A quick synopsis of blockchain technology

Veeramani Karthika* and Suresh Jaganathan

Department of Computer Science and Engineering,
SSN College of Engineering,
Tamilnadu, India
Email: vkarthikatnj@gmail.com
Email: drjs72@outlook.com
*Corresponding author

Abstract: Blockchain evolved as a core technology of Bitcoin, and earned a significant attraction for entrepreneurs and researchers nowadays. The blockchain is an open, immutable distributed public ledger that allows transactions to take place in a decentralised manner without a need for a trusted third party. Bitcoin, the first successful cryptocurrency, is a peer-to-peer electronic payment system. The thought for Bitcoin started as a means for making a secure currency that had no centralised control. Blockchain application is not only restricted to Bitcoin, but it also ignited the idea of using it for a wide range of fields such as ehealth, governance, arts, culture, education, electricity trading, etc. To apply this technology to many areas, one should have a complete understanding of what it is, this paper is meant to give a quick synopsis of *blockchain technology* (BT).

Keywords: distributed public ledger; decentralisation; consensus mechanisms; digital signature; hash function; blockchain protocols.

Reference to this paper should be made as follows: Karthika, V. and Jaganathan, S. (2019) 'A quick synopsis of blockchain technology', *Int. J. Blockchains and Cryptocurrencies*, Vol. 1, No. 1, pp.54–66.

Biographical notes: Veeramani Karthika is a Research Scholar in the Department of Computer Science and Engineering, Sri Sivasubramaniya Nadar College of Engineering. She obtained her ME in Computer Science and Engineering from the Anna University and BTech in Information Technology from the University College of Engineering, BIT Campus Tiruchirappalli. She has published a paper in a reputed international conference. She had two years of industrial experience working as a Programmer Analyst in Cognizant Technology Solutions, Chennai. Apart from this, she filed a software patent on regularised discriminant analysis and also uploaded R packages in CRAN. Her areas of interest are big data analytics, machine learning and blockchain technology.

Suresh Jaganathan is an Associate Professor in the Department of Computer Science and Engineering and has more than 22 years of teaching experience. He received his PhD in Computer Science from the Jawaharlal Nehru Technological University, Hyderabad, ME in Software Engineering from the Anna University and BE in Computer Science and Engineering from the Mepco Schlenk Engineering College, Sivakasi, Madurai Kamarajar University, Madurai. He has more than 25 publications in refereed

international journals and conferences. Apart from this, to his credit he filed two patents and written a book, *Cloud Computing: A Practical Approach for Learning and Implementation*, published by Pearson Publications. His areas of interest are distributed computing, big data analytics, machine learning and blockchain technology.

1 Introduction

The blockchain is an emerging technology that rethinks trust in the contemporary generation systems. BT made its public debut when Satoshi Nakamoto released the whitepaper 'Bitcoin: a peer to peer electronic cash system' Nakamoto (2009). Nakamoto tried to establish trust in a trustless distributed system without a mediator. BT has developed into one of today's most prominent cutting-edge technologies with the potential to influence every field from financial to supply chain to healthcare and many.

The history of blockchain technology (BT) cannot be discussed without first starting with a discussion about Bitcoin. The Satoshi Nakamoto, a pseudonymous developer, proposed an open source software Bitcoin in the year 2009. Bitcoin is a cryptocurrency, as it applies cryptography to manage the production and transfer of money. It uses peer-to-peer (P2P) Bitcoin network to send decentralised digital currency from one user to other.

BT removes the need for intermediaries and facilitates digital trust. Digital trust is accomplished by recording the essential information in an open network and does not let anyone remove it. Also, it has some fundamental features such as decentralisation, time stamping, and transparency. Even though blockchain and Bitcoin are not the same, many believe both are the same even now. Those who started to realise around the year 2014 that it could be used for more than cryptocurrency began to invest and explore how it could amend many different kinds of operations.

The blockchain is an open, decentralised/distributed public ledger that records transactions between two parties permanently without needing the third party. In simple words, blockchain is a chain of blocks, each one is made of a header and body. It exists on a P2P network where every node stores a local copy of public ledger. There is no central authority to supervise the blockchain ledger. Each record in the ledger is called a block and includes details such as the transaction timestamp, hash pointer to its previous block. The hash pointer makes it impractical for anyone to change information about the transactions retrospectively. Also, the technology is safe by design, as the database system of multiple nodes records the same transaction. In this manner, the information can never be altered or erased.

Blockchain systems are currently categorised into three types. There are public blockchain, consortium blockchain and private blockchain (Buterin, 2015). Table 1 lists the comparisons among three kinds of blockchain systems from a different perspective (Zheng et al., 2018). The rest of paper is organised as follows, Section 2 explains the fundamental concepts of blockchain, Section 3 describes the core concepts used, Section 4 discusses the regulatory body, Section 5 analyses the BT development, Section 6 concludes the paper.

Table 1 Comparison of three blockchain types

Property	*Public*	*Consortium*	*Private*
Read permission	Open	Restricted	Restricted
Consensus	Open to all nodes	Group of nodes	Nodes determination
Peers in consensus	Permissionless	Permissioned	Permissioned process

2 Fundamental concepts

2.1 Decentralised

There are two main architectural approaches for any network scheme, i.e., centralised and decentralised. In a centralised network, the nodes are connected with each other with one central node of authority. The primary concern of this network is a single point of failure. On the contrary, a decentralised network has several nodes connected with each other without any central node of control. In the decentralised network, data consistency is maintained by consensus algorithms in the blockchain. Figure 1 depicts the architecture of the two network schemes.

Figure 1 The architecture of two network schemes

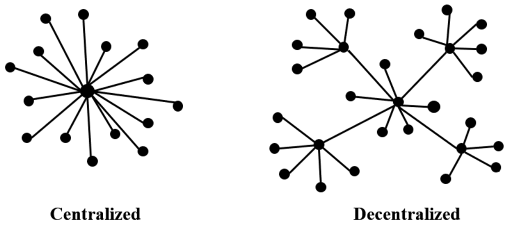
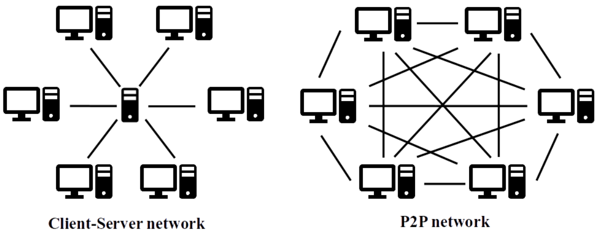


Figure 2 Client-server and P2P network models



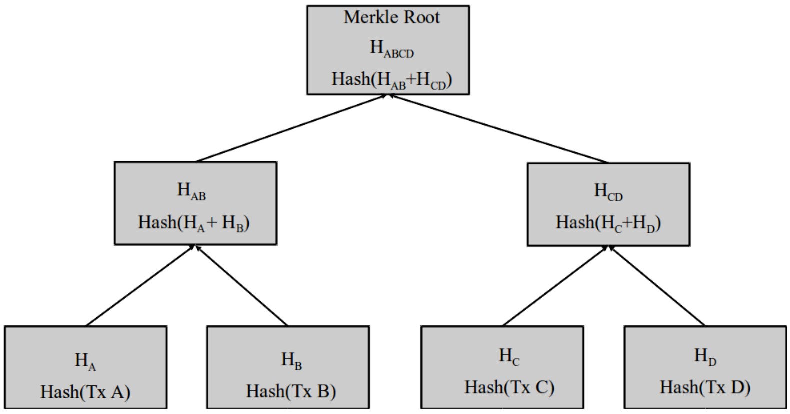
2.2 P2P network

The P2P network comprises of a group of peers communicating directly among themselves. In the P2P network, every peer has the same capabilities and responsibilities. Each peer acts as both server and client in contrast to the traditional client-server model in which the clients and servers are divided. Figure 2 illustrates the client-server and P2P network models.

2.3 Merkle tree

Merkle tree or hash tree is a tree in which the hash of a data block tagged in every leaf node, and the cryptographic hash of the labels of its child tagged in every non-leaf node. A small change in a data block has the significant impact on the hash of the Merkle root. Thus, hash trees provide adequate and reliable verification of the data. Hash trees link the idea of hash chains with hash lists. Figure 3 shows the structure of the Merkle tree with an example.

Figure 3 Structure of the Merkle tree



2.4 Decentralised applications

Decentralised applications (*dApps*) work on a P2P network and does not require any individual entity to manage it. It is similar to a typical application from a user's viewpoint. The difference between normal and *dApps* lies in the backend. While the normal application uses a server as the backend, the *dApps* uses a distributed P2P network, hence has an immense number of nodes. It does not necessarily require to run on blockchain network. The traditional *dApps* such as BitTorrent, Tor, BitMessage, Popcorn Time, run on a P2P network but not on blockchain network.

2.5 Hash functions

A Hash function is an essential part of BT. A hash function (Pierro, 2017) maps any sized data to a fixed size. The result of the hash function referred to as a message digest or digital fingerprint. The main properties of the hash function include,

1 The hash function is commonly a one-way function which is non-reversible. Given a data x, one can compute message digest $H(x)$. But, given a $H(x)$, no deterministic algorithm can compute x. In this way, the data is cryptographically secure.

2 For any two different inputs $x1$ and $x2$, $H(x1)$ and $H(x2)$ should be different. Moreover, a simple change in the data can result in the significant difference in the message digest referred to as Avalanche effect.

3 Message digest $H(x)$ does not reveal information on data x.

Blockchain makes utilisation of hash function all over the place. Hashing is applied to information on each block before it is added to the blockchain to ensure the integrity of the information. If someone tried to temper the data in the blockchain, it could be easily detected by others as the hashed value would be different. The previous block hash value is utilised to estimate the hashed value of the current block, thereby creating a link between the blocks. Bitcoin network uses SHA256 hash function for mining and creation of Bitcoin addresses. It takes an input of any length and produces an output of 256 bits.

2.6 Key characteristics of BT

The key characteristics of BT include the following

1 Immutability: Once the transaction represented in the block is added to the blockchain, the transaction becomes irreversible.

2 Transparency: It is achieved by making the public ledger available to everyone to inspect the blocks and the transactions at any point in time.

3 Availability: Blockchain network is continuously available, even though if some peers exit from the blockchain network

4 Privacy: Achieved through anonymity. Users in the blockchain network stay anonymous by using their public key as an address which does not reveal the real identity of the user.

5 Consistency: When all the miners agree on the validity of the block, the block gets added to the blockchain, makes the distributed ledger consistent and changes are infeasible.

3 Core concepts

3.1 Distributed ledger

A distributed ledger is a replicated, shared, decentralised and synchronised record of transactions between parties, moreover, it is cryptographically secured. Unlike a distributed database, nodes of a distributed ledger cannot trust others nodes in the network, and so it should verify the transaction independently before applying them with its local copy. There are two main classes in distributed ledgers. First, those that aim to diminish the role of trusted third parties, and second those that mainly depend on identifiable third parties for some subset of the system's properties. Not all distributed ledgers are blockchains, but all blockchains are distributed ledgers.

3.2 Consensus mechanisms

In blockchain, how consensus is made among the untrustworthy nodes to append new blocks is a conversion of the byzantine generals (BG) problem (Lamport et al., 1982). In BG problem, a gang of generals who directs a part of the Byzantine army strikes the city. Some generals choose to attack while others decide to retreat. However, the strike would fail if only part of them attack the city. Thus, they have to come to an affirmation whether to attack or retreat. The challenge here is how the agreement should be made in a distributed environment. As the blockchain network is distributed, it is also a threat for blockchain. Some protocols are required to assure consistency of public ledger in all blockchain nodes. This section presents some of the consensus algorithms which plays a vital role to reach agreement among participating nodes in the blockchain network.

3.2.1 Proof of work

Proof of work (PoW) is generally a cryptographic puzzle that is very difficult to solve but easy to verify. Miners solve a cryptographic problem to add a block to the blockchain. When a miner solves the puzzle, they present their block for verification to the blockchain network. Then, the other miners verify the PoW done by the successful miner and add it to their blockchain.

Bitcoin is the notable cryptocurrency that uses PoW as their consensus algorithm. In PoW, each node of the Bitcoin network calculates a hash value of the block header. The process of generating and validating a block is called mining. The node which does mining is called a miner. The task of the miner is to find out the nonce value to get the necessary hash value. The calculated hash value should be equal to or less than a given difficulty target. Then, the consensus should be reached on calculated hash value. When a miner finds the nonce value, it will broadcast the block to other miners in the network. The other miners in the network should validate the correctness of the calculated nonce. After successful block validation by other miners, the block gets appended to the blockchain.

The PoW consensus algorithm answered many questions when it arose to solve the BGs problem, but there are some unanswered problems associated with it. Though PoW mining ensures high security of blockchain, it results in computation intensive that requires a high amount of power consumption. To mitigate the energy loss, PoW protocol like Primecoin King (2013) searches for special prime number chains that can be used for mathematical research. But, those who have faster and more robust computers have the higher possibility of mining than others. As a consequence, Bitcoin is not as decentralised as it needs to be. Moreover, large mining pools can pull up with each other and introduce a 51% attack on the blockchain network.

3.2.2 Proof of stake

Proof of stacke (PoS) developed as an energy efficient alternative to PoW. In PoS, the miners get replaced with validators. Once the validators lock some coins as stake, they start the process of verifying the blocks. The validators will gain a reward equitable to their stake after the block gets appended to the blockchain. In this way, the PoS is a lot more resource friendly than PoW. One of the most popular blockchain protocols Ethereum currently relies on PoW but is planning a move to the PoS in early 2018.

3.2.3 Delegated proof of stack

An interesting form of PoS named as delegated proof of stake (DPoS). EOS blockchain protocol uses this consensus algorithm in order to do millions of transactions per second. Firstly, anyone who possesses tokens on the blockchain can be combined into the EOS.IO Software (2018). They can elect the block producers by the voting system. Anyone can join in the block producer election and can produce blocks proportionate to total votes when compared to other producers.

3.2.4 Practical byzantine fault tolerance

Practical byzantine fault tolerance (PBFT) (De Angelis et al., 2017) can handle Byzantine fault if more than two-thirds honest nodes are in the network. As the first step in PBFT, a leader node generates a new candidate block. Every node in the network will get a chance to be leader. There are three main phases in PBFT:

1 pre-prepare

2 prepare

3 commit.

In pre-prepare phase, the candidate block is broadcasted to all other consensus nodes by the leader. In prepare phase, the node which receives the block will recognise the block validity and broadcast the block hash to other nodes. Once the node gets more than two-thirds of the prepare message (block hash) of the total nodes, the commit message is computed and broadcasted to every other in the network. Then the consensus should be reached on candidate block. The block can be appended into the blockchain, if more than two-thirds of the commit message are received on it.

3.3 Protocols

A protocol is a program which forms the software backbone of the network, and this is where the significant modifications are done by different blockchain projects. Several protocols are designed for different objectives and use cases; hence there exist some differences in the protocol design. e.g., Bitcoin was designed for disintermediated digital payments on a decentralised network, while Ethereum focusses on dApps which could be developed using smart contracts (Kosba et al., 2016). Though there are many protocols, this section explains the most commonly used blockchain protocols.

3.3.1 Bitcoin

Bitcoin protocol was the earliest of the blockchain protocol on which the cryptocurrency Bitcoin is transacted. It is a permissionless public blockchain, where anyone can join in the Bitcoin network. Cryptographic hash function, digital signature, private-public encryption and P2P network are the underlying technology used in this protocol. PoW is the consensus algorithm utilised to reach the consensus of a majority of the participants in the network. The primary benefit of using BT to Bitcoin prevents double spending problem and also decreases transaction fee compared to the traditional central banking system.

Bitcoin protocol enables the user to perform immutable transactions directly without any trusted third party. Each transaction contains individual transaction ID, sender Bitcoin address, recipient Bitcoin address and the Bitcoins to transfer. The nodes in the Bitcoin network process a block which includes the transactions every ten minutes. After the successful miner, solves a difficult cryptographic problem, the block is broadcasted to other miners in the network for verification. Once the majority of the miners verify the PoW, the successful miner gets the Bitcoin as a reward. The consensus algorithm used in this Bitcoin protocol results in scalability issue as it requires the approval of the majority of the participating nodes in the network.

3.3.2 Ethereum

There exist many similarities between Bitcoin and Ethereum protocol. Ethereum protocol is also a permissionless public blockchain. It applies the identical technological components such as P2P network, digital signature, public key encryption, cryptographic hash function. The consensus algorithm called Ethash (Wood, 2017), a kind of PoW, is used at the beginning, but Ethereum planned to move to Casper (Zamfir, 2015), a kind of PoS. The native cryptocurrency *Ether* owns the next largest exchange value behind Bitcoin.

Bitcoin was developed for supporting crypto fee operations on top of peer to peer network, but Ethereum was developed with many broader goals in thought. Ethereum is a public, open source and blockchain based distributed computing protocol that supports smart contract functionality. Smart contract is lines of code that gets executed when specific condition meets. It is coded using Ethereum's exclusive language Solidity. Ethereum allows the developers to start their blockchain projects which include creating a new cryptocurrency. It can also be used to develop decentralised autonomous organisations (DAO) and dApps. Some of the popular cryptocurrency projects like OmiseGo, VeChain are developed by utilising Ethereum virtual machine (EVM). Ethereum presents a means to specify the cost of computing power needed to perform a transaction for the user with the help of a measure termed 'gas'. The gas limit is usually specified by the user. The transaction is executed only if it is within that gas limit. However, the transaction is undone if it surpasses the limit. Simple pay operations need fewer gas, whereas difficult operations like smart contract deployment need higher gas.

3.3.3 Hyperledger

Hyperledger (2015) is a open source (https://www.hyperledger.org/about), public, permissioned, and blockchain platform. It was developed by the Linux Foundation with many other companies such as Intel, Cisco, American Express, IBM, SAP, Daimler to build enterprise blockchains in 2015, aiming to promote the blockchain based distributed ledgers. This protocol focuses on ledgers developed to assist economic and financial activities with the objective to enhance feature such as reliability, performance.

Fabric (Androulaki et al., 2018), Sawtooth projects are some of the variants of Hyperledger. Only the users of the organisation can join in the Hyperledger blockchain because it is permissioned blockchain. Hyperledger project insists on building collaborative efforts to develop open standards and protocols. This is achieved by creating a platform that supports diverse elements for different applications having board features such as identity, storage, own consensus mechanism, contracts, and access control.

The consensus mechanism used in Hyperledger views at the complete transaction steps and each node has various roles with numerous tasks. Each node is varied based on their roles. A node can be a client, peer or orderer. The client generates and requests transactions. The Peers are responsible for managing the ledger. The transaction will be committed into the blockchain once the updated information is obtained from orderers. A particular type of peers named endorsers investigates whether the transactions satisfy required conditions and confirm them.

3.3.4 Ripple protocol

In 2012, a protocol named Ripple transaction protocol (RTXP) was designed based on internet protocol, an open source distributed ledger. It uses most of the characteristics of public, permissionless blockchain protocols such as Bitcoin and Ethereum. The components include decentralisation, cryptographic hash functions, P2P network, public key encryption. However, Ripple was explicitly designed to promote quick and affordable global transfer of funds. XRP (ripples) is the currency used by the Ripple protocol.

The transactions in the Ripple protocol are cryptographically approved. Ripple protocol allows for quick and secure global fee settlement and it is achieved by Ripple protocol consensus algorithm (RPCA) (Schwartz et al., 2014). The idea behind RPCA is proof of correctness. All nodes in the blockchain network implement RPCA at some interval of time. Once the consensus is reached, a ledger is acknowledged as closed which is the final ledger. All nodes will have same final ledger.

In the network, nodes are divided into two types: server to participate in consensus process and client to transfer funds. Each server maintains a unique node list (UNL), and the server would ask the nodes in the UNL to reach consensus. If the server received 80% of the nodes agreement, then that transaction would be packed into the ledger. Behind Bitcoin and Ethereum, Ripple is the third largest cryptocurrency regarding market capitalisation.

3.3.5 R3s Corda

An open source protocol Corda is an enterprise blockchain designed by the company R3. It is developed with the intention to record, supervise and synchronise the financial transactions amongst regulated financial organisations. R3 Corda also uses smart contracts which have particular legal representations. It is similar to Hyperledger fabric as it sees at the complete transactions and assigning distinct roles to nodes. In this, consensus does not reach on mining and PoW. Validity and uniqueness of the transaction are expected to reach an agreement. Validity is guaranteed by smart contracts. The transaction is unique when none other transaction employs any of its input.

3.3.6 Symbiont distributed ledger

In October 2016, symbiont distributed ledger protocol is a smart contract platform that uses BT. Institutional finance is the most suitable use case for symbiont distributed ledger protocol. Symbiont distributed ledger protocol can process up to 80,000 transactions each second. The significant benefits of this protocol lie with its security and high performing byzantine fault tolerant.

3.4 Digital signature

In an untrustworthy environment, it is necessary to secure the origin of transactions. The digital signature (Yuan et al., 2017) based on asymmetric cryptography provides authentication in the blockchain. Each user owns a private-public key pair. The transactions in the block are signed by the private key. Signing and verification phases are the two phases involved in the typical digital signature. For example, Alice wants to transfer a message to Bob. In signing phase, Alice encrypts the data with her private key and broadcast the digitally signed message throughout the network. After receiving the digitally signed message, Bob decrypts the message with Alice's public key in the verification phase. In that manner, Bob could easily verify if the message has been tampered or not. The most commonly used digital signature algorithm in blockchain is the Elliptic curve digital signature algorithm (ECDSA) (Johnson et al., 2001; Kikwai, 2017).

4 Regulatory body in blockchain

Blockchain technology, though widely discussed and used is still not been regulated which brings risk into the blockchain applications. The regulations mainly depend on the blockchain applications. However, BT is considered beneficial to be utilised in the financial domain, legal domain and possibly other domains such as healthcare. The current state of regulation on blockchain for the financial sector is that each country is developing different regulations. A unified regulatory framework does not exist to date. The Department of Finance Ireland (2018) published a *Discussion Paper: Virtual Currencies and Blockchain Technology* on digital currencies and BT in March 2018. This discussion paper highlights some of the critical issues that arise in respect of this technology and proposes that a Working Group should be established inside the Department of Finance which will monitor further developments in the cryptocurrencies.

The European Commission also in March 2018 announced a Fintech action plan to explore opportunities in respect of creating more innovations within the financial sector in Europe. This action plan sets out many proposals in regard of cryptocurrencies, especially for initial coin offerings (ICOs).

5 Blockchain development

5.1 Blockchain 1.0 digital decentralised currency

Blockchain 1.0 permits for the use of BT to exchange digital currency between any two parties without any trusted third party. Bitcoin was the earliest application of this revolutionary technology in 2009. The advantage of using this technology to Bitcoin is for its reduced transaction fee compared to the traditional central banking system, anonymity and to protect it against inflation (Sovbetov, 2018). The applications of the first generation BT diversify from intending to store a value to a form of exchange of digital currency. It can also be utilised to offer remittance service and e-payment. In general, Blockchain 1.0 is a public distributed ledger that holds the transactions of digital currency or remittance or e-payment that occur over a period.

5.2 Blockchain 2.0 digital economy

While Blockchain 1.0 use case is restricted to decentralised digital currency, Blockchain 2.0 evolved with the objective of applying BT to the digital economy. Blockchain 2.0 employs a broad range of economic and financial applications ahead simple payment. In this generation, assets, in general, to be maintained by the blockchain. The asset includes stocks, bonds, loans, mortgages, property, etc. Moreover, Ethereum made its famous contribution to second generation blockchain by designing a platform to implement smart contracts. Smart contracts are self-executing contracts when a specific condition meets. Executing smart contracts through blockchain reduces the value of verifying information and also simplifies human intense tasks.

5.3 Blockchain 3.0 digital society

Blockchain 3.0, a step ahead offering blockchain-based solutions to digital currency and digital economy (Efanov and Roschin, 2018). It does more that merely involve in economic and financial applications. The applications includes e-health (Rifi et al., 2017), education (Grech and Camilleri, 2017), arts, culture, governance, supply chain, science, distributed cloud storage (Li et al., 2018), digital rights management (Ma et al., 2018), and internet of things (Jesus et al., 2018). The most promising application is of Blockchain 3.0 is the smart cities (Sun et al., 2016; Sharma and Park, 2018) which covers most of the elements including mobility, living governance, etc. e-residency (Sullivan and Burger, 2017) in estonia is achieved using BT, has the potential to transform the idea of controlling and authenticating identity information of residents. Yang et al. (2018) proposed a scheme adopting BT for public verification of data deletion scheme in cloud storage. Thompson (2017) explored the means of utilising the BT to preserve digital signatures and public-private key pairs.

6 Conclusions

Blockchain, a groundbreaking technology throws light on how to process, verify and store any transaction without a third party. One of the most interesting features of BT is that it is completely decentralised, rather than stored in one central point. It eliminates the need for influential central authorities, and instead hands control back to the individual user. Blockchain, a distributed ledger technology, is a chain of a block of information that contains transactions. Bitcoin is the first practical application of BT, yet it opened the doors to many other use cases. This study gave a quick synopsis of BT and explained its fundamental concepts, core concepts, regulatory body, and its use cases. Nowadays blockchain protocols are springing up, and we plan to conduct in-depth investigations of blockchain protocols in the future.

References

Androulaki, E., Barger, A., Bortniko, V. et al. (2018) 'Hyperledger fabric: a distributed operating system for permissioned blockchains', *Proceedings of the 13th EuroSys Conference*, pp.30:1–30:15.

Buterin, V. (2015) *On Public and Private Blockchains* [online] https://bit.ly/1UsVKV4 (accessed 25 August 2018).

De Angelis, S., Aniello, L. and Baldoni (2017) 'PBFT vs. proof-of-authority: applying the cap theorem to permissioned blockchain', *Italian Conference on Cyber Security*, pp.1–11.

Department of Finance Ireland (2018) *Discussion Paper: Virtual Currencies and Blockchain Technology*, Department of Finance Ireland [online] https://bit.ly/2o19Q79 (accessed 20 August 2018).

Efanov, D. and Roschin, P. (2018) 'The all-pervasiveness of the blockchain technology', *Procedia Computer Science*, Vol. 123, pp.116–121, DOI: 10.1016/j.procs.2018.01.019.

EOS.IO Software (2018) *EOS.IO* [online] https://eos.io/ (accessed 20 August 2018).

Grech, A. and Camilleri, A.F. (2017) *Blockchain in Education*, JRC Science for Policy Report.

Hyperledger (2015) *Hyperledger Project* [online] https://www.hyperledger.org/.

Jesus, E.F. and Chicarino, R.L. (2018) 'A survey of how to use blockchain to secure internet of things and the stalker attack', *Security and Communication Networks*, Vol. 2018, Article ID 9675050, pp.1–27, DOI: 10.1155/2018/9675050.

Johnson, D., Menezes, A. and Vanstone, S. (2001) 'The elliptic curve digital signature algorithm (ECDSA)', *International Journal of Information Security*, Vol. 1, No. 1, pp.36–63.

Kikwai, B.K. (2017) 'Elliptic curve digital signatures and their application in the bitcoin crypto-currency transactions', *International Journal of Scientific and Research Publications*, Vol. 7, No. 11, pp.135–138, ISSN: 2250-3153.

King, S. (2013) *Primecoin: Cryptocurrency with Prime Number Proof-of-Work* [online] http://primecoin.io/bin/primecoin-paper.pdf (21 August 2018).

Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016) 'Hawk: the blockchain model of cryptography and privacy-preserving smart contracts', *IEEE Symposium on Security and Privacy (SP)*, pp.839–858.

Lamport, L., Shostak, R. and Pease, M. (1982) 'The byzantine generals problem', *ACM Trans. Program. Lang. Syst.*, Vol. 4, No. 3, pp.382–401.

Li, J., Wu, J. and Chen, L. (2018) 'Block-secure: blockchain based scheme for secure P2P cloud storage', *Information Sciences*, Vol. 465, pp.219–231, DOI: 10.1016/j.ins.2018.06.071.

Ma, Z., Jiang, M., Gao, H. and Wang, Z. (2018) 'Blockchain for digital rights management', *Future Generation Computer Systems*, Vol. 89, pp.746–764, DOI: 10.1016/j.future.2018.07.029.

Nakamoto, S. (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System* [online] https://bitcoin.org/bitcoin.pdf (18 August 2018).

Pierro, M.D. (2017) 'What is the blockchain?', *Computing in Science Engineering*, Vol. 19, No. 5, pp.92–95.

Rifi, N., Rachkidi, E., Agoulmine, N. and Taher, N.C. (2017) 'Towards using blockchain technology for ehealth data access management', *Fourth International Conference on Advances in Biomedical Engineering (ICABME)*, pp.1–4.

Schwartz, D., Youngs, N. and Britto, A. (2014) *The Ripple Protocol Consensus Algorithm*, Ripple Labs Inc. White Paper [online] https://ripple.com/files/ripple_consensus_whitepaper.pdf (18 August 2018).

Sharma, P.K. and Park, J.H. (2018) 'Blockchain based hybrid network architecture for the smart city', *Future Generation Computer Systems*, Vol.86, pp.650–655, DOI: 10.1016/j.future.2018.04.060.

Sovbetov, Y. (2018) 'Factors influencing cryptocurrency prices: evidence from bitcoin, ethereum, dash, litcoin, and monero', *Journal of Economics and Financial Analysis*, Vol. 2, No. 2, pp.1–27.

Sullivan, C. and Burger, E. (2017) 'E-residency and blockchain', *Computer Law and Security Review*, Vol. 33, No. 4, pp.470–481.

Sun, J., Yan, J., Zhang, J. and Kem, Z.K. (2016) 'Blockchain-based sharing services: What blockchain technology can contribute to smart cities', *Financial Innovation*, Vol. 2, No. 26, pp.1–9, DOI: 10.1186/s40854-016-0040-y.

Thompson, S. (2017) 'The preservation of digital signatures on the blockchain', *University of British Columbia iSchool Student Journal*, Vol. 3, pp.1–17.

Wood, G. (2017) *Ethereum: A Secure Decentralised Generalised Transaction Ledger eip-150 Revision (759dccd - 2017-08-07)*, Ethereum Project Yellow Paper [online] https://bit.ly/2w69z7o (20 August 2018).

Yang, C., Chen, X. and Xiang, Y. (2018) 'Blockchain-based publicly verifiable data deletion scheme for cloud storage', *Journal of Network and Computer Applications*, Vol. 103, pp.185–193, DOI: 10.1016/j.jnca.2017.11.011.

Yuan, C., Xu, M. and Si, X. (2017) 'Research on a new signature scheme on blockchain', *Security and Communication Networks*, Vol. 2017, No. 10, pp.1–10, DOI: 10.1155/2017/4746586.

Zamfir, V. (2015) *Introducing Casper the Friendly Ghost* [online] https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ (accessed 18 August 2018).

Zheng, Z., Xie, S. and Wang, H. (2018) 'Blockchain challenges and opportunities: a survey', *International Journal of Web and Grid Services*, Vol. 14, No. 4, pp.352–375, DOI: 10.1504/IJWGS.2018.095647.