Proof-of-Review: A Review based Consensus Protocol for Blockchain Application

Dodo Khan[1], Low Tang Jung[2], Manzoor Ahmed Hashmani[3]
Department of Computer and Information Science
UniversitiTeknologi Petronas, Seri Iskandar
32610 Perak DarulRidzuan, Malaysia

***Abstract*—Blockchain is considered one of the most disruptive technologies of our time and in the last 2 decades andhas drawn attention from research and industrial communities. Blockchain is basically a distributed ledger with immutable records, mostly utilized to perform the transactions across various nodes after achieving the mutual consensus between all the associated nodes. The consensus protocol is a core component of Blockchain technology, playing a vital role in Blockchain's success, global emergence, and disruption capability.Many consensus protocols such as PoW, PoS, PoET, etc. have been proposed to make Blockchain more efficient to meet real-time application requirements. However, these protocols have their respective limitations of low throughput and high latency and sacrifice on scalability.These limitations have motivated this research team to introduce a novel review-based consensus protocol called Proof-of-Review, which is aimed to establish an efficient, reliable, and scalable Blockchain. The "review" in the proposed protocol is referring to the community trust on a node, which is entirely depending on the node's previous behavior within the network which includes the previous transactions and interaction with other nodes. Those reviews eventually become the trust value gained by the node. The more positive the reviews the more trustworthyis the nodeto be considered in the network and vice versa. The most trustworthy node is selected to become the round leader and allows to publish a new block. The architecture of the proposed protocol is based on two parallel chains i.e. Transaction Chain and Review Chain. Both chains are linked to each other. The transaction chain stores the transaction whereas the review chain will store the reviews and be analyzed with an NLP algorithm to find the round leader for the next round.**

Keywords*—Blockchain; consensus protocol; transaction chain; review chain; prove-of-review; PoW; PoS

I. INTRODUCTION

Blockchain technology is oneof the most hyped decentralized innovation these days with an enlightening future. Initially, Blockchain was introduced by Haber and Stornetta [1] and latergainedintense attention because of the Bitcoin byNamakoto in 2008 [2]. Bitcoin earns intense success in the cryptocurrencyarena. Many similar currencies have seen been launched in the following years. There are 2017crypto currencies available on the internet by 2019 [3] with the different business models. Besides global cryptocurrency hype, Bitcoin holds the highest market capitalization of up to 53%. Blockchain is serving as the fundamental technology behind Bitcoin. Besides cryptocurrency, Blockchain gain lots of attraction from a diverse range of fields and has shown a noticeable growthlike in insurance[4], healthcare[5-7], economics [8-10], IoT [11-13], supply chain, software engineering [14-16], transport, government agencies, distributed video coding [58] and finance. As per the survey conducted by World Economic Forum [17], Blockchain will be soaring to 10% of global GDP by 2027.

The primary properties of this technology are decentralization, resiliency, integrity, anonymity which are the driving force for industries to adopt Blockchain.Along with various technical components, the consensus protocol is the main component in which Blockchain relies on. Consensus protocol plays a vital role in blockchain's success, global emergence, and disruption.It serves to achieve the consensus of information sharing, replicating state, and broadcast the transaction amongst the Blockchain network participants without any controlled 3rd party or authority. The success of Blockchain isheavily dependent onan efficient consensus mechanism forits great impactson the overall performance which shall include transaction throughput, latency, scalability, and fault tolerance.

There are many comprehensive definitions of consensus protocol available in the literature. However, in this study "The agreement on the commonstate of ledger in between the group of nodes in Blockchain application" is adopted as the definition.There are ranges of consensus protocols availablefor Blockchain implementations. Nakamoto proposed PoW[2]with Bitcoin to address double spending issue in digital cryptocurrency system in a trustless environment. Since the day Bitcoin is launched, it is continuously growing in terms of the number of transactions and the nodes. Due to the exponential growth,it encounters several performance issues. The most highlighted are the huge amount of energy consumption, low transaction throughput, high latency,and poor scalability.Currently, the Bitcoin network consists of around 10 thousand nodes [18] while it can only process 7 transactions per second (TPS) with a latency of 10 min. Moreover, the transaction throughput can possibly be raised to 25 TPS after fine tuningof the key parameters without compromising the security [19] and it also consumes huge amount of energy [20].

There are centralized applications performing better than Bitcoin. For example,VISAnetwork is comprising of around 50 millionusers and at maximum, it can process up to 65000 TPS [1]. Researchers tried to address the blockchain limitations with new consensus mechanisms/approachesto reduce energy-intensive mining and the energy

consumptionwhile increasing throughput. For example,Proof of luck [21], Proof of Authority (PoA), Proof of space [22], Proof of Elapsed time (PoET) [23], and Proof of Stake (PoS). Every available protocol comes with its own advantages and disadvantages but mostly lacking in real-time transaction processing. Besides, there is no universal generic consensus protocol so far which can possibly be implemented in every domain with diverse set application requirements.

This research utilizes an emerging area of Blockchain consensus protocol but least investigated, the review-based approach. This approach intends to make every node accountable for every transaction and allowing all the nodes as a whole to decide which node will generate the next Block. The "reviews" is referring to the community trust on a node, which entirely depends on the node's previous behavior within the network which shall include the previous transactions and interaction with other nodes. Every node will share its experience with other nodes in the reviews form and those reviews will eventually become the trust value of the node after the analysis through an NLP algorithm. The more positive the reviews the more trustworthy a node shall be considered in the network and vice versa. Securing good and positive reviews is not easy and not a one-day job. It needs consistently good behavior to earn others' trust. It cannot be spent and bought therefore theonly way to increase trust is to behave honestly. Blockchain and reviews would be a good combinationwhere reviews serve as an incentive and blockchain is responsible to keep reviews record safe.

In this study, we propose a new proof-of-review consensusprotocol to establish a reliable and scalable Blockchain.This protocol intends to address the shortcoming of the previous model in terms of throughput, latency, scalability, and energy consumption. The architecture of the proposed protocolis based on 2 parallel chains, the transaction chain, and the review chain. Both chains are linked to each other. The transaction chain, as usual, stores the transactions whereas the review chain will store the reviews and those that will be analyzed by an NLP algorithm to determine a round leader to generate a new Block while other nodes will be involved in the block verification process. The proposed protocol is also tolerant to some of the major attacks such as Sybil attack, bad-mouthing, on-off, etc.

The rest of the paper isstructured as follows. In Section 2, we discuss the Background of Blockchain and the consensus model. Section 3 discusses the related work in consensus model. Section 4 describes the proposed proof-of-review (PoRv) consensus protocol with details. Section 5 discusses the block structure. Section 6 is about thesecurity analysis of PoRvwhich includes the potential attacks and strategies to address the attacks. Section 7 discuss the preliminary results and Sections 8 and 9 discuss the conclusion and future work respectively.

II. Blockchain Background

A. Blockchain Characteristics

There are several definitions of Blockchain available in the literature. Most of themdefine the context itis supposed to be used. For example, apublicly shared ledger for maintaining the transaction by many nodes anonymously without control of any central party [24]. A decentralized database with the capacity to work in the decentralized environment without trustingthe intermediaries [24]. A shared, distributed, immutable replicated, and tamper-evident ledger letting every participant to access read, and verify the legitimacy [25]. A type of distributed ledger maintaining the information regarding the transaction which are shared between all the participants in the network[26].Transparency, Immutability, distributed database, ledger, auditability, and intermediary are the common terminologies used in every definition.

Fig. 1 illustrates that in the Blockchain, the first Block is referred as Genesis Block. The previous hash in the genesis block would be equal to Zero. The Block in the Blockchain containsan organized set of records and every block is cryptographically coupled with the next block. Since Blockchain works in distributed and decentralized fashion, it maintains a long list of Block and every Block contains many transactions depending on its size. Moreover, Blocks are divided into two sections: Block header and transaction. Block header compromised of Version, Prev_Hash, Merke root, timestamp, nonce Hash (the unique identity of each Block) which is entirely different for every block like figure prints.

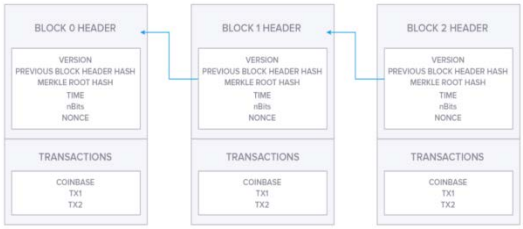

Fig. 1. Bitcoin Blockchain Structure.

Every Block carries the hash of prior block therefore every block is connected to one another through the hash. Any manipulation in the information of the block alters the hash number and that block will be unrecognizable for the next block [27]. Fig. 1 shows the Bitcoin blockchain structure.

In general, Blockchain is classified into three different categories. Namely, Public Blockchain, consortium Blockchain, and Private Blockchain [28]. The major differencesin these categories are based on who can participate in the Blockchain consensus process [29]. For example, in Public Blockchain all nodes are welcome to participate in the consensus process whereas in Consortium and Private Blockchain only selected and validated set of nodes can participate.

- Public Blockchain: The Public Blockchain network is entirely opened for everyone to freely join and leave at any timeas they please.Therefore, it works in between completely anonymous and entrusted nodes. In Public Blockchain, information is accessible and shared to all network participants. It comes under the umbrella of as permissionless Blockchain. Moreover, every node iswelcome to participate in the consensus processto ensure the validity and integrity of data. Bitcoin and Ethereum are classic examples of Public Blockchain.

- Federated Blockchain: Federated Blockchains are also referred as Consortium Blockchain. In which every node can access data. However, only a predetermined group of nodes would be able to change and take part in the consensus process. Most of theconsortium Blockchain are implemented in banking sector [30]. Because in the banking settings, the idea is to share the power between the authorities rather than one controlled authority who can possibly make biased decisions. Here are some well-known examples of Consortium Blockchain, R3 (Bank), EWF (Energy), B3i (Insurance).
- Private Blockchain:Federated Private Blockchain is kind of centralized blockchain in which central authority or predefined group of nodes canread and write or participate in the blockchain. Only pre-validated nodes would be able to join the network. Furthermore, the known and authorized nodes take responsibility to maintain the consensusprocess.Private Blockchain are considered as Permissioned Blockchain where data is accessible to authorized groups of nodes. These groups can change acceptance by consensus procedure. Private Blockchain is designed for settings where all nodes are known and authorized.

B. Key Properties of Blockchain

Some of the key properties of blockchain are described in this section,

- Persistency: Blockchain transactions are maintained in shared ledger which are considered as persistent because the ledger is shared across the distributed network, where every node is made accountable and on control of its record and maintains the integrity by the consensus protocol. So,persistency can only be retained if majority of the nodes acts honestly. Several Blockchain properties are derived from persistency, i.e., transparency, immutability which makes Blockchain auditable [31].
- Validity: Unlike several distributed system, Blockchain does not need every node to perform validation. Blocks and transaction are broadcasted across distributed network and their legitimacy will be validated by all other nodes that process is referred as consensus mechanism. Therefore, any illegitimate action would easily be identified with the source node. There are 3 major roles for this process. (1) Proposer: the one who proposes the value (2) Acceptor: The one who verify the value and take a decision and (3) Learner who accepts on the chose value [24].
- Anonymity and Identity: Anonymity is one of the primaryproperties of Public Blockchain. Node identification could be linked with the real-life identity. A single user can acquire multiple identitiesfor avoidingidentity exposure [32]. There is no central entity is required to maintain the private data such as identity. On the other hand, in private Blockchain identities are required to operate and governed by known entities and authorized group of nodes.

C. Consensus Characterization

In Blockchain the key tasks are the block validation and the continuous maintaining of the security which can be achieved by a well-structured mechanism called consensus protocol. Since Blockchain is a distributed and a shared ledger so there is no need for a centralized authority to ensure the legitimacy of all the transactions. Therefore, it is challenging to achieve consensus among the nodes on the transaction in a block without compromising on the security [26]. Therefore, the consensus protocol is considered asthe heart of any Blockchain application. In the distributed environment, achieving consensus is not a trivial task to getall network participants (Nodes) to agree on accepting or rejecting a potential block.Once a new Block is accepted, all node members are supposed to append this block into their respective chain.

The consensus protocol is an active research area in the last two decades. It has been and being deep studiesfor its resilient for a node failure, message delay, portioning of the network, message out of order or missing.In Blockchain network, the consensus protocolis supposed to deal with the malicious, selfish, faulty nodes and make sure that all nodes have reached consensus among themon the global state of the ledger. In the context of Blockchain, the three key properties of consensus mechanismnamely Safety, Liveness, and Fault Toleranceshall determine the applicability and efficiency of any consensus protocol [31].

- Safety: This property is the responsible for ensuring that nothing malicious will ever take place in the Blockchain. It refers to the properties of validity and agreement in the conventional consensus set out in the distributed systems. Validity is defined as “A correct mechanism proposed a value X then another correct mechanismshould also produce the same the value X". Whereas the Agreement property made responsible to ensure that two correct processes should not provide different output. Generally, consensus protocol is considered safe when uponone honest node produces valid output and subsequentlyevery other node in the network obtain the same output. The produced output should be valid and be the same as all other nodes, referring to consistency of the share state [33].
- Liveness: This property ensures that eventually, something good will take place. Liveness of consensus mechanism can only be ensured if all honest nodes participate in the consensus process and ultimately generate a value and all right/correct requests will eventually be processed. There is no time limit to decide on a value, it is not necessary for all nodes to have a same state at a given point of time.
- Fault Tolerance: A consensus protocol is considered fault tolerant when it is resilient to failure of nodes which are participating in the consensus process. The node failure can be planned in two types.

Fail-Stop - It deals with all nodes who discontinue processing temporarily or permanently. And those also stop producing, receiving messages, or taking part in consensus process.

Byzantine failure – It deals with faulty and malicious nodes specially designed to crash consensus mechanism properties. Leslie Lamport [34] identified and characterized as the Byzantine General's Problem.

Considering the importance of consensus mechanism in Blockchain implementations, all the three properties are essential for any consensus protocol. However, it is agreed by many researchers [35] that all three properties can't be achieved at one time. A deterministic asynchronous consensus mechanism can possiblyachieve at most of two out of three properties and compromise onat leastone of them. Itis not random task to select two properties and compromise on one,but it entirely depends on application requirements. Fault tolerance can't be comprised because it is the most important property [33] for any blockchain implementation. Therefore, the nature of application is to decide which property to let go of,either on liveness or safety. For instance, Raft [36], Paxos [37], view-stamped replication used consensus protocol that take fault tolerance and safety and let go the liveness. Bitcoin [2], Ethereum [38], Ripple [39], stellar [40] and other cryptocurrencieschose fault tolerance and liveness and sacrifice on the safety.

III. Related Work

Nakamoto launched Bitcoin in 2008 [2] with its secured intense success in the field of cryptocurrency. Therefore, many similar currencies have been launched in the following years. There are 2017cryptocurrencies available on internet by 2019 [3] with different business models.Besides global cryptocurrency hype, Bitcoin holds the highest market capitalization of up to 53%. Blockchain is serving as fundamental technology behind Bitcoin. It aims to influence almost every industry. Its applicationis not restricted to only financial eco-system [3] but it is set to revolutionize the politics, healthcare, and society science arena [41].

The consensus protocol is the main and core component of Blockchain technology, and it plays a vital role in Blockchain for its success as global emergence and disruptive technology. Nguyen and kin [42][43] recommend in their respective research to categorize the Blockchain consensus mechanism into two major groups. Proof Based and Voting Basedconsensus mechanism. Proof-based consensus mechanisms are mostly used in permissionless Blockchain in which anyone is free to join and leave at any time they want. They are supported by the several cryptographic techniques and the incentive-based design. Moreover, this group of consensus mechanism, offer comparatively better support for nodes scalability but the on the cost of performance which includes the throughput and latency. In proof based consensus model performance of Blockchain compromised with increasing size of network.Whereas, voting based consensus model mostly utilized in permissioned Blockchain. It offers quick consensus finality which eventually bring high number throughput [44]. In the voting based consensus model nodes communicate with each other, due to high communication complexity it doesn'tsupport large network and restricted to small network.

Bitcoin uses Proof of work consensus protocol. Therefore, it has attracted wide research interest in last two decades. Due to the complex block mining process, it consumes huge amount energy and require other specialized equipment do intensive mathematical computation. Therefore, it is also referred as resource hungry and energy inefficient and eventually, it offers low throughput and high latency. Moreover, most important concern of research community in PoW is limited scalability, it only supports seven transaction per second (TPS) which is entirely not acceptable in business real world application. Firstly, Proof of stake(PoS) was presented at Bitcoin community forum later Ethereum adopted it. It was proposed to provide ease in block mining and reduce high wastage of energy in PoW and referred as energy efficient variant of PoW. This new idea changed entire Block mining concept, so theexpensive and extremely powerful equipment'sare no longer needed for block mining. However, miners (nodes) are required to hold and show stake in the form of certain number of coins. The node holding high stake has more chances to become block producer and earn the reward. Apparently, it certainly saves more energy as comparison to PoW but there are different attacks arises such as nothing at stake problem. Ethereum only support 15 transaction per second (TPS) which is also very low in comparison with other mainstream application. There is another proposed alternate, proof of space it strives to utilize physical storage resources as a substitute of computational power in PoW [45] [22].

Proof of Coin Age [46] support the same mechanism as proof of stake. Where nodes are needed to show the ownership of certain amount currency for performing the virtual mining. Proof of activity [47] create the mining lottery of every node own the number of coins. The lottery winner will produce the block and claim its reward by signing message within interval of time. Intel proposed proof of elapsed time [48] and which has been implemented in HyperLedger project. Proof of elapsed time are required to use the Intel SGX supported CPUs for performing the online voting via random sleeping time. Researcher tried to address above discussed limitations with various new consensus mechanism and approaches, which do not require energy intensive mining, and reduce the energy consumption and increase throughput, For example proof of space [49], Proof of Authority (PoA), Proof of luck [21].

Besides all the approaches, there is another emerging areafor Blockchain consensus model but unfortunately least investigated. Reputation based consensus mechanism. This area intended to make every node accountable on every transaction and return power to the nodes as whole.

A recent published study proposed the Proof of Reputation (PoR) [50] in which reputation would be served as the incentive for nodes positive behavior, time, utilized energy as well as block publication rather thanthecoins. Therefore, mining node are no longer required in this technique. The lab-based simulation proved that it can be scaled up to the thousand nodes with processing capacity ofmore than hundreds of transactions (TPS). Reputation scheme [51]

designed on the similar concept of PoR. It involves both honest nodes as well as malicious nodes together in the positive manner. It rewards the good behavior as reputation and, alsoproposed the punishment factor in the revenue payment function of reputation. Therefore, the cooperative behavior would be rewarded, and non-cooperative behavior would be punished.The implementation of this reputation-based incentive module on state-of-the-art PoX protocol can achieve better results than usual. Another protocol Proof of QoS [52] designed on the similar idea of reputation, where good quality of service would be encouraged. Mostly it has been used in permissionless Blockchain. In this protocol, the whole network would be categorized into small group and each group will nominate a node based on its quality of service, then the consensus would be achieved in between the nominated nodes with Byzantine Fault Tolerance (BFT). The architecture of Proof of QoS has entirely based a hybrid protocol, where it utilizes Proof-of-QoS to select nodes for running BFT-style consensus.

Proof of X-repute protocol designed for Blockchain enabled - IoT systems[53] it introduced new module of repute method and to illustrate the potential of repute that it can be utilized to manage the integrity of consensus protocol. The reward and punishment in the repute method sets the nodes repute values; the nodes behavior would either be rewarded or punished which certainly impact the security and integrity of consensus protocol. Another study proposed Blockchain Reputation based consensus (BRBC) [54] protocol for private blockchain networks. In this protocol network setsa trust threshold level and all nodes are supposed to secure higher reputation score than trust threshold for getting a chance to append a new block in the chain. Moreover, miner (nodes) activities are monitored by randomly selected judges and they sign their reputation score based on their behavior. Judges will reward good and cooperative behavior whereas punishment factor also included on the malicious and non-cooperative behavior.

In one study reputation integrated as moduleReCon [55] in which external reputation system has been integrated with Blockchain consensus protocol to achieve scalable permissionless consensus protocol. Where it utilizesexternal reputation ranking mechanism as input to ranks the nodes. Node ranking would be done based on the result of consensus rounds performed by small committee. Therefore, current reputation would be used to select the committee. Delegated Proof of Reputation [56] designed to replace coin-based stake with the reputation ranking system. The reputation system developed on design of famous raking theories (PageRank, NCDawareRank and HodgeRank). RepuCoin [57], uses miner reputation as its strength as key function of its work and energy integrated over the time of complete Blockchain rather than immediate computational power with possibility of borrowing, temporarily and rapidly. Whereas the reputation would be earning with the span of time. RepuCoin claims that it will tolerant 51% attack and put limits on the rate of voting power growth of the entire system.

IV. Protocol Description

A. Important Definition

- Block: A block is the main data structure of Blockchain. It consists of Block header and list of transaction, Block header containing metadata i.e., timestamp, Prev_Hash, Merkle tree etc. Like figure print, Hash is the unique identity of every block and it is identified the with its hash. The prev_Hash in the metadata of every block is to connect the prior block and this series of chronologically connected blocks forms chain.
- Genesis Block:The first Block in the Blockchain is referred as Genesis Block. Therefore, the previous hash must be equivalent to zero because there is no block before it. If you start from any block and following the chronologically chain backward you will reach at genesis block.
- Round: The round is a set of five steps to achieve consensus. At the end of round, a block supposed to be added intoboth chains i.e., transaction chain as well as reviewchain.
- Nominated Round leader (NRL): Nominated Round leaders are the nodes selected based on their behavior in the network and sentiment analysis of the review with NLP algorithm. In every round top three nodes with highest positive reviews will be selected as NRL. Initially every node strives to become NRL and get a chance to become round leader. To become an NRL it is required to meet minimum criteria which is the node should not be currently blacklisted and minimum positive reviews.
- Round Leader: Round Leader is node with highest positive reviews selected from NRLor the most trustworthy node selected from NRL. RL will only be selected from list NRL. A new RL will selected for every round to propose a block, and the selection process are independently done through an NLP algorithm. To become RL it is required to meet minimum criteria which is node should not be blacklisted and minimum positive reviews.
- Step verifier (SV): Step verifiers are the set of nodes independently selected on the basis on their behavior and availability in the network. A new set of SVs are selected for every step in the consensus process and each SV are tasked to perform different activities to contribute toeach step in the round.Each step verifier is required to meet a minimum review and not currently blacklisted.

B. Overview

The core idea behind the proposed Proof-of-Review consensus protocol is toallow and therefore to givepower to each node to post reviewsand rating in the form of stars for every other node. Nodes are required to maintain their good and positive behavior consistently to secure positive reviews from other nodes, and those reviews will eventually become their trust value in the network. The trust value cannot be bought, spent, or sharedbut it can only be earned with good

and positive behavior. The node with more positive reviews will be considered more trustworthy in the network.The most trustworthy node will get higher chance to publish a new block.

- If node maintain a good and positive behavior, it will receive a good and encouraging feedback/review and which eventually increase their trust value in the network.
- If node act maliciously, selfishly, it will get negative feedback/review, and which decrease the trust value in the network.

The proposed model works on a 2-chain architecture. There would be 2 parallel chains – the first chain as usual will store the transactions and referred as transaction chain whereas the other chain is designed to store the reviews given by nodes and referred as Review Chain.

To achieve the proposed protocol, we will answer following questions:

C. Question 1: In this Model, How to keep Ledger and Review Consensus?

As Bitcoin uses the PoW consensus protocol, which strives to allowentire network of nodes to agree on every single block in the chain. The first node that has solved the computationally intensive puzzle securethe right to publish the block, while remaining nodes will be allowed to take part in Block verification. Similarly, in Proof-of-Review (PoRv), the node with most positive reviews will get a chance to publish the Block. Positive reviewsfrom other nodes will eventually become their trust value, which means the most positive reviews means more trustworthy and vice versa. And the block verification is open for all other nodes. Since PoRvprotocol work on the 2-chainarchitecture, a Transaction chain and Review chain, therefore every node is required to agree on both the transaction and the review block.

D. Question 2: How to Produce Block through PoRv

The response of this concern will be likeBitcoin, it utilized the proof of work consensus protocol, in which the node solves the mathematical puzzle before all other nodes will get a chance to publish the next Block in the Blockchain while other nodes will verify the block. In PoRv protocol, the node with most positive review (which eventually becomes the trust value), will generate and publish a new blockwhile other nodes can verify the block. Every node is required to maintain the good behavior consistently because any bad review will cause a reduction in the trust value.

E. Question 3: How to Encourage other Nodes to Publish Block

There is no reward or incentive in this model for publishing new block as comparing to cryptocurrencies like Bitcoin and Ethereum. In this model we are giving power back to every node in the network. This is to empower every node to rate and to post reviews on others' behavior in the network. Those reviews will become trust value or trustworthiness of a node which cannot be bought, spent, and transferred but the only way to earn trust value is to stay honest and with good behavior consistently. Nodes with highest positive reviewsreflects the high trust value and comparatively offer better services as well as not likely to attack the system. In every round only one node with highest trust value will be selected as Round Leader and publish the block. Publishing a block will certainly help to get more positivereviews from other nodes which eventually increase the trust value.

In each round the PoRv execute the following task. A around starts with a transaction and ends with new Block being added to Ledger.

- Step # 1. Select Nominated Round Leader (NRL)

All online nodes appear to be Potential Round Leader (PRL) and get a chance to become Nominated Round Leader (NRL). The restriction of minimum trust value and not to be blacklisted will be applied to all nodes in the network. Each PRL will evaluate their own reviews (text format).

The evaluation calls on the Natural Language processing (NLP) to evaluate the text to determine a trust value. Then, the trust value will be compared against their rating. The PRL's trustand rating should be identical with negligible difference otherwise the node will be blacklisted with status involved in "Malicious Activity" for current round.

Top 3 nodes with highest positive Reviews/trust value out of all PRL will be selected as Nominated Round Leader (NRL). NRL will propagated a message using GOSSIP protocol to all other nodes in the network which includes their (NRL) trust value and their hashed credentials.

- Step # 2. Select Round Leader

All nodes in the network will listen message a from NRL from Step 1.

Nodes with highest online time will be identified and selected as "Step Verifier". (Other nodes which are not selected as Step Verifier, they need stay online for next step to be selected as Step Verifier). The restriction of minimum trust value and not to be blacklisted will be applied to each "Step Verifier".

Each SV will wait certain amount to time (System defined duration) to receive the messages from 3 NRL (from Step 1).NRL are selected with condition to be online, there are less changes of no message.

SV will re-evaluate reviews of each NRL. If results are identical with received, the minor difference is negligible. The node with highest trust value will become a Round Leader (RL) and other 2 nodes will remain Nominated Round Leader (NRL)and stay in a queue.

If re-evaluation results are not identical for node with a highest trust value,then that particular node will be blacklisted with status involved in "Malicious Activity" and re-evaluation will be done for next node from NRL and process goes until the RL is selected.

SV will propagate a message using GOSSIP protocol to all nodes in the network which includes the RL recommendation and its trust value.

- Step # 3. Propose a Block

All nodes will listen message from SV from Step 2.

Nodes with highest online time will be identified and selected as "Step Verifier". The restriction of minimum trust value and not to be blacklisted will be applied to each "Step Verifier". SV will wait maximum amount of time (System defined duration) to receive the minimum number of messages (from Step 2) for RL recommendation and its review number (SV are selected with condition to be online, there are less chances of no message.).

SV will re-evaluate the reviews of RL and compare it with the one received in the message from Step 2. If result is identical only then the process will move on otherwise RL will be blacklisted and it goes back to Step 2 and select a new RL from the remaining NRL.

If all go well, the RL will assemble a block and add transaction from its transaction poll until the block size hit. RL will technically verify the Transaction (e-signature) and sign a Block.

RL will prorogate a message which includes its RL trust value as a Signed Block.

- Step # 4. Block Verification

All nodes will listen message from SV from Step 3.

Nodes with highest online time will be identified and selected as "Step Verifier". The restriction of minimum Review Number and not to be blacklisted will be applied to each "Step Verifier". SV will wait maximum amount of time (System defined duration) to receive the message From (from Step 3) the Signed Block and its trust value.

SV will re-evaluate reviews of RL and compare with the one received in the message from Step 3. If result is identical the process will move on otherwise RL will be blacklisted and it goes back to Step 2 and select a new RL from remaining NRL.

Each SV seeks to verify and validate the block and its associated transactions. Each SV will iterate over transactions in the block. With each transaction, every SV will evaluate the transaction by processing it into its VERIFY () function. The verify function will either return a Yes or No. "YES" means Transaction is good and "NO" means Transaction is bad. If it returned Yes, and remaining technical checks are good (e.g e-signature), SV will move to next transaction. Once all the transaction are verified and validated as good and no disagreement found, each SV will propagate a message with vote in continuance of this RL and Block and its trust value.

Verify – Another parameter will also be part of message, YES/NO depending on the number of votes in confidence. YES, when the number of votes in confidence meets minimum threshold value and vote is still in agreement for a leader. Otherwise,ifit is Nofor any transaction, it is considered a bad transaction. This disagreement will allow verifier to conclude the RL evaluation is bad and consequently the RL is acting maliciously and Blacklisted and it goes back to Step 2 and select a new RL.

- Step # 5. Block Decision

All nodes will listen message from SV from Step 4.

Nodes with highest online time will be identified and selected as "Step Verifier". The restriction of minimum trust value and not to be blacklisted will be applied to each "Step Verifier". SV will wait maximum amount of time (System defined duration) to receive the minimum number of messages (from Step 4)for Verify value YES. (SV are selected with condition to be online, there are less changes of no message.).

SV will re-evaluate reviews of RL and compare with the one received in the message from Step 4. If result is identical the process will move on, otherwise RL will be blacklisted, and it goes back to Step 2 and select a new RL from NRL.

Each SV will come to a final decision on the Block.SV are listening to messages that includes a signed value Yes or No in addition to the vote of confidence to Round Leader and a Block. If they receive the maximum number messagescontaining Yes along of the vote of confidence to RL and a Block, SV will approve the Block and the same block is supposed to be broadcasted to all other nodes.

V. Block Structure

This consensus protocol is entirely dependent on the community (other nodes) reviews. It is essential to store the reviews whose legitimacy is verified by all other nodes. Therefore, in the proposed protocol, there would be 2 parallel chains. First chain will store the transactions and referred as Transaction chain whereas the other chain is designed to store the reviews given by step verifiers and it is referred to as Review Chain shown in Fig. 2.

The block structure of the first chain would be as usual as in conventional Blockchain, which is separated into 2 parts. Block header and list of transaction. Block header contains the version, prev_hash, timestamp, nonce, Merkle root, transaction parts contain the transaction only. The structure is illustrated in Fig. 3.

Whereas the Block structure for review chain is a bit different. It is also divided into two parts, Block header and Review Transaction. Blockheader contains the version, previous hash, timestamp, merkel root, hash of thetransaction Block. Therefore, both the chains are linked with each other but carrying different information. The review transaction part contains the list of reviews and public keys of the node that have written the review. The structure is illustrated in Fig. 4.

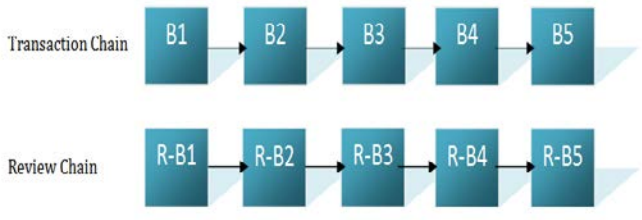

Fig. 2. 2 Parallel Chain Architecture.

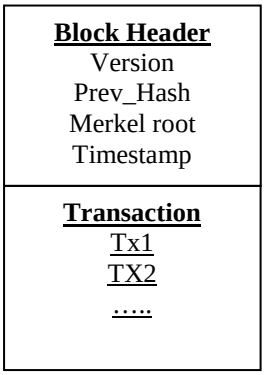

Fig. 3. The Block Structure of Transaction Chain.

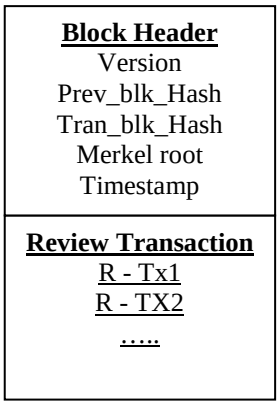

Fig. 4. The Block Structure of Review Chain.

The Fig. 5 explains the complete workflow of the proposed protocol system. Basically, thereare two parallel chains. This system works in round structure, where in each round a new Round Leader will be selected. The Round Leader willbe responsible to generate two blocks in one round, the transaction Block, and the Review Block and both blocks would be linked to each other. Initially, RL generates the transaction Block after successfully achieving the consensus then Step verifier will be allowedto posttheir reviews and ratings.Consensus will also be achieved on the reviews. Then the RL generates the Review Block which will hold the hash of transaction Block. For the next round, the new RL will be selected from the latest Review Block, and Block generation process will continue.

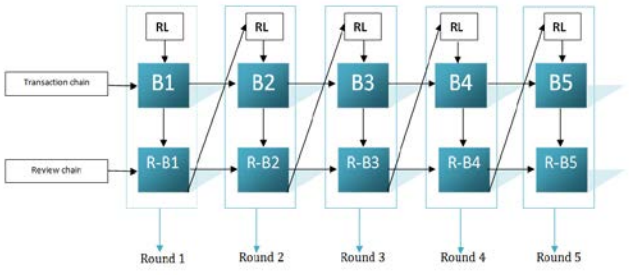

Fig. 5. The Complete Workflow of PoR Consensus Protocol.

VI. Security Analysis

We presume the communication between the nodes in the network are set up through a reliable peer-to-peer network but there are chances it can still be damaged by selfish behavior, malicious attack, or node failure. This section will discuss some potential attacks in peer-to-peer networks and specially in trust-based protocols and strategies to address them efficiently without damaging the network.

Following are several potential attacks [20] and strategy to address them.

- Bad-mouthing attack: In this attack, malicious nodes want negatively to influence other node's trust value. Therefore, they deliberately and continuously give bad/negative reviews to one or all nodes to undermine their trust value or defame the good nodes. which eventually help them level up their trust level.

In our model, reviews are associated with the step verifiers, andnew step verifiers are selected on every step in the consensus process. Moreover, the reviews will be analyzed with strong NLP algorithm which confirm the date and time of the reviews and the sentiments. TheNLP algorithm will not count any malicious review or any review with malicious doubt therefore it would not affect the system.

- Camouflage attack: In this attack, malicious nodes show of the honest and good behavior to secure positive reviews which increase its trust value. Once they got required trust value, they randomly attack the system. The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.

In our model, there are two chain architecture, it stores reviews of every node in the separate chain. A NLP algorithm measure the trust level and ensures the legitimacy of every review on every step of consensus process. Therefore, any random malicious act will be easily detected, and malicious node will be blacklisted right away.

- Sybil Attack: This attack has been discussed in almost all consensus Model. In this attack, malicious node creates multiple account. if one account gets defame by getting negative review and acting maliciously, it quickly switches to other account and start.

In our model, every node needs to earn positives review consistently, if a malicious node switches new account, so it wouldn't be able to hurt because it needs a minimum trust valueto participate in consensus process which make it to act honestly, and it wouldn’t cost effect to create a new account every now and then.

- On-off attack: In this attack, the attacker shows mix of behaviors, good as well as bad alternatively. In order to get mix reviews therefore remain undetectable and occasionally cause damage.

In our protocol, there are two chains architecture, a separate chain is recording the reviews of every node in the network and NLP algorithm measure the overall trust level and analyze the legitimacy of every node in the step verifiers on every step in the consensus process. Therefore, any On-off attack can be easily reported.

The reason for attackers to attack the system is 2-fold, they want to downgrade other nodes' trustvalue to push up their trust in the network to get more chances to perform malicious actions.Other reason could be they want to damage the system. Our model discourages any kind of malicious activity and provide equal opportunities to all nodes to earn more positive reviews and increase their trust value in the network. It entirely works on the other node's reviews and the nodes trust value to make every node act and behave honestly and consistently.

VII. Preliminary Results

This section will discuss the Proof of concept (PoC) for evaluating reviews which is done on by performing the sentiment analysis of reviews (Text) through NLP. Therefore, we used freely available on the standard Kaggle dataset. It consists of reviews (tweets) for six US based airlines. The tweet is the mix of positives, negative and neutral. However, our focus was on the positives and negative. The analysis was done on those tweets to find the most trustworthiness of airlines and exactly sample idea would be replicated in the proposed system.

Sentiment analysis is performed to analyze the feeling and opinion about anything i.e., Text or image. Basically, it is used for decision making when you have multiple choices and you need to select the most reliable.

A simple program has been written in python programming language using multiple NLP libraries and all the coding work has been done on Jupyter Notebook.

The Fig. 6 illustrates the sentimental analysis of tweet for six US based airlines those are United, US airways, Southwest, Delta, Virgin America. The analysis is measured either positive and negative and the neutral category is discarded for this evaluation. In the figure x-axis presents the number of reviews (tweets) and y-axis shows the airlines. The figure illustratescomparatively their high number of negative and less positive for all the airlines.

However, our focus is on the positives, and the southwest got the highest number of positive tweets and followed by the Delta andtheUnited.

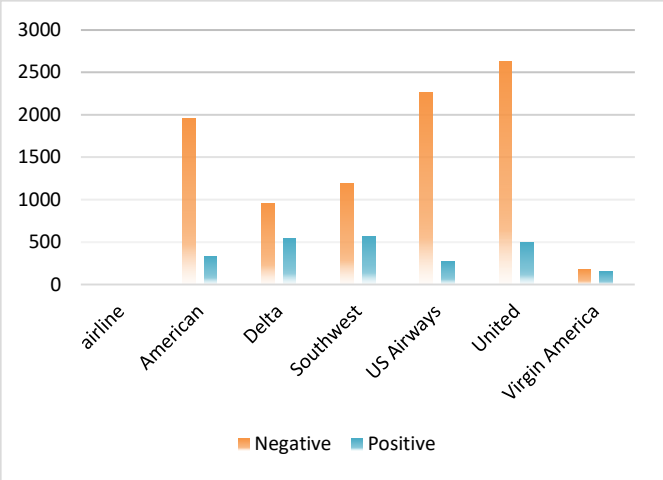

Fig. 6. Sentimental Analysis of Tweet for 6 US based Airlines.

VIII. Conclusion

To conclude, we propose a new PoRv consensus protocol to make blockchain more efficient, reliable, and scalable. In this protocol, we are utilizing the trustworthiness of node by empowering every node to post reviews for every other node on their previous behavior within the network. The trust may include the previous transactions and interaction with other nodes. An NLP algorithmis used to analyze the reviews and to calculate the trust value of every node. The trust value will be linked to every node to efficiently select the round leader node and that will increase the throughput with less latency.Node with most positive reviews will be selected as the round leader and canpublish new block to earn more positive reviews. The proposed protocol is designed on a 2-chain architecture that both chains are cryptographically linked to each other. The first chain is utilized to store the transaction whereas the second chain is used to store the reviews. The proposed system is found to be tolerant to some major attacks such as Sybil attack, bad-mouthing, and on-off attack.

IX. Future Work

The in-depth/detailed investigation and experiments of the proposed protocol is ongoing.The separate blockchainsare in the development phase based on the PoRv consensus protocol. Experiment/simulation are to be used to validate and verify the proposed protocol. The implementation and experiments on the proposed PoRv shall be published in the future papers.

Acknowledgment

This study is conducted in UniversitiTeknologi PETRONAS (UTP) as "Generic Consensus Model for Improving Nodes Syndicating Performance in Blockchain" under the Fundamental Research Grant Scheme (FRGS) from the Ministry of Higher Education (MOHE) Malaysia.

REFERENCES

[1] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in Conference on the Theory and Application of Cryptography, 1990: Springer, pp. 437-455.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, 2019.

[3] A. Tapscott and D. Tapscott, "How blockchain is changing finance," Harvard Business Review, vol. 1, no. 9, pp. 2-5, 2017.

[4] Z. Hess, Y. Malahov, and J. Pettersson, "Æternity blockchain," Online]. Available: https://aeternity. com/aeternity-blockchainwhitepaper. pdf, 2017.

[5] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data," in Proceedings of IEEE open & big data conference, 2016, vol. 13, p. 13.

[6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), 2016: IEEE, pp. 25-30.

[7] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, pp. 1-8, 2016.

[8] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," Procedia computer science, vol. 98, pp. 461-466, 2016.

[9] P. Bylica, L. Glen, P. Janiuk, A. Skrzypcaz, and A. Zawlocki, "A Probabilistic Nanopayment Scheme for Golem," ed, 2015.

[10] P. Hurich, "The virtual is real: An argument for characterizing bitcoins as private property," Banking & Finance Law Review, vol. 31, no. 3, p. 573, 2016.

[11] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017: IEEE, pp. 618-623.

[12] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983-994, 2017.

[13] J. Sun, J. Yan, and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, vol. 2, no. 1, pp. 1-9, 2016.

[14] X. Xu et al., "The blockchain as a software connector," in 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), 2016: IEEE, pp. 182-191.

[15] E. Nordström, "Personal clouds: Concedo," ed, 2015.

[16] J. S. Czepluch, N. Z. Lollike, and S. O. Malone, "The use of block chain technology in different application domains," The IT University of Copenhagen, Copenhagen, 2015.

[17] D. Shift, "Technology tipping points and societal impact," in World Economic Forum Survey Report, available at: http://www3. weforum. org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015. pdf (last accessed 20.08. 2018), 2015.

[18] A. Yeow, "Global Bitcoin Nodes Distribution," URL: https://bitnodes. earn. com/(accessed 08 November 2018), 2015.

[19] K. Croman et al., "On scaling decentralized blockchains," in International conference on financial cryptography and data security, 2016: Springer, pp. 106-125.

[20] B. Obama, "The White House: Office of the Press Secretary," Presidential Studies Quarterly, vol. 39, no. 3, p. 429, 2009.

[21] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in proceedings of the 1st Workshop on System Software for Trusted Execution, 2016, pp. 1-6.

[22] S. Park, A. Kwon, G. Fuchsbauer, P. Gaži, J. Alwen, and K. Pietrzak, "Spacemint: A cryptocurrency based on proofs of space," in International Conference on Financial Cryptography and Data Security, 2018: Springer, pp. 480-499.

[23] B. Curran, "What is Proof of Elapsed Time Consensus?(PoET) Complete Beginner's Guide," ed: Accessed: Mar, 2019.

[24] M. Correia, G. S. Veronese, N. F. Neves, and P. Verissimo, "Byzantine consensus in asynchronous message-passing systems: a survey," International Journal of Critical Computer-Based Systems, vol. 2, no. 2, pp. 141-161, 2011.

[25] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841-853, 2020.

[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE international congress on big data (BigData congress), 2017: IEEE, pp. 557-564.

[27] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in proceedings of the 50th Hawaii international conference on system sciences, 2017.

[28] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.

[29] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," International Journal On Advances in Telecommunications, vol. 11, no. 1&2, pp. 51-64, 2018.

[30] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in Proceedings of the 2017 ACM International Conference on Management of Data, 2017, pp. 1085-1100.

[31] C. Hammerschmidt, "Consensus in blockchain systems," URL https://medium. com/@ chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe, 2017.

[32] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues," IEEE Access, vol. 6, pp. 1513-1524, 2017.

[33] A. Baliga, "Understanding blockchain consensus models," Persistent, vol. 4, pp. 1-14, 2017.

[34] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in Concurrency: the Works of Leslie Lamport, 2019, pp. 203-226.

[35] N. A. Lynch, M. J. Fischer, and R. Fowler, "A Simple and Efficient Byzantine Generals Algorithm," Georgia Inst of Tech Atlanta School of Information And Computer Science, 1982.

[36] D. Middleton, "Hyperledger's Sawtooth Lake Aims at a Thousand Transactions per Second," ed, 2017.

[37] C. Gutierrez, "Hyperledger's Sawtooth Lake Aims at a Thousand Transactions per Second," ed: March, 2017.

[38] V. Buterin, "What is Ethereum?," Ethereum Official webpage. Available: http://www. ethdocs. org/en/latest/introduction/what-is-ethereum. html, 2016.

[39] A. Harðarson, "Can Ripple disrupt the global payments market?," 2018.

[40] D. Mazieres, "The Stellar Consensus Protocol," A Federated Model for Internet-level Consensus. Version July, vol. 14, 2015.

[41] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, 2016.

[42] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," Journal of Information processing systems, vol. 14, no. 1, pp. 101-128, 2018.

[43] J. Bou Abdo, R. El Sibai, K. Kambhampaty, and J. Demerjian, "Permissionless reputation-based consensus algorithm for blockchain," Internet Technology Letters, vol. 3, no. 3, p. e151, 2020.

[44] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in International workshop on open problems in network security, 2015: Springer, pp. 112-125.

[45] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in 2014 IEEE Symposium on Security and Privacy, 2014: IEEE, pp. 475-490.

[46] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August, vol. 19, p. 1, 2012.

[47] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, pp. 34-37, 2014.

[48] D. Khan, L. T. Jung, M. A. Hashmani, and A. Waqas, "A Critical Review of Blockchain Consensus Model," in 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2020: IEEE, pp. 1-6.

[49] S. Park, K. Pietrzak, J. Alwen, G. Fuchsbauer, and P. Gazi, "Spacecoin: A cryptocurrency based on proofs of space," IACR Cryptology ePrint Archive, vol. 2015, p. 528, 2015.

[50] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in International Conference on Database Systems for Advanced Applications, 2018: Springer, pp. 666-681.

[51] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, "PoRX: A reputation incentive scheme for blockchain consensus of IIoT," Future Generation Computer Systems, vol. 102, pp. 140-151, 2020.

[52] B. Yu, J. Liu, S. Nepal, J. Yu, and P. Rimba, "Proof-of-QoS: QoS based blockchain consensus protocol," Computers & Security, vol. 87, p. 101580, 2019.

[53] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. K. Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," Computers & Security, vol. 95, p. 101871, 2020.

[54] M. T. de Oliveira, L. H. Reis, D. S. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. Mattos, "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," Computer Networks, vol. 179, p. 107367, 2020.

[55] A. Biryukov and D. Feher, "ReCon: Sybil-resistant consensus from reputation," Pervasive and Mobile Computing, vol. 61, p. 101109, 2020.

[56] T. Do, T. Nguyen, and H. Pham, "Delegated proof of reputation: A novel blockchain consensus," in Proceedings of the 2019 International Electronics Communication Conference, 2019, pp. 90-98.

[57] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, "Repucoin: Your reputation is your power," IEEE Transactions on Computers, vol. 68, no. 8, pp. 1225-1237, 2019.

[58] Khursheed, S., Jeoti, V., Badruddin, N., & Hashmani, M. A. (2020, July). Low complexity Phase-based Interpolation for side information generation for Wyner-Ziv coding at DVC decoder. In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) (pp. 1-6). IEEE.