostak, and Pease is not efficient enough in terms of number of messages required to achieve consensus with a higher number of possible traitors. Many different ways have been proposed and implemented to achieve consensus on a decentralized blockchain. The algorithms differentiate from each other primarily by how they delegate and reward verification of transaction blocks. Examples of consensus mechanisms used on blockchains are proof-of-work, proof-of-stake, delegated proof-of-stake, proof-of-importance, directed acyclic graph, and practical Byzantine fault tolerance.

Proof-of-Work

Satoshi Nakamoto proposed proof-of-work chain to solve the Byzantine Generals Problem in bitcoin blockchain, which is also the most popular algorithm used on many other blockchains. Proof-of-work powered blockchains currently account for more than 90% of the total market capitalization of existing digital cryptocurrencies [22]. Proof-of-work requires nodes in the network to solve complex mathematical one-way functions before they could add blocks into the blockchain. The process of finding correct proofs solving cryptographic functions is called mining, and the nodes or individuals participating in this process are called miners. Characteristics of cryptographic one-way functions were discussed in "Blockchain Concepts" section, which makes

the only way to find a solution to the function is by brute force. Therefore probabilistically, the ones with the majority of CPU power have more opportunity to find the answer for the function in proof-of-work algorithm. As a reward for solving the complex mathematical function by expediting computational power and electricity, miners are rewarded with newly minted coins, which are also called the block reward. Miners compete with each other to find the correct hash value with a dynamically adjusting difficulty in the algorithm, which ensures block interval to be consistent. The proof-of-work difficulty is an intrinsic feature for security as it prohibits the adversary from flooding the network with messages and gives the opportunity to the honest nodes to converge to a unified view [23]. Proof-of-work algorithm-based Bitcoin blockchain generates blocks in every 10 min, Litecoin in 2.5 min, and Dogecoin in every 1 min. As soon as a miner finds the correct hash value for the proof-of-work chain, miner broadcasts the message to the network and nodes verify the hash value and accept the value by working on the next block, with the verified value as the hash of the previous block. Since proof-of-work requires brute force effort to figure out the hash value for the block, the process is very energy and resource intensive, with the difficulty and block storage ever increasing, proof-of-work-based blockchains also have possible risk of centralization for miners. In a pure proof-of-work cryptocurrency, security depends on the mining market, while network mining income and sum of all miners income is a direct measurement across competing proof-of-work blockchains [24]. Bitcoin with high rewards for its miners dominates proof-of-work blockchains. It is also believed that the only way to attack the proof-of-work-based blockchain is to own the majority of total computational power called " 51% attack", which will be discussed in "Issues and Improvements" section.

Proof-of-Stake

In proof-of-stake, the algorithm chooses individuals called validators to generate blocks based on a defined criteria. The criteria defines how validators are selected to vote and generate blocks based on their economic stake in the network, thereby rewarding users who are conserving long term value of the blockchain. The probability of being selected as a validator increases depending on the amount of coins held in the individual's wallet. But the proof-of-stake systems also use a randomization or coin age-based approach to make sure individuals with the highest number of stake will not always get priority. Coin age is the value of coin amount multiplied by the number of days that the coins have been held in the wallet. Coin age is simply defined as currency amount times holding period [25]. Therefore, with a coin age-based proof-of-stake system an individual holding a large amount of coins for a lengthy period is more likely to be selected to generate a block. The rationale behind proof-of-stake is that entities who hold a stake in the system are well-suited to maintain its security, since their stake will diminish in value when the security of the system erodes [26]. Proof-of-stake-based system requires significantly less amount of energy and less computing resources compared to proof-of-work-based system to operate, as in proof-of-work blockchain, where all nodes compete with each other solving countless complex mathematical functions to append the next right block. In Proof-of-Work networks mint rate slows gradually, eventually forcing miners to raise transaction fees to sustain security, in addition to high resource and energy consumption. Proof-of-Stake eliminates both these issues in the long run. Blackcoin, PeerCoin, and Nxt are examples for proof-of-stake-based blockchains. Ethereum's upcoming Casper implementation will also use proof-of-stake algorithm. Casper's implemented incentives mechanism ensures liveness, while providing safety guarantees that improve over standard Proof-of-Work protocols [27]. The main problem with proof-of-stake is called " nothing-at-stake" problem, when working on multiple forks of the chain, which will be discussed in "Issues and Improvements" section.

Delegated Proof-of-Stake

Delegated proof-of-stake is a variant algorithm of proof-of-stake, where an elected list of nodes called block producers or witnesses generate blocks in the network, in turns. This approach is much more scalable than proof-of-work and also proof-of-stake as the number of block producers are limited. The coin holders of the network vote proportional to their coin stake in order to elect a list of block producer nodes, which generate transaction blocks to append into the delegated proof-of-stake blockchain. Coin holders as voters can also fire the block producers, if they found to be malicious. Block validators run full nodes, so that they can verify that the block producers follow consensus algorithm. In delegated proof-of-stake-based blockchain, not all validators are block producers but anyone can become a validator by running a full node. Due to the fixed list of block producers, delegated proof-of-stake allows to generate a new block at fixed rate with minimal computational requirements. This means that the blockchain can process more transactions in significantly less time and at almost no cost compared to proof-of-work-based blockchains [28]. Unlike some competing algorithms, delegated proof-of-stake can continue to function when a majority of producers fail. During this process the community can vote to replace the failed producers until it can resume full participation [29]. Delegated proof-of-stake algorithm sacrifices decentralization concept in blockchain to achieve high transaction throughput, which is criticized by blockchain community and regarded as an improper consensus mechanism for blockchains that handle

transactions. EOS, BitShares, Steemit, and Lisk are examples for delegated proof-of-stake blockchains.

Proof-of-Importance

New Economy Movement Foundation introduced proof-of-importance consensus mechanism in their blockchain for XEM coin. Proof-of-importance is similar to proof-of-stake except that it does not entirely depend on coin stake. With proof-of-importance algorithm, each node is assigned an importance score that showcases its aggregate importance to coin's economy. A node with higher importance score has higher probability for generating or harvesting blocks. Since all transactions are publicly available, transaction graphs can be calculated and used as an input into the importance of an account. It incorporates factors such as total spent in the last 30 days, vested amount of currency, and interconnection between other nodes in the graph as a measure to be selected as a harvester to generate blocks. Using these factors, proof-of-importance attempts to reward active economy participants at the expense of inactive users and diminishes chances of rich getting richer effect, which is possible with proof-of-stake [30]. Harvesters receive fees as a financial reward for generating blocks. To be eligible for entering the importance calculation in NEM, account must have a minimum of 10,000 XEM balance.

Directed Acyclic Graph

Need for transaction fee is eliminated with the concept of Directed Acyclic Graph. Transactions issued by the nodes constitute a tangle graph, which is the distributed ledger for storing transactions. A node must verify two previous transactions in order to add a new transaction into the ledger, by doing this transaction fee is reduced to zero. No node in the network can reference back to itself and therefore called acyclic. The approach is lightweight and easily scalable, but the network becomes faster and secure, when more and more participants continuously add new transactions. IOTA implements a successful directed acyclic graph called tangle as the consensus mechanism. The algorithm used in the IOTA implementation is structured such that the time to find a nonce is not much larger than the time needed for other tasks that are necessary to issue a transaction. The approach is much more resistant against quantum computing and therefore gives the tangle much more protection against an adversary with a quantum computer when compared to the Bitcoin blockchain [31].

Practical Byzantine Fault Tolerance

Byzantine fault tolerance we discussed previously is considered too slow to be used in practice with its synchronous behavior. Practical Byzantine Fault Tolerance addresses this weakness and can be used in an asynchronous environment with improved response time with an order of magnitude compared to other Byzantine fault tolerant algorithms [32]. Practical Byzantine fault tolerance is commonly used in permissioned blockchains as a consensus mechanism. It usually uses less than 20 pre-selected validator nodes as message count exponentially increases with the increase of number of nodes. As the message count required for consensus is lower for a selected limited number of participants, the algorithm is pretty energy efficient and mainly used only in permissioned blockchains for enterprises, where a limited number of participants are involved and the participants are partially trusted.

Blockchain Types

According to our survey findings, blockchains can be categorized into two main types namely permissionless blockchains and permissioned blockchains.

Permissionless Blockchains

Permissionless blockchains do not enforce any restrictions on its nodes; anyone can openly read data, inspect data, and participate in validation and writing of the data in accordance with the consensus protocol of the particular blockchain. Bitcoin, Ethereum and many other cryptocurrencies run on permissionless blockchains. These blockchains are considered fully decentralized and secured using advanced cryptography, whereas economic incentives are provided for users who work to keep the integrity of the network. The transactions are completely irreversible on a permissionless blockchain by its design, meaning once confirmed by its nodes the blockchain transactions cannot be reversed. Due to the security considerations and strict restrictions, transaction throughput of a permissionless blockchain is comparatively lesser than one of a permissioned blockchain. Permissionless blockchains are fully decentralized and transparent.

Permissioned Blockchains

Permissioned blockchains restrict the writing access for a limited set of participants, and a consensus mechanism is used to validate the writing of data among its privileged participants. Read access could either be open to anyone or closed to the public based on the requirement of the permissioned blockchain. This type of blockchains has evolved as an alternative to initial permissionless blockchains, to address the requirement for running blockchain technology among a set of known and identifiable participants that have to be explicitly responsible to the

blockchain network, while participants need not be fully trusting each other [33]. The permissioned blockchains are mainly useful for business and social applications, which requires blockchain distributed ledger technology without the need of a incentifying cryptocurrency. Based on the read access mentioned, permissioned blockchains are further divided as open and closed—open permissioned blockchains are partially decentralized, anyone can read its data, whereas closed permissioned blockchains are fully centralized, data is visible only to the participants.

We thoroughly believe blockchain technology is rather necessary only for permissionless blockchains, and open permissioned blockchains. Closed permissioned blockchains can be argued as restricted distributed databases which are facelifted with the blockchain term. The initial idea of introducing blockchain concept was to remove centralization and add transparency to everyone to read and update its data. Open permissioned blockchains mostly adhere to this principle of transparency even though somewhat centralized in writing its data and could be useful for applications such as identity systems, academic certification systems, where anyone can read its data but only a certain set of participants are privileged to write the data into blockchain. Closed permissioned blockchains are fully centralized and also not transparent to anyone, dismantling the core concept of a blockchain. Therefore, these blockchains can be replaced with distributed database systems with restrictions implemented on top of it. For example, a supply chain management system for a private organization can be implemented without the concepts of blockchain. In order to support our argument on closed permissioned blockchains, we have presented a characteristic comparison of different blockchain types compared with restricted distributed database systems in Table 1. The comparison shows that all of the characteristics in closed permissioned blockchains are comparatively similar to that of restricted database systems. In addition to this categorization, there is also another blockchain categorization called public, consortium, and private blockchains [34]. In simple terms, public blockchains are permissionless blockchains, whereas consortium and private blockchains fall into permissioned blockchains.

Applications of Blockchain

Blockchain was introduced with Bitcoin whitepaper to resolve the double-spending problem of electronic cash in a decentralized environment. The first and most exciting application of blockchain is electronic cash. People have soon realized, the immutable distributed ledger technology and decentralized concepts behind blockchain can be further customized and used for several other applications like smart contracts, property title registries, digital voting, supply chain management, identity management, digital ownership management, and many more. Therefore, a considerable amount of research and development has since been started on applications of blockchain and further new researches are emerging everyday on possible future applications.

When we discuss blockchain applications, it is important to understand the concept of fat protocols and thin applications as well. A protocol is a commonly accepted, well-defined set of rules and guidelines, which could be used to build applications. Rules and guidelines are defined for each and every step of the process to be followed by the particular application. The main difference between Internet and Blockchain lies how the value is captured on the protocol layer. Internet stack runs on top of open protocols like TCP/IP, HTTP, HTTPS, SMTP, IMAP, etc. The internet works because of TCP/IP, Web works because of HTTP and HTTPS, and the Email works because of SMTP and IMAP, etc. These open protocols allow different applications to communicate with one another, and work together, producing immense amounts of value. Even though open protocols make internet work seamlessly, the produced value is captured by applications run on it. For example, Facebook, Twitter, and Gmail captures huge value running on top of these open protocols, whereas protocols receive significantly less value and attraction in return. In other words, investing

Table 1 Characteristics of blockchain types and restricted distributed database systems

	Permissionless blockchain	Open permissioned blockchain	Closed permissioned blockchain	Restricted distributed database
Public read access	Available	Available	Not available	Not available
Public write access	Available	Not available	Not available	Not available
Immutability	High	Medium	Low	Low
Throughput	Low	Medium	High	High
Scalability	Low	Medium	High	High
Decentralization	High	Medium	Low	Low
Distribution	High	Medium	Low	Low
Auditability	High	High	Low	Low

in applications results in high returns, whereas investing in protocols would result in low returns. As a result, many of the internet open protocols are currently maintained by non-profit organizations. Thus, the internet stack is composed of thin protocols and fat applications in terms of how the value is captured. In contrast, blockchain stack is composed of fat protocols and thin applications in terms of how value is captured. Value is concentrated at the open protocol layer and only a fraction of its value is distributed along at the application layer [35]. In order to understand this value distribution, we can consider market capitalization of two main blockchain networks, Bitcoin and Ethereum. The Bitcoin network has a market capitalization of over 200 billion USD as of June 2019, yet the largest companies built on top of multiple cryptocurrencies such as Coinbase valued only few billions. Similarly, Ethereum network has a market capitalization of over 30 billion currently, yet applications built on top of Ethereum are yet to make an impact to get even a fraction of its value. And the most valued tokens for largest exchanges like Binance, Bitfinex, built on top of Ethereum are worth around 4 billion and 1 billion, respectively. Therefore, it is clear that protocol layer captured a significant amount of value in blockchain, and the concepts that made this possible are also a novel innovation of blockchain.

Two factors which made capturing value at protocol layer a reality are shared data layer and cryptographic tokens introduced with blockchain. Firstly, the shared data layer on blockchain enabled an ecosystem, in which anyone can enter and build competitive applications without restrictions on data access. Previously, information gathered by internet-based applications added restrictions on how other competitors or new entrants could access the information through APIs, sometimes even totally closed for other entrants as information is centralized. For example, switching from one cryptocurrency exchange to a newly found exchange is almost just a matter of the decision due to shared data layer, when compared to switching from Gmail to new email service provider, when all of your data is pretty much stored at a centralized place over a long period of time. Thereby, the shared data layer factor, restricted creating large monopolies over an open blockchain protocol, forced the market to find new ways to reduce costs, and provided an opportunity to invent better products. Secondly, economic incentives provided as cryptographic tokens in blockchain are the other key factor, which incentivizes protocol development and adoption. Blockchains provide the mechanism to issue cryptographic tokens digitally, which could be issued either on top of an existing blockchain, or on a completely separate blockchain. Startups for creating new blockchain protocols and applications can now issue cryptographic tokens as a way to raise funds for the startup, usually by also keeping a stake of tokens in hand for the future growth. The issued cryptographic tokens would be the payment method to use the application features, as well as rewarding mechanism for contributing users. The value of the token is appreciated and adjusted based on the success of the startup. The stakeholders of the token also work towards promotion and speculation of the new application, as they have already invested in its success. The supply of the tokens is usually pre-defined and fixed at a maximum token amount that will ever be generated over a period of time in future at a defined rate. Since the tokens are limited in amount, if the interest on the application grows a lot faster than supply of the tokens, it could perhaps lead to bubble-style appreciation in token value. Except for fraudulent schemes, this appreciation of tokens is beneficiary for the blockchain application creators, as they can create money by selling some of their previously retained tokens, when the token value is higher, also retain tokens further expecting future value appreciation. With that, they would continue to expand their applications expecting further value appreciation. The appreciation in value will attract more new users and stakeholders to invest in applications and protocol. The process may continuously function as a loop for blockchain applications, expecting further appreciation in value. The significance of this process is that the market capitalization of original protocol grows much faster than the combined value of applications built on top, since the success of application layer promotes further adoption in protocol layer [35]. As described, shared data layer, and cryptographic tokens in blockchain aggregates created value in protocol layer, unlike in internet protocols, where individual applications aggregated huge amounts of value created by internet protocols. Therefore, blockchain stack is composed of fat protocols and thin applications, backed by shared data layer and cryptographic tokens as shown in Fig. 4.

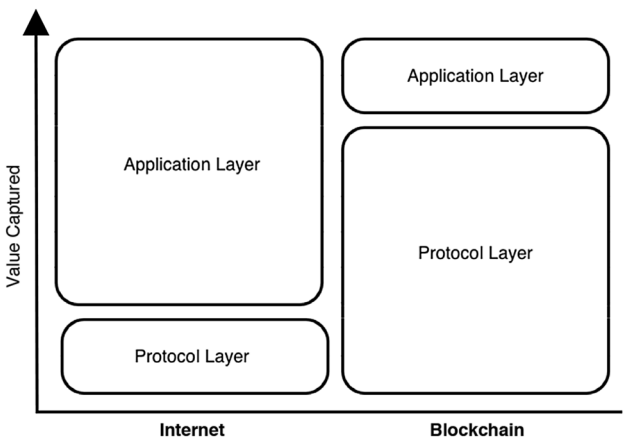

Fig. 4 Value captured on protocol layer and application layer, internet versus blockchain

Currency

Decentralized Currency was the founding application of blockchain technology with the implementation of Bitcoin. Blockchain-based currencies are called cryptocurrencies in general and can be categorized into two main types called coins and tokens. Coins run on a separate blockchain of its own, whereas tokens run on top of an existing blockchain. For example, Ethereum is a standalone coin and a cryptocurrency which runs on Ethereum's blockchain. But ERC-20 tokens such as Binance Coin, Tether USD, Maker, and Basic Attention Token are cryptocurrencies that run on existing Ethereum blockchain, therefore considered as tokens. Similar to fiat currencies, cryptocurrencies also have an associated value based on the trust people have on the particular cryptocurrency. Even though coins mainly serve the purpose of a currency, tokens are usually representation of an asset for a product, service, an investment, or even a right. Well-accepted cryptocurrencies are open source, and new coins are generated from a computational process defined with a consensus mechanism accepted by its community forming the immutable blockchain of the particular cryptocurrency. Several consensus mechanisms used on different blockchains to keep the trust among its users have been discussed in "Consensus Algorithms" section. These mechanisms ensure the integrity and immutability of the blockchain-based cryptocurrency ledger without central authority controlling it's management. As of today, there are thousands of cryptocurrencies among circulation and 15 of them have already passed market capitalization of over 1 billion US dollars [36]. Bitcoin leads the market with a market capitalization of over 180 billion US Dollars, with a coin valued over 10,000 dollars as of today, although this value is highly volatile. USA, Netherlands, Canada, South Korea, and a few other countries are progressively open for Bitcoin as a payment method. Bitcoin can be exchanged directly between two participants as a payment without involving a third party, or even can be changed into another form of currency using an exchange nowadays. Cryptocurrencies are also considered by some central banks as an external asset, when researching on diversifying their portfolio of assets [37]. Most popular blockchain-based currencies are Bitcoin, Ethereum, Ripple, Litecoin, Bitcoin Cash, Binance Coin, EOS, Tether, Bitcoin SV, Steller, Tron. The blockchain-based currencies have been proposed to serve different purposes and some of the currencies have sacrificed decentralization in order for higher transaction throughput as listed in Table 2.

Smart Contracts

Self executing contractual clauses in the form of Smart contracts can be embedded in hardware and software in such a way that makes breach of contract expensive for the breacher [39]. Even though the concept has been discussed since the late nineties, the platforms to execute smart contracts without third party involvement were possible only after the introduction of blockchain. Mutually distrustful parties can transact with each other using smart contract systems over decentralized currencies, while contractual breaches are addressed using the blockchain ensuring honest parties obtain commensurate compensation [40]. Blockchain provides a decentralized tamper-proof open platform to run self executing smart contracts, when terms for the participants have been satisfied. A smart contract is written as a tiny program and executed on blockchain automatically without third party involvement, when programmed conditions meet. Usually, in a smart contract the participants transfer units of currency into the contract once contractual terms are negotiated and programmed. The smart contract is automatically validated and executed on blockchain at a certain point of

Table 2 Most popular cryptocurrencies by market capitalization [23]

Cryptocurrency	Started	Market cap	Mining method, notes
Bitcoin	2008	$180,161,192,066	Proof-of-work (SHA-256)
Ethereum	2013	$23,946,557,985	Proof-of-work (Ethash)
Ripple	2012	$13,328,900,008	NA, Controlled by Ripple Labs
Litecoin	2011	$5,768,253,401	Proof-of-work (scrypt), Fork of Bitcoin
Bitcoin Cash	2017	$5,324,549,061	Proof-of-work (SHA-256), Fork of Bitcoin to increase block size
Binance Coin	2017	$4,450,667,739	NA, ERC-20 token premined by Binance exchange
EOS	2017	$4,162,880,697	NA, ERC-20 token distributed by block.one later moved to EOS mainnet
Tether	2014	$4,028,690,237	NA, Issued by Tether Limited
Bitcoin SV	2018	$2,818,645,358	Proof-of-work (SHA-256), Fork of Bitcoin Cash with different block size
Steller	2014	$1,652,660,513	NA, Open-source, Distributed by non-profit Steller Development Foundation
TRON	2018	$1,495,759,495	Delegated proof-of-stake [38]
Cardano	2017	$1,482,240,820	Proof-of-stake (Ouroboros algorithm)

NA not available

time as per the terms; then the funds in contract will be released for relevant party/parties if contractual conditions are met, or returned back to initial users, when conditions are not met. Blockchain not only offers the platform to execute smart contracts, but also mechanism for anonymous participants to execute trusted irreversible transactions without involvement of centralized third party. Immutability, self-execution, cost-effectiveness, accuracy, inspectability, and trustlessness are key features of blockchain-based smart contracts. Both Bitcoin and Ethereum blockchains offer ability to execute smart contracts, even though Bitcoin blockchain has very less programmable support for smart contracts. Scripting provided with Bitcoin blockchain is scant of turing completeness, state awareness, value and blockchain awareness, thus making it very difficult to write smart contracts. Ethereum is the first blockchain platform, which was designed smart contracts and decentralized applications in mind. The Ethereum platform comes up with a fully fledged turing-complete programming language that is capable of creating "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems such as colored coins, smart property, name-coin as well as many others, simply by writing up the logic in a few lines of code [2]. Even though Ethereum platform provides much needed programmable support for smart contracts, it is currently limited in the number of transactions that can be processed per second. In addition to this scalability issue, similar blockchain-related issues will be discussed in detail under "Issues and Improvements" section. Zilliqa is a blockchain platform that is designed to scale in transaction rates, which also proposes a special-purpose smart contract language and execution environment that leverages the underlying architecture to provide a large scale and highly efficient computation [41]. EOS is yet another powerful smart contract platform which provides decentralized version of an operating system that scales up to millions of transactions per second [42]. Ethereum, EOS, and Zilliqa are few of the blockchain platforms that are optimized for writing and executing smart contracts on blockchain. Through a combination of written smart contracts, developers can build much complex decentralized applications that can be run on the internet without control of a centralized entity.

Property Title Registries

Property title registries can be listed as an important possible application of distributed blockchain technology. Written records of property rights have proven to be quite vulnerable to abuse by means like confiscation of land via forgery or destruction of public records. Reconstruction from informal records in such an event is also costly, error-prone, and potential for fraud. Direct transcription of written records into a centralized online repository of electronic records can make issues even worse with possible loss of data and forgery. Distributed title database prevents such attacks against property rights [43]. Blockchain would help to provide the platform with openly auditable distributed ledger to store property titles with immutable history. Anyone could publicly inspect the property records on blockchain with minimum cost. The open nature of blockchain property title records would also enable developers to come up with new applications providing easier ways for accessing, processing, and inspecting these records. Mainly, fraud elimination, transparency, cost-effectiveness, transfer of rights without third-party notary involvement are the key benefits of a blockchain-based property title registry.

Digital Voting

Blockchain-based digital voting is another important application which could run on an open permissioned blockchain. Elections are under threat from malicious actors that can infiltrate voting machines, alter voter registration databases, coordinate disinformation campaigns, compromise election reporting systems, and more. Transparency, immutability, and accountability characteristics of blockchain underscore the technology's potential for securing elections [44]. During pre-election, cryptography in underlying blockchain could help to ensure that digital content comes from a trusted accountable source, which reduces propaganda affecting voter judgments allegedly. During the election, blockchain's immutable distributed ledger could help to store identity data for authenticating voters, and help securely record digital votes for tabulation, thereby eliminating the risk of hacked voter databases and tabulation systems. Finally, after the election independent auditors and anyone in public may audit the election results recorded on an open permissioned blockchain, without revealing any information about individual voter identities. West Virginia has successfully run a mobile voting pilot project backed by distributed and redundant network of blockchain servers for military personnel, and their families working abroad to vote during 2018 midterm United States elections [45]. Even though the pilot project was said to be successful and showed interesting initiative towards blockchain-based voting, we believe that the project did not include sufficient transparency as the voting happened on a closed permissioned blockchain, and this limitation needs to be addressed. In conclusion, transforming paper-based and legacy electronic voting systems into blockchain-based digital voting systems would ensure voter confidentiality and transparency in digital voting.

Supply Chain Management

Supply chain management operations are dominated by paper-based methods requiring letters of credit with costs

nearly 1–3%, factoring with costs 5–10%, thereby increasing costs to an estimated trillion dollars and also slowing down transactions. Such additional costs could be reduced substantially, using blockchain technology that will eliminate intermediaries by establishing trust between buyers and sellers during this process [46]. Measurement of supply chain management is often described in terms of objectives such as quality, speed, dependability, cost, and flexibility. With the use of RFID tags, sensors, barcodes, GPS tags and chips, the locations of products, packages and shipping containers can be tracked real-time at each step of the supply chain [47]. The blockchain-based supply chain management application with above IoT applications could effectively establish trust among various parties by assuring firms receiving proper materials as well as customers assured on authenticity of the final products, indirectly making sure that the original producers and suppliers receive value for their effort against counterfeit products. Intermediate firms and customers may inspect the blockchain records in real-time to see the durations of materials at each destination to determine the speed of delivery and dependability of the materials. In case of a dispute, all relevant parties may go back and inspect immutable blockchain records to resolve the dispute, which adds flexibility into supply chain management. Therefore, a blockchain backed supply chain management system significantly enhances measurement objectives of supply chain operations in a transparent manner.

In addition to the applications discussed, Zīle and Strazdiņa lists nearly fifty blockchain use cases in their study such as cloud storage, identity data management, digital content publishing, academic certification, ride sharing, software license validation, health care record storing, and many more [48]. Considering the large amount of use cases, the future potentials in blockchain-based applications are enormous. The blockchain-based technological innovation and advancement is beneficial for the data security and preservation, while safe-guarding individual privacy. Estonia as a country looked more seriously into their electronic data security after a nationwide cyber attack in 2007, and founded their own KSI blockchain, becoming the first country to use blockchain on a national level. KSI is a blockchain technology designed in Estonia and used globally to make sure networks, systems and data are free of compromise, all while retaining full data privacy [49]. Estonia has digitized almost all of their government services with electronic identity for every citizen, including electronic health records, land registry, business registry, voting, and many other services with the help of KSI blockchain and cryptography. Generally, most of the applications developed for blockchain industry are currently related to Banking and Finance sector, but with time to come blockchain applications related to industries such as Insurance, Healthcare, Media, Entertainment, and other services tend to grow in numbers [50]. But when considering current blockchain applications, we believe that some of the applications with permissioned closed blockchains are not necessarily required to be run on a blockchain, which are developed with closed blockchains to get the hype of the blockchain term into their business.

Issues and Improvements

Possibilities of blockchain become limited with its current issues that have to be addressed with possible improvements. Each core function of blockchain has several significant threats that need to be evaluated and counter measured before implementation. Not always these risks will be purely technical, because risks can also arise from legal, economic, even cultural areas [48]. One of the ideas of blockchain was that anyone with a computer would be able to participate in the block generation process joining its peer to peer distributed network. Bitcoin blockchain size including block headers and transactions without database indexes as of August, 2019 has grown to over 220 GB [51]. Ethereum introduced a concept called “pruning” to counter attack the ever growing storage size, which required downloading only a certain number of blocks with fast sync mode in the client app to become a full node. Even with pruning, Ethereum blockchain currently accounts to over 120 GB [52]. This significantly reduces the ability of individuals with personal computers to be able to participate in the blockchain network as full nodes. In addition to storage size issue, transaction speed is another scalability issue for the blockchains. Transaction speed mainly concerns on how long it takes for an individual transaction to be confirmed on the blockchain, not about how long it takes for a block to be added into the ledger. On average bitcoin processes about 7 transactions per second [3], 15 by Ethereum [53], and 1500 by Ripple [54], but Visa in its peak can handle 56,000 transactions per second [55, 56]. Due to the amount of network activity and transaction fees variations individual transaction verification times vary on Bitcoin and Ethereum networks, making it difficult to use Bitcoin and Ethereum as a stable payment mechanism. Block size and block interval parameters controls the maximum rate at which blockchain systems can perform transactions. Increasing block size improves throughput, but the resulting bigger blocks take longer to propagate in the peer-to-peer network. Even though reducing block interval shortens latency, nodes might be prompted to disagreements and reorganizations of blocks. Therefore to improve efficiency, one has to trade off throughput for latency [57]. The Bitcoin developer community has come up with two solutions—Segregated Witness and Lightning Network, allowing more transactions to be processed per block. SegWit reduces the weight of transactions by

separating signature and transaction data, creating more room in blocks to add additional transactions. Lightning Network enables transactions to happen on "off-chain" while adding only the final result into the main blockchain. Using a large network of micropayment channels [58] Bitcoin scalability is achieved in Lightning Network, while preventing blockchain centralization. Micropayment channels are real Bitcoin multisignature transactions and not a separate trusted network [59]. Ethereum community also working on a solution called sharding to scalability issues, which groups network nodes into subsets of groups called "shards" that processes transactions specific to only that group together with a cross-shard communication capability [60].

Another main concern with blockchain comes with the control of decentralized blockchain networks. Level of computing activity on the Bitcoin network is measured in terms of the hash rate [61]. "51% attack" is such an issue on proof-of-work-based blockchains, which describes a situation in which one or collection of nodes control over 51% of total computational power/hash rate, thereby gaining possibility to confirm blocks with incorrect transactions within the network. However, since it requires a vast amount of computational power on a much established network, the feasibility of such an attack is nearly impossible. But if the scalability issues on blockchain size are not addressed properly, there could even be such attacks from organized set of miners in future on a diminished network of full nodes. Honest miners must constantly invest more computing power than a potential adversary could accumulate in order to prevent double spending, thereby adversely increasing energy consumption. Proof-of-stake was proposed to decrease high energy consumption and increase the lower transaction speeds of proof-of-work-based blockchains. "nothing-at-stake" problem is an issue on proof-of-stake blockchains, that arises when validators approving transactions on multiple parallel forks to receive block rewards, so that they can double spend the earnings from both forks. Unlike in proof-of-work blockchains, proof-of-stake blockchains does not require expediting computational resources to approve blocks, therefore later versions of proof-of-stake blockchains required imposing penalties for misbehavior. The nothing-at-stake problem alleges that attackers face no cost by deferring consensus. However, within a proof-of-stake protocol, all attackers with the ability to delay consensus own some coins, and delaying consensus reduces the value of those coins [62]. Ethereum's Casper upgrade to proof-of-stake-based consensus involves imposing penalties for misbehavior. In addition to the issues we have discussed, there are also possible security risks due to lack of standardization of blockchain security measures, as well as threats coming from illegal usages of anonymity in blockchains with that possible governmental regulations.

Conclusion

The survey paper has come up with a definition for the blockchain and explained concepts unwrapping the blockchain definition—immutable, distributed, digital ledger, cryptography, peer-to-peer network, consensus mechanism, decentralization. The paper also described the most widely used consensus algorithms used on blockchains in order to determine the valid blocks, which keeps the accuracy of the blockchain. The permissionless and permissioned blockchain types were explained in detail with an explanation on why we believe that closed permissioned blockchains can be implemented without the need of blockchain technology. Then, we have discussed how blockchain captured most of the value in protocol layer unlike in internet where most of the value was captured in application layer. The future potentials of blockchain-based applications were discussed thereafter describing several blockchain-based applications like smart contracts, property title registries, digital voting, and supply chain management as well as listing several other use cases. Finally, issues of the existing blockchains were discussed such as 51% attack, nothing-at-stake problem together with improvements for the scalability issues in current blockchains. By and large, the paper has provided a brief but comprehensive overview of blockchain with its history, concepts, terms, consensus algorithms, types, applications, and issues within single paper useful for a blockchain technology enthusiast. The concepts and findings learned here can be studied in depth based on the need of the readers.

Compliance with Ethical Standards

Conflict of Interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.
2. Buterin V. A next generation smart contract and decentralized application platform. 2013.
3. Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gün E. On scaling decentralized blockchains. Lecture Notes in Computer Science. 2016;106–25. https://doi.org/10.1007/978-3-662-53357-4_8.
4. Chaum D. Blind signatures for untraceable payments. Adv Cryptol. 1983;. https://doi.org/10.1007/978-1-4757-0602-4_18.
5. Bitcoin Wiki. E-gold. 2018. https://en.bitcoin.it/wiki/E-gold. Accessed Jan 2019.
6. Dai W. B-Money. 1998.

7. Finney H. RPOW—reusable proofs of work. 1999. https://nakamotoinstitute.org/finney/rpow/index.html. Accessed Jan 2019.
8. Back A. Hashcash—a denial of service counter-measure. 2002. http://www.hashcash.org/hashcash.pdf. Accessed Jan 2019.
9. Wood G. Ethereum: a secure decentralised generalised transaction ledger. 2014.
10. Fenu G, Marchesi L, Marchesi M, Tonelli R. The ICO phenomenon and its relationships with ethereum smart contract environment. In: 2018 international workshop on blockchain oriented software engineering (IWBOSE), Campobasso, Italy, 2018 (pp. 26–32). https://doi.org/10.1109/iwbose.2018.8327568.
11. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE symposium on security and privacy, 2015. https://doi.org/10.1109/sp.2015.14.
12. Christin N. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. 2013.
13. Huang DY, Dharmdasani H, Meiklejohn S, Dave V, Grier C, McCoy D, Savage S, Weaver N, Snoeren AC, Levchenko K. Botcoin: monetizing stolen cycles. 2014.
14. Le Jamtel E. Swimming in the Monero pools. In: 2018 11th international conference on IT security incident management & IT forensics (IMF), 2018. https://doi.org/10.1109/imf.2018.00016.
15. Garber L. Government officials disrupt two major cyberattack systems. News Briefs. 2014;47(7):16–21. https://doi.org/10.1109/mc.2014.189.
16. Moore T, Christin N. Beware the middleman: empirical analysis of bitcoin-exchange risk. Lecture Notes in Computer Science. 2013;2013(7859):25–33. https://doi.org/10.1007/978-3-642-39884-1_3.
17. Grigg I. Tripple entry accounting. 2005.
18. Merkle RC. Protocols for public key cryptosystems. In: 1980 IEEE symposium on security and privacy. IEEE, 1980. https://doi.org/10.1109/SP.1980.10006.
19. Merkle RC. A certified digital signature. Lecture Notes in Computer Science. 1979;435:218–38. https://doi.org/10.1007/0-387-34805-0_21.
20. Buterin V. Merkling in Ethereum. 2015. https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/. Accessed Mar 2020.
21. Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans Program Lang Syst. 1982;4(3):382–401. https://doi.org/10.1145/357172.357176.
22. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security - CCS'16, 2016; 16: 3–16. https://doi.org/10.1145/2976749.2978341.
23. Kiayias A, Panagiotakos G. Speed-security tradeoffs in bitcoin protocols. 2016.
24. King S. Primecoin: cryptocurrency with prime number proof-of-work. 2013.
25. King S, Nadal S. PPCoin: peer-to-peer crypto-currency with proof-of-stake. 2012.
26. Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. Lecture Notes in Computer Science. 2016;9604:142–57. https://doi.org/10.1007/978-3-662-53357-4_10.
27. Buterin V, Reijsbergen D, Leonardos S, Piliouras G. Incentives in Ethereum's hybrid casper protocol. In: 2019 IEEE international conference on blockchain and cryptocurrency (ICBC), 2019. https://doi.org/10.1109/bloc.2019.8751241.
28. BitShares Blockchain Foundation. The bitshares blockchain. 2015. https://www.bitshares.foundation/papers/BitSharesBlockchain.pdf. Accessed May 2019.
29. Dantheman. DPOS consensus algorithm—the missing whitepaper. 2017. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper. Accessed Apr 2019.
30. NEM. NEM Technical Reference. 2018. https://nem.io/NEM_techRef.pdf. Accessed May 2019.
31. Popov S. The Tangle. 2019. https://iota.org/IOTA_Whitepaper.pdf. Accessed May 2019.
32. Castro M, Liskov B. Practical byzantine fault tolerance. In: Proceedings of the symposium on operating system design and implementation. 1999;20:398–461. https://doi.org/10.1145/571637.571640.
33. Vukolić M. Rethinking permissioned blockchains. In: BCC 2017—Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts, co-located with ASIA CCS 2017. https://doi.org/10.1145/3055518.3055526.
34. Buterin V. On public and private blockchains. 2015. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed Jun 2019.
35. Monégro J. Fat protocols. 2016. http://www.usv.com/blog/fat-protocols. Accessed June 2019.
36. CoinMarketCap. 2019. https://coinmarketcap.com. Accessed July 2019.
37. Moore W, Stephen J. Should cryptocurrencies be included in the portfolio of international reserves held by central banks? Cogent Econ Finance. 2016;1:4. https://doi.org/10.1080/23322039.2016.1147119.
38. Tron Foundation. Advanced decentralized platform. White Paper: Version 2.0. 2018. https://tron.network/static/doc/white_paper_v_2_0.pdf. Accessed July 2019.
39. Szabo N. The idea of smart contracts. 1997.
40. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE symposium on security and privacy (SP), 2016. https://doi.org/10.1109/sp.2016.55.
41. The Zilliqa Team. The Zilliqa technical white paper. Version 0.1. 2017. https://docs.zilliqa.com/whitepaper.pdf. Accessed July 2019.
42. Block.one. EOS.IO technical white paper v2. 2018. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. Accessed July 2019.
43. Szabo N. Secure property titles with owner authority. 1998.
44. CBInsights. How blockchain could secure elections. 2018. https://www.cbinsights.com/research/report/blockchain-election-security/. Accessed Aug 2019.
45. Moore N, Sawhney N. Under the Hood, The West Virginia Mobile Voting Pilot. 2019. https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf. Accessed Aug 2019.
46. Makridakis S, Polemitis A, Giaglis G, Louca S. Blockchain: The next breakthrough in the rapid progress of AI. In: Artificial intelligence—emerging trends and applications, InTech, 2018. https://doi.org/10.5772/intechopen.75668.
47. Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. Int J Inf Manag. 2018;39:80–9. https://doi.org/10.1016/j.ijinfomgt.2017.12.005.
48. Zīle K, Strazdiņa R. Blockchain use cases and their feasibility. Appl Comput Syst. 2018;23(1):12–20. https://doi.org/10.2478/acss-2018-0002.
49. E-Estonia. KSI Blockchain. 2017. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/. Accessed Aug 2019.
50. Hileman G, Rauchs M. Global blockchain benchmarking study. SSRN Electron J. 2017;. https://doi.org/10.2139/ssrn.3040224.
51. Blockchain.com. Blockchain Size. 2019. https://www.blockchain.com/charts/blocks-size. Accessed Aug 2019.
52. Etherscan.io. Ethereum chain data size (Geth w/FAST Sync). 2019. https://etherscan.io/chart2/chaindatasizefast. Accessed Aug 2019.
53. Ethereum Wiki. Sharding FAQ. 2019. https://github.com/ethereum/wiki/wiki/Sharding-FAQ. Accessed Mar 2020.

54. Ripple.com. XRP | Ripple. 2019. https://ripple.com/xrp/. Accessed Mar 2020.
55. Herrera-Joancomartí J, Pérez-Solà C. Privacy in bitcoin transactions: new challenges from blockchain scalability solutions. Lecture Notes in Computer Science. 2016;26–44. https://doi.org/10.1007/978-3-319-45656-0_3.
56. Visa Inc. Visa: 56,582 transaction messages per second! 2014. http://visatechmatters.tumblr.com/post/108952718025/56582-transaction-messages-per-second. Accessed Mar 2020.
57. Eyal I, Gencer AE, Sirer EG, Renesse R. Bitcoin-NG: A Scalable Blockchain Protocol. In: Proceedings of the 13th USENIX symposium on networked systems design and implementation (NSDI '16), 2016.
58. Decker C, Wattenhofer R. A fast and scalable payment network with bitcoin duplex micropayment channels. Stabilization, safety, and security of distributed systems. SSS 2015. Lecture Notes in Computer Science, 2015; 9212: 3–18. https://doi.org/10.1007/978-3-319-21741-3_1.
59. Poon J, Dryja T. The bitcoin lightning network: scalable off-chain instant payments. 2016.
60. MacManus R. Blockchain speeds and the scalability debate. 2018. https://blocksplain.com/2018/02/28/transaction-speeds/. Accessed Aug 2019.
61. Bradbury D. The problem with bitcoin. Comput Fraud Secur. 2013;2013(11):5–8. https://doi.org/10.1016/s1361-3723(13)70101-5.
62. Saleh F. Blockchain without waste: proof-of-stake. SSRN Electron J. 2019;. https://doi.org/10.2139/ssrn.3183935.