A Delegated Proof of Proximity Scheme for Industrial Internet of Things Consensus

1st Lehlogonolo P.I. Ledwaba
Department of Computer Science
City University of Hong Kong
Kowloon, Hong Kong SAR
lpledwaba2-c@my.cityu.edu.hk

2nd Gerhard P. Hancke
Department of Computer Science
City University of Hong Kong
Kowloon, Hong Kong SAR
gp.hancke@cityu.edu.hk

3rd Aikaterini Mitrokotsa
Department of Computer Science & Engineering
Chalmers University of Technology
Gothenburg, Sweden
aikmitr@chalmers.se

4th Sherrin J. Isaac
NextGen Enterprises and Institutions
Council for Scientific and Industrial Research
Pretoria, South Africa
SIsaac@csir.co.za

***Abstract*—Recently, work with Distributed Ledger Technologies (DLTs) has focussed on leveraging the decentralised, immutable ledger for use outside of cryptocurrency. One industry poised to benefit from DLTs is the Industrial Internet of Things (IIoT); as the inherent cryptographic mechanisms and alternative trust model make DLTs an attractive solution for distributed networks. Existing DLTs are unsuitable for the IIoT, owing to the large computational and energy requirements for consensus operations and the slow throughput of validated blocks. With limited processing, energy and storage resources and a deadline sensitive operational environment, DLTs in their current state could serve to introduce intolerable latency into IIoT processes and deplete constrained, device resources. Designed for the IIoT context, and based off Delegated Proof of Stake, this work serves to introduce a new consensus mechanism called Delegated Proof of Proximity (DPoP). Using existing location discovery processes, nodes in close proximity to a sensor event are elected as delegates; whose role is to handle consensus and block generation. In using information already known to IIoT devices, DPoP aims to reduce wasted effort, improve throughput by limiting the number of nodes required for consensus operations and improve scalability and flexibility of DLT solutions as the IIoT network continues to grow.**

***Index Terms*—Blockchain, Consensus, Delegated Proof of Proximity, Distributed Ledger Technologies, Industrial Internet of Things**

I. Introduction

In recent years, work with Distributed Ledger Technologies (DLTs) has moved away from pure cryptocurrency applications into multiple other domains. The decentralised and immutable nature of the ledger makes it ideal for reducing information duplication across silo'd databases while consensus-based confirmations present an independent verification which does not rely on pre-existing trust or individual trust establishment [1], [2]. The inherent cryptographic mechanisms present in the design of DLTs also ensures the continuous protection of network data. The nature of DLTs make them an interesting solution to use in conjunction with Industrial Internet of Things (IIoT) technologies. The IIoT provides sensing, processing and actuation and can be deployed to cover a large domain space. The main problem seen in the IIoT is the data management of such a large array of devices. Information needs to be available at all levels and to all devices in the network timeously and without compromising security. As the IIoT operates in both the physical and cyber domain, secure, decentralised data management with secure data transmission is trickier to implement as both physical and cyber attacks need to be considered. It is here that DLTs could be well equipped to work within the IIoT application space [2].

Despite the inherent attractiveness of the DLT-enabled IIoT, a number of challenges currently impact the effectiveness of this solution. Most DLTs require a Proof of Work (PoW) consensus to prevent double spending, determine the true ledger view and add new transactions into the ledger. Many criticisms of PoW include [3]:

- the lack of useful work being done by the consensus mechanisms,
- the high energy and processing capabilities required by mining nodes in order to maintain the DLT network,
- the long confirmation times for transactions and transaction blocks,
- the high transaction fees required in order to speed up a transaction's confirmation time and
- the lack of scalability of the resultant network without significant throughput slow down.

Current consensus mechanisms are designed to allow network growth at a predetermined pace– such as the Bitcoin network. IIoT application spaces have limited tolerance owing to hard real time or near real time deadlines. Thus, the long confirmation times seen in DLTs would not be acceptable [3]. Additionally, the limited energy and processing resources available on IIoT devices means that the energy wasted on consensus operations would shorten the device lifetime while

This project was partially supported by the Research Grants Council of Hong Kong under Project CityU 21204716 and by City University of Hong Kong under Project 9678131.

introducing latencies into concurrent IIoT device processes [2]. This would then have a cascading effect throughout the entirety of the IIoT network. The lack of scalability seen in traditional DLT solutions is also of concern given that IIoT deployments could typically consist of hundreds of thousands of devices. Alternative DLT structures have been explored to try and solve some of the problems seen with PoW consensus and the blockchain ledger structure however these solutions require resources exceeding those available on IIoT devices; thus making them unsuitable for the IIoT application space [4].

In order to ensure that DLT-IIoT solutions are able to work concurrently, a new consensus mechanism may be required that includes existing IIoT processes and the work they are doing. This work proposes a modified consensus mechanisms, called Delegated Proof of Proximity (DPoP), which serves to combine IIoT neighbour discovery processes used for data transmission as part of the process used to elect nodes which are to take part in the voting-based consensus process. By selecting voting nodes that are closer to the transaction event, consensus processes are not required to run on nodes further away from the event which won't have a clear image of the triggering event. This allows the operation in the larger portion of the IIoT network to continued uninterrupted. Nodes closer to the transaction event would be able to vote as to the legitimacy of the transaction event by comparing their own environmental observations to those being reported in the transaction event. This form of consensus would allow for minimum disruptions to the IIoT network's operation while utilising work that is already being conducted as part of the consensus; eliminating the need to allocate a large number of additional resources specifically for the DLT process.

The remainder of this work is organised as follows. Section II explores existing consensus mechanisms and work that has been conducted towards improving their efficiency for other application spaces. Section III looks into the requirements when designing a consensus algorithm for the IIoT. Section IV introduces the DPoP consensus algorithm broadly while Section V concludes this work and highlights areas in which further work shall be conducted towards improving and realising the new consensus algorithm.

II. Related Work

The consensus mechanisms provide the method in which the state of the ledger is agreed upon, specifically what transactions have taken place, the identities of the transacting parties, the validity of the transactions and the order in which transactions took place. Some mechanisms are more computationally heavy than others at the expense of tighter, distributed security, while lighter mechanisms have been found to be prone to various security vulnerabilities.

Proof of Work (PoW) ledger technologies are open networks were any peer may participate, but is not required to trust the other peers in the network [1], [5]. The proof of work algorithm is used in order to establish trust in transactions through consensus by peer nodes and through transactional history in the ledger [1], [5]. This mitigates the susceptibility to DoS attacks but comes at the cost of reduced transactional time and scalability issues as the network continues to grow. Here, particularly in blockchain technologies, peers may still change the transactional order by refusing to publish certain transactions within the block [1], [5].

Non-proof of work ledger technologies are typically seen in permissioned DLTs, where all the peers in the network are known and trusted [5]. This allows for the replacement of the proof of work sections in the ledger algorithm to be replaced with a simpler, less secure alternative where a leader may also be established [5]. This, however, makes the ledger technology susceptible to denial of service attacks. Non-PoW technologies may also be manipulated by the publishing peer as they may choose to refuse the publication of given blocks or may choose transaction orders within the transaction block [5].

One of the most commonly seen non-PoW consensus algorithms is Proof of Stake (PoS). These algorithms eliminate the need for mining by having network participants 'bet' a portion of their owned coins on a mempool to be validated into a block. The more coins 'bet' on the mempool for longer, the higher the probability of the staker being chosen as the transaction validator. When a mempool is successfully validated as a block, stakers are rewarded with the full transaction fee [1]. Another consensus mechanism that is not based on PoW is voting. Voting based technologies historically enabled the network community to vote yes or no on an issue [5]. Multiple voting rounds would be established with a peer sending a vote to all other peers in each round. These systems are not widely used in industrial contexts owing to gross inefficiency in bandwidth and latency. The systems have also been shown to be not completely fair in the ordering of transactions with a trade-off between efficiency and fairness [5].

As a combination of these two techniques, Delegated Proof of Stake (DPoS) elects nodes in the network to act as delegates in order to generate new blocks [6]. Each user in the network elects one delegate to validate and generate blocks on their behalf by placing a certain amount of coins as stake on their chosen delegate [6]. The more stake placed on a node, the more weight their vote holds- similar to governance models [7]. Delegates verify all transactions collected since the last instance a block was generated. A reward is allocated when all block transactions are verified and signed to be shared with the electing nodes. Should a delegate fail to verify all transactions within a specified time period, the block gets missed, transactions are unverified and no reward is awarded [6]. The DPoS consensus allows for earlier detection of network-related problems while protecting against double spending attacks as a result of the short time period allocated for transaction verification [7].

In an effort to make DLTs more viable for use in the IIoT, work has been done towards improving how consensus can be achieved efficiently while allowing for better network scalability.

Huang *et al* [8] developed a credit-based, PoW consensus mechanism for the IoT. Nodes are allocated a credit value that changes based on real time node behaviour. Normal behaviours increase the credit while abnormal behaviours decrease the node credit. The difficulty of the PoW is adjusted for individual nodes based on their credit score. Nodes with a low credit score are forced to spend more time and effort solving the PoW, allowing honest nodes more time to solve the PoW while expending less resources [8]. The credit consensus is built upon a directed acyclic graph (DAG) blockchain called the Tangle and utilises full and light nodes [8]. During evaluation, the authors found that the credit-based PoW spent 0.118s per transactions for honest nodes as opposed to 0.7s per transaction for original PoW [8]. The authors also noted that for malicious nodes, the penalty time grew exponentially to the number of attack experienced in the network; indicating that the consensus mechanism could adequately defend against sudden malicious behaviours [8].

The authors in [9] developed a hybrid consensus mechanism, also based on Proof-of-Credit (PoC), such that lightweight DLT operation can be implemented in the IoT. Xu *et al* combine PoC with voting-based chain finality (VCF) such that the microchain solution selects a subset of nodes to act as validators and form a committee that performs the consensus operations [9]. The goal of Microchain is to enable lightweight DLT by running a more efficient consensus mechanism on a reduced number of validating nodes. Transactions are processed in a fixed time period and selection committee nodes is completed at random to ensure unpredictability. At the beginning of each lifetime, the committee selection protocol utilises verifiable random function (VRF) based cryptographic sorting to choose a subset of nodes to act as validators based on their credit weight [9]. This committee is added to the current block. Block proposal is handled using the PoC protocol and only validators from the current committee are capable of proposing new blocks. Block history is verified using a voting-based, chain finality mechanism in order to resolve issues of forking and to increase the cost of attack. A reward, in the form of fees and credit value, is awarded to validator nodes that propose, verify and vote during block finalisation checkpoints [9]. During evaluation, the authors note that the Microchain solution improved upon the block confirmation time seen in existing blockchains. Although larger latency was observed as the committee size increased, this could be combated through proper adjustment of the network configuration. In terms of performance, while Microchain was found to introduced increased overhead for the host node , as the verify and mining processes relied heavily on database querying, its performance still improved upon PoW consensus operations [9].

Lao *et al* [10] propose a mechanism that uses an existing property in IIoT nodes. Using GPS positioning in order to get fixed location of the nodes; Geographic Practical Byzantine Fault Tolerant (G-PBFT) operations were developed in order to achieve consensus in an IoT blockchain network. The consensus makes use of geographic and time information generated by the network nodes and assumes that fixed, IoT devices, such as gateways, are less likely to become malicious owing to their ownership by larger corporations [10]. Nodes are divided into two roles–an endorser and client– and Crypto Spatial Coordinates are used to allocate a blockchain address to a node location- with longer addresses indicating more specific locations and shorter addresses a larger area [10]. IoT devices are elected into the endorser role where then block validation and production occurs according to the G-PBFT consensus. A geographic timer forms the basis of the election and incentive process, with longer times indicating greater loyalty to and honesty in network operations [10]. On the successful validation of a block, the timer is reset and 70% of the transaction fee is awarded as a reward. For endorsers that endorse blocks not generated by themselves, 30% of the transaction fee is awarded. For the G-PBFT consensus, the authors reported an improvement in overall performance when compared to general PBFT and saw a reduction in communication latency owing to the more limited communications exchanged. In both cases, the authors noted that increasing the size of the IoT network would lead to further improvements in the performance and communications latency observed, displaying better scalability than PBFT [10].

III. Designing an Industrial IoT Consensus Algorithm

A consensus solution for the IIoT needs to be able to adequately address the challenges seen in existing IoT-blockchain applications. Improvements to the computational requirements and transaction throughput would be needed for improved performance in the IIoT space while providing flexibility and scalability for changes in the network size and topology [11]. A consensus for IIoT should thus be able to utilise existing device properties and operations to guarantee lower computation and network overhead, reduce the amount of useless work, while displaying faster convergence and greater network growth without bottlenecking [11].

A. Consensus Requirements

DPoS has been seen to be to be a highly scalable consensus algorithm, that requires few processing and hardware resources. It manages to yield a fast transaction generation throughput as well as having fast transaction confirmation times and a more fair distribution of rewards. With voters immediately detecting malicious behaviours and being capable to voting out malicious actors, DPoS inherently provides real-time voting security [7].

IIoT application spaces often require real time or near real time operations. In a previous study, it was seen that the inclusion of native DLT in the IIoT introduced latency that affected the ability of an IIoT node to meet its operational baseline time. The processing requirements of Ethereum were more than what could be adequately provided by the IIoT node– owing to the large number of additional operations that are associated with the generation of an Ethereum transaction– and thus delays were seen in the speed of transactions throughput, the confirmation of transactions and the run time of a concurrent IIoT operation [4]. A new DPoP consensus would need to effectively use the inherent node proximity discovery protocol to minimise the number of operations being introduced onto the IIoT node. This would reduce the latency introduced in other IIoT operations without negatively impacting the efficiency of the proximity discovery protocol. DPoP would also have to demonstrate better scalability than the current Ethereum consensus. Operation of the network should not be significantly impacted by the DLT processes as the number of IIoT nodes increases. Even at larger network sizes, transaction confirmations should be achieved with real time or near real time constraints.

One of the immediate challenges of the new DPoP is providing adequate incentive for nodes in the network to participate in the transaction validation process once voted in as a representative. Apathy from elected delegate nodes would impact the network's ability to function effectively [7]. Transaction confirmation operations would need to be designed such that there is little disruption to the IIoT nodes' normal operations while pushing for a fast confirmation response from the delegated representative nodes. Another challenge is in maintaining the security of the DLT network. Voting schemes and the use of representative nodes brings with it an element of centralisation that is not part of native Proof of Work schemes. This makes a network more susceptible to a 51% attack as well as denial of service attacks. In addition, guards would need to be incorporated against double spending while proximity discovery processes are in progress [7].

B. Proximity in IIoT Nodes

In selected application spaces, proving the physical proximity of nodes is an inherent operation that needs to be provided by IIoT devices. For advanced metering infrastructure, relay attacks on smart meters are partially prevented by implementing proximity proofs based on environmental observations. Smart meters include their location or an observed environmental event within messages to controller units, which then compare against their own location [12].

Physical proximity of IIoT nodes can be determined using numerous mechanisms and neighbour discovery protocols. Easiest is using environmental context to determine node positioning. Absolute location of a node can be determined when the coordinates of two devices is known. Coordinates can be easily obtained using built in geographic equipment, such as GPS devices [13]. Relative location of a node determines the positioning of two devices based upon a communication landmark or against the position of the devices relative to each other; verifying that devices are in the same environment but not requiring knowledge of their position in the existing network. Often, relative location would be determined by using distance-bounding protocols [13].

Distance-bounding relies on one node, the *prover*, to prove its proximity to another node, the *verifier*, which then validates whether the node's proximity claim is true. This is achieved by time-sensitive cryptographic challenge-response exchanges which are designed for time measurement through predictable or constant time responses [14]. The time required for a round trip of challenge-response exchanges allows for the calculation of an upper bound physical distance that is used as a cryptographic proof of proximity [14].

Apart from distance bounding protocols, device proximity may be determined using a variety of other characteristics. For radio-equipped edge devices, proximity may be determined through the received signal strength of the communications. Different radios used in the IIoT– such as those utilising 802.15.4– specify specific ranges between transmissions. Utilising the built-in transceivers, the unique characteristics displayed by received signals may be quantified and used to determine the distance at which nodes are at proximity with each other [15]. In industrial application spaces where radio frequency positioning systems are used for tracking, accurate node proximity can be determined when using existing solutions such as ultra-wideband localization [16].

C. Security

The security of DPoP consensus is built in from both the node proximity determination protocol and from the characteristics of DPoS. Distance bounding protocols cryptographically prove the relative distances between two nodes and addresses relay attacks, where a third party replays stale challenge-response communications, distance fraud, where nodes try to appear closer than they are physically, and terrorist attacks, where nodes co-operate with a nearby third part to appear closer in proximity [13]. In addition to the security provided by the blockchain, secure distance-bounding provides detectable protection for network tampering activities; which is important given the cyber-physical nature of the IIoT application space [14]. Device authentication services may be added using distance bounding protocols, such as in [17], to prevent man-in-the-middle attacks. Protection against terrorist fraud may be implemented through the intentional modification of exchanged responses such that an attacker would need to expend more effort to recover the prover's secret key [18].

DPoS consensus mechanisms, similar to normal PoS, have been found to be vulnerable to a variety of attack types including long range, denial of service, and Sybil attacks. The reduced decentralization of the consensus mechanism also brings with it worries of attacks, such as the 51% attack, which would target voting nodes in an effort to seize control of the network [19]. Previous works have identified DPoS as more vulnerable to 51%, Sybil and denial of service attacks owing to the decreased decentralisation that occurs when reducing the number of nodes participating in consensus processes. Work is being conducted towards improving the security of DPoS by implementing protocols that allow for better detection of malicious behaviours and down-voting or voting out malicious nodes [20]. DPoP would also be offered additional protection from Sybil attacks by the distance-bounding and radio based authentication protocols, as cryptographic challenge-response pairs and time-bounded transaction periods would allow for the detection of Sybil nodes in the similar manner to relay and terrorist attacks.

IV. Delegated Proof of Proximity Consensus for Industrial IoT Applications

The main idea behind delegated proof of proximity consensus (DPoP) is that nodes vote for their delegates/representative using their stake– which is determined by the node's relative proximity to a sensor event– instead of on the validity of an individual block. Delegates have the responsibility of validating transactions and deciding on the block order by comparing to their own observations of the sensor event. To avoid being targeted, chosen delegates are shuffled from the pool of nodes so that for each round of consensus, a different set of nodes are participating in the delegate role.

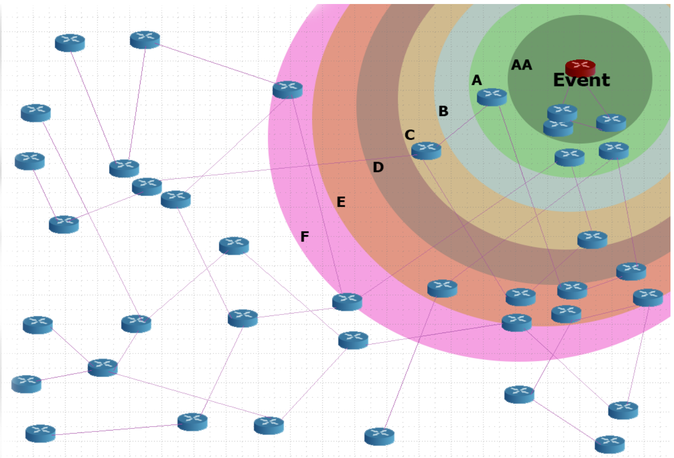

Fig. 1. Delegated Proof of Proximity Network Division Zones

Figure 1 illustrates a network with a sensor event and network nodes divided into seven proximity zones where barrier cut-offs are determined from AA to F. Each zone excludes nodes falling within the boundaries determined by a preceding zone. As the scale of IIoT network deployments are often very large and include hundreds of thousands of nodes, the only nodes that would be eligible for delegate elections would come from a range [AA-B]. This range is determined by how close to the initial sensor event the nodes are. Nodes in range [C-F] then vote for their delegate. Nodes beyond zone F would be considered too far from the initial event to have an accurate view of the sensor event and are thus ineligible for voting. Once delegates have been voted for, these nodes then vote on the validity of the transactions and block order based on their own observations of the event. The closer to the event the delegate is, the more weight awarded to the vote. When two-thirds of the vote is in agreement as the majority (67%), transactions are then considered valid and the blocks are published into the distributed ledger. The voting percentage and range distances for the zones are to be adjustable based on the neighbour discovery protocol being used, the error rate associated with the sensor result as distance increases, the overall network size and the sensitivity of the network operations. Algorithm 1 gives the steps required in order to achieve DPoP consensus.

Algorithm 1 Delegated Proof of Proximity Consensus

```
Determine and Sort Range
if $Proximity \geq Boundary\_Distance$ then
    return $Range$
end if
Select Delegates
for all $Range$ such that $Range \in$ [C,F] do
    SELECT RAND FROM [AA-B]
    ADD TO $Delegates[]$
end for
Delegate Vote
for all $Delegates[]$ do
    if $event\_Val \equiv (observ\_Val \pm Error)$ then
        INCREMENT $Range\_True\_Vote$
    else
        INCREMENT $False\_Vote$
    end if
end for
Determine Consensus
$True\_Votes$ = $Range\_True\_Vote$ x $Range\_Weight$;
if $True\_Votes \geq 67\%$ then
    CONSENSUS ACHIEVED
else
    CONSENSUS NOT REACHED
end if
```

A. Sorting and Delegate Selection

Prior to selecting delegates, nodes whose location is relative to the sensor event would need to be sorted into their proximity zones. Do to this, each node calculates their distance-bound position from the sensing node. Based on the network's zoning configuration, nodes are sorted from range AA to range F. During the sorting process, counters would keep track of the number of nodes being sorted into each zone.

Once zoning is completed, nodes falling in the set $\{x \mid x \in [C, F]\}$ would be prompted to select a node *n* at random from the set $\{n \mid n \in [AA, B]\}$. The selected nodes shall form an electoral body *Delegates* which shall be execute the consensus mechanisms.

B. Establishing Consensus

Delegates vote on the network consensus by comparing the triggering sensor value, called an *event*, with their own view of the environment, called an *observation*. Owing to minute differences in manufacturing and sensitivity between sensors, allowances for some variance needs to be built in for the observations made by *Delegates*. As such, the allowed *Error* for each range is determined from the variance data given in the sensor data-sheet. Additionally, *Delegate* votes are weighted in order to account for the decreasing accuracy and granularity experienced by nodes furtherest away from the *event*. Consensus votes cast by nodes in range AA thus hold more stake than votes cast by nodes in range B.

As *Delegates* compare their *observation* to the *event*, nodes cast a *TRUE* vote if the *event* is found to be within the margin of error allowed for the range. If not, nodes cast a *FALSE* vote. Weighting is applied to the votes cast in each range before all *TRUE* votes and *FALSE* votes are accumulated. The percentage of *TRUE* votes from the total number of voting *Delegates* is calculated. If a two-thirds majority is achieved by *TRUE* votes, consensus is achieved, the *event* transaction is verified and a block is published. A reward is given to *Delegates* which is shared with their selector nodes from range [C,F]. Should consensus not be achieved, the transaction is discarded, no reward is given and the consensus process is concluded.

V. Future Work

The high computational and energy requirements, wasted effort from consensus operations, limited throughput and lack of scalability restricted the use of blockchain solutions in the IIoT application space. This work served to introduce a consensus mechanism designed in consideration of the requirements and limitations of an IIoT network. Based on the existing DPoS mechanism, DPoP served to utilise IIoT relative location discovery processes as the fundamental basis from which nodes are selected to participate in validation and block generation activities and environmental sensing activity as the means of achieving voting-based consensus. This aimed to reduce wasted resource efforts, improve scalability and throughput as a smaller portion of the network is required to perform blockchain operations; allowing other IIoT processes to run uninterrupted. DPoP alters traditional DPoS to be better suited in the IIoT context while retaining the advantages observed by its parent mechanism.

To further the development of this consensus mechanism, a thorough evaluation on the effectiveness of the DPoP consensus shall be conducted through implementation and performance testing on a physical IIoT edge device. DPoP shall be evaluated against the established performance of PoW in the IIoT context in terms of transaction throughput, block generation time, energy and computational usage as well as performance when run concurrently with an independent IIoT device process. The scalability of the consensus mechanism shall be evaluated through simulation of a growing IIoT network. To improve the overall security, cryptographic proximity proofs shall be used to provide authentication services alongside distance bounding proximity location as a main part of the DPoP delegate selection and consensus operations.

The fundamental structure of blockchain and DLTs have a high potential to work well in enhancing and improving operations and processes in IIoT application spaces. While existing solutions have various shortcomings that make them unsuited for the IIoT, by carefully designing solutions that are able to work with the various requirements and restrictions of a constrained, real time environment, progress can be made towards realising a blockchain-enable IIoT.

References

[1] N. Teslya and I. Ryabchikov, “Blockchain Platforms Overview for Industrial IoT Purposes,” in *2018 22nd Conference of Open Innovations Association (FRUCT)*, 2018, pp. 250–256.

[2] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, “A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modelling,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–32, 2020.

[3] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, “When Internet of Things Meets Blockchain: Challenges in Distributed Consensus,” *IEEE Network*, vol. PP, p. 1, 03 2019.

[4] L. P. I. Ledwaba, G. P. Hancke, S. J. Isaac, and H. S. Venter, “Developing a Secure, Smart Microgrid Energy Market using Distributed Ledger Technologies,” in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1, 2019, pp. 1725–1728.

[5] M. Harmon, “Choosing the right distributed ledger algorithm,” January 18, 2017. [Online]. Available: https://www.pingidentity.com/en/company/blog/2017/01/18/choosing_the_right_distributed_ledger_algorithm.html

[6] MediaWiki, “Delegated Proof of State,” Sep 23, 2019. [Online]. Available: https://en.bitcoin.it/wiki/Delegated_proof_of_stake

[7] T. Jenks, “Pros and Cons of the Delegated Proof-of-Stake Consensus Model,” Aug 16 2018. [Online]. Available: https://www.verypossible.com/blog/pros-and-cons-of-the-delegated-proof-of-stake-consensus-model

[8] J. Huang, L. Kong, G. Chen, L. Cheng, K. Wu, and X. Liu, “B-IoT: Blockchain Driven Internet of Things with Credit-Based Consensus Mechanism,” in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 1348–1357.

[9] R. Xu, Y. Chen, E. Blasch, and G. Chen, “Microchain: A Hybrid Consensus Mechanism for Lightweight Distributed Ledger for IoT,” Dec 24, 2019. [Online]. Available: https://arxiv.org/pdf/1909.10948.pdf

[10] L. Lao, X. Dai, B. Xiao, and S. Guo, “G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications,” unpublished.

[11] M. Salimitari and M. Chatterjee, “An Overview of Blockchain and Consensus Protocols for IoT Networks,” Sep 14, 2018. [Online]. Available: https://www.groundai.com/project/an-overview-of-blockchain-and-consensus-protocols-for-iot-networks/1#bib.bib2

[12] Y.-C. Hu, A. Perrig, and D. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks,” in *Proceedings - IEEE INFOCOM*, vol. 3, 2003, pp. 1976–1986.

[13] Q. Hu, J. Zhang, A. Mitrokotsa, and G. Hancke, “Tangible security: Survey of methods supporting secure ad-hoc connects of edge devices with physical context,” *Computers Security*, vol. 78, pp. 281 – 300, 2018.

[14] G. Hancke, K. Mayes, and K. Markantonakis, “Confidence in smart token proximity: Relay attacks revisited,” *Computers Security*, vol. 28, no. 7, pp. 615 – 627, 2009.

[15] U. M. Qureshi, G. P. Hancke, T. Gebremichael, U. Jennehag, S. Forsstrm, and M. Gidlund, “Survey of Proximity Based Authentication Mechanisms for the Industrial Internet of Things,” in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 5246–5251.

[16] B. Silva, Z. Pang, J. erberg, J. Neander, and G. Hancke, “Positioning infrastructure for industrial automation systems based on UWB wireless communication,” in *IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society*, 2014, pp. 3919–3925.

[17] E. Pagnin, A. Yang, G. Hancke, and A. Mitrokotsa, “HB+DB, Mitigating Man-in-the-Middle Attacks against HB+ with Distance Bounding,” in *Proceedings of the 8th ACM Conference on Security Privacy in Wireless and Mobile Networks*, ser. WiSec 15. New York, NY, USA: Association for Computing Machinery, 2015. [Online]. Available: https://doi.org/10.1145/2766498.2766516

[18] G. P. Hancke, “Distance-bounding for RFID: Effectiveness of terrorist fraud in the presence of bit errors,” in *2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, 2012, pp. 91–96.

[19] S. Sayeed and H. Marco-Gisbert, “Assessing blockchain consensus and security mechanisms against the 51% attack,” *Applied Sciences*, vol. 9, no. 9, p. 1788, 2019.

[20] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,” *IEEE Access*, vol. 7, pp. 118 541–118 555, 2019.