International Journal of Innovative Computing 9(2) 51-57

INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Concept of Blockchain Technology

Muhammad Anwar Hussain*, Muhammad Shafie Abd Latiff, Syed Hamid Hussain Madni
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
81310 UTM Johor Bahru, Johor, Malaysia
Email: anwarhussain@graduate.utm.my* , shafie@utm.my

Raja Zuraidah Raja Mohd Rasi
Faculty of Technology Management, Universiti Tun Hussein Onn Malaysia
86400 Parit Raja, Batu Pahat, Johor, Malaysia

Mohd Fairuz Iskandar Othman
Faculty of Information & Communication Technology
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal
Melaka, Malaysia

Submitted: 23/07/2019. Revised edition: 16/10/2019. Accepted: 17/10/2019. Published online: 28/11/2019
DOI: https://doi.org/10.11113/ijic.v9n2.238

***Abstract*—Blockchain, Bitcoin's core technology, and spinal cord have received enthusiastic attention since the last couple of decades. The Blockchain serves as a paradigm for distributed and unchangeable computations for bitcoins and cryptocurrencies. The key features behind this technology are to create a reliable, secure, transparent, decentralized, and reliable autonomous ecosystem. It is useful for a variety of applications, especially for legacy devices, resources, and infrastructure. In this article, we presented a technical overview, its application, and the challenges associated with blockchain technology and cryptocurrencies. This study aims to provide a ground-breaking overview and future research direction and promising importance of Blockchain.**

Keywords: **Blockchain, internet of things, bitcoin, digital signature, classification**

I. INTRODUCTION

Blockchain technology is the new pragmatic wave of disruption evolution that has previously underway to re-shape the digital economy, business, political, and social communications. Blockchain is considered to be another way of digital value exchange in this new era of Information and Communication Technology. Moreover, it is not just changing, but also evolutionary change, and a vigorous phenomenon that is already on the way to evolutionary motion [1]. Despite the hype of Blockchain, top more than 40 financial organizations and many others have already started to explore Blockchain to minimize transaction costs, transaction efficiency, avoid the risk of fraud, and eliminate intermediary services and middleman role [2]. Fewer organizations are trying to adopt new technology by replacing traditional or legacy systems. New and next-generation technology offers a new horizon of services to stack holders.

Nowadays, the digital currency has become the top 20 keywords and buzzword in both academia and industry. Being one of the most successful cryptocurrencies, Bitcoin has gained immense success in a market approaching U$ 66.18 billion in the 4th quarter of 2018 (coindesk, 2018). The core behind Bitcoin is the Blockchain. The first time in history blockchain was proposed in 2008 and implemented in 2009 [3]. Blockchain is considered as public-ledger that holds whole committed transactions linked in a chain of blocks. This link list of transactions grows and new block relayed on a chain and this record of list continuously increases. Distributed consensus algorithms and asymmetric cryptography have been applied to ensure user security and ledger consistency. Critical characteristics of blockchain

technology are trust, decentralization, anonymity, persistency, and audibility. Owing to these traits, blockchain technology can significantly improve efficiency and save costs [4].

Blockchain has two-fold features organizational and technical aspects that can be described as "TRUE" and DAO [4]. The first denotes trustable, reliable, usable, and efficient. Later denotes decentralized, and distributed, autonomous and automated, as-well-as ordered and organized. In net-shell, Blockchain is considered a novel distributed paradigm and decentralized architecture for computing. That store encrypted data into blocks and linked each other and form the chain of blocks. Then stored data is validated through distributed consensus mechanism and ensures data security and privacy in data access and transmitted over network crypto-graphically, and represents data in self-executable script program (i.e. Smart Contract) [5, 6].

It allows a financial transaction to be done without any intermediary or any bank or third party. Blockchain has many financial implications, such as remittance, electronic assets, and online payments [7, 8]. Nowadays, it can apply to other areas like smart contracts [9], Internet of things [10], public services [11], security services [12], and reputation systems [13]. The remaining paper is organized as follows. Section II describes the architecture of Blockchain. Section III shows challenges and recent advances in Blockchain. Section IV explores possible future directions. Section V summarizes possible future direction. Section VI discusses the constrains of blockchain adoption, and section VII concludes the paper.

II. Architecture of Blockchain

The Blockchain is composed of linear chronological transactions list of sequenced blocks just link-list data structure that holds old transaction records in old legacy traditional public ledger [14]. Every block point to predecessor block via reference pointer. It contains a hash value of immediately predecessor blocks known as parent block. Furthermore, it is essential to note that block does not have parent block means uncle blocks (the block's ancestors have no founder) hashes values would keep in Ethereum blockchain [15]. The first block of the link list is called genesis that has no parent block. Fig. 1 demonstrates an example of a blockchain link list [14]. This part illustrates the internal architecture of the Blockchain. The rest of this part will describe the digital signature, key artifacts of Blockchain, and the taxonomy of Blockchain.

A. Inside the Block

The block composes of a header of the block in hashes and body of block illustrates in Fig. 2. Inner building blocks are divined to dissect; header includes:

- **Version of Block**: It identifies validation rules that need to follow in the block.
- **Hash value of parent**: It is a hash value of 256-bit, which refers to a predecessor block.
- **Hash value of merkle tree**: It contains hash values of all transactions.
- coindesk: Timestamp of current time in seconds since 1970-01-01T00:00 UTC.
- **nBits**: It is a compact format of target hashing.
- **Nonce**: It holds arbitrary value starts with Zero and increases sequentially for each hash value calculation of the 4-byte field.

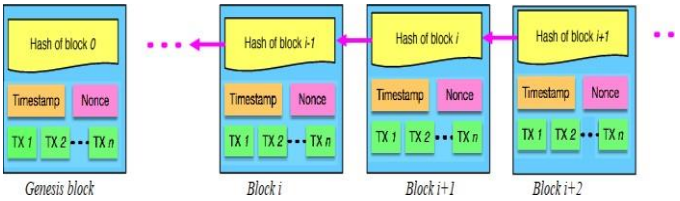

Fig. 1. Exemplary view of blockchain comprises of consecutive sequence of blocks

Block Version	03000000
Parent Block Hash	B6f0b1b1680a2a30ca44d346d9e8 910d334beb48ca0c000000000000
Markel Tree Root	9d10ab53ee959487ca9286953c0f 60dda20811decd12bc9b04aabb31
Timestamp	25d93a54
nBits	30c31b18
Nonce	Fe9f0864

Transaction Counter

Tx1 Tx2 Tx3 … Txn

Fig. 2. Inside view of block

The intrinsic structure of the block is composed of transactions and counter [14]. The block size depends upon the maximum number of transactions size of transaction that a block hold. Blockchain uses Asymmetric cryptographic algorithms (i.e., SHA-256) to secure and authenticate transactions record [16]. The untrustworthy environment of transactions based on asymmetric cryptography digital signature.

B. Digital Signature

On the Peer-to-Peer network of nodes in Blockchain, each user holds its own pair of keys, first is called private key or secret key, and the second is called public key or address key. The prime function of the private key that is used to sign transactions in a block digitally. Digital signed transactions are broadcast over the entire network, and that can be accessed only through public keys. That is visible to every node in the network. Fig. 3 illustrates a sample of digital or e-signature of Blockchain. In the classic technique of digital, e-signature is involved in two-fold phases: In the first fold, the transactions are signed, and in

the second fold, verification is done. Refer to Fig. 3, where user Alice intends to sign-up transaction process. She in first step generates hash values of transaction and then triggered. After that, she encrypts transactions hash values with the help of her private key and sends back to the third user. Bob encrypts hash values of the original data. When Bob receives the request, he verifies transactions and compares between the decrypted hash values (public key of Alice's used) and then hash value is devised from received data from hash Algorithms function as Alice's. Elliptic curve digital signature algorithms (ECDSA) in [15] used digital signature algorithms in Blockchain.

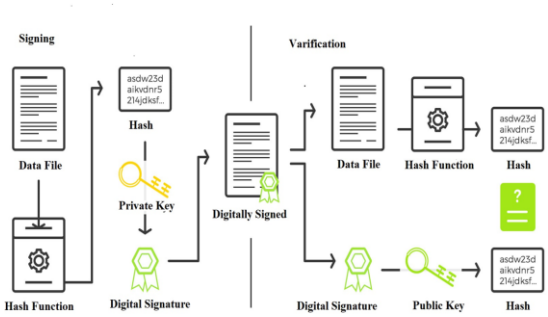

Fig. 3. Digital signature used in blockchain

C. Key Features of Blockchain

Prime and key features in Blockchain that are inherited are given below.

- **Decentralization**: In the traditional centralized system as compared to decentralization, each transaction on the Peer-to-Peer blockchain network is being validated and verified without a central trusted agency. As a result of this central trusted agency (e.g., the central bank) the invite cost and performance are issued by central servers. Consequently, a transaction in the Blockchain between any two peers (P2P) is authenticated without a central agency. However, in this way Blockchain reduces the server costs (Sum up of operation and development) significantly that can alleviate performance issues at a central position server [17].
- **The Persistency:** Every transaction over a network needs to be confirmed and finally appended in blocks across a distributed node of network by honest miners. It is zero level tolerance to delete or rollback validated transactions once it is appended on blockchain. In validating the transaction, a block immediately discovered, therefore any forge, falsification easily detected.
- **The Anonymity**: Each user can interact with the generated address with the Blockchain, which does not expose the real identity. There is no central authority that keeps the user private information secret. This mechanism provides a pseudonymous guarantee of privacy in transactions within a Blockchain [18]. It is worth note that Blockchain cannot provide assurance to transactions privacy due to the essential constraints.
- **Auditability**: Auditability feature validate the transactions and permanently recorded with a timestamp. Owing to this property, the user can smoothly trace and verify all old records since the inception of Blockchain in a distributed environment. This mechanism improves the transparency and traceability of the stored data in the Blockchain [19].
- **Immutability**: This feature of Blockchain provides an alter proof mechanism. It means when a record writes in a block is never be changed forever. But this feature prone to 51% attack, nodes take control over 51% can alter the record.
- **Trustable**: This feature provides complete transparency of data over Blockchain. This reality of transparency ensures trust among stakeholders over the blockchain P2P network. Anyone can trust over system blindly.

D. Blockchain Classification

Blockchain can be divided into three different types: Public, Private, and Consortium [17, 20, 21]. We distinguish the three types in different perspectives, as shown in Fig. 4.

In the first type of Blockchain (public), all transaction records are readable and viewable of every node of the network. Anyone could take part in the process of consensus. In private Blockchain only selected nodes or designated nodes come from the specific organization could be allowed to take part in the consensus process. While in consortium blockchain, an only pre-defined groups from organizations could take part in the consensus process. In summary, private Blockchain followed centralized control by one organization, public Blockchain decentralized and consortium Blockchain partially decentralized. We summarize the comparative analysis of three different types of Blockchain in Table 1.

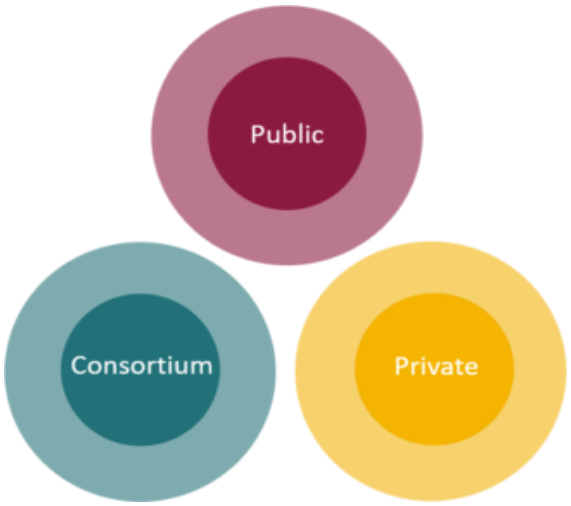

Fig. 4. Blockchain types

TABLE 1. Comparisons between Private, Public and Consortium Blockchain

Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission Read	Public Class	Could be public or restricted	May be public or restricted
Determination of Consensus	All miners	Only one organization	Designated set of nodes
Efficiency	Low	High	High
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Consensus	Permissionless	Permissioned	Permissioned

III. Challenges and Recent Advances

As an emerging and prevalent technology, Blockchain is facing enumerate challenges, and some of them succinct elaborated in the following.

A. Scalability

As blockchain size is growing up and list of records and transaction increases in size as well. This process leads to the need of more storage capacity for storing transactions record. Presently, Cryptocurrency Bitcoin backed by Blockchain attains a maximum of 100GB storage nowadays. The whole transactions need to be validating each transaction in a chain. In spite of the original constraint of block size, a new block is generated a in a specified time interval. The Bitcoin transactions per second time is 7 (TPS) that is not enough for millions of transactions in real-time. The miners prefer high fee payers and put in delay small capacity of transactions. As a result, the propagation speed slows down and big size blocks delayed, and the performance of the network reduced automatically. When the chain becomes larger it leads to branches and therefore, the scalability issue exists in Blockchain.

B. Privacy Leakage

The Blockchain provides a secure and save path for nodes over P2P network to create transactions addresses that is real-time identity of the users. Users envision many addresses, and sometimes information leakage may happen. Therefore, as discussed in [16] and [10] Blockchain cannot guarantee transactional privacy and balances for each public key that is publicly visible. Besides that, the study in [15] have shown Bitcoins transactions are linked to reveal user's information. Furthermore, disclose a method to connect user pseudonyms.

C. Selfish Mining

Disruptive blockchain technology is subject to plotting and comes up with a selfish miner's attack. Typically, nodes convinced to take over 51% of computing power and do happened transactions reversed. A recent study shows nodes having less than 51% of computing power are also vulnerable to the blockchain network. In actual, [22] describes the network is prone to even a small part of hashing in cheating. In selfish mining issues, mined blocks are kept hidden without broadcasting over the peer-to-peer network. This leads to becoming a private branch to the public by fulfilling a few requirements. By this process, the private branch becomes longer than the public chain. The other miners over network is accepted by incentive fee holding miners as well. Host miners waste their computing resources in private blockchain publication, and on the other hand, selfish miners are mining without competitors on the private chain. So selfish mind miners earn more revenue. Rational miners are attracted by the selfish pool of miners, and selfish strategy miners could exceed 51% of computing power quickly.

IV. Blockchain Applications

The blockchain diverse in its application. In this section, we sum up a few important blockchain applications. We categorize applications into finance, IoT, e-Business, security and privacy, social and public services from a broader perspective.

A. Finance

Financial services since the inception of Blockchain such as Bitcoin and Hyperledger, has a massive impact on traditional business and financial services. [23] describes that being disruptive technology, Blockchain revolutionized

financial sectors like the banking world. This technology applied in the clearing and settlement area of asset management. [24] mentions collateralization of business derivatives in real use cases could leverage to minimize costs and risks. Large companies like Microsoft and IBM started using the Blockchain-as-a-services in cloud computing.

B. Internet of Things (IoT)

Internet of things (IoT) is a prominent information and communication technology (ICT) that gaining global market attention in recent years. The IoT devices are sensor-enabled that integrate physical objects into smart via the Internet and provides a bundle of services. The important applications of IoT include smart homes, logistic management with RFID technology, smart energy, e-health, smart homes, smart grid, and Maritime Industry. Blockchain technology has the potential to improve IoT services such as E-business, safety, privacy, and many more [25].

C. E-Business

[9] purposes E-business model that realize smart property payment transaction based on Blockchain and smart contract. This model used a Distributed Autonomous Corporation (DAC) property for a decentralized transaction. Trading personal used DACs to exchange coin and sensor data without intermediaries.

D. Safety and Privacy

Safety and privacy are another concern for Internet of things (IoT) Industries. IoT applications' privacy can be improved with the help of Blockchain. [25] suggest a privacy-preserving method for the installation of IoT objects into the cloud ecosystem. Furthermore, a new architecture model was proposed to prove manufacturing provenance authentication without a third party. IBM in 2015 revealed its proof of concept for Autonomous-decentralized Peer to Peer Telemetry (ADEPT), which used blockchain technologies to build up a distributed network of nodes. With the help of ADEPT, devices are connected to the Internet from home, easily identify the problem and get software updates on their own.

E. Public and Social Services

There are many applications of Blockchain in social and public services. It includes land registration, energy-saving, education, and free-speech right. In life, land information is a tangible physical entity, and ownership rights can be published and registered on Blockchain-based services. Any changes made on land, transfer of land, and mortgage can be recorded and managed on Blockchain, and as a result, it improves the efficiency of public services.

V. Possible Future Directions

Due to the open behavior of public Blockchain, it attracts communities' active users. New public Blockchain emerges daily. Business applications are primary users of consortium blockchain, recently Hyperledger developing framework for the business process by using consortium blockchain. Blockchain second generation Ethereum is also providing tools of Blockchain based on for consortium type. Many companies are still implementing efficiency and auditability.

Blockchain technology shows exponential growth and potential in academia and industry. Some possible future directions are:

A. Blockchain Testing

Blockchain testing comprises of two phases: First is called standardization, and the second is called the testing phase. In the later phase, complete criteria have to be made and agreed upon when blockchain dawn up and tested it with agreed-upon criteria to validate developer work. In the later phase, testing needs to be carried out with different criteria. For example, a user who may be the supervisor of online retail business is cautious in throughput of the blockchain transaction, so he examines the average time of the transaction to be packed into Blockchain, block capacity, etc.

B. Big data Analytics

Blockchain technology could be merged with big data. There are two types of combinations: data management and data analytics. For data management, Blockchain could be used to preserve important data because it is distributed and secured. In big data analytics transactions data is tempered proof and must be kept on Blockchain that could be used for big data analytics. For example, client trading patterns might be forecasted. The client can predict their partner's trading behaviors with the use of big data analytics.

VI. Constraints of Blockchain Technology Adoption

Disruptive technology of blockchain facing some critical issues. Few projects of Blockchain have entered into full implementation from pilot testing. According to [23], enumerate obstacles are limit the adoption of Blockchain in the mainstream.

A. Slow operation of Blockchain

In spite of inevitable efficiency as compared to the multiday authorization of bank transactions and consensus operations in credit, companies still generate long delays on a distributed public ledger network. In addition to that, obfuscation and encryption of traditional layers that keep data confidential required more time for processing.

Consumers and businesses expect speedy and instantaneous operations for customer value creation.

B. Data Breaches

Cryptocurrency trading platforms reports about breaches of data contrasted crypto requirements that needed for the ironclad type of data security, across distributed ecosystems, as well as refraining manager in the adoption of Blockchain technology.

C. Lack of Standardized Architecture

There are more than 6500 blockchain active projects enlisted on GitHub as of 2018. Since blockchain architectures are not standardized until now, Projects are based on different privacy measures, protocols, consensus, and code writing languages. Due to the lack of standardization, business connections between firms are difficult to establish.

D. High Cost

The development of blockchain application conforms to customer specifications, needed expensive, specialized, and complex integration efforts.

E. Legislation Constraints

Another obstacle for consideration while adopting Blockchain are innovative projects include a smart contract and regulation requirements. Regulatory constraints, particularly in medical and financial applications, refrain and rollout of smart contact applications in many countries.

F. Obstacle of Mass Users

A final hindrance is a critical mass of users that enables the mass adoption of blockchain technology. Everest's has taken large-scale human beings' projects initiatives for the marginalized of blockchain either to checkout on the belief that will address needs of acceleration on blockchain technology.

VII. CONCLUSION

The Blockchain depends on its decentralized, peer-to-peer and secured cryptographic algorithms, and endorsed and appraised by industry and academia. However, many prominent researches think Bitcoin shielded by blockchain technology. But Blockchain could be applied to a variety of fields far beyond Bitcoin. Blockchain transforms the traditional industry into disruptive technology due to its key features, persistency, decentralization, anonymity, and auditability. In this paper, we present a brief overview of the blockchain concept, including blockchain architecture and key characteristics of the Blockchain. In addition to that, we enlist some issues and concerns that would hinder the development of Blockchain. Finally, we summarized existing approaches to address these issues and possible future directions.

ACKNOWLEDGEMENTS

We would like to express the appreciation to Universiti Teknologi Malaysia (UTM) for supporting this research via the Collaborative Research Grant (CRG grant number: Q.J130000.2451.07G35). Thanks to all other members from Universiti Tun Hussein Onn Malaysia (UTHM) and Universiti Teknikal Malaysia Melaka (UTeM).

REFERENCES

[1] D. Tapscott and A. Tapscott. (2018). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Portfolio.

[2] Y. Yuan, T. Zhou, A. Zhou, Y. Duan, and F. Wang. (2017). Blockchain Technology: From data intelligence to knowledge automation. *Acta Automatica Sinica*, 43(9): 1485-1490,

[3] S. Nakamoto. (2008). Bitcoin: A Peer-to-peer Electronic Cash System.

[4] F. Wang. (2018). Blockchain Intelligence: Cornerstone of the Future Smart Economy and Smart Societies. *Proc. 2nd World Intell. Congr.*

[5] Y. Yuan and F.-Y. Wang. (2016). Blockchain: The State of the Art and Future Trends. *Acta Automatica Sinica*, 42(4), 481-494.

[6] Y. Yuan and F.-Y. Wang. (2016). Towards Blockchain-based Intelligent Transportation Systems. *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2663-2668, IEEE.

[7] G. Peters, E. Panayi, and A. Chapelle. (2015). Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. *Journal of Financial Perspectives*, 3(3).

[8] N. Gogerty and J. Zitoli. (2011). DeKo: An Electricity-backed Currency Proposal. *Social Science Research Network.*

[9] Z. Zheng, S. Xie, H. Dai, and H. Wang. 2016. Blockchain Challenges and Opportunities: A Survey; Work Paper. Ed: Inderscience Publishers: Geneva, Switzerland.

[10] Y. Zhang and J. Wen. (2015). An IoT Electric Business Model Based on the Protocol of Bitcoin. *2015 18th International Conference on Intelligence in Next Generation Networks*, 184-191, IEEE.

[11] B. W. Akins, J. L. Chapman, and J. M. Gordon. (2014). A Whole New World: Income Tax Considerations of the Bitcoin Economy. *Pitt. Tax Rev.*, 12, 25.

[12] C. Noyes. (2016). Bitav: Fast Anti-malware by Distributed Blockchain Consensus and Feedforward Scanning. *arXiv preprint arXiv:1601.01405.*

[13] M. Sharples and J. Domingue. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. *European Conference on Technology Enhanced Learning*, 490-496: Springer.

[14] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang. 2018. Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14(4), 352-375.

[15] D. Johnson, A. Menezes, and S. Vanstone. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1), 36-63.

[16] S. Omohundro. (2014). Cryptocurrencies, Smart Contracts, and Artificial Intelligence. *AI matters*, 1(2), 19-21.

[17] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, and K. Ko. (2017). Decentralized Consensus for Edge-centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access*. 6, 1513-1524.

[18] M. Moser. (2013). Anonymity of Bitcoin Transactions.

[19] G. Zyskind and O. Nathan. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE Security and Privacy Workshops*, 180-184, IEEE.

[20] V. Buterin. (2014). A Next-generation Smart Contract and Decentralized Application Platform. *White Paper*, 3, 37.

[21] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain. (2017). *Business & Information Systems Engineering*, 59(3), 183-187.

[22] I. Eyal and E. G. Sirer. (2018). Majority is Not Enough: Bitcoin Mining is Vulnerable. *Communications of the ACM*, 61(7), 95-102.

[23] G. W. Peters and E. Panayi. (2016). Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. *Banking Beyond Banks and Money*. Springer, 239-278.

[24] M. Morini. (2016). From 'Blockchain hype' to a Real Business Case for Financial Markets. *Available at SSRN 2760184*.

[25] T. Hardjono and N. Smith. (2016). Cloud-based Commissioning of Constrained Devices Using Permissioned Blockchains. *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*, pp. 29-36. ACM.