The Analysis of the Blockchain Technology and Challenges Hampering Its Adoption

Sthembile Mthethwa

***Abstract*—**With the rise in the usage of internet in the past decades, this presented an opportunity for users to transact with each other over the use of internet. Cryptocurrencies have been introduced, which allow users to transact with each other without the involvement of a third party, e.g. the bank. These systems are widely known as cryptocurrencies or digital currencies and the first system to be introduced was Bitcoin which has been receiving a lot of attention. Bitcoin introduced a new technology known as the blockchain technology. In the past years, blockchain has been getting attention; whereby new applications are introduced that utilize blockchain. Yet, most people are still hesitant about the adoption of blockchain and the adoption of cryptocurrencies at large. Some people still do not understand the technology. Thus, it leads to the slow adoption of this technology. In this paper, a review of the blockchain is provided, whereby the different types of blockchain are discussed in details. Details of the things that contribute to the hindrance of the process of adoption are discussed.

***Keywords*—**Bitcoin, blockchain, cryptocurrency, payment system.

I. Introduction

THE rise in the use of internet, in the past decades has been enormous. The advent of the internet has made the rise of social media possible, and billions of people as well as thousands of corporations are now connected and interacting on a daily basis [1]. Thus, the rise in the use of internet has introduced technologies that incorporate the use of internet [1]. As we stand today, we are at the edge of new revolution of digital currencies or cryptocurrencies, whereby the internet is beginning a new phase of decentralization [2].

For the past decades, there has been a considerable advance in cryptography and decentralized computer networks fields, resulting in the emergence of a profound new technology [2]. This technology was introduced in 2008 when the first cryptocurrency was represented as Bitcoin [3]. Bitcoin introduced a way for two unrelated parties to transact with each other without the involvement of a third party [3]. This technology is known as blockchain, and it is said to possess a lot of potential of fundamentally changing the way in which society or systems operate [2]. A blockchain is essentially a distributed database whereby it records all the transactions that have occurred since from the inception of blockchain until now [4]. All the transactions in the blockchain are verified by consensus of the participants in the system, and once it is recorded in the blockchain, it cannot be erased [4]. The blockchain technology has the capacity of eliminating the role and the need of depending on a third party widely known as the middleman [2]. As the first successful cryptocurrency, it presented opportunities, whereby other cryptocurrencies have been introduced utilizing the same technology and these are called altcoins. That was not the end, as it is said that blockchain has a lot of potential for systems other than digital currencies and it lead to the introduction of blockchain to other systems like smart contracts [5].

In this study, presented is the technology introduced by Bitcoin known as blockchain. This study will contribute by presenting a review or study on the blockchain technology. The organization and layout of the paper is as follows. Section II presents the background and related work of payment systems and how this led to the introduction of blockchain. Section III presents the protocol used by Bitcoin leading to blockchain. Section IV describes different types of blockchains and how they might be adopted for other systems. Section V describes challenges and benefits that might come with the adoption of blockchain to other systems, and finally conclusion is given in Section VI.

II. Literature Review

Payment involves two parties, a payer and a payee. Payment can be defined as “the transfer of funds which discharges an obligation on the payer's side vis-a-vis a payee” [6]. For payments to be successful, payment systems have to be in place to assist with payments and to ensure that payments follow the right procedures. Payment systems have been defined as "the complete set of instruments, intermediaries, rules, procedures, processes and interbank funds, transfer systems which facilitate the circulation of money in a country or currency area” [6]. Payment systems have evolved drastically in the past decades.

The initial and ancient system to be used is known as the bartering system, whereby goods and services were exchanged for other goods and services [7]. This method was also known as direct exchange and it required one to find an individual who had the goods one was looking for and at the same time in need of the goods one has. This method was sought a better way of exchange, yet it was cumbersome with regards to the time required to find the right person to trade with. This gave rise to commodity currencies.

Commodity currency is actually based on the idea that commodities have value on them [8]. People had to choose their own good and amongst them, dyes, beads, shell jewelry were used. An improvement to these was gold and silver and it became the famous form of commodity money. Despite the

S. N. Mthethwa is with the Council of Scientific and Industrial Research (CSIR), Pretoria, South Africa and currently registered for a Master’s Degree at University of Fort Hare, Alice, South Africa (e-mail: smthethwa@csir.co.za).

improvement achieved through commodity currencies, the goods used were not convenient due to their sizes and weight to be carried around. This led to the introduction of metal coins. The value of the metal coin was actually based on the intrinsic value of metal used to make the coin [9].

As a stepping stone to coin money, paper money was introduced. Initially paper money was in a form of a receipt which was issued by the bank to the depositor and was redeemable for whatever gold/silver they had stored [8]. This became the most successful way of making payments as it was convenient. Researchers continued proposing better and improved ways of payments, whereby cards were introduced. Cards introduced a new way of payment whereby one does not necessarily need to carry cash around. The increase in the use of technology and internet presented an opportunity of using them to better the way payments are made. Today, it is a norm for people to prefer the use of technology (mobile phones, cards, and internet) to conduct payments rather than cash as it is prone to theft. Payments systems such as M-Pesa have been introduced, which utilizes mobile phones in order to conduct payments [10]. M-Pesa presented an opportunity for the unbanked to transfer money between each other and the only requirement is a mobile phone. It is said to the most successful payment system in Africa.

From the success of M-Pesa, other payment systems using mobile phones were introduced even in South Africa, e.g. Instant money and e-Wallet. As technology keeps on improving, so does payment systems making things much easier for people. A new payment system that is currently gaining momentum is known as digital payment systems widely known as electronic cash or cryptocurrencies.

Even though the idea of electronic cash is gaining momentum now, it is not something new [11]. It was brought forth by Cypherpunk movement which was launched in 1990 [12]. Cypherpunk movement was a series of meetings attended by cryptographers and was based on the early cryptographic developments, e.g. blind signature, public key cryptography, but then it was discontinued [12]. The first system to be introduced was e-cash which was introduced by Chaum [13]. Another system was introduced known as Hashcash, introduced by Back [14], which was a method for spam limitation using proof of work. In 2004, Finney made an improvement to hashcash and it was known as RPOW (Reusable Proofs of Work) but was later discontinued [15]. In 2008, Bitcoin was introduced and was the first successful cryptocurrency to be introduced [3]. The main aim of Bitcoin was to allow two parties to transact with each other with the involvement of a third party, e.g. the bank. Bitcoin also provides a solution to a long standing problem in computer science known as double spending. The solution involves the use of peer to peer network that uses proof of work to record history of all transactions in a public ledger called blockchain, and this was the main innovation introduces by Bitcoin.

The success of Bitcoin piqued a lot of interest, leading to other cryptocurrencies being introduced known as altcoins, e.g. Litecoin, Peercoin, Darkcoin, Namecoin. The journey did not end there, researchers started studying blockchain for the aim of being used in other systems other than digital currencies, e.g. smart contracts, electronic voting, intellectual property etc. [16], [17].

III. The Bitcoin Protocol

In this section, a general overview about Bitcoin, adding the details that will be needed later in this paper. Because Bitcoin does not depend on a central authority to control the supply, distribution and verification of the validity of transactions, but it relies on a network of volunteers known as miners.

A. Transactions and Blocks

A transaction is when bitcoins are being moved from one or more sources to one or more destinations [18]. At an abstract level when transactions are created, they must be published to the network whereby miners are required to verify whether the transaction meets the following criteria defined by [18]:

- Output may be claimed once;
- New outputs are created as a result of a transaction;
- Sum of inputs has to be greater or equal to the sum of outputs.

Whereby the references to be claimed outputs along with the proofs of ownership form an input [18], and output is where the bitcoins are being sent to. Thus, at all times, transactions must meet this requirement:

$$sum\ of\ outputs \leq sum\ of\ inputs \quad (1)$$

Once a transaction has been verified, then it can be added to a pool (collection of verified transactions that still need to be added to the blockchain) and later added to a block.

Miners group transactions into blocks and they race or compete in order to find a solution to cryptographic puzzle, this is known as proof of work. Computational power needs to be utilised to find a solution and a solution needs to found after every 10 minutes. This is ensured by increasing or decreasing the difficulty level of the problem after every 2016 blocks, which is approximately two weeks. When a miner successfully finds a solution, it must be published to the network for other miners to verify and then abandon the block they are working on and move on to another block. Transactions not included in the current published block would be moved to the next block to be created. As a compensation for miners to utilise their computational power, 25BTC (which is halved every four years) are given to them when they find a solution and this is the only way new coins are introduced to the system.

B. Blockchain and Blockchain Forks

Blockchain is a public record of all transactions grouped into blocks that have occurred from the entire existence of Bitcoin. Blocks are linked together (thus the name blockchain) and the linking leads to the first block to be published in the system known as the genesis block. Blocks are connected to their predecessors via a hash and the chaining of blocks is used in order to assign a chronological order of the

transactions [18]. Fig. 1 visualizes the structure of the blockchain.

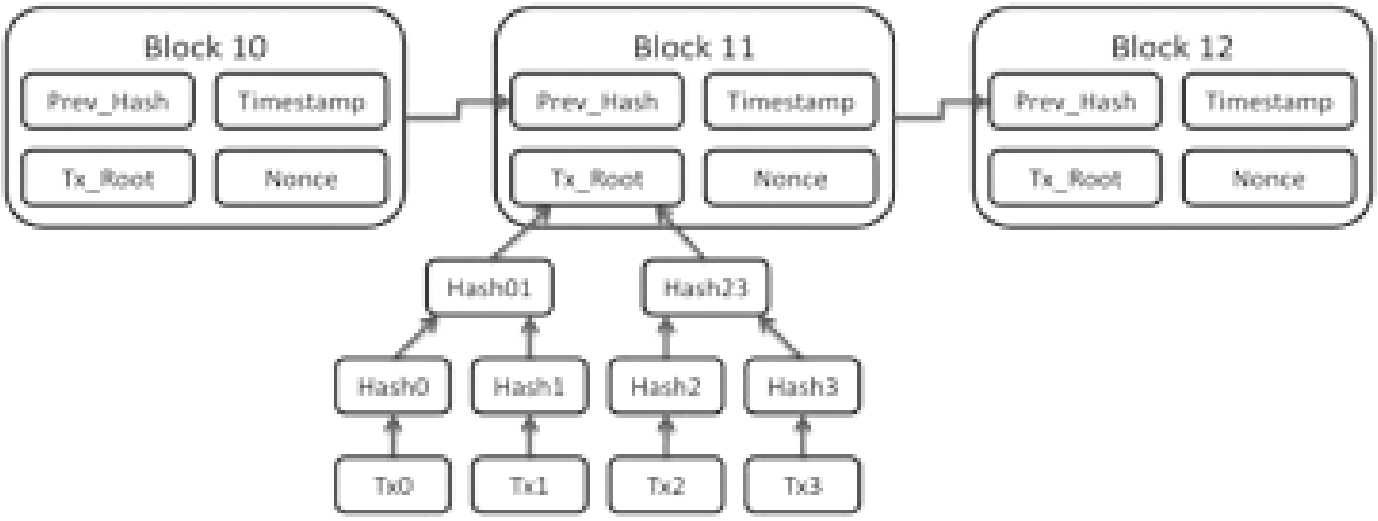

Fig. 1 Blockchain Structure from [3]

Messages in the network are propagated in a gossip method, whereby messages are transactions and blocks. To avoid messages being sent to nodes that already have them, messages are not sent directly to nodes. Instead, the availability of messages is broadcasted in the network by sending an *inv message* to neighbours. These are only sent when the transaction and blocks have been verified. Upon receiving the message, a node that does not possess this information would request it by sending a *getdatamesage* to the sender of the *inv message*. Fig. 2 visualizes the flow of messages in the network.

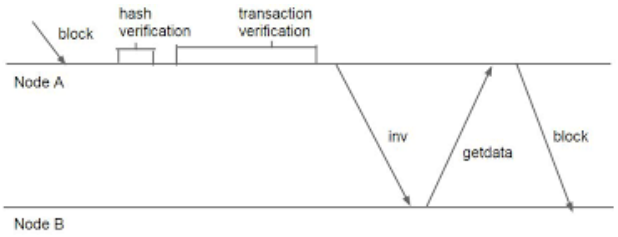

Fig. 2 Information Propagation from [18]

Each message broadcast is likely to experience propagation delay, [18] defines a propagation delay as the combination of transmission time (including announcement known as*inv message*, request from receiving node and a delivery) and the local verification of the block or transaction.

Due to communication delays, it happens that two blocks gets to be published at the same time in the network leading to a blockchain split known as blockchain fork. When this happens, miners consider the first block they receive to be the blockchain head and continue building on top of that [26] and Fig. 3 depicts how this looks like. This is resolved when one chain becomes longer than the other; therefore, all miners switch to the longest chain which is considered the main chain. Blocks on the other chain become orphans; nonetheless transactions included in those blocks are added to the next blocks to be added to the chain. It is advised that a transaction be considered tentatively confirmed when it is six blocks deep in the blockchain, this way it is difficult for an attacker to change the contents of a transaction.

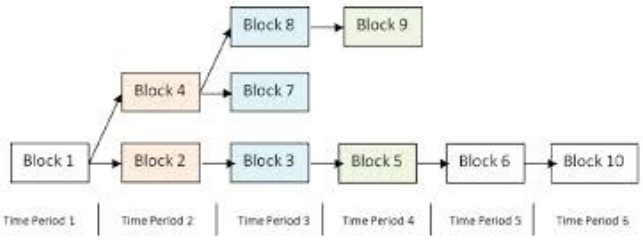

Fig. 3 Blockchain Fork from [19]

IV. Different Types of Blockchains

Blockchain can be characterized into different types, which are discussed here.

A. Permissionless Blockchains

This is where everyone is allowed to participate during the process of verification meaning that no authorisation is required, if one has the requirements (computing power), one can join and start verifying [1]. This is because these verifiers are vital to the operation of the network, and for this a reward or incentive through the issuance of coins is given to them to encourage their participation [20]. An example of this type of blockchain is Bitcoin and many other cryptocurrencies.

Permissioned blockchains are intended to be purpose built, and can be created to maintain compatibility with existing applications [21]. The main advantage of this type is that it can accommodate anonymous or pseudonymous actors [22] and protect against a Sybil (identity-forging) attack [23].

B. Permissioned Blockchains

This is when the nodes responsible for the process of verification are preselected by the central authority or consortium [1]. If all the participants in the network are known and can be trusted to vote honestly, there is no need to introduce the artificial incentives to ensure that cooperation will take place. Thus, by selecting trusted members to participate in the verification process, the operation of the network can be made faster, more flexible and most importantly, much more efficient. Nonetheless, at the cost of reduced security, immutability and censorship-resistance. This procedure is almost the same to the finance setting of Know Your Customer (KYC) procedure.

The intention behind knowing nodes responsible for verification is that they are legally accountable for their activity. An advantage of this type of blockchain is scalability. Only a small number of preselected participants are responsible for verification, and if transactions come from large institutions, they will be able to scale their computing power in line with the increase in the number of transactions. However, because of the smaller number of participants, it is much easier for a group of users to collaborate and alter the rules or change transactions and in addition it is easy for them to reject transactions. Therefore, it is not censorship-resistant like a permissionless blockchain would be [1]. Examples of this type include Hyperledger, Eris, Ripple, and others [24].

C. Public Blockchains

This whereby anyone can read and submit transactions to the blockchain [21]. Most permissionless blockchains have public access and this includes most of the cryptocurrencies. Properties of public blockchains include:

- Easy entry and exit
- Openness
- Transparency
- Built-in-precautions for operation in untrusted environment

These properties could be beneficial for their adoption for decentralized applications.

D. Private Blockchains

This type of blockchain limits read access to the predefined list of entities (e.g., blockchain operators and auditors). End users need to depend on interfaces provided by blockchain operators in order to read and submit transactions [20]. These could only be permissioned [21].

Private blockchains could maintain the dependency on middleman (third etities) for operations, thus limiting innovation [20]. Table I shows a comparison between the different types of blockchains.

TABLE I
TRADE-OFFS BETWEEN TYPES OF BLOCKCHAIN ARCHITECTURE FROM [5]

Category	Permissioned	Permissionless
Fast	yes	no
Energy-efficient	yes	no
Easy to scale	yes	no
Censorship resistant	no	yes
Tamperproof	no	yes

V. RISKS AND CHALLENGES FOR BLOCKCHAIN ADOPTION

Blockchain is a promising breakthrough technology [5]. Few different start-ups have been proposed, trying to create their own blockchains with specific use cases yet this defeat the purpose of having a network itself because it just recreates silos [22]. These spams from financial to non-financial applications like Notary services, smart contracts, electronic voting, and intellectual property [16]. Most of these are radical innovations and as it happens with adoption with radical innovations, there are significant risks of adoption [4]. The section below gives a description of these risks.

A. Awareness and Understanding

The main challenge with blockchain is the lack of awareness and this hinders its adoption because it is difficult for people or companies to adopt something they do not entirely understand. Banking sectors are still behind and they are not willing to accept blockchain, and other sectors are still in doubt with blockchain and this hampers the exploration of this technology.

B. Security and Privacy

Many blockchains used by cryptocurrencies like Bitcoin offers users with the chance of using theses currencies without revealing their identities. Thus, these cryptocurrencies offer 'pseudonymity'. This then introduces a problem to those applications that require user's identities. Most applications need to ensure that user's information is secured all times, and because everything in the blockchain is public, they become hesitant about the adoption of the blockchain technology to their applications. The concern of security plays a major role to the technology being accepted or not. Though the most concern comes from lack of understanding, because there would know that it is possible to make the blockchain suitable for any use case.

C. Regulations and Governance

Trying to keep up with the advances and improvements in technology has always been a problem or struggle especially when it comes to the governance and regulations (it takes a while for them to adapt and accept new technologies) [22]. The blockchain technology presented a new method of transacting which bypasses the current regulations making it very difficult for the government to accept the opportunity presented by this technology. Yet, many applications are being introduced utilizing blockchain and this might sway or convince the government into regulating cryptocurrencies. Yet, this might be twofold whereby the government might regulate it and then pass laws for compliance or they might slow its adoption. Therefore, this might slow the process of adoption.

D. Scalability

Generally, this is a very important concern in any system [9]. Taking into consideration Bitcoin, currently the size of a block is limited to 1 MB meaning approximately 2200

transactions are included in a block which includes few transactions per second as depicted in Figs. 4-6. This then posse a challenge for systems that require more transactions to be processes in a second, e.g. Visa processes approximately 2000 tps. Another issue with scalability is the fact that transactions are considered confirmed when the block that contains the transaction is six blocks deep in the blockchain [27], [28]. This might be problem for transactions that need to be processed and confirmed faster. Currently in the Bitcoin system, every node responsible for mining in the network keeps the full copy of the blockchain which increases incredibly and the diagram below shows its size. The size of the blockchain is increased after every 10 minutes. Thus said, this shows that blockchain might not be scalable enough for some applications, yet some improvements can be made for it to work better with those applications.

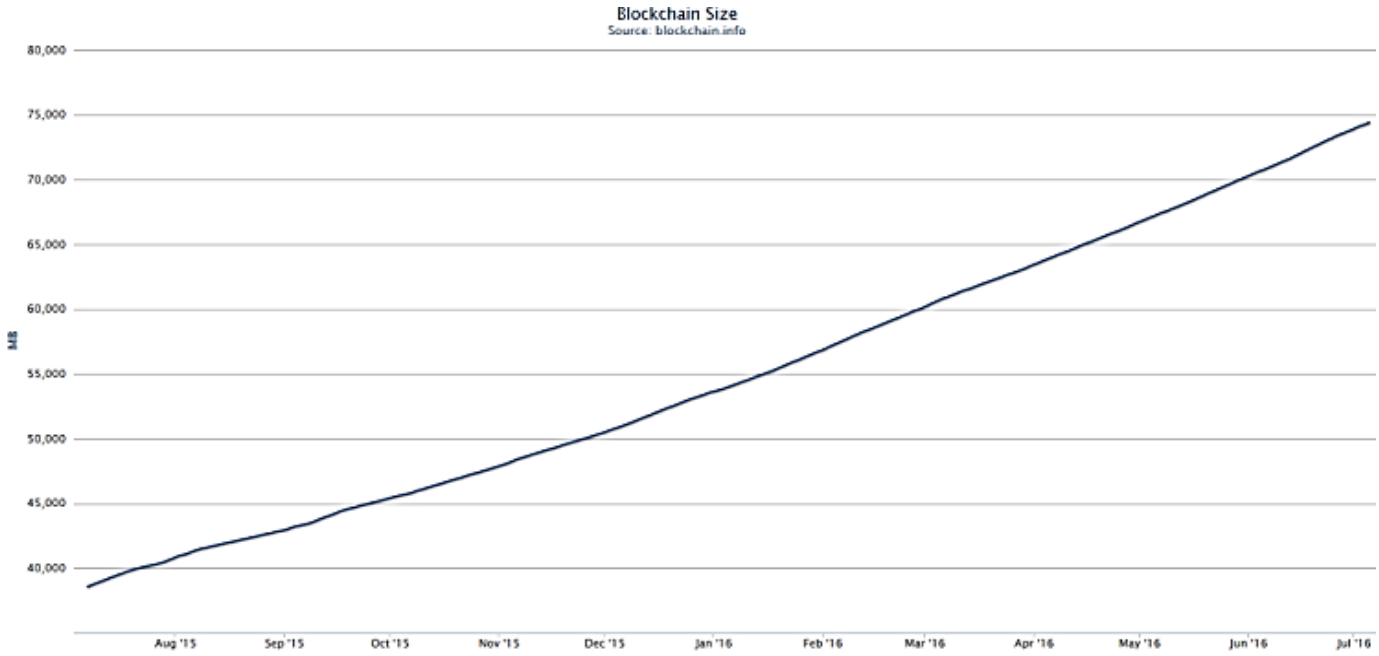

Fig. 4 Blockchain Size from [25]

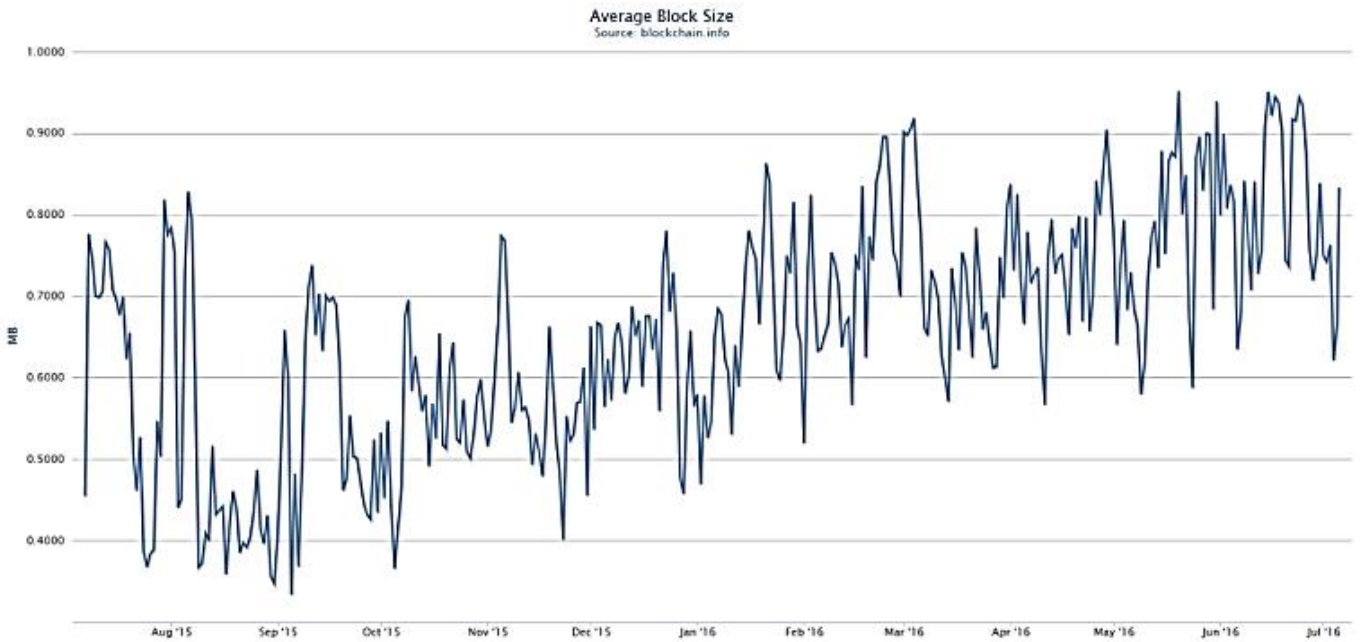

Fig. 5 Average Block Size from [25]

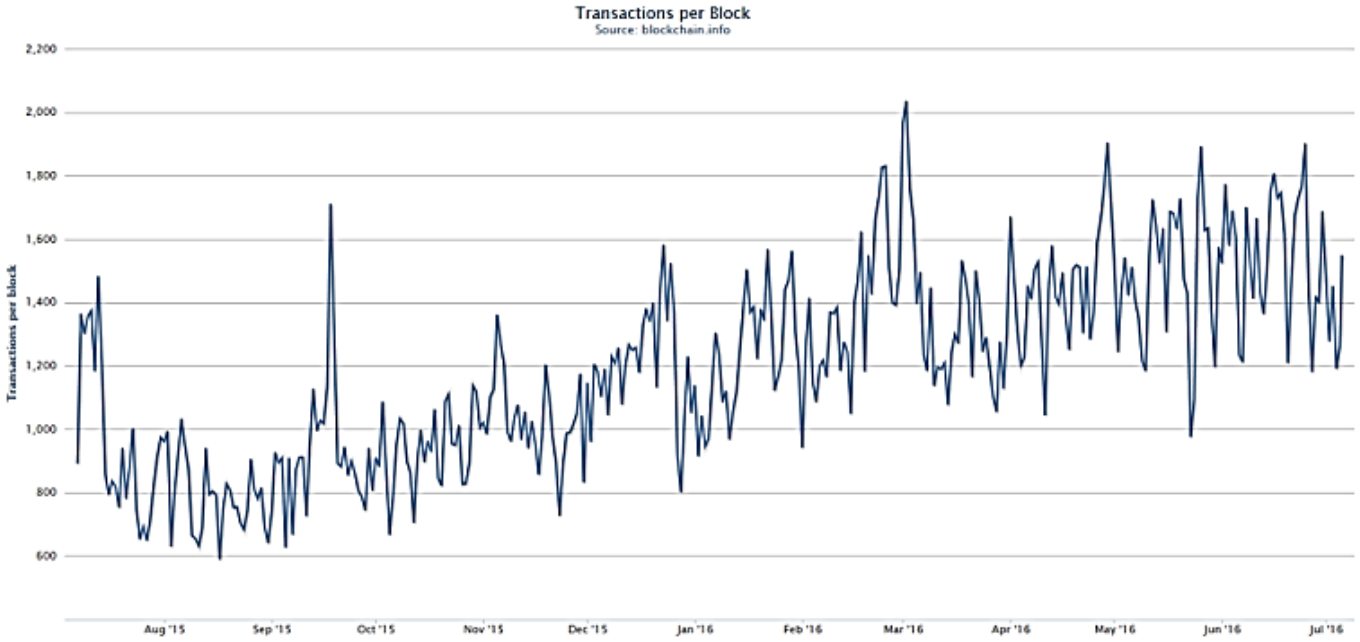

Fig. 6 Average Transactions per Block from [25]

E. Computing Power

Blockchain is protected by an encryption algorithm and miners are required to solve a mathematical problem. Once a miner submits a solution to this problem, a reward is given to them which is in a form of newly minted coins. At the beginning, CPUs were used for the process of mining but then those were not enough as the adoption increased [29]. GPUs were then used, which later became slower therefore FPGAs were adapted [30]. These also became slower leading to ASICs which are incredibly fast [31]. These kept on changing drastically just because more people were joining the network and the target or difficulty also increased as depicted in Fig. 7. The main problem with mining is that a lot of computing power is needed for someone to start the mining process, so this must be considered because the blockchain must be secured using this algorithm. Because of this other means of mining have been introduced, e.g. Proof of Stake, Proof of Burn to try and limit the use of more computational power [32]-[35]. Therefore, presenting opportunities for applications to choose which one might be suitable for them.

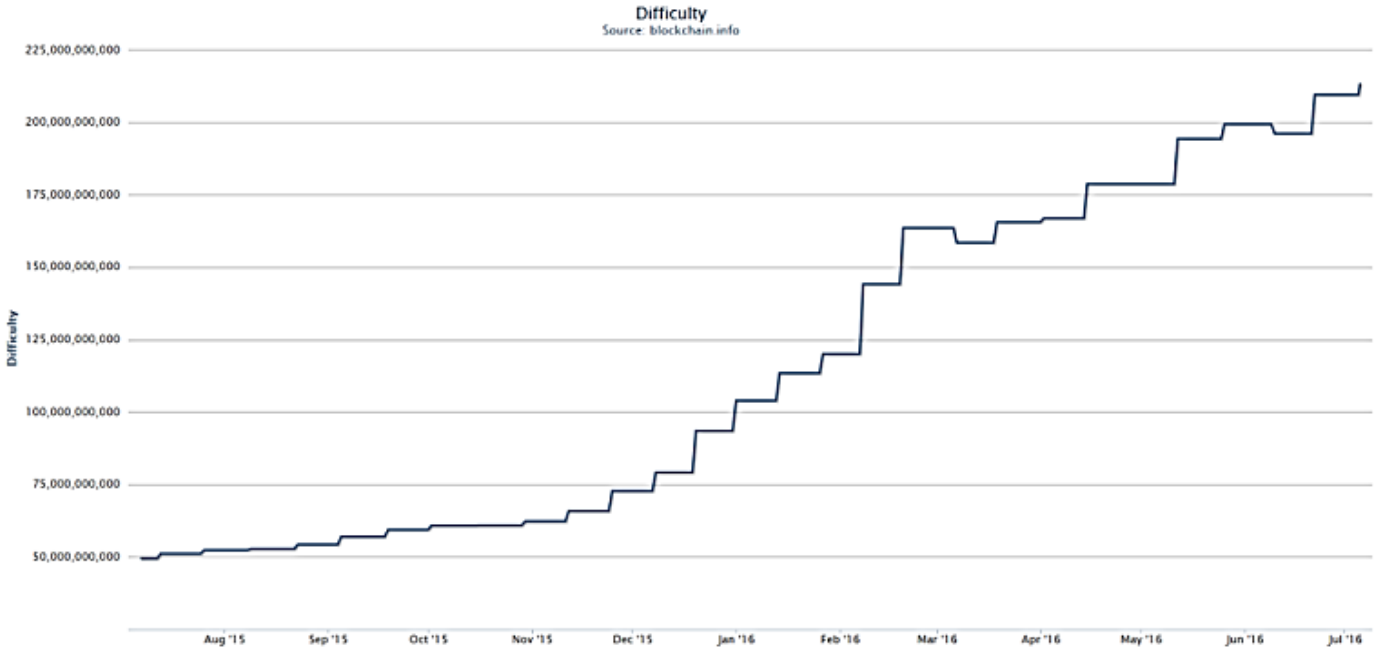

Fig. 7 Mining Difficulty from [25]

VI. Conclusion

Blockchain technology is a promising technology for many applications other than those in the financial sector. Yet, the problem with its adoption is presented by lack of understanding on how this technology functions. Therefore, this paper presents a review of the blockchain leading to in depth knowledge that could be used as motivation when it comes to its adoption. Few points have been discussed that need to be considered and understood thoroughly before adopting blockchain and these currently hinders the adoption of this technology.

Acknowledgment

The author would like to acknowledge the department of Science and Technology and CSIR, for funding this research.

References

[1] G. W. Peters, and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," Available at SSRN 2692487, 2015.

[2] A. Wright, and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," Available at SSRN 2580664, 2015.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/en/developer-documentation, 2008, Accessed: July 2016.

[4] M. Crosby, N. Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, 2016.

[5] J. Mattila, "The blockchain phenomenon The Disruptive Potential of Distributed Consensus Architectures," BRIE Working Paper, 2016.

[6] T. Kokkola, "The payment system. Payments, Securities and Derivatives, and the role of the eurosystem," Frankfurt am Main: ecB, 2010.

[7] W. V. Volker, "Essential Guide to Payments," Veritas Books, 2013.

[8] K. Menger, "On the origin of money," in The Economic Journal, 2(6):239{255, 1892.

[9] M. Mwale, "Modelling the dynamics of the bitcoin blockchain," thesis, Stellenbosch: Stellenbosch University, 2016.

[10] I. Mas, and D. Radcliffe, "Mobile payments go viral: M-pesa in Kenya," 2010.

[11] M. Moser, "Anonymity of bitcoin transactions: An analysis of mixing Services," In Proceedings of Munster Bitcoin Conference, 2013.

[12] P. Franco, "Understanding Bitcoin: Cryptography, engineering and economics," John Wiley & Sons, 2014.

[13] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28(10):1030{1044, 1985.

[14] A. Back, "Hashcash-a denial of service counter-measure," http://www. hashcash. org/papers/hashcash, 2002, Accessed: July 2016.

[15] H. Finney, "Rpow: Reusable proofs of work," Cypherpunks, 2004.

[16] G. Foroglou, and A. Tsilidou, "Further applications of the blockchain," 2015.

[17] P. Tasca, "Digital currencies: Principles, trends, opportunities, and risks. Trends, Opportunities, and Risks," September 2015.

[18] C. Decker, and R. Wattenhofer, "Information propagation in the bitcoin network," In IEEE P2P 2013 Proceedings, pages 1{10. IEEE, 2013.

[19] B. L. Shultz, and D. Bayer, "Certication of witness: Mitigating blockchain fork attacks," 2015.

[20] Bitfury Group, "Digital assets on public blockchains," Bitfury Group Limited, 2016.

[21] Bitfury Group and J. Garzik, "Public versus private blockchains part 2: Permissionless blockchains," Bitfury Group Limited, 2015.

[22] T. Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems," 2015.

[23] J. R Douceur, "The sybil attack," In International Workshop on Peer-to Peer Systems, pages 251{260. Springer, 2002.

[24] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," In International Conference on Trust and Trustworthy Computing, pages 163{180.Springer, 2015.

[25] "Blockchain Info," https://blockchain.info/charts, accessed in July 2016.

[26] J. Gobel, G.P. Groenewald, A.E. Krzesinski, and M. Mwale, "Simulation Modelling of Bitcoin Blockchain," SATNAC, 2015.

[27] I. Eyal, A. E. Gencer, E.G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)* (pp. 45-59), 2016.

[28] K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, and E. Gün, "On scaling decentralized blockchains," In *Proc. 3rd Workshop on Bitcoin and Blockchain Research*, 2016.

[29] N. T. Courtois, M. Grajek, and R. Naik, "The unreasonable fundamental incertitudes behind bitcoin mining," *arXiv preprint arXiv:1310.793*, 2013.

[30] M. Sprague, "Optimizing BitcoinGeneration and the Feasibility of Profitability," 2013.

[31] M. Vilim, H. Duwe, and R. Kumar, "Approximate Bitcoin Mining," in Proceedings of the 53rd Annual Design Automation Conference, p.g. 7, ACM, 2016.

[32] B. Laurie, and R. Clayton, "Proof-of-Work proves not to work; version 0.2," In *Workshop on Economics and Information, Security*, 2004.

[33] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," *arXiv preprint arXiv: 1406.5694*, 2014.

[34] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake (Extended Abstract)," in *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34-37, 2014.

[35] P4Titan, "Slimcoin A Peer-to-Peer Crypto-Currency with Proof-of-Burn Mining Without Powerful Hardware," 2014.

Sthembile N. Mthethwa is currently pursuing her Masters in Computer Science at the University of Fort Hare funded by the CSIR. She holds an Honours Degree in Information System and Technology from the University of KwaZulu-Natal.