Security of Blockchain Transaction

Moulika Chadalavada, Muazzam A. Khan
School of Computing and Engineering
University of Missouri Kansas City
Kansas City, MO 64110, USA
mc7d8@mail.umkc.edu, khattakm@umkc.edu

***Abstract*—A blockchain is distributed ledger which orders and verified transactions. Distributed Ledger is that in which date is spread across distributed network. It transforms basic pillars of our society and changes our perspective on trade, trust. Blockchain transactions are verified by consensus. Also, the entered information cannot be erased. Bitcoin, the first decentralized digital currency, which uses blockchain technology. Bitcoin is electronic cash system that introduces blockchain technology for permission less and resistant e-cash on internet. Bitcoin is controversial but Blockchain worked efficiently in both nonfinancial and financial world. Blockchain establishes system for creating distributed consensus in the digital world. It helps in developing digital economy that is scalable. Proper security and privacy has to be considered to secure blockchain technology. There are many techniques and platforms that are introduced to enhance blockchain technology. Few of the techniques are already implemented and few of them are still under development. These techniques can be used in respective applications to gain the benefits of blockchain technology. This paper compares various security measures implemented for protecting Blockchain transaction.**

***Index Terms*— Bitcoin, decentralized network, hashing, security, privacy**

I. INTRODUCTION

Blockchain is a distributed database that maintains increasing list of records called as blocks. Every block stores information such as transaction date, time, participants and information about transaction which is managed by peer-to-peer network, that validates any new block [1]. They are resistant to data modification; also, once modified, and recorded data cannot be altered without altering all its subsequent blocks. Blockchain is an open and distributed ledger which records all transactions between users efficiently in permanent way [1]. **Bitcoin** is the first decentralized digital crypto currency introduced as open source software in 2009. Cryptocurrency is designed to secure transactions using cryptography. Bitcoin system is peer-to-peer where transactions happen between users without any third party such as banks. These transactions are stored in distributed ledger (public) which is called as blockchain. According to 2017, research 2.9 to 5.8 million users are using bitcoin digital currency wallet [2].

First, secured chain of blocks explained by Stuart Haber and Scott W.Stornetta in 1991. Further in 1998 Nick Szabo started working on decentralized currency (bit gold). Satoshi Nakamoto conceptualized first blockchain in 2008. This lead to invention of blockchain for bitcoin without any trusted admin [5]. In 2014, the blockchain file size was 20gigabytes, by the end of 2016 the size grew to 100gigabytes [10]. In 2014, Blockchain 2.0 is released that is used to think beyond transactions. By 2016, Russian Federation started NXT Blockchain 2.0 project (pilot-based) and in the same year IBM started blockchain research center.

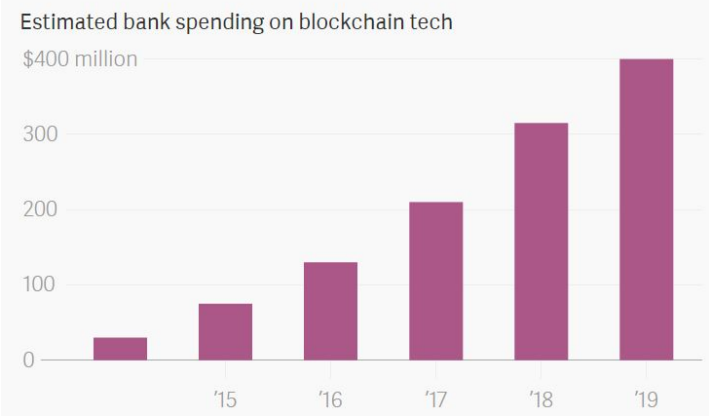

Fig. 1. Estimation of banks spending on Blockchain [2]

All online transactions trust someone which can be email service telling that mail is delivered or it can be social media for example Facebook that tells our posts are shared only to friends. We live in digital world trusting third party for security, privacy of our personal information or assets. Third party can be hacked or it can also be compromised, at this situation blockchain technology come into picture. It has ability verify each and every transaction that involves in accessing digital assets. Blockchain does all this without compromising about privacy and security. The two important characteristics of this technology is anonymity and distributed consensus [2].

Since Bitcoin creation in 2009, interest on blockchain technology increased continuously and spiked development. Blockchains are majorly used for cryptocurrencies and is also used for smart contract. As proposed by Nick Szabo Smart Contracts are used to validate and facilitate performance of a contract. Blockchains smart contract is transparent to all users, so it may lead to attacks and have security holes and these cannot be fixed quickly [3]. Proof of Work (PoW) algorithm is used to reduce denial of service attacks and other spam on the network.

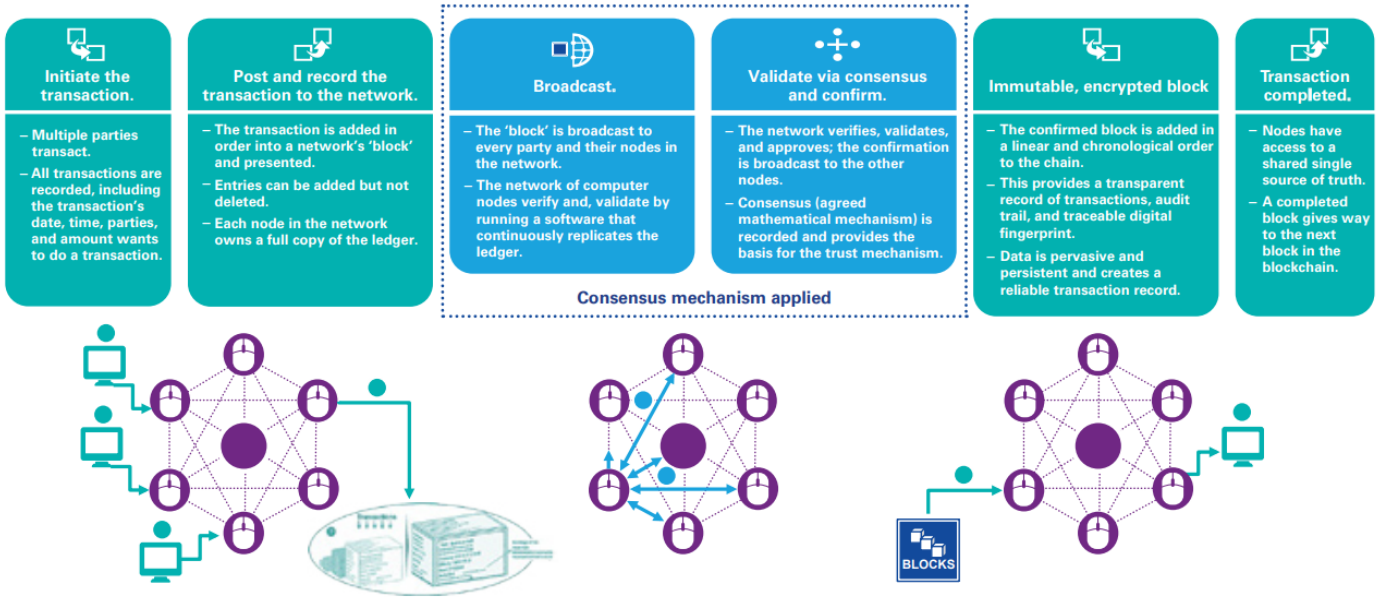

Fig. 2. Blockchain transaction flow [4]

As mentioned earlier blockchain carry out online transactions securely and the records cannot be altered without altering subsequent blocks. This method helps participants to audit, verify transactions inexpensively. Generally, Blockchain database has records of two kinds, they are blocks and transactions. Each block contains hash value of its previous block that links two. All the linked blocks form Chain. As per Fig 2, each transaction will broadcast to all other nodes in the network of Bitcoin and after verification recorded on public ledger. Before being recorded every transaction has to be verified to check if valid transaction is performed or not. Verifying every node has to ensure below two things to before recording the transaction:

1. Spender should own cryptocurrency i.e. verifying digital signature of the transaction.

2. Spender has adequate digital currency in the account, checking each transaction against his/her account in ledger to ensure that he/she has adequate amount in sender's account.

Blockchain provides security capabilities such as Unaltered Data, Single Version of Truth, Auditable, Complete Provenance, Instant Distributed Transaction, and Security by Encryption. In Section II, discussed literature review of Blockchain security mechanisms, which contains working, advantages, and disadvantages. Further in Section III performed comparison analysis of these techniques and provided analysis on these comparisons and finally Section IV is about conclusion and future work. Section V included References of all research papers that helped in analyzing different techniques.

II. Literature Review

In this section, we look at the literature review of various security methods followed by Blockchain technology. As Blockchain uses decentralized process risks are eliminated which are common in centralized systems. The Blockchains uses distributed networking and message passing. All security methods of Blockchain include public-key cryptography [5]. A public key is blockchain address and private key is secret password that provides access to owners to his/her digital assets. Database replication obtains data quality in Blockchain. Consensus mechanisms are used to update distributed state securely. In distributed systems achieving consensus is very challenging. Consensus algorithms has to be very flexible to handle node failures, network partitioning, delay in messages, corrupted messages. The three key properties of consensus protocol are Safety, Liveliness, Fault Tolerance. Below are different protocols that are used to maintain blockchain security.

A. Proof-of-Work (PoW)

Bitcoin's blockchain replicates on multiple nodes and these nodes maintain order transactions based on consensus mechanism Proof-of-Work (PoW) [5]. Each node has to prove that some amount of work is performed to add the blocks to blockchain, this is known Proof-of-Work. This mechanism ensures that one block is added for every ten minutes. To find winning hash value PoW has to be solved this is called as Mining. First winning hash value node gets chance to add block to blockchain. If there are two nodes that finds hash value then temporary fork in blockchain occurs where some nodes add blocks to one branch and others add to another branch. The branch that has maximum PoW is added in blockchain and others will be dropped which leads to eventual consistency [5].

Bitcoin PoW works better in open environment (infinite number of nodes take part in network. Knowledge or Authentication is not needed so this model is highly scalable. However, it is vulnerable to 51% attack [6], and the advantage to attacker is that his own digital assets can be double spent and can also drop transactions that is don't want on blockchain. 51% attack is that which is attack in Blockchain, in which a group of miners will control 50% or more hashrate of mining. It stop transactions between legitimate users. Another type of attack can take place with approach selfish mining, where honest miners support attacker and carry out 51% attack by joining with them.

Ethereum is another blockchain platform which supports smart contracts. Like Bitcoin, Ethereum is also open and permissionless that executes smart contract on nodes. Ethereum also uses its own PoW model known as EthHash. This method provides quick confirmation and to prevent 51% attack establishes ASIC resistance. To restrict mining centralization EthHash uses two techniques [6] (i) Memory Hardness – Instead of performing calculations computer circulated data across memory (ii) GHOSH- contain headers of orphaned blocks known as uncles. It also uses same concept as Bitcoin PoW for finding correct input to generate hash value. All PoW algorithms are time consuming. PoW algorithm works by selecting fixed resource that depends on block header which is called as directed acyclic graph (DAG). DAG needs for mining but not for verification.

B. Proof-of-Stake (PoS)

This method is introduced to overcome drawbacks of PoW algorithms with reference to huge electricity consumption in mining. PoS method replaces mining operation by alternate approach that involves user stake in blockchain system [7]. For example, instead of spending $2000 in purchasing mining equipment to gain PoW algorithm but with PoS user can buy cryptocurrency of $2000. PoS algorithm choose validators randomly for blockchain block creation, and ensure that validator cannot predict in advance. The problem from which Naïve PoS algorithm suffers is Nothing-at-Stake [7]. These implementations don't give impetuses to vote on right block for nodes. In this way nodes can vote various blocks that supports different forks to amplify their odds of winning reward. For correct and effective PoS implementation Nothing-at-Stake problem needs to be tackled carefully.

Ethereum uses PoS algorithm known as Casper is advance PoS algorithm. It is under testing and expected to release under Serenity version. With Ethereum system by introducing the security deposits, node bonding is allowed [8]. Nodes are reinforced validators and show responsibility and enthusiasm for propelling the Ethereum blockchain through staking their security stores. The underlying list of validators are followed by contract called as Casper contract. From that point, validator list developed based on new nodes entering and old node exiting from the system. To generate block from vital validator set, each validator has to be selected pseudo randomly. If validator is offline then multiple different validator selection is repeated until validator becomes online.

If block produced by validator included in chain, then validator gets block reward that is equal to entire ether of validator list that is active. If block not included in chain, then validator misses the security depositor. This mechanism resolves Nothing-at-Stake problem which eliminates blocks that are not getting included in chain [8]. PeerCoin uses Naive version of Proof-of-Stake. BitShares, Tendermint, NXT use different PoS variations. Ethereum is still under development and has bugs to be fixed. But Ethereum in one of the most fast-growing mechanism like Bitcoin and can be used as blockchain application

C. Byzantine Fault Tolerance and Variants

Hyperledger Fabric, most famous permissioned blockchain platform designed by Linux foundations. It provides more flexible design with pluggable consensus mechanism. Fabric is mainly designed for an association of several companies, in which not only participants are known but also participants identities are recorded and verified with registry maintained with in system. Fabric supports smart contracts called as chain code. HyperLedger supports popular consensus model, they are Practical Byzantine Fault Tolerance algorithm (PBFT), SEIVE and Crash Fault Tolerance (XFT) [10]. Most of the current projects supporting XFT which has BFT built-in.

i. PBFT (Practical Byzantine Fault Tolerance) algorithm presented by Barbara Liskov and Miguel Castro is the first solution for gaining consensus in Byzantine failures [10]. For state changes, it uses voting by replicas and replicates the state machine. It also provides optimizations like encryption and digital signing of messages that are exchanges between clients and replicas. This is carried on by reducing message size and count of messages getting exchanged for the system. To implement this algorithm "3f+1" replicas should be able to countenance "f" node failures. With this approach, there will be less overhead can performance of replicated service. Network File System produced 3% of overhead when experimented [10]. As number of replicas increases message overhead also increases.

ii. ***SIEVE*** consensus method is introduced to handle indeterminism in execution of chaincode. If non-determinism is in chaincode, then for different replicas it produces different output in network [11]. SIEVE handles the transactions which will be mostly deterministic buy may lead to non- deterministic occasionally. This protocol deals chaincode as black box. All operations are first executed speculatively and further compares the output will all the available replicas. If any minor divergence is detected then those values will be sieved out. If divergence occurs among more number of processes then the operation itself will be examined further.

iii. Cross-Fault Tolerance (XFT) is new trending protocol that makes BFT more feasible and efficient, also attack model is simplified. [12] Most of the BFT protocols believes in adversary which is used to handle compromised nodes, also message delivery of entire network. To handle such a powerful adversity results complexity and therefore becomes less efficient. To overcome this issue XFT is used to provide perfect service as long as replicas are perfect and communicates with each other continuously. Same number of resources are uses as used by protocols that can handle failures and also can tolerate failures of Byzantine.

D. Federated Byzantine Agreement – Ripple & Stellar

Ripple and Stellar are blockchain systems that uses editions over Byzantine Fault Tolerance (BFT) consensus mechanism via construction to them open-ended with respect according to node participation [13]. These blockchain systems aims at financial use cases yet the repayments area is particular. They furnish payment protocols, that settles cross-border transactions of a matter within seconds as adversarial in accordance with today's infrastructure that takes days for the same. Ripple and Stellar use its own consensus models where BFT structure is modified to include open-ended participation.

i. Ripple Consensus Protocol: In this algorithm, each node defines as Unique Node List (UNL) [13]. UNL list consists other Ripples nodes which are trusted and don't collude against the given node. Consensus is achieved in Ripple when each node communicates with other nodes in UNL. Every UNL should have overlap of 40% with rest of nodes on network [13]. Nodes will verify and validate transactions, vote and broadcast these votes across network. Based on votes that are accumulated, every node fine-tune candidate set and the candidate which receives more votes are moved to next round. When candidate set gains 80% of votes from rest of nodes in UNL, then this set becomes valid block and is also named as "ledger". This ledger will be finalized and is treated as Last Closed Ledger (LCL), which is further added to Ripple Blockchain by every node. The next round will be started with new and pending transactions which are not participated in previous round.

ii. Stellar Consensus Protocol: This algorithm [14] uses quorums and quorum slices. Quorum is set of nodes that are required to meet agreement, quorum slice is known as quorum subset which can convince a node about the agreement. Steller uses quorum slices to allow open participation i.e. every node can select set of nodes from slice. These are based on business relationships among various entities thus holds trust which exists already in business models.

Every node performs voting initially on transactions, which is the first step of voting process in federated system. Every node selects its statements and never select or vote for another statement those are contradicting its decision. A different statement can be accepted if quorum slice accepted any different statement. The next step will be acceptance step [15]. A node will accept vote or statement if it never taken statement that is contradicting existing statement. Also, every node present in v-blocking set should also accept that particular statement. Quorum slices impacts one another that leads to quorums which agrees upon particular statement. This step is called as ratification, which occurs when all participants in quorum approves a statement. The final step of this voting process is Confirmation which indicates agreement at system level. This confirmation step indicates that all participating nodes send messages so that every node accepts final value in system. Ripple can be used in banks which transforms money all around the world, also provides financial settlement solutions [15]. Ripple solution lowers cost by enabling banks to do transactions instantly, directly. Stellar is used to expand literacy and financial access around the world. Stellar is platform which connect banks, people and payment systems.

E. Tindermint

Tindermint is deposit based consensus protocol, which serves consensus by generating blocks. This protocol controls the security deposits which controls impetus of validators implicitly [17]. The leader is selected based on chain rule technique known as GHOST (Greedy Heaviest Observed Sub Tree). The main advantage of this GHOST mechanism is that it completely either adopts or abandon every block. The modification of GHOST implies that the blocks which are out of the chain can contribute to the irreversibility of main chain.

Tindermint will work efficiently even one-third of systems fail with different reasons. Basically, the ability to handle these arbitrary failures in system is known as BFT as discussed previously [17]. BFT is old and came into picture with its use in blockchain technology. Blockchain mechanism is nothing but characterization of BFT, including authentication in peer-to-peer network. Tindermint's two main components are consensus engine and application interface. Consensus Engine also known as Tindermint Core make sure that on every machine same transactions registered in same order. Application Blockchain Interface [17] make sure that using any kind of programming language transactions can be processed.

Tindermint is mainly designed for simple understanding, ease-to-use, useful on wide range of distributed applications. But when the leader or validator verifies transaction which GHOST assumes as invalid, then the leader loses his advantage of participating in consensus mechanism and also loses his deposit. This problem is known as nothing-at-stake.

F. Delegated Proof of Stake (DPoS)

Delegated PoS is mainly developed to combine characteristics of PoW and PoS. It uses voting process that is decentralized and acts a path to reduce network centralization. DPoS was first used in blockchain BitShares application [16]. In

PoS mechanism the coins in every wallet should be stake i.e. earning coins back, establishing distributed consensus, validating the transactions. Where as in DPoS every pack with coins is eligible to vote representatives and these representatives will take care of validating the transactions and in return collects fee for transaction processing. To gain consensus DPoS uses real-time voting system i.e. allowing only trusted members to participate and are also eligible for creating blocks.

DPoS has lots of advantages when compared to traditional PoS, few of them are: transactions are fast, efficient, flexible, decentralized voting process. As claimed earlier DPoS as efficient mechanism than PoS, but whereas PoS is non-profitable to most of its user will small amount in wallets else set to high transaction fee [16]. However, DPoS has enhanced efficiency which takes low fee, provided faster confirmations and gives increased profits. This all shows that without compromising staking benefits of PoS lightweight wallets can be used by people.

DPoS optimizes performance by providing 100% nodes participation in distributed network. But DPoS unable to solve few problems like how database inconsistency is resolved, how transactions recorded securely, who is legitimate person to update database [16]. Also, it suffers from apathy of voters like other systems. This may lead to problem where large stakeholders vote to themselves.

G. Proof of Elapsed Time(PoET) – Sawtooth Lake

Another flexible open-source blockchain platform developed by Intel is called as Intel Sawtooth Lake (Intel Ledger) which is now officially under HyperLedger project of Linux. Consensus algorithm used by Intel is Proof of Elapsed Time(PoET) [9] and PoET executed on Trusted Execution Environment (TEE). This process is called as Software Guard Extension(SGX). Based on SGX, PoET mechanism uses random election or lottery based election. In this method to finalize block, leader is selected randomly. This random leader election algorithm is used to handle untrusted nodes. Random distribution of leader election has to take place among all nodes for consensus to work efficiently and correctly. Also needs to check if correct leader is selected without need of further manipulation. This can be achieved through TEE which guaranteed randomness and safety for electing leader.

Random election will work as follows. Using SGX all validating nodes should run TEE. From running code inside TEE every validator will request for wait time [9]. The validator which has least wait time will win lottery and becomes leader. Functions designed in TEE in such a way that execution cannot be influenced with exterior software. Before mining next block, every node has to prove its least wait time to claim as leader. Wait time assigning among nodes is random, so the leader role will be distributed randomly among validating nodes. The drawback with this algorithm is the dependency on specialized hardware. Intel's Sawtooth Lake is flexible blockchain mechanism with its extensible exchange nature. In its present stage, it is not applicable for few chain-based applications, especially for these which require high security.

III. Comparative Analysis of Different Blockchain Security Mechanisms

Even though there exist different types of Blockchains, the common elements in all of them are i. Blockchain is distributed digitally in real-time across huge number of systems/computers. ii. To reach consensus many participants are used iii. To prove identity digital signatures and cryptography is used iv. It is very hard to manipulate historical records v. It is time-stamped vi. It is programmable. Many blockchain types and independent Blockchains emerged but they were yet not able to gain same scale as that of Bitcoin but they provide larger data capacities, increase speed, advance functionality, and consensus methods. The comparison is based on various parameters such as Blockchain Type (indicates blockchain platform type i.e. permissioned/permissionless), Transaction Finality (whether transaction entered blockchain is final or not), Transaction Rate, Token Needed, Cost of Participation, Scalability, Trust Model (nodes participating can be trusted or not), Adverse Tolerance (Without consensus being affected network is compromised).

As per Table-1, PoW and Federated BFT are mainly developed for permissionless platforms, they can also be used as permissioned but it is not an ideal setting. As PoW and PoET carry multiple blocks risk at same time and creates temporary forks and eventual chain will be main chain which leads to probabilistic transaction. Clients has to wait longer to be finalized or confirmed. But with PoS only for less period temporary forks exist if in parallel validators vote. However, Casper like good algorithm have penalties for multiple chain voting causes lose on security deposits. In further models, there is immediate finality when block is included on transaction and it cannot be rollbacked. Transaction rate is high on platforms that immediately confirm transactions and reach consensus fast. PoW algorithm approach is probabilistic and should spend time on solving puzzle. So, PoW have more transaction latencies and less transaction rate. Because of a speed mechanism in leader election PoET high transaction rate than PoW. So, it supports transaction rate that is medium. BFT, PBFT and PoS can have high transaction light as transactions confirmation is fast.

For PoW and PoS mechanisms cryptographic token is required as its inherit design build with token. The other models don't require token for consensus mechanism to function. These models are used in certain platforms as anti-span and anti-DDoS measure. PoW and PoS have a characteristic cost related for support in consensus. PoW spends energy, which is resource that would be exterior to consensus mechanism. Whereas PoS needs particular nodes to get cryptocurrency for generating security deposit. Scalability of the consensus models is its capacity to achieve agreement when number of peering nodes are continually expanding.

TABLE I
COMPARISON OF BLOCKCHAIN SECURITY MECHANISMS

Comparative Analysis of Different Blockchain Security Consensus Mechanisms											
#	**Parameters / Method**	**Blockchain Type**	**Scalability**	**Trust Model**	**Token Needed**	**Transaction Rate**	**Adversary Tolerance**	**Participation Cost**	**Transaction Finality**	**Decentralized Control**	**Applications Used**
1	PoW [5]	PL	H	UT	Y	L	<=25%	Y	PB	Y	BC ETH
2	PoS [7]	PD	H	UT	Y	H	Based on algorithm used	Y	PB	Y	ETH
3	PoET [9]	Both	H	UT	N	M	Unknown	N	PB	Y	ISL
4	BFT and variants [10]	PD	L	ST	N	H	<=33%	N	IM	N	HF
5	Federated BFT [13]	PL	H	ST	N	H	<=33%	N	IM	N	BA
6	DPoS [16]	PD	H	ST	Y	M	<=33%	N	PB	Y	BS
7	Tindermint [17]	PD	H	ST	Y	H	<=33%	N	PB	Y	ER

DPoS: Delegated Proof of Stake
BFT: Byzantine Fault Tolerance
PoW: Proof-of-Work PoS: Proof-of-Stake PoET: Proof-of-Elapsed Time
PD: Permissioned PL: Permissionless L: Low H: High M: Medium
UT: Untrusted ST: Semi-trusted Y: Yes N: No
PB: Probablistic IM: Immediate ER: Eris
BC: Bitcoin ETH: Ethereum ISL: Intel Sawtooth Lake
HF: Hyperledger Fabric BA: Banking Applications BS: BitShares

Except BFT and variants, all other mechanisms have scalability. In BFT and variants numbers of peers of consensus matrix has to be less than 20. If the number of peers increases more than 20 then it causes gradual increase of messages sent which result in immense increase of overhead.

Consensus decision may not be affected until 25-50% of network is not opposing. For blockchains that are using BFT, peer nodes have to be known in advance and has to be registered with system to get involved in consensus decisions. At some point, nodes might get compromised but consensus process will be unimpaired as long as nodes are not compromised more than 33%. Using Federated Byzantine method, each node in network must ensure that it contains all trustworthy nodes in active trusted list. Without consensus getting affected the small fraction of system can be compromised. For adversary tolerance, each consensus mechanism has particular threshold.

IV. Conclusion And Future Work

A. Conclusion

This paper discussed history and working of Blockchain, different challenges in achieving Blockchain security. In today's world Blockchain technology has grown to great extent that is used in most of the applications by maintaining security standards. The above discussed Consensus models are used in all blockchain platforms now-a-days and are largely managed by the type of applications the platform wants to serve and the threats it visualizes for the chain's integrity. Generally, the permissionless platforms are attaining robust consensus among huge number of untrusted peer nodes by using memory complexity or computational. But at the same time this is done by sacrificing throughput and transaction finality. On the other hand, permissioned blockchain platforms are aiming for less scalable but higher throughput to gain faster transaction finality. It is important to consider scale of network along with Blockchain technology to solve any business problem, to maintain relationship between participants and functional and non-functional aspects such as confidentiality and performance before deciding correct platform and consensus model.

B. Future Work

As mentioned earlier, blockchain technology is fast growing digitalized cryptocurrency concept where transactions or smart contracts maintained in public ledger. As compared above different security consensus mechanisms, PoS method is more efficient for business related applications, so it is preferred by Ethereum platform. Blockchain technology can be applied in identity applications such as Passports, Digital identities, Birth Certificates etc. If security is required for applications then Federated BFT mechanism can be used.

V. References

[1] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, "Blockchain contract: A complete consensus using blockchain", Consumer Electronics (GCCE) 2015 IEEE 4th Global Conference on, pp. 577-578, 2015.

[2] Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, "BRIGHT: A concept for a decentralized rights management system based on blockchain", IEEE 5th International Conference on Data Analytics, pp. 345-346, 2015.

[3] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," IEEE 14th International Conference on Smart City (HPCC/SmartCity/DSS), Sydney, NSW, 2016, pp. 1392-1393, 2016.

[4] K. Christidis M. Devetsikiotis "Blockchains and Smart Contracts for the IoTs" IEEE Access Special section on the plethora of Research in IoT pp. 2292-2303, 2016.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", IEEE 2nd International Conference on Security, pp. 34-37, 2009.

[6] Nian, Lam Pak; Chuen, David LEE Kuo, "A Light Touch of Regulation for Virtual Currencies", Handbook of Digital Currency: Bitcoin, Innovation, Financial,2015.

[7] Macdonald, L. Liu-Thorrold, R. Julien, "The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin", IEEE Access Special section on Security, 2017.

[8] Tapscott. Don, Tapscott, Alex, "The Blockchain Revolution, how the Technology Behind Bitcoin is Changing Money, Business, and the World", ISBN 978-0-670-06997-2, 2013.

[9] Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain" in the 10th International Conference for Internet Technology and Secured Transactions(ICITST-2015), pp. 131 –138,2015.

[10] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence" in AI Matters, vol. 1, no. 2, pp. 19 –21,2014

[11] Jean-Pierre Buntinx, "Future Use Cases for Blockchain Technology: Copyright Registration", vol. 3, in Saint Bitts, 2016.

[12] dinbits Staff, "The "Blockchain Technology, Bandwagon Has A Lesson Left To Learn", vol. 1, IN WEAS 04, 2011.

[13] Karl J. O'Dwyer , David Malone, "Bitcoin mining and its energy footprint", Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET. 2014

[14] Peck, M., "Ethereum's Blockchain-Powered Fund Opens Just as Researchers Call For Halt". IEEE Spectrum Institute of Electrical and Electronics Engineers, 2016.

[15] Florian Tschorsch, Björn Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies", *Communications Surveys & Tutorials IEEE*, vol. 18, pp. 2084-2123, 2016.

[16] Eduardo A. Alchieri, Alysson Neves Bessani, Joni Silva Fraga, and Fabola Greve, "Byzantine Consensus with Unknown Participants", In Proceedings of the 12th International Conference on Principles of Distributed Systems. 22–40,2015

[17] A. Juels and J. Brainard, "Client puzzles: Cryptographic Countermeasure Against Connection Depletion Attacks." in: Proceedings of NDSS '99 (Networks and Distributed Systems Security), pp. 151–165, 2010.

[18] Miguel Castro, Barbara Liskov, "Practical Byzantine Fault Tolerance", Proceedings of the Third Conference on Operating Systems Design & Implementation, New Orleans, USA, February 2012.