A Synopsis of Blockchain Technology

Alex Kibet[1], Prof. Simon Maina Karume[2]

***Abstract*—When Satoshi Takemoto (the father of blockchain) released the whitepaper Bitcoin in 2008 that described a "purely peer-to-peer version of electronic cash" known as Bitcoin, blockchain technology made its public debut. Since then Blockchain has been considered an emerging technology for decentralized and transactional data sharing across a large network of untrusted participants. It enables new forms of distributed software architectures, where agreement on shared states can be established without trusting a central integration point. It enables the creation of a decentralized environment, where transactions and data are not under the control of any third party organization. Any transaction ever completed is recorded in a public ledger in a verifiable, secure, transparent and permanent way, with a timestamp and other details. For these features blockchain has developed into one of today's biggest ground-breaking technologies with potential to impact every industry from financial to manufacturing to educational institutions. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system, Internet of Things (IoT), and so on. This paper presents a comprehensive overview of blockchain technology by giving its brief history, describing its architecture, highlighting the challenges facing blockchain technology currently and consensus algorithms used in blockchain-based systems. Furthermore, some thoughts about where it might go in the future are briefly discussed.**

***Index Terms*—Blockchain, decentralization, consensus, consensus algorithm.**

I. INTRODUCTION

Cryptocurrency has become a buzzword in both industry and academic world. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 (Zheng et al, 2016). With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009 (Barber et al, 2012). According to (Cachin & Vukolić (2017) Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency (Zheng et al, 2017). The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency. Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment (Atzori, 2015). Furthermore, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services (Zheng et al, 2016). Those fields favour blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Moreover, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed automatically once the contract has been deployed on the blockchain.

There is a lot of literature on blockchain from several sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. (Tschorsch & Scheuermann, 2016) made a technical review about decentralized digital currencies including Bitcoin. Compared to, this paper focuses on blockchain technology instead of digital currencies. The paper (Lin & Liao, 2017) gave a Survey of Blockchain Security Issues and Challenges. Contrast to paper (Lin & Liao, 2017), this paper focuses on state-of-art blockchain researches including Historical perspective, Architecture, Consensus, and Future Trends.

II. BLOCKCHAIN DESIGN AND ARCHITECTURE

A. Introduction

The blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger (Lee Kuo Chuen, 2015). Figure 1 demonstrates an example of a blockchain. Each block points to the immediately previous block via a reference that is essentially a hash value of the previous block called parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in ethereum blockchain (Buterin, 2014). The first block of a blockchain is called genesis block which has no parent block.

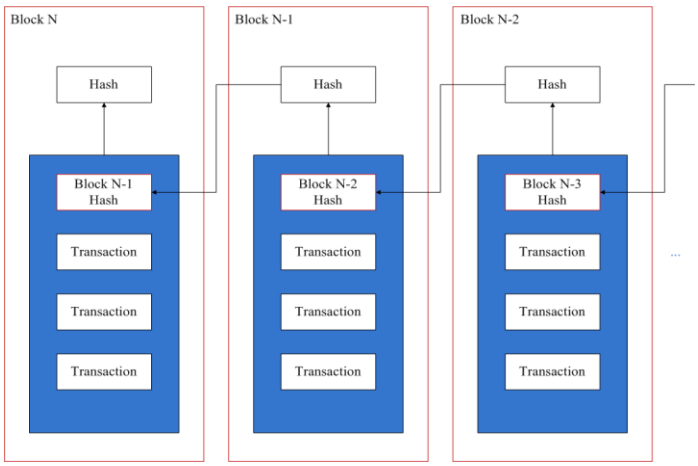

Figure 1 an example of blockchain which consists of a continuous sequence of blocks (Cachin, 2016)

Manuscript received November, 2018.

*Mr. **Alex Kibet**, Department of Computing and Informatics, Laikipia University, Nairobi, Kenya.*

***Prof. Simon Maina Karume**, C.O.D Department of Computing and Informatics, Laikipia University, Nairobi, Kenya.*

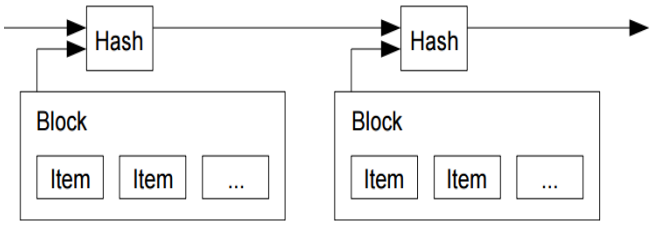

Figure 2 an example of blockchain which consists of a continuous sequence of blocks pointing to previous blocks ash value (Cachin, 2016)

B. Blockchain Block

A block is an aggregated set of data. Data are collected and processed to fit in a block through a process called mining. Each block could be identified using a cryptographic hash (also known as a digital fingerprint). The block formed will contain a hash of the previous block, so that blocks can form a chain from the first block ever (known as the Genesis Block) to the formed block. In this way, all the data could be connected via a linked list structure (Eyal & Sirer, 2018). In particular, the block header includes:

- Block version: indicates which set of block validation rules to follow.
- Parent block hash: a 256-bit hash value that points to the previous block.
- Merkle tree root hash: the hash value of all the transactions in the block.
- Timestamp: current timestamp.
- nBits: current hashing target in a compact format.
- Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions (Aitzhan & Svetinovic, 2018). A digital signature based on asymmetric cryptography is used in an untrustworthy environment. Below is a brief illustration of Block body.

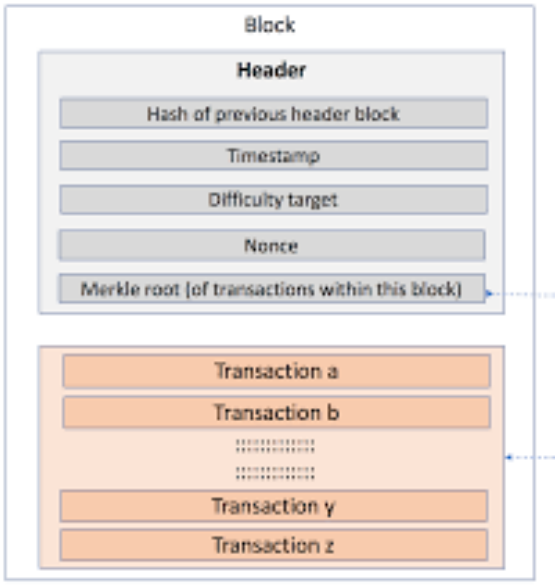

Figure 3 Block structure (Back, 2014)

version	01000000
input count	01
previous hash	0000000000000000000000000000000000000000000000000000000000000000
index	ffffffff
scriptlen	60
script	03636004062f503253482f04358b0553084404f253000017e446522cfabe6d6d690688fb886c0df0c87cbc7ea4f7f1b5c0050bd0ac3751cfc997d9d6971328de040000000000000004861707079204e592120596f7572732047486173682e494f
sequence	00000000
output count	01
value	cb81319500000000
scriptlen	19
script	76a91480ad90d403581fa3bf46086a91b2d9d4125db6c188ac
lock time	00000000

Figure 4 Block structure (Back, 2014)

C. Hashing and Digital signature

Hashing provides a way for everyone on the blockchain to agree on the current world state (Hunt & Koved, 2018), while digital signatures provide a way to ensure that all transactions are only made by the rightful owners (Ozercan et al, 2018). These two properties ensures that blockchain has not been corrupted or compromised. Each user owns a pair of private key and public key. The private key is used to sign the transactions. The digital signed transactions are spread throughout the whole network and then are accessed by public keys, which are visible to everyone in the network (Eskandari et al, 2018). The typical digital signature is involved with two phases: the signing phase and the verification phase. To sign a transaction, a hash value is first generated from the transaction then encryption of this hash value by using senders' private key and sends the encrypted hash with the original data to the receiver. The receiver verifies the received transaction through the comparison between the decrypted hash (by using senders' public key) and the hash value derived from the received data by the same hash function as the sender. The typical digital signature algorithms used in blockchains include ECDSA (Elliptic Curve Digital Signature Algorithm) (Bi et al, 2018).

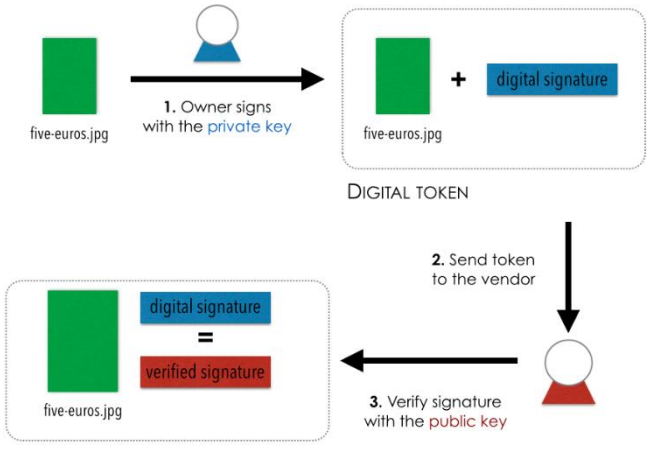

Figure 3 Digital signature and hashing used in blockchain (Zyskind & Nathan, 2015)

D. Major Features of Blockchain

According to (Data Flair, 2018), blockchain has following key characteristics.

Decentralization. In most conventional centralised transaction systems, transaction requires to be authorised through the central trusted parties (such as the central bank) inevitably causing the cost and the performance hold-ups at the central servers. Inversely, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency (Tosh, 2017). In this manner, blockchain can significantly mitigate the performance bottlenecks at the central server. Through this, people trading on a blockchain based applications have a direct control over their accounts by the means of a key that is linked to their accounts which gives the owners a power to transfer their assets to anyone they want. The Blockchain technology has proved to be a really effective tool for decentralizing the web. And it does possess the power to bring massive changes in the industries (Swan, 2015).

Immutability. Since each of the transactions spreading across the network needs to be confirmed and recorded in blocks distributed in the whole network, it is nearly impossible to tamper. Additionally, each broadcasted block would be validated by other nodes and transactions would be checked. So any falsification could be detected easily.

Anonymity. Each user can interact with the blockchain network with a generated address. Further, a user could generate many addresses to avoid identity exposure. There is no longer any central party keeping users' private information. This mechanism preserves a certain amount of privacy on the transactions included in the blockchain. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint that are yet to be discussed.

Auditability. Since each of the transactions on the blockchain is validated and recorded with a timestamp, users can easily verify and trace the previous records through accessing any node in the distributed network (Zheng et al, 2016). In Bitcoin blockchain, each transaction could be traced to previous transactions iteratively (Aitzhan & Svetinovic, 2018). This improves the traceability and the transparency of the data stored in the blockchain.

E. Classification of blockchain and blockchain based systems

There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world: public blockchain, private blockchain and consortium blockchain (Guo & Liang 2016).

Public blockchain- all records are visible to the public and everyone could take part in the consensus process. Here no one is in charge and anyone can participate in reading/writing/auditing the blockchain (Sato & Matsuo, 2017). These types of blockchain are open and transparent hence anyone can review anything at a given point of time on a public blockchain. For example Bitcoin, Litecoin and ethereum (Gervais et al, 2016). With these blockchain networks;

- Anybody can run BTC/LTC/ETH full node and start mining.
- Anybody can make transactions on BTC/LTC/ETH chain.
- Anybody can review/audit the blockchain in a Blockchain explorer.

Private blockchain- This is a private property owned by an individual or an organization. Only those nodes that come from one specific organization would be allowed to join the consensus process (Rouhani & Deters, 2017). Unlike public blockchain this chain has an in charge who looks after of important things such selectively giving access to read or vice versa. Here the consensus is achieved on the whims of the central in-charge who can give mining rights to anyone or not give at all. This makes it centralized again where various rights are exercised and vested in a central trusted party but yet it is cryptographically secured from the company's point of view and more cost-effective for them. For Example: Bankchain. With these types of blockchain networks;

- Anybody cannot run a full node and start mining.
- Anybody cannot make transactions on the chain.
- Anybody cannot review/audit the blockchain in a Blockchain explorer.

Consortium blockchain- This blockchain tries to remove the sole autonomy which gets vested in just one entity by using private blockchains. It ensures that only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. Such that instead of one in charge, there would be more than one in charge. Fundamentally, a group of companies or representative individuals come together and make decisions for the best benefit of the entire network (Li et al, 2018). Such groups are named consortiums or a federation. Example of this type of blockchain include R3 and EWF. In this type of blockchain:

- Members of the consortium can run a full node and start mining.
- Members of the consortium can make transactions/decisions on the chain.
- Members of the consortium can review/audit the blockchain in a Blockchain explorer.

To compare the three types of blockchain this paper is looking at how each of these blockchains deal with Consensus determination, Reading permissions, Immutability, Efficiency, Centralization and Consensus process. The following table gives the summery comparison among the above discussed blockchain types.

Table i: Comparisons among public blockchain, consortium blockchain and private blockchain (Lin & Liao, 2017)

Feature	**Private chain**	**Federation chain**	**Public chain**
Efficiency	High	High	Low
Consensus determination	One organization	Selected set of nodes	All miners
Reading permissions	Could be public or restricted	Could be public or restricted	Public
Immutability	Could be tampered	Could be tampered	Nearly impossible to tamper
Centralization	Yes	Partial	No
Consensus process	Permissioned	Permissioned	Permissionless

F. Challenges facing blockchain

Several blockchain based application are being implemented in a large number of industries, ranging from supply chain to financial services mainly to explore the blockchain technology. While there is no doubt that distributed ledger technology is one of the greatest innovations of recent times, it is likely that it will take a substantial amount of time before the technology is adopted widely. That is because there are several challenges associated with blockchain adoption that must first be mitigated before widespread integration can happen. In this paper, some challenges that needs to be addressed before blockchain mass adoption is possible are discussed. Below are discussed challenges;

Scalability- Blockchains technologies are having trouble in effectively supporting a large number of users on the blockchain network (Crosby et al, 2016). The current leading blockchain networks (Bitcoin and Ethereum), have experienced slowed transaction speeds and higher fees charged per transaction as a result of a substantial increase in users (Catalini & Gans, 2016). Bitcoin block size is currently limited to 1 MB while a block is mined at about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading (Zheng et al, 2017). However, larger blocks means larger storage space and slower propagation in the network. This will lead to centralization gradually as less users would like to maintain such a large blockchain. Therefore the trade-offs between block size and security has been a tough challenge. Therefore, Scalability concerns must be effectively addressed before the blockchain can be adopted on a wide scale.

The Criminal Connection- Since its launch, Bitcoin has long been associated with the shadowy dealings of the black market and the dark web. Because this is the first interaction of the public with blockchain technology, this connection has persisted with Bitcoin, altcoins, and the technology underlying it as well. According to (Li et al, 2017) a team of researchers found that crypto-currencies are used by criminals to facilitate purchases of restricted materials on online marketplaces, as a tool for money laundering, as well as payment methods for ransomware. Although these activities are illegal, they are a result of people's applications of digital currencies and fiat currency too. However, for blockchain technology to be accepted by the public, it must shake this shadowy association.

Inefficient Technological Design- the Ethereum smart contract platform allows developers to deploy their own decentralized applications (DApps) for a varied array of uses. While Bitcoin is the leading cryptocurrency, the Ethereum network allows users to transfer the potential of the blockchain to real-world applications. However, (Metke & Ekl, 2010) has shown that a substantial number of smart contracts deployed on the platform have vulnerabilities due to their coding. Moreover, the Bitcoin network is designed to include a significant amount of data with each transaction. While some of this information is important, not all of it is essential. This makes the Bitcoin blockchain heavy and rather slow. This calls for streamlining and optimization of blockchain design to minimize these inefficiencies to result in widespread adoption.

Energy Consuming Consensus Mechanisms-The majority of blockchains use proof-of-work (PoW) in order to achieve consensus (Androulaki et al, 2017). PoW involves the use of the computational power of a machine to solve complex mathematical equations in order to verify a transaction and add it to a block. While this mechanism works well, as is witnessed in the Bitcoin network, it does consume a lot of energy. It has been reported that the miners who work to validate transactions in the Bitcoin blockchain consume about 0.2 percent of the global electricity total per year (Belle, 2017). Moreover, going on the current trend it is being estimated that by 2020 the Bitcoin network will require more electricity than what the entire world currently uses (Taylor, 2018). Considering the current concerns about global energy production and consumption, blockchains will need to use other methods to achieve consensus, such as the proof-of-stake algorithm which requires much less energy. This will allow the technology to be integrated into a future, which is increasingly conscious of energy matters.

Privacy-The Bitcoin blockchain is designed to be publicly visible. All the information pertaining to a transaction is available for anyone to view. With the exception of privacy-centric coins, this is the same with many of the blockchains currently in existence (O'Leary, 2018). While this feature may be important in some contexts, it becomes a liability if distributed ledgers are to be used in sensitive environments. For instance, private patient data should not be available for all as is the case with proprietary business data. This is also applicable to government data or financial data. For blockchain technology to be adopted on a wide scale, the ledgers need to be altered in order to limit access to the data contained therein to only those who have the necessary clearance.

Security-While it is rather unlikely to happen to large blockchain networks, blockchains are vulnerable to a 51% attack (Eyal & Sirer 2018). This refers to a situation where a miner or a group of miners control more than 50 percent of the mining power. In such a scenario, the miners would be able to control the confirmations of new transactions, especially those by other miners. Moreover, they would be able to reverse the transactions they confirmed and therefore double spend tokens (Aitzhan & Svetinovic, 2018). While the controlling miners would not be able to alter old blocks, this would severely affect the integrity of the token with the affected blockchain and it would need to recover in the public eye. Luckily, the probability of this attack is reduced as more people participate in the network as miners (Sompolinsky & Zohar, 2018).

Costs-Blockchain technology is an effective tool for reducing costs. It reduces the fees associated with transferring value and can streamline operational processes. However, because it is a relatively new innovation, it is difficult to integrate it with legacy systems. Such a process is likely to be an expensive affair that many corporations and governments will be unwilling to undertake (Gomber et al, 2018).

The above-mentioned list of challenges clearly highlight the need for technological improvements to the current state

of blockchain technology for this innovative new technology to take hold on a large scale.

III. CONSENSUS ALGORITHMS

A fundamental problem in distributed computing and multi-agent systems is to achieve overall system reliability in the presence of a number of faulty processes (Calvaresi et al, 2018). This often requires processes to agree on some data value that is needed during computation. How to reach a consensus in distributed environment is a challenge. Blockchains are inherently decentralized systems which consist of different actors who act depending on their incentives and on the information that is available to them (Wright, & De Filippi, 2015). Whenever a new transaction gets broadcasted to the network, nodes have the option to include that transaction to the copy of their ledger or to ignore it. When the majority of the actors which comprise the network decide on a single acceptable state, a 'consensus' is achieved. In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the BG (Byzantine Generals) Problem, which was raised in (ACM Digital Library, 2006). In BG problem, a group of generals who command a portion of Byzantine army circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack would fail if only part of the generals attack the city. Thus, they have to reach an agreement to attack or retreat. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Some protocols are needed to ensure ledgers in different nodes are consistent. For cryptocurrency exchanges, smart contracts and distributed ledger based on blockchain to be led effectively, they should be affirmed by the blockchain. These affirmations depend on what is alluded to as consensus mechanisms. These mechanisms empowers the system to continue working regardless of whether some of its members are coming up short. Below presents several common methods to reach a consensus in blockchain distributed network.

A. Approaches to consensus

Proof of work is a protocol that has the main goal of preventing cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests (Tahir et al, 2018). Satoshi Nakamoto applied this technique to his/her digital currency revolutionizing the way traditional transactions are set. Proof of work is a requirement to define an expensive computer calculation, also called mining that needs to be performed in order to create a new group of trustless transactions (block) on a blockchain distributed ledger. The mining process verifies the legitimacy of a transaction, or avoiding the so-called double-spending and also to create a new digital currencies by rewarding miners for performing the previous task. Anytime a transaction using POW algorithm is set, the following happens behind the scenes:

i. Transactions are bundled together into a block;
ii. Miners verify that transactions within each block are legitimate;
iii. To do so, miners should solve a mathematical puzzle known as proof-of-work problem;
iv. A reward is given to the first miner who solves each blocks problem;
v. Verified transactions are stored in the public blockchain

In PoW, each node of the network is calculating a hash value of the block header using a mathematical puzzle. This "mathematical puzzle" has a key feature: asymmetry (Miraz, & Donald, 2018). The block header contains a nonce and miners would change the nonce frequently to get different hash values. The consensus requires that the calculated value must be equal to or smaller than a certain given value. When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own Blockchains. Nodes that calculate the hash values are called miners and the PoW procedure is called mining in Bitcoin. In the decentralized network, valid blocks might be generated simultaneously when multiple nodes find the suitable nonce nearly at the same time. As a result, branches may be generated (Bergstra & Burgess, 2018).

i. Limitations of POW.

- Selfish Mining Attack—an attacker selectively reveals mined blocks in order to waste computational resources of honest miners.
- In small proof of work-based networks, attackers can easily gain 51% of their computing power at a much lower cost.

POS (Proof of stake) is an energy-saving alternative to PoW. Miners in PoS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network (Caubet, 2018). The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence.

Advances on consensus algorithms

A good consensus algorithm means efficiency, safety and Convenience. Recently, a number of endeavours have been made to improve consensus algorithms in blockchain. New consensus algorithms are devised aiming to solve some specific problems of blockchain. The following gives strengths of consensus mechanism.

PeerCensus - according to (Zheng, 2016) is to decouple block creation and transaction confirmation so that the consensus speed can be significantly increased.

Kraft - (Zheng, 2016) proposed this as new consensus method to ensure that a block is generated in a relatively stable speed. It is known that high blocks generation rate compromise Bitcoin's security. So the GHOST (Greedy Heaviest-Observed Sub-Tree) chain selection rule is proposed to solve this problem. Instead of the longest branch scheme, GHOST weights the branches and miners could choose the better one to follow.

Peer-to-peer consensus algorithm – Chepurnoy et al

through (Chepurnoy et al, 2016) presented a new consensus algorithm for peer-to-peer blockchain systems where anyone who provides non-interactive proofs of retrieving the past state snapshots based on agreed to generate the block. In such a protocol, miners only have to store old block headers instead of full blocks.

IV. FUTURE POSSIBILITIES OF BLOCKCHAIN

Blockchain has shown its potential in industry and academia. This section presents possible future directions with respect to four areas:

1. Blockchain testing
2. Stop the tendency to centralization,
3. Big data analytics
4. Blockchain application.

A. **Blockchain testing**:recently different kinds of blockchains appear and over 700 crypto-currencies are listed in up to now. However, some developers might falsify their blockchain performance to attract investors driven by the huge profit (Zheng, 2016). Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains. Blockchain testing could be separated into two phases: standardization phase and testing phase (Zheng, 2016). In standardization phase, all criteria have to be made and agreed. When a blockchain is born, it could be tested with the agreed criteria to valid if the blockchain works fine as developers claim. As for testing phase, blockchain testing needs to be performed with different criteria.

B. **Stop the tendency to centralization**: Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network (Gipp, Meuschke & Gernandt, 2015). Apart from that, selfish mining strategy (Zheng, 2016) showed that pools with over 25% of total computing power could get more revenue than fair share. Rational miners would be attracted into the selfish pool and finally the pool could easily exceed 51% of the total power. As the blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

C. **Big data analytics:** Blockchain could be well combined with big data for data management and data analytics (Zheng, 2016). As for data management, blockchain could be used to store important data as it is distributed and secure (eg medical records). Blockchain could also ensure the data is original. For the data analytics, transactions on blockchain could be used for big data analytics (Zyskind & Nathan, 2015).

D. **Blockchain applications**: Currently most Blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. For example, user reputations could be stored on blockchain. At the same time, the up-and-coming industry could make use of blockchain to improve performance. A smart contract based on blockchain transaction protocol that executes the terms of a contract are also possible. In blockchain, smart contract is a code fragment that could be executed by miners automatically (Luu et al, 2016). Smart contract has transformative potential in various fields like real estate and any financial services.

REFERENCES

ACM Digital Library. (2006). *ACM transactions on programming languages and systems* (Vol. 28). Association for Computing Machinery.

Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840-852.

Androulaki, E., Cachin, C., De Caro, A., Kind, A., & Osborne, M. (2017, January). Cryptography and protocols in hyperledger fabric. In *Real-World Cryptography Conference*.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?

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

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012, February). Bitter to better—how to make bitcoin a better currency. In International Conference on Financial Cryptography and Data Security (pp. 399-414). Springer, Berlin, Heidelberg.

Belle, I. (2017). The architecture, engineering and construction industry and blockchain technology. *Digital Culture*, 279-284.

Bergstra, J. A., & Burgess, M. (2018). Blockchain Technology and its Applications A Promise Theory view-V0. 11.

Cachin, C., & Vukolić, M. (2017). Blockchains consensus protocols in the wild. arXiv preprint arXiv:1707.01873.

Calvaresi, D., Appoggetti, K., Lustrissimi, L., Marinoni, M., Sernani, P., Dragoni, A. F., & Schumacher, M. (2018). Multi-Agent Systems' Negotiation Protocols for Cyber-Physical Systems: Results from a Systematic Literature Review. In *ICAART (1)* (pp. 224-235).

Catalini, C., & Gans, J. S. (2016). *Some simple economics of the blockchain* (No. w22952). National Bureau of Economic Research.

Chalaemwongwan, N., & Kurutach, W. (2018, January). State of the art and challenges facing consensus protocols on blockchain.

In *Information Networking (ICOIN), 2018 International Conference on* (pp. 957-962). IEEE.

Chepurnoy, A., Larangeira, M., & Ojiganov, A. (2016). A prunable blockchain consensus protocol based on non-interactive proofs of past states retrievability. arXiv preprint. *arXiv preprint arXiv:1603.07926*.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6-10.

Data Flair. (2018, jan 1). *Features Of Blockchain*. Retrieved from Data Flair: https://data-flair.training/blogs/features-of-blockchain/

Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). A first look at the usability of bitcoin key management. arXiv preprint arXiv:1802.04351.

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95-102.

F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

Fernàndez-València, R., Caubet, J., & Vila, A. (2018). Cryptography Working Group Introduction to Blockchain Technology.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3-16). ACM.

Gipp, B., Meuschke, N., & Gernandt, A. (2015). Decentralized trusted timestamping using the crypto currency bitcoin. *arXiv preprint arXiv:1502.04015*.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220-265.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*(1), 24.

Hunt, G. D., & Koved, L. (2018). U.S. Patent Application No. 15/632,522.

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

Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. IJ Network Security, 19(5), 653-659.

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254-269). ACM.

Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, *1*(1), 99-107.

Miraz, M. H., & Donald, D. C. (2018). Application of Blockchain in Booking and Registration Systems of Securities Exchanges. *arXiv preprint arXiv:1806.09687*.

NRI, "Survey on blockchain technologies and related services," Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf

O'Leary, D. E. (2018). Open Information Enterprise Transactions: Business Intelligence and Wash and Spoof Transactions in Blockchain and Social Commerce. *Intelligent Systems in Accounting, Finance and Management*, *25*(3), 148-158.

Ozercan, H. I., Ileri, A. M., Ayday, E., & Alkan, C. (2018). Realizing the potential of blockchain technologies in genomics. Genome research, 28(9), 1255-1263.

Sompolinsky, Y., & Zohar, A. (2018). Bitcoin's underlying incentives. *Communications of the ACM*, *61*(3), 46-53.

Tahir, M., Li, M., Ayoub, N., Shehzaib, U., & Wagan, A. (2018). A Novel DDoS Floods Detection and Testing Approaches for Network Traffic based on Linux Techniques. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, *9*(2), 341-357.

Taylor, D. (2018). An Analysis of Bitcoin and the Proof of Work Protocols Energy Consumption, Growth, Impact and Sustainability.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia.

Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. Work Pap.–2016.

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

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.

Mr. Alex Kibet (BSc)
Designation/Rank: Graduate Assistant at Laikipia University, Department - Computing & Informatics, School of Science & Applied Technology Email Address: alexriongosha@gmail.com, akibet@laikipia.ac.ke

Prof. Karume Simon Maina (PhD)
Designation/Rank: Associate Professor, Laikipia University Chairperson of Department - Computing & Informatics, School of Science & Applied Technology Email Address: smkarume@gmail.com, skarume@laikipia.ac.ke