BLOCKCHAIN POWERED FRAMEWORK FOR DEPOSITORY FINANCIAL INSTITUTION

Dipak Prabhu Kandare[1], Dr. Mohammad J. Haque[2], Dr. Mohammad Muqeem[3]

[1] *M.Tech Scholar, School Of Computer Science And Engineering, Sandip University, Nashik, Maharashtra, India.*
[2] *Guide, SOCSE, Sandip University, Nashik, Maharashtra, India.*
[3] *Guide, SOCSE, Sandip University, Nashik, Maharashtra, India.*

---***---

Abstract - *Blockchain is considered as the important technological innovation behind Bitcoin system. It facilitates the transaction payment process by creating a decentralized, general ledger to improve regulatory capacity and remove unnecessary intermediaries. At present, the blockchain technology has been employed in the financial industry for a wide range of experimental application and exploration. In this paper, we firstly analyze the principal architecture and the technical characteristics of blockchain. Then its current research achievements and application scenarios are introduced. Finally, the application of blockchain in Indian Foreign Exchange Trade System is designed and explored. Combining with the credit matching trading system X-Swap, an inter-bank application based on the blockchain technology is implemented*

Key Words: **Blockchain, Digital currency, Inter-bank application, Transaction clearing.**

1.INTRODUCTION

Blockchain, as the term suggests, is the chain linked by blocks. It is a decentralized, general ledger. The blockchain holds a complete, all-agreed transaction records. Thanks to the information stored in the block header, the records cannot be modified Any modification will cause the hash value of the information in the block to be inconsistent with that recorded in the block header . This creates an open distributed general ledger system.

The most significant difference between the transaction structure based on block chain and the traditional transaction structure is that all participants share a common ledger, and all participants have a complete general ledger (even if some transactions are not relevant to it). Then the two nodes will no longer carry out transactions by a central institution, but by means of public ledger. Because there are no central institutions, the blockchain technology firstly need to solve the problem of data accuracy and reliability in the process of transaction. The POW, POS, DPOS and other consensus mechanisms can be employed to achieve node consistency in a decentralized distributed system. That is to solve the problem of the Byzantine General, thus ensuring the transactions can be completed correctly, quickly and safely without supervision.

The payment and transfer behaviour of digital currency (such as Bitcoin) is supported by blockchain and can be used for a number of payment scenarios. Among these scenarios, the blockchain has a greater significance in the public financing and charitable donation. The characteristics of blockchain make the information (e.g. fund source and flow) open and transparent, which can reduce the regulatory costs and improve the regulatory efficiency. Meanwhile, using blockchain in the field of finance and securities can reduce the settlement and clearing costs of the exchange. For some products, it can provide 24-hour trading and real-time settlement. Blockchains can also be used for the registration and certification of various tangible or intangible assets, including text, pictures and other intellectual property rights and even proof of property, vote statistics and so on. As the record cannot be changed once it is written in blockchain, the blockchain technology has inherent advantages in the field of data protection and notarozatopm.

2. RELATED WORK

The blockchain technology is derived from Satoshi Nakamoto's foundational paper "Bitcoin: a peer-to-peer electronic cash system", which describes in detail how to build a new, decentralized and point-point trading system. It has been proven by Bitcoin in 2009 [1]. As Bitcoin becomeincreasingly popular, various research and applications of the underlying blockchain technology has shown a blowout trend [2].

The original Bitcoin is programming limit, numerous previous endeavors make great efforts on building applications on the Bitcoin. However, lottery, micropayments, verifiable computation have been proven to implement difficultly by using Bitcoin's scripting language [3]. Ethereum is the first Turing-complete decentralized trading system [4]. Numbers of companies and enthusiasts created a wide range of smart contract applications on Ethereum. Such as supply chain provenance, crowd-based fundraising, derivatives trading and prediction markets [5].

The consensus mechanism is one of the most important part of blockchain technology. How to reach a consensus efficiently in the distributed system is a significant research problem in the field of distributed computation. Bitcoin has achieved the consistency of distributed account books through POW (Proof of work) mechanism, which is highly dependent on node computing power [1]. Along with the development of blockchain technique, the researchers have proposed a variety of protocols which can reach a consensus mechanism independent of calculation. For instance, POS (Proof of stake) [6] and DPOS (Delegated Proof of Stake) [7] is currently the two most popular protocols. IBM HyperLedger used the PBFT (Practical Byzantine Fault Tolerant) mechanism to reach a consensus [8], which is the first application of the BFT protocol [9]. Vukolic compared the two mechanisms of POW and BFT, and focused on their scalability limits in a detailed analysis, and then he made some improved recommendations [10]. Eval proposed new measures to quantify the security and efficiency of blockchain protocol, and designed a new BTF protocol named Bitcoin-NG, which does not exist the scalability limits in Bitcoin [11]. The Luu team, has proposed a new consensus protocol named SCP, which has a mechanism that allows reaching consensus without broadcasting actual block data that still enabling valid blocks verification [12]. Additionally, they recently proposed a new distributed agreement protocol for permission-less blockchains named ELASTICO, which is deemed to the first candidate for a secure sharding protocol with presence of byzantine adversaries [13].

At present, the security of the blockchain also attach the focus of attention of the researchers. What the most important problem POW mechanism facing is 51% attack problem [1]. The POS mechanism solve the 51% attack problem restricted to a certain extent, but also led in N@S (Nothing at stake) attack problem [14]. Bissias builds a mathematical model quantifies the importance of several factors that determine the attack's success, including confirmation depth, attacker mining power, and any confirmation deadline set by the merchant [15]. However, there is still no ideal solution for the attacks, which requires further research breakthroughs.

The world's leading financial institutions are stepping up to explore the blockchain of landing applications. UBS is exploring a blockchain-based "utility settlement coins" to solve the efficiency of settlement [16]. Citibank is a global banking network and is exploring ways to use blockchain technology for cross-border flows of funds across their banking networks, which will help simplify cross-border transfers and reduce transfer costs [17]. The Australian Stock Exchange believes that the distributed general ledger technology can greatly simplify and accelerate the post-transaction processes, reduce risk, reduce management and compliance expenditures, and allow investors to access almost real-time settlement and securities trading speed [18]. Nasdaq Private Equity Market recently launches a blockchain-based financial service platform Linq. As a complement of its private equity trading platform, Linq expands and enhances its stock management capabilities [19]

3. TYPICAL ARCHITECTURE AND MAIN FEATURES OF BLOCKCHAIN APPLICATIONS

The typical architecture of blockchain application consists of the application layer, the interface layer, the shared protocol layer, and the shared data layer (see Figure 1). The hierarchical characteristics of the blockchain application and the traditional application are very different.

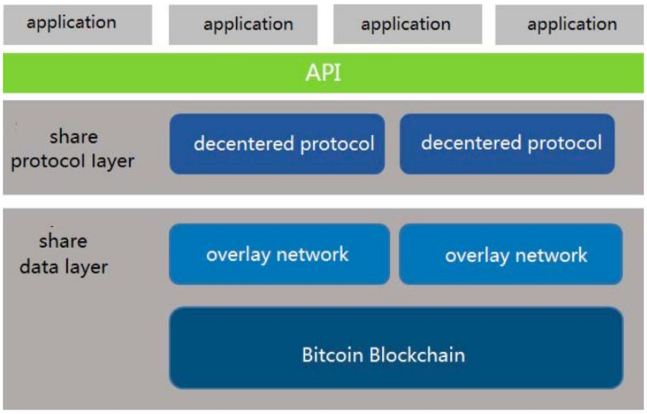

Fig-1 Application Architecture based on Blockchain

Take the bitcoin as an example, the blockchain is the shared data layer, and the de-centralized protocol is located in the shared protocol layer. These two parts are in the gray rectangles in the figure, which are decentralized, open source, and uncontrolled by any organizations or individuals. The shared protocol layer and shared data layer account for 80% of the proportion in the entire architecture. The higher the level, the lower the proportion. While in the typical network applications based TCP/IP and HTTP, the decentralized and open source parts usually account for about 15%. It now appears that the blockchain has the potential to make the current transaction process more efficient, and can improve the regulatory capacity and remove unnecessary intermediaries. Blockchain has the following advantages which make it possible to subvert the current business transaction model:

A. Distributed database

Blockchain technology make each node has a complete transaction records by synchronizing transaction data between all nodes. Even if one or several nodes fail, it will not affect the transactions stored on other nodes. Therefore, the transaction records will not be lost. If the blockchain is applied to the financial system, the central authority of the trading system is no longer responsible for the storage of transactions, which will reduce and even eliminate the risk of server downtime. This is the main embodiment of blockchain's advantages.

B. Smart contract

Smart contract is the programming script which puts a set of contract terms into an agreement. The contract codes will be executed automatically by the computer when the conditions are stratified. Take bitcoin as an example (see Fig- 2). At first, user A creates and publishes a smart contract to raise bitcoins. The content of this contract is that it will divide 10% of the profits to his investors. Then there are three investors bought the contract, the amount is 35, 50 and 80 bitcoins (or the equivalent currency). When user A obtain 100 dollars in profits in a transaction, the 10% of the profits, 10 US dollars, will be dividends to the three investors in accordance with the proportion of investment. This is a regular dividend process, but the dividend process can be automatically executed by the computer under the smart contract support.

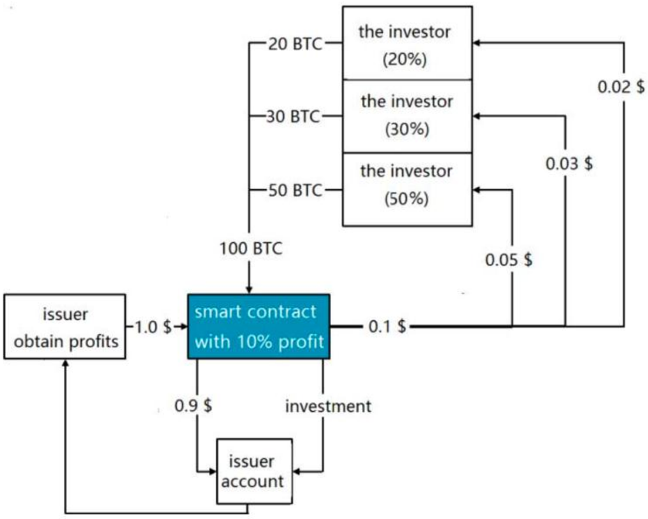

Fig- 2 Smart Contract

A. Payment area

The original application of the blockchain was to build a system for payment. The issuer and receiver do not need the central transaction party during the payment process. It is necessary to firstly explain how the current payment system works to demonstrate the potential value of blockchain for financial institutions. In a standard inter-bank fund transfer process, if the issuing bank and the receiving bank do not open an account with each other, they will must rely on a central clearinghouse or associated bank (see Fig-3). Workflow takes several days from the implementation of the settlement, and in the meanwhile we should pay the middle party a fee.

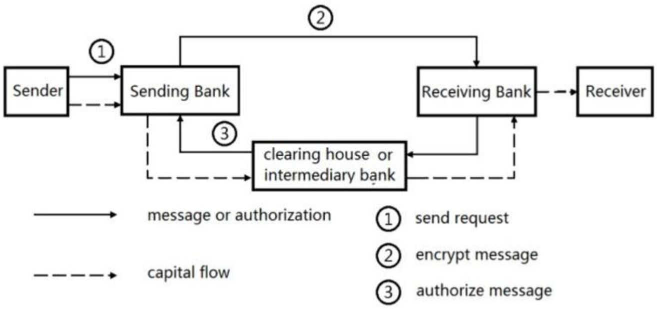

Fig- 3 Traditional Inter-Bank Market Payment Process

For the payment system of legal entities belonging to the same banking group, inter-bank payments are often done by central counterparties, each bank have a local database (see Fig- 4). This database records all account balances and transaction flows as an authoritative general ledger. But this payment structure has two drawbacks: First, the local database must be reconciled and synchronized. Second, the central counterparties are required to make payments after offsetting the borrowings of different accounts.

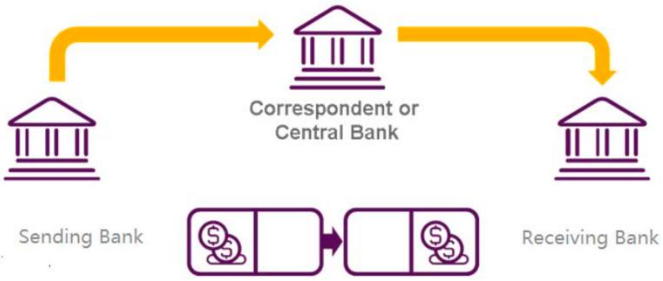

Fig- 4 Agency Banking Mode

For the same group of banks, the initial solution is to use blockchain to generate a general ledger for the payment behaviour. Each bank can be a participant in a private blockchain network, take part in the consensus process and complete the transaction (see Fig-5).

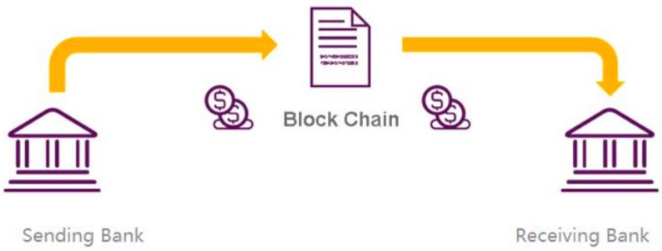

Fig- 5 Blockchain Mode

With this solution, the inter-bank payments no longer require reconciliation between the different databases since the blockchain consensus algorithm has become a single, authoritative general ledger. In addition, the payment can be carried out between banks without the intermediate party, which reduce effectively the cost. Such transactions are almost real-time and peer-to-peer, which reduce counterparty risk and settlement time in milliseconds. In the view of regulators, a blockchain is an invariable general ledger which shared by all transactions which can be accessed by all regulators and auditors. The transaction privacy of different legal entities could be a serious problem. Because in the traditional blockchain, each legal entity's node can access the records of other participants. This may be inconsistent with the privacy related legal framework. Using a key (public key, private key) to encrypt a transaction could be a way to solve this problem. A legal entity can only view transactions of its own, while the supervisor have sufficient authority to view all the information. The initial solution can extend to banks or cross-border payment networks that belong to different groups. Inter-bank payments are settled by multiple central counter parties which active in specific network for clearing between debtor and creditor. In order to minimize counterparty risk, each bank must set up a reserve account for each payment network, which is shown in Fig-6.

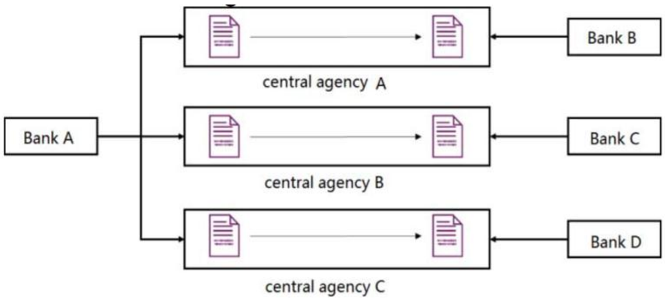

Fig- 6 Linear Structure

In this case, the private blockchain can be implemented among banks belonging to different groups. The key advantage is that cross-border payments can get rid of the involvement of related banks. Through this structure, we can save the funds of the original payment transaction intermediaries. Then the resources which can be allocated to their own banking business will increase greatly, and it also simplifies the management of the bank at same time.

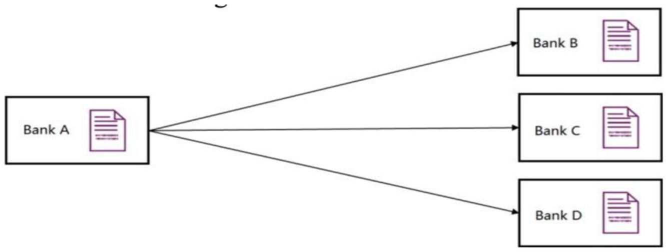

Fig- 7 Network Structure

Fig-7 shows a whole network blockchain platform structure, we can carry on transactions with only one reserve account. When a large number of banks participate in this network, this solution will be more attractive than the previous one. Ripple is an example of a blockchain-based cross-border payment system. In Ripple, the node verification is operated by a recognized financial institution which observe consistency. Ripple can also integrate currency exchange capabilities to provide liquidity for cross-border payments.

B. Inter-bank bill transactions

At present, the inter-bank bill transaction has not formed an independent trading centre, and there is also no authoritative trading platform. Therefore, some scholars believe that it is the time to establish a clearinghouse. This clearinghouse should be dominated by the central bank and attract many financial institutions to participate in. In addition, this clearinghouse should contain the whole process of business products except the acceptance business, which involves paper and electronic commercial bills. And this clearinghouse should take the business transactions and integration of information as the ultimate goal. The participants of the conventional bill transaction and their relationships are shown in fig-8:

clearinghouse should be dominated by the central bank and attract many financial institutions to participate in. In addition, this clearinghouse should contain the whole process of business products except the acceptance business, which involves paper and electronic commercial bills. And this clearinghouse should take the business transactions and integration of information as the ultimate goal. The participants of the conventional bill transaction and their relationships are shown in figure 8:

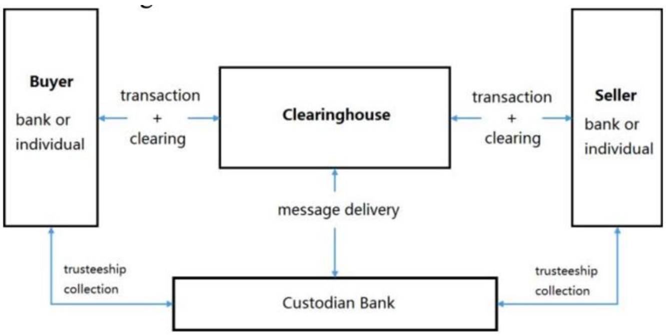

Fig- 8 Traditional Bill Transaction Mode

The bills of the buyers and sellers are entrusted in the custodian bank when the clearinghouse provides trading (including matching) and clearing services. And then the custodian bank will conduct clearing with the clearing house. In transactions, both the clearinghouse and the custodian bank are trusted third-party institutions, which indicate that this is a typical centralized transaction structure like the current securities transaction structure.

Such a transaction structure is a reasonable solution, but also a conservative solution. At present, the trading structure of almost all financial institutions are similar. There are central institutions leading the transaction clearing and settlement. Of course, people have not found a significant flaw in such transaction structure. However, the central body downtime and data loss problem is inevitable, which is also the reason that financial magnates actively looking for a decentralized trading structure. The emergence of blockchain is to meet such a demand.

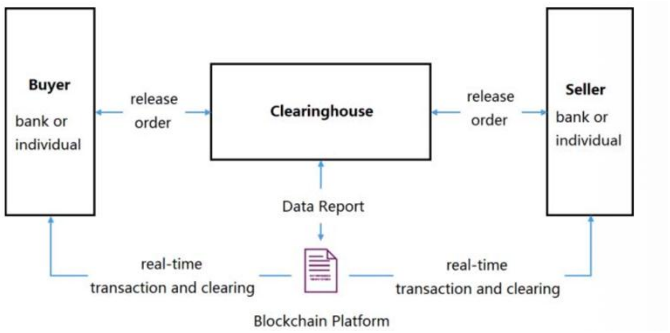

Fig- 9 Transaction Mode Combined with Blockchain

Combining with the blockchain technology, we can transform the bill trading structure (see Figure 9). The clearinghouse only provides matching services, the actual transaction and clearing takes place on a decentralized blockchain platform. As is already mentioned in the previous, the blockchain technology can greatly speed up the payment and clearing process between transactions, which make the payment and clearing almost become real time. It is recommended that using the private blockchain platform to limit the participants to the participating banks or giving the full responsible management to the clearinghouse. From the trader's point of view, the most intuitive change is the speeding up of the clearing service and the eliminating of the custodian fees charged by the custodian bank. In addition, the tamper-resistant feature of the blockchain also ensures the security of the bills, which is more reliable than the current physical bill transactions. Banks participating in the blockchain maintenance will receive a corresponding "reward" as the compensation for the construction of the associated system. Meanwhile, the clearinghouse can still guarantee revenue by charging a matching service fee. The blockchain makes the whole transaction process decentralization, faster and safer while excluding centralized custodian bank from this structure.

To develop a secure, transparent, and efficient blockchain-powered framework that enhances the operational integrity, trustworthiness, and efficiency of depository financial institutions by leveraging distributed ledger technology.

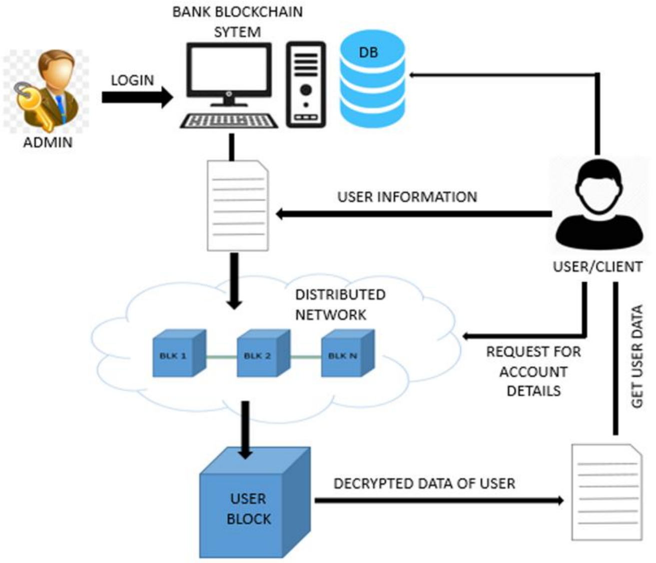

Fig- 10 System Architecture

4. CONCLUSIONS

The Bitcoin is the first successful implementation of blockchain. Today, the world has found applications of blockchain technology in several industries, where the trust without the involvement of a centralized authority is desired. So welcome to the world of Blockchain.

Blockchain technology is only going to grow in the fields of business, finance, law, medicine, and real estate. Whether you're an experienced Blockchain developer, or you're aspiring to break into this exciting industry, enrolling in our Blockchain Certification Training program will help individuals with all levels of experience to learn Blockchain developer techniques and strategies.

REFERENCES

[1] Aswini.R1, Kiruba.K2, College Fees Transaction Using Hash Functions of Blockchain Model", vol. 48, no. 9, pp. 1421{142,July 1, 2019

[2] M. Mahdi H. Miraz, Maaruf Ali "Applications of Blockchain Technology Beyond Cryptocurrency", Annals of Emerging Technologies in Computing (AETiC), pp. 1-6, Vol. 2, No. 1, 1st January 2018.

[3] Carmen Holotescu "Understanding Blockchain Technology and How to Get Involved", The 14th International Scientific Conference eLearning and Software for Education Bucharest, April 19-20, 2018

[4] Pradip Kumar Sharma, Jong Hyuk Park "Blockchain Based Hybrid Network Architecture for the Smart City", Elsevier,Volume. 86, pp 650-655, September 2018

[5] "Zonyin Shae , Jeffrey J. P.Tsai "Transform Blockchain into Distributed Parallel Computing Architecture for Precision Medicine", IEEE 38th International Conference on Distributed Computing Systems, 23 July 2018

[6] Janusz J. Sikorski, Joy Haughton, Markus Kraft "Blockchain technology in the chemical industry: Machine-to-machine electricity market", Elsevier, Volume. 195, pp 234-246, 1 June 2017.

[7] Bhabendu kumar Mohanta, Soumyashree S Panda, Debasish Jena "An Overview of Smart Contract and Use Cases in Blockchain Technology",IEEE, 9th ICCCNT, July 2018

[8] Nakamoto S. "Bitcoin: a peer-to-peer electronic cash system"[Online], available: https://bitcoin.org/bitcoin.pdf, 2009

[9] YUAN Y, WANG F Y. "Block chain: the state of the art and future trends[J]". Acta Automatica Sinica, 42(4): 481-494, 2016.

[10] Bentov, I., & Kumaresan, R. "How to use bitcoin to design fair protocol"s. In International Cryptology Conference, pp. 421-439 August, 2014.

[11] Ethereum White Paper. "A next-generation smart contract and decentralized application platform" [Online], available:

[12] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. "Hawk: The blockchain model of cryptography and privacy- preserving smart contracts". University of Maryland and Cornell University, 2015.

[13] Larimer D. "Transactions as proof-of-stake" [Online], available:http://7fvhfe.com1.z0.glb.clouddn.com/@/ wpcontent/uploads/20 14/01/TransactionsAsProofOfStake10. pdf, 2013

[14] Larimer D. "Delegated proof-of-stake white paper" [Online], available: http://www.bts.hk/dpos-baipishu.html, 2014

[15] Castro, M., & Liskov, B. "Practical Byzantine fault tolerance. In OSDI", Vol. 99, pp. 173-186, February, 1999.

[16] Cachin, C. "Architecture of the Hyperledger Blockchain Fabric", 2016.

[17] Vukolić, M. "The quest for scalable blockchain fabric: Proof-of- work vs. BFT replication". In International Workshop on Open Problems in Network Security. Springer International Publishing, pp. 112-125, October, 2015.

[18] Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R.

"Bitcoin-NG: A scalable blockchain protocol". In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), pp. 45-59, 2016.

[19] Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., & Saxena, P. "SCP: a computationally-scalable Byzantine consensus protocol for blockchains". Cryptology ePrint Archive, 2015.

[20] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. "A secure sharding protocol for open blockchains". In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 17-30, October, 2016.