PalArch's Journal of Archaeology of Egypt / Egyptology

HIGHLIGHTS OF BLOCKCHAIN TECHNOLOGY

P.Sivalakshmi[1], *K.Sangeethalakshmi*[2], *G.Sandhiya*[3]

[1,2,3]Assistant Professor

[1, 2, 3] Dept. of Electronics and Communication Engineering, R.M.K College of Engineering &Technology, TN, India

Dr. Saddam Rateb Darawsheh: Highlights Of Blockchain Technology -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x

Keywords: Blockchain Technology, industry, architecture, Consensus, agro-sector.

ABSTRACT

In the recent decade, blockchain technology had been extensively referred by the research scholars and the industrialists. Also the nation is gradually shifting towards intelligence and digitalization; many industries like Oil & Gas, Power Grid, Health care, Vehicular, Goods Supply chain Management, E-Polling, financial organizations, government organizations for various Application software's & Internet of Things working on blockchain technology for its significant improvement in management level, efficiency and data security. This article aims to let many people in the academics and industries to understand the basics, Application software's, challenges of blockchain technology. Also analysis, of various consensus models has been performed and proposed for reference the same is used for next agro based sector article

1. **Introduction**

Blockchain is a technology not a cryptocurrency, like a ledger to store the transaction details of cryptocurrencies like BTC, ETH, XRP, etc. The number of transaction increases the size of the blockchain. The components of decentralized architecture like transaction, block, P2P network and consensus algorithm are generalized, modified according to the necessity, leading to different blockchain platforms like bitcoin, ethereum, and hyperledger [2]. In Ethereum, each and every transaction records in a blockchain system, consist of mainly receiver address, a sender address, nonce value, miner's price and ether value. The owner transfers the ether value by digitally signing the hash produced by adding the previous transaction and the public key of the receiver. All transaction records together are delivered to each node in a block. Transaction records are time-stamped and collected in a block. Anybody authorized can perform a transaction in blockchain (peer-to-peer network). The security and trust of an immutable transaction records is ensured through a consensus algorithms. Evidence of work is utilized by public blockchain as a consensus algorithm. Miners named nodes validate each transaction records [3]. Specific public or private key is shared among all the participants to execute each of the transaction records. If any record is tempered, then remaining peer nodes would invalidate the transaction records. On Basis of safer, coherent and expandable consensus algorithms [4]. Public blockchain algorithms are expandable, however permissioned blockchain algorithms are coherent and safe, but not quite expandable. Internet-of-Things platforms, started adopting few public consensus algorithms like (DAG) Directed Acyclic Graph [5] for their security, privacy and provenance tracking issue.

2. **Blockchain architecture**

Blockchain is a shared system, its architecture is basically categorised as 4 modules like Framework, Platform, Shared computing, and Application software's. Fig.1 brief's the blockchain architecture [6]. Nodes, Storage & network facilities to run a blockchain composes the Framework module. In this network, there are three different types of node participants simple, full, and mining. Usually nodes involved in transaction records does not store a copy of the transaction, nor authorizes the transaction called simple node. Whereas a full node does, also is responsible for generating a new block. The platform module uses remote procedure Calls, web programming interface, and representational transfer algorithms, to ensure the communication message between the participants. The process of access to data, Malicious tolerance, immutability, privacy, authentication, and safety for the transacted data are ensured by shared computing module protocol. The main characteristics of blockchain, immutability which doesn't allow any modifications in the ledger once. This module uses a consensus algorithms to take care of the transaction records, agreement between nodes, updating the ledger and selection of a miner for next block generation in the chain. Also, this module monitors user identification and data privacy using a cryptography and hashing logic. The Application software's module also known as business logic module can be accessed by the clients for digital asset transaction records and execution of smart contracts.

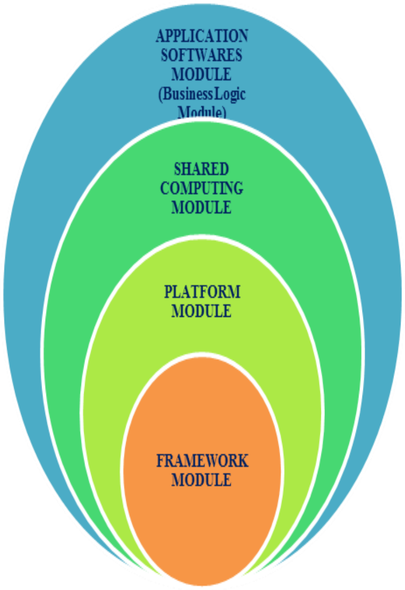


Figure.1 *Overview of architecture.*

The traditional two types of blockchain architecture are public & private networks. A public network, also named permission-less network, participants allowed without permission with a pseudo-name identity (public key) as a simple node, authorising node or a block generating node [12][13]. The main drawback is transaction detail is public leading to the issue of data privacy [14]. A private network, named as permissioned, involves an authorization, nobody can enter the network without permission which is adopted by Multichain, Hyperledger Fabric, Parity, BigChainDB, Interplanetary, Corda and Quorum [12], [15], [16]. Below fig brief's the blockchain evolution. First generation of Blockchain technology adapted by Bitcoin cryptocurrency was introduced in 2008 for a peer to peer transaction in permission-less networks. Second generation of Blockchain technology with some enhancements adopted as Smart Contracts in 2013 for a peer programmable transaction in permission-less network e.g. Escrow [18] & Ethereum [17]. Third generation Blockchain-Decentralised Application software's was introduce in 2015 for development of permission-less or permissioned Application software's. Fourth generation Blockchain-interoperable Application software's was introduced in 2018 for cross blockchain communication message networks [6].

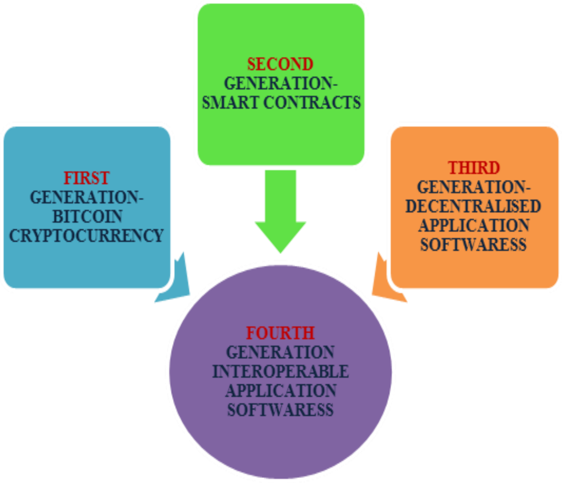

SECOND GENERATION- SMART CONTRACTS
FIRST GENERATION- BITCOIN CRYPTOCURRENCY
THIRD GENERATION- DECENTRALISED APPLICATION SOFTWARESS
FOURTH GENERATION INTEROPERABLE APPLICATION SOFTWARESS

Figure.2 *Blockchain Evolution*

The rapid increase in blockchain platforms resulted in different architecture to cater the need of different network Application software's. As shows in below table.1 [6], [19]-[21].

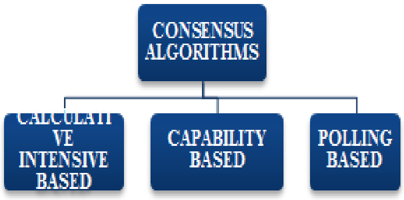
TYPES	**Public Network**	**Private Network**	**Hybrid Network**
Single Ledger operability based architecture.	In **2013,** by Ethereum Platform, the transaction after being validated, then relayed to the miners. All valid transaction records is initiated by a specific miner and again verified by the validators and finally ledger is updated. **Application software's**: Smart resource chain management and project management, digital copy right content ownership, finance and energy resources resource trading sectors.	In **2015**, by Multichain platform, using public key and private keys, the handshaking mechanism occurs to serve the purpose of authentication Thus entrenches connections among them. **Application software's**: Medicare, Knowledge Resource transfer, governance, and national policies.	In **2016,** by Quorum Platform, Here the transaction manager so as to keep the information private and safe, it broadcasts the hashed info to the network. The operation of hashing, cryptography are responsible by the enclave. **Application software's**: Plot/Flat Sale, social networks platforms, retail industry, Medical care, and R&D.

Multiple Ledger operability based architecture.	-	**In 2016**, Hyperledger Fabric, [22], [23] in an organization or a group, confidentiality among them is maintained. It divides the organisation or group into channels to enable private networking information exchange among the members of a channel in the organization [24].	-
Interoperability based architecture	-	-	**In 2017**, by Elements the safety of a blockchain is promised by linking it to another blockchain. That is even side chain of other miners connected to the Bitcoin main blockchain. This process of anchoring and ensuring high immutability of the side chain is done by Elements platform [25] [26].

Table.1 *Evolution of Blockchain Architectures*

3. **Consensus Algorithms Overview**

The consensus process allows reading updating also promises integrity of the transaction information dispersed in a decentralized manner. The blockchain involves consensus models like Evidence of work, Evidence of byzantine malicious tolerance, Evidence of stake, and Evidence of elapsed Time. Consensus algorithms are chosen based on three essential properties like Safety, aliveness, and malicious tolerance. We present some of the consensus algorithms in the following subsections of this article briefly. Basically the model is differentiated into three as shown in figure.3. Basic classifications of Consensus Algorithms.



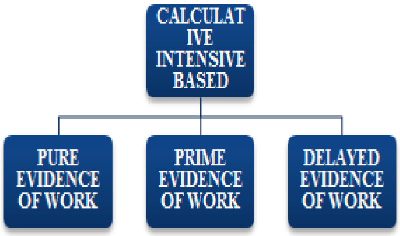


Figure.3 *Classification of Consensus Algorithms.* ***Figure.4*** *Classification of CI Based Protocol.*

3.1 Calculative Intensive Based Protocol

From figure.4, it is evident that furthermore, we can differentiate them into Evidence of work, prime POW& delayed POW. In this, article, we would present brief information on Evidence of work alone, because other two mainly used for Bitcoin.

3.1.1 Evidence-Of-Work

To add a block to a blockchain, few Evidence of work has to done initially. It requires the initiator to solve a puzzle, at times, more than one node solves the puzzle at the same instance of time. This situation creates a fork and is resolved by the network by analysing the maximum value of Evidence-of-work i.e. maximum work done by a node. The update request by the node with minimum Evidence-of-work is discarded. This way the consistency of state among all nodes is ensured. It fits best for those networks that requires scalability. Mostly public blockchain utilizes this kind of protocol to authorize a participating node,

3.2 Capability Based Protocol

The computing power of miners wins the right to mine the next block in the calculative based algorithms like prim & delayed Evidence of Work. As a consequence, several consensus protocol in this article were proposed to select a miner based on non-computing capability, based on factors such as the amount, miners contribution to the community, miner's trust in the network, or the miners amount of storage. In this paper, we classify those consensuses under capability-based algorithms into eleven types. [6], [27] and briefed few of them below.

3.2.1 Evidence-of-Stake

Evidence of work model, consumes more power, i.e. instead purchasing equipment's to generate wining values, Evidence of Stake involves purchasing of cryptocurrencies, using the same can win chances of block creation in blockchain.

3.2.2 Evidence-of-Elapsed Time

To select a leader among all the participants trusted execution environment (TEE) conducts an election, to ensure fairness the same broadcasted in the model. Thereafter to mine a block the leader has to produce a Evidence from TEE for verification process. A shortest wait time is provided for the same before mining the block. The only drawback of this consensus mechanism is it utilizes specialised hardware.

3.2.3 Evidence-of Authority

It is used by private network blockchain like Vechain, Ethereum, Kovan, and Testnet. In this validators are provided with incentives for validating and pushing the transaction into the block once the identity is verified on-chain using a software. It's an energy resources fast and coherent consensus mechanism.

3.2.4 Evidence-of-Reputation

A well reputed organisation would be voted as an authoritative node and serves as Evidence-of-Authority for signing and validating blocks. The nodes cheated the network will be facing the financial consequences that are considered by the PoR. It is a collaborative consensus procedure, which ensures the security of the network, by considering the reputation of the participant.

3.2.5 Evidence-of-Space

It doesn't require huge computation as demanded by Evidence of work. It process each of the request like an e-mail, only a non-trivial amount of disk space is to be allocated that will be needed during solving a challenge posted by service providers.

3.2.6 The Evidence-of-History

It shows the transaction is occurred before the occurrence of an event or after the occurrence of an event. The Evidence of History provides a record based on a particular history that serves as Evidence for the specific time period. An example is timestamps which can better elaborate the mechanism.

3.2.7 Evidence-of-Stake Velocity

It serves as an alternative to Evidence of Work and Evidence of Stake by encouraging ownership and activity in the network. This authorizes the transaction records and safe decentralised network.

3.2.8 Evidence of Burn

It refers to a process of sending the digital currency to an address from which it cannot be retrieved back. This process is similar to the Evidence-of-work protocol. By burning the coins, the node gets a chance to be selected in the lottery to mine the upcoming block. The more the coins are burned the maximum chances are availed by the nodes. So, the Evidence-of-burn just provides opportunities to those who are ready to burn more money.

In summary, most of the above algorithms have not been evaluated for security and privacy issues [27]. The calculative-intensive-based algorithms overcomes the drawback of capability-based consensus like high energy resources consumption but on its own suffers, the issues of the rich always get richer, malicious activities and centralization of the network. As a solution, Polling-based consensus algorithms were proposed, which is presented below.

3.3 Polling-Based Consensus Algorithms

This protocol adapted a Polling system to select a miner for generating a block, furthermore selection is based on wealth dominance. It is also designed to tolerate the independent node failures in the network or some of the malicious behaviour of them.

Polling-based algorithms are basically differentiated into Byzantine Malicious Tolerance and Crash Malicious Tolerance as given below. BMT avoids the node failure and occurrence of malicious node. It is derived from the byzantine general's problem [28]. Furthermore it is differentiated as practical BMT, delegated BMT, and federated BMT. CMT-based consensus avoids failing or crashing of nodes. It is furthermore differentiated as raft and federated CMT.

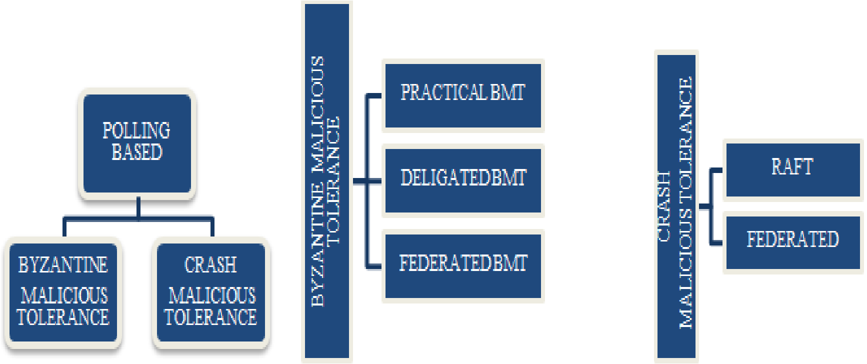

POLLING BASED
BYZANTINE MALICIOUS TOLERANCE
CRASH MALICIOUS TOLERANCE
BYZANTINE MALICIOUS TOLERANCE
PRACTICAL BMT
DELIGATEDBMT
FEDERATEDBMT
CRASH MALICIOUS TOLERANCE
RAFT
FEDERATED

Figure.5 Classifications of Polling Based Protocol.

3.3.1 Practical Byzantine Malicious Tolerance

Node failure and malicious node in a network are prevented in BMT-based consensus algorithm, which is derived from the byzantine problem. In this protocol, one node acts as a leader others acts as a backup nodes selection is done by a common authority. The nodes in the network communicates, assuming that all the nodes are honest, and possess the exact copy of the ledger.

3.3.2 Delegated Byzantine Malicious Tolerance

Based on Polling system, leader node called speaker and backup nodes called delegates are chosen. Delegates in the network having enough cryptocurrency involves in the process of Polling to select the speaker. The vote is weighed by the amount of currency held by that delegates in the network. Higher the currency, the priority of that delegates votes increased.

3.3.3 Federated Byzantine Agreement

If 3/4th of the nodes in the network agree on the status of the transaction then added as a new transaction is into the block of chains. Likewise any node can participate, doesn't require authentication of a common authority to validate and process the transaction records.

3.3.4 Raft (Crash Malicious Tolerance)

The drawback, communication message overhead of BMT-based consensus algorithms is eliminated in the CMT-based algorithms by allowing only leader and backup nodes to communicate and blocking the communication message between the backup nodes. The raft algorithm involves three phases: (1) leader election, (2) log replication and (3) Transaction execution. But it has its own disadvantage of data integrity. If the leader nodes behaves maliciously and executes invalid transaction records, the entire blockchain becomes invalid.

3.3.5 Federated (Crash Malicious Tolerance)

In this protocol selection of leader and backup nodes is done by the network authority, hence less decentralize. The transaction records validation and the creation of a block are monitored by a block generator node, and the verification of the blocks are monitored by block signers called backup nodes. The round-robin fashion is used to select a leader in a group of nodes. The leader authorizes transaction done by the clients. Which in-turn relay the valid transaction records-info to all the block signers in the network.

Issues Suffered	Calculative based	Capability based	Polling based
High resource consumption	✓	-	-
Pollution	✓	-	-
Low transact-throughput	✓	-	-
Low expandability	✓		-
Wealth dominance	-	✓	-
Malicious attacks	-	✓	-
Decentralizes networks	-	-	✓

Table 2. *Summary of issues suffered by consensus algorithms*

Consequently, from the above summary Tabulation.2 it's evident that Polling based consensus algorithm is best with a lag in decentralization of the network. Next comes in the priority is capability based consensus algorithm with a drawback of malicious attack and wealth dominance. Finally based on the requirement we need to adapt the consensus algorithm.

4. Conclusion

Though in the abstract we have mentioned so many areas of application, this article is very particular on emphasising another important field of Application named agriculture. Wherein this era, and the future needs to nurture the agriculture sector along with latest technologies, so that nation would make a revolution in the process of food supply from the farm to the plate. The main drawback in the agriculture supply chain is lack of transparency in food production and distribution, costly middleman, limited financial resources & disconnection between supplier and retailer. So in future using the suitable architecture and consensus models discussed above also considering all the issues highlighted in this agro-sector, we would like to give the solution by improving the transparency in the supply chain, by providing farmers direct access to suppliers with an option of immediate payment on delivery & transparent transaction information to them. Further we can provide traceability options for consumers.

References

Dwyer and Malone, “Bitcoin mining and its energy resources footprint,” in Proc. 25th IET Irish Signals Syst. Conf., Limerick, Ireland, 2014.

J. Becker, D. Breuker, T. Heide, J. Holler, H.P. Raure, and R. Bohme, “Can we afford integrity by Evidence-of-work? Scenarios inspired by the Bitcoin currency,” in The Economics of Information Security and Privacy. Berlin, Germany: Springer, 2013, pp. 135-156.

Kroll, Davey and Felten, “The economics of bitcoin mining, or bitcoin in the presence of adversaries,” in Proc. WEIS, 2013

A. Baliga, “Understanding blockchain consensus models,” Persistent, vol. 2017.

S. Popov, “The tangle,” Cit. On, vol. 2017, p131, Oct. 2016 2017.

Use Case, Challenges, and Solutions by Leila Ismail and Huned Materwala Symmetry, Vol. 11, issue. 10.2019.

Remote Procedure Call Wikipedia.

Web API—Wikipedia.

Representational State Transfer Wikipedia.

Merkle, Digital Signature Based on a Conventional Encryption Function. In Proceedings of the Conference on the Theory and Application software’s of Cryptographic Techniques on Advances in Cryptology, Springer: London, UK, 1988.

Blockchain: Blueprint for a New Economy; O’Reilly Media, Inc.: Newton, MA, USA, 2015.

Zheng, Z. Xie, S.Dai, H.N.Wang, H. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 2018.

Pseudonymity. Available online

Han, M. Wang, Y. A survey on security and privacy issues of blockchain technology. Math. Found. Comput.

G. Greenspan. (2015). Multichain Private Blockchain-White Paper. [Online]. Available:

C. Cachin, “Architecture of the hyperledger blockchain fabric,” in Proc. Workshop Distrib.

Cryptocurrencies Consensus Ledgers.

“Ethereum: A safe decentralized transaction ledger,” Daniel Wood

P.E. O’Neil, “The escrow transactional method,” ACM Trans. Database Syst., vol. 11, 1986.

Lai, Chuen, Blockchain—from public to private. In Handbook of Blockchain,

Greenspan, G. Multichain Private Blockchain—White Paper. 2015

Quorum Overview. Available online

Andreoulakis, Barger, Brotinkov, Cachin, Christidis, Hyperledger Fabric: A Shared Operating System for Permissioned Block chains. In Proceedings of the Thirteenth EuroSys Conference,

Hyperledger Fabric— Available online.

Channels. Available online.

Elements|elementproject.org. Available online

Overview of Opechain.Availableonline.

Blockchain Architecture and Its Application software's: Problems and Recommendations Toqeer ali syed, Ali alzahrani, Salman jan, Muhammad shoaib Siddiqui, Adnan nadeem, and Turki alghamdi.

Lamport, L. shostak, R. Pease, M. The Byzantine general problem. ACM Trans. Program.

Lang. Syst. (TOPLAS) 1982,

Tromp, J. Cuckoo Cycle: A memory-hard Evidence-of-work system. IACR Cryptol. E-Print Arch. 2014,