Blockchain-based Sensor Data Validation for Security in the Future Electric Grid

A. G. Colaço*, K. G. Nagananda*, R. S. Blum*, H. F. Korth†
*Department of ECE, †Department of CSE,
Lehigh University,
Bethlehem PA 18015, USA.
Email: {asc219,kgn209,rb0f,hfk2}@lehigh.edu

***Abstract*—This paper explores the feasibility of using blockchain technology to validate that measured sensor data approximately follows a known accepted model to enhance sensor data security in electricity grid systems. This provides a more robust information infrastructure that can be secured against not only failures but also malicious attacks. Such robustness is valuable in envisioned electricity grids that are distributed at a global scale including both small and large nodes. While this may be valuable, blockchain's security benefits come at the cost of computation of cryptographic functions and the cost of reaching distributed consensus. We report experimental results showing that, for the proposed application and assumptions, the time for these computations is small enough to not negatively impact the overall system operation. From this we conclude that it is indeed worthwhile to further study the application of blockchain technology in the electricity grid, removing the assumptions we make and integrating blockchain in a much more extensive manner. To the best of our knowledge, this is the first instance where blockchain is used to validate the measured sensor data in the electricity grid, thus providing security to other system operations.**

***Index Terms*—Blockchains, Iota, sensor data validation, data security.**

I. Introduction

Rapid developments in communications and computational technology have provided a solid foundation and necessary conditions for the implementation of robust infrastructure for the next-generation electric power grid [1]. In this direction, the introduction of advanced sensing and measurement technologies, which acquire and transform data into information, will enhance multiple aspects of the energy management system (EMS). Sensing technologies are quintessential to maintain the health and integrity of the electricity grid; they are coordinated into the EMS to alleviate billing estimation, prevent energy thefts, support frequent meter readings, *etc*., leading to improved demand-response programs [2]. Given that major electrical grids (US, China, Europe) are going through a paradigm shift moving towards increased sensing and information technology, sensing mechanisms need be bolstered with newer security features that are more robust to cyberattacks than the existing architectures [3].

One of the most appealing developments in cybersecurity in recent times is blockchain technology [4] in which data are stored as a growing list of records (typically grouped into blocks) linked via cryptographic hash pointers to the previous block. Each block contains a timestamp and transaction data. The central feature of blockchains is their resistance to modification of data (immutability), thereby providing "security by design". Although blockchains are immutable by design, the data they contain are visible to all nodes participating in the system except for data items that are specifically encrypted. Transactions are signed cryptographically using *public-key encryption* [5] by the submitter, thus making transactions irrefutable. Blocks are added to the chain via distributed consensus over a network of computers (nodes) that verify data-transactions. Since electricity producers and consumers are connected via a grid spread over wide geographical areas, sharing (*i.e.*, distributed transactions) massive data sets, the blockchain lends itself naturally to the context of the electric grid security; see, for example, [6]–[11].

Recently, blockchain for the electric grid is beginning to receive significant attention in the power systems literature. For example, blockchain is now incorporated into data aggregation and regulation mechanism [12], for electric vehicle charging [13], for power line communication [14], to design smart contracts that enable efficient usage of in-home electric appliances [15]–[17] and efficient demand-response programs [18]–[22], to develop smart cities with the aid of Internet of Things (IoT) [23], and to incentivize load-shifting to reduce peak-hour loads [24]. Blockchains have also been employed to analyze the trade-off between electric utilities (intending to make profits) and network operators (aiming to maintain stability of the power network) using game-theoretic frameworks [25]. Peer-to-peer energy trading schemes have been developed using blockchains by taking into account the variations in the voltage levels and network capacity in [26]. Countermeasures to cyberattacks and data manipulation using blockchains, and its impact on dynamic state estimation in power networks has been analyzed in [27].

In this paper, we introduce a new application of blockchains for power systems operations. Specifically, we integrate blockchain to validate that the measured sensor data follows an accepted system model, thereby providing data security to other important system operations that rely on the measured sensor data. To the best of our knowledge, such sensor data validation mechanisms via blockchains which enhances data

security in power systems, though relevant, has not appeared in the literature and is the subject topic of this paper.

In a typical power grid, the sensors could be in the form of phasor measurement units (PMUs), transducers, smart metering, *etc* [2]. Sensor data is used for numerous purposes; for example, in fault detection and isolation. In this paper we propose checking the validity of the data using a model we assume is already available. The model might have been obtained using something similar to what is called the state estimation process, as illustrated in Fig. 1. The long-standing

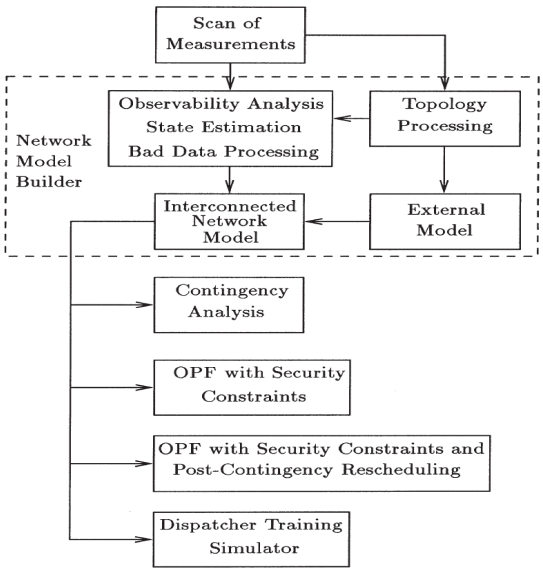

Fig. 1: Real-time network analysis functions [28, Fig. 1.2]

standard practice is that the state estimation procedure is repeated at 15 minute intervals. Current standard practice may be less acceptable in the future for several reasons: (i) The nature of future attacks on the grid may necessitate the ability to have a shorter response time to anomalies; (ii) centralization of data collection and of action based on those data presents a single point of failure; (iii) adversarial takeover of some nodes may lead to the submission of intentionally erroneous data for malicious purposes. Impersonation of nodes is also a potential threat; (iv) the increased openness of the grid to power input from retail sources of renewable energy will cause the grid to evolve from its relatively closed, private status to something more akin to the Internet.

Blockchain technology is able to address these issues, as we shall describe below. However, the distributed consensus required in a blockchain system can have long response times, depending on the consensus mechanism used. For this reason, we have implemented a testbed proof-of-concept of our solution in which we ensure that not only is performance acceptable, but furthermore, that it enables significantly faster response to anomalies and permits any node to take action, not only the command center.

The remainder of the paper is organized as follows. In Section II, we provide details of the steady state model we assume, which is similar to the one typically employed in current grid operations. The benefits offered by blockchains for secure state estimation are highlighted in Section III. Experimental results are presented in Section IV. Concluding remarks are provided in Section V.

II. Sensor Data Validation

We consider a power network with N buses and assume the available model for checking the data is a steady state linear DC power flow model to illustrate our ideas. While these steady state models are used in practice today [28], our ideas can be seamlessly extended for any future models, including dynamic and nonlinear models. The model variables include bus voltage angles, branch active power flows, and bus active power loads. These variables are connected by a set of network equations (network model) that express the power balance at network buses and the relationship between nodal voltage angles and branch active power flows.

The steady state DC model we employ can be described as:

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x}, \tag{1}$$

where $\boldsymbol{z} \in \mathbb{R}^{m\times 1}$ and $\boldsymbol{x} \in \mathbb{R}^{n\times 1}$ are the sensor measurements at various nodes in the power network which we will check. We assume $\boldsymbol{z}$ and $\boldsymbol{x}$ are available, along with $\boldsymbol{H}$, when the check is performed.

We will use blockchain to help us make sure that the measured data ($\boldsymbol{z}$ and $\boldsymbol{x}$) fits the known model in (1) with small errors. Towards this end, we assume that the system matrix $\boldsymbol{H}$ is recent and not stale. Interestingly, our analysis can be extended without significant alterations to the scenario where the system model is nonlinear, which highlights the generality of the proposed idea. Furthermore, our validation mechanism can be adopted to any sensor application where a model is available and is not restricted to power systems operations alone.

III. How blockchain enables secure distributed data collection

A. The structure of a blockchain

Blockchain security is based upon a cryptographic hash function. Such functions, denoted here by h, map their input to a bit string with randomness and uniform distribution properties that ensure the following properties:

(a) *Collision resistance*: it is infeasible to find two distinct values x and y such that $h(x) = h(y)$;
(b) *Irreversibility*: Given $h(x)$, it is infeasible to find x

By *infeasible*, we mean that there is a strong mathematical argument that it impossible to do any better than random guessing. Typically the range of a cryptographic hash function is a 256-bit number, making the probability of a successful guess 1 in 2^{256}. Another key component of blockchain security is *public-key encryption*, in which each user has two cryptographic keys: a *public key* and a *private key*. The public key is published openly. The private key is kept secure. To send a user a secure message, the sender encrypts using the

receiver's public key. Then only the intended recipient can decrypt it using its secret private key. Users are able to sign a document cryptographically by encrypting the document using their private key. Anyone can then decrypt using the user's public key and compare that result with the document. Since the private key is secret, this provides proof that the owner of that private key "signed" the document. See [5] for details of public-key cryptosystems.

Blockchains have two key data-security properties that are relevant to our application:

(1) *Immutability*: Blocks on the blockchain are connected by hash-pointers, which are pointers in the normal sense of a computer data structure, augmented by a cryptographic hash of the block to which it points. This means that it suffices to hold the root hash of a blockchain in order to ensure the validity of an entire chain.
(2) *Irrefutability*: Transactions submitted to a blockchain are signed by the submitter. This provides public and irrefutable proof that the alleged submitted is indeed the actual submitter.

These two properties together create a "trustless" mode of interaction in which no intermediary is needed to ensure validity of data published on the blockchain. They allow any node on the grid to validate that data received truly came from the claimed originating node. Furthermore, they allow a node to avoid needing to store historical data since data can be downloaded at a later time and verified cryptographically. (There are data structures, notably Merkle trees [29], that enable fast implementations of this capability, but these details are beyond the scope of this paper.)

Blockchains provide important decentralization properties. All nodes agree on the contents of the blockchain. This agreement is maintained by a consensus mechanism for adding new blocks to the chain. A node seeking to add to the chain would validate the transactions being added and then start the consensus process. There are many such mechanisms. The most widely known is Bitcoin's energy-intensive proof-of-work algorithm [30]. Not only is Bitcoin's approach highly consumptive of energy, but also it has a long *time to finality*, the time between transaction submission and the time that transaction is deemed to be permanently and immutably on the blockchain. Bitcoin's mechanism is designed for a *public* blockchain in which any machine can become a node. Enterprise blockchain applications typically are not public but instead are *permissioned*, which means that there is a process through which a node gets permission to join the blockchain system. Permissioning eliminates the threat of *Sybil attacks*, in which an adversary attempts to overwhelm the network with a huge number of notes. Freedom from Sybil attacks enables the use of faster, more efficient consensus mechanisms. In particular, Byzantine-consensus algorithms are robust to as many as $1/3$ of the nodes failing in a malicious manner. Malicious failure means taking precisely the most damaging course of action. There are many variants of Byzantine consensus, including classics [31], [32], and such recent contributions as [33], [34]. Note that every node can validate transactions in a new block and thus ensure that it will not agree to accept blocks with invalid transactions.

B. A high-level view of blockchain for checking sensor data

We envision a blockchain shared among nodes of the power grid. A group of nodes may transmit sensor data check information as transactions on the blockchain. Our experimental results in Section IV show that transactions can be processed in extremely short time intervals, on the order of a second or less. These transactions are then added to the blockchain via the consensus mechanism. All nodes than then see the entire state, detect anomalies, and respond appropriately.

From this high-level perspective, any blockchain would work. However, we desire an implementation that presents minimal demand on grid nodes, is not overly energy-intensive, and has performance characteristics meeting our goal of rapid response to changing grid status.

IV. Experiments and results

For our experiments, we chose the Iota blockchain [35]. We did so due to its design, which is targeted to applications in the domain of the Internet of Things (IoT). Instead of adding large blocks of transactions at once, it permits transactions to be added individually. Instead of the traditional chain-of-blocks data structure, Iota transactions are stored in a directed-acyclic-graph (DAG) structure. The claimed performance characteristics of Iota match our goals and our experiments were designed to evaluate those claims.

For our experiments, we deployed a private Iota tangle using a structure similar to that on the Iota Devnet, which is a free, developer version of public Iota network (Mainnet) on which Iota tokens are traded. We simulated client sensors connected to a server node via a TCP network. The sensor data matrix is generated from a MATLAB simulation and converted to numeric strings. These numeric strings are attached to the tangle as transactions. We validate the transaction attached to the tangle by multiplying its data with a G matrix and checking if the product matches a predefined state. A transaction is validated based on this Boolean result.

The tangle employs a *coordinator*, which is an application that creates, signs, and sends bundles of transactions from a single address. The transactions referenced by these bundles are used as milestones by other nodes for reaching a consensus. We used Iotas *Compass* to run our coordinator and simulated various configurations for the tangle. We used our own coordinator because we are running our own test environment. The actual public Iota blockchain uses a coordinator provided by the Iota Foundation. The need for a coordinator of any sort is being phased out in the near term as the Iota blockchain system grows and evolves. The removal of the coordinator will result in a fully decentralized system.

Compass allows us to define the various parameters for the Tangle: depth, minimum weight magnitude (MWM), tick, seed, security, host. We describe the first three below as those

are the parameters that are most relevant to overall system performance (though all matter in a production system).

The *depth* parameter defines how many key-address pairs Compass can use (2^{depth}). The greater the depth, the longer it will take to validate transactions. However, this increases the number of transactions that can be confirmed in one milestone. Stately differently, the depth parameter allow us to tune the system to trade worst-case latency versus overall system throughput.

The *minimum weight magnitude* (MWM) parameter defines the difficulty of the *proof of work* (PoW) computation that a node is required to do to send a transaction to the tangle. As is the case for Bitcoin, a PoW barrier serves to prevent Sybil attacks. Unlike the case of Bitcoin, the Iota PoW overhead is significantly lower and can be outsourced by low-power nodes to high-power nodes. Of course, in a power network, unlike an IoT network, power usage is less of a concern. That could change, however, in a future power-grad environment where retail customers also sell power to the grid. A lower MWM means it is easier to validate and send transactions to the tangle.

The *tick* parameter defines how much time Compass waits before creating and sending a milestone in the network. The longer the tick value, the longer it takes to confirm transactions in the network. We assume that we are receiving data for state estimation from the sensors in real time and validating them as stated by the Boolean function and then attaching them to the tangle as transactions.

As the sampling rate is high for these sensors, we need a lightweight configuration to decrease the time required to attach transactions to the tangle. At the same time, we need to ascertain that the transactions are confirmed at a similar rate so that the network does not back up.

We tested the following configurations for the tangle and timed the results:

1) Depth = 8, MWM = 9, tick = 60000
2) Depth = 16, MWM = 5, tick = 2000
3) Depth = 16, MWM = 2, tick = 2000
4) Depth = 16, MWM = 2, tick = 10000

The first configuration is similar to the Iota Devnet configuration. We assume that a transaction consists of the average of the sampling of the sensor over the sampling period. The frequency of the sensor is 60 samples per second. Our simulation sends a transaction every second to the node to be added to the tangle.

The following are the timing results based on the cases stated above. We show the average time in seconds to send a transaction and the average time in seconds to confirm a transaction (*i.e.* time-to-finality).

Config.	Send Time	Confirm Time
1	1.300	30.00
2	0.793	4.833
3	0.487	3.667
4	0.268	5.333

From the table above, we see that the more resource-intensive Iota Devnet configuration (configuration 1) has a much higher latency. This is due to the fact that it models a public tangle and needs to have a higher difficulty PoW (higher MWM) to protect from attack. The other three configurations are appropriate for our private tangle. The latency is much lower and the adding of transactions is easier.

In a private tangle, the MWM value can be set considering that the transaction rate is known. A higher MWM causes a larger latency in sending transactions to the tangle, therefore moderating the number of transactions at any given time on the network. The risk of a Sybil attack can be mitigated by a permissioning agent that controls admission of nodes to the network. In our experimental system, we focused on performance, but we discuss the broader issues in Section V.

From configurations 2 through 4, we see the influence of the tick parameter setting on sending and confirmation time. Having Compass wake up less often reduces its load on the system, but increases confirmation time since one must wait for the Compass coordinate to mark a milestone by sending a bundle of its transactions.

In a production system, additional research would be required to find a good setting for the parameters, but all of the results shown, including the Devnet configuration (configuration 1) show performance that is hugely better than the current 15-minute intervals. This shows that the added security and decentralization of a blockchain-based system can be achieved while not only maintaining acceptable performance but moreover performing at a level that enables anomaly detection in seconds rather than tens of minutes.

V. Concluding Remarks

In this paper we have just taken the first steps to demonstrate the feasibility of employing blockchain to enhance electricity grid operation in a very limited way under limiting assumptions made to simplify matters. Thus, much more work needs to be done and the purpose of this paper is to suggest this work should be done. One should not assume the computational complexity of cryptographic functions and the cost of reaching distributed consensus make blockchain impractical for electricity grids. In the future, we need further study on the feasibility for employing blockchain to enhance electricity grid operation when blockchain is employed in a much more extensive manner without limiting assumptions. For example, even for the limited application of sensor measurement checking we focused on, blockchain could be employed in the network model building process (see Fig. 1) and all operations can be made completely decentralized. Ultimately, it would be interesting to consider blockchain integration with all aspects of electricity grid operation.

This work is a proof-of-concept feasibility study that shows that a blockchain-based system for sensor data validation seems feasible. This, then, opens the question of designing a control-and-governance model for a grid with a large number of participants whose degree of mutual trust may be limited. There is a large spectrum of choices ranging from the total

public openness of Bitcoin, to the collection of small trust groups used by Ripple (XRP) and Stellar (XLM) in the financial world, to the highly-controlled permissioned environments of several recent supply-chain blockchain deployments. This spectrum is discussed in detail in [36].

With a future-grid blockchain design in hand, the next research question is how best to use this new capability to create a grid-information infrastructure that is robust to some participants failing to behave in the expected manner, whether due to malfunction or malicious intent. A grid that is robust to such failures may simply tolerate those failures, but it could also identify the sources of those failures and appropriately "punish" offenders, possibly by expulsion from the network, a financial penalty (imposed either in-network or externally), or some other policy-based action.

A national, or possibly international, grid whose participants range from traditionally sized nodes to retail-level nodes, will, no doubt, be of regulatory interest to governmental leaders and policy-makers. A design based on the secure mathematics of blockchain systems, along with an appropriate governance model may well evolve beyond being an opportunity to being a necessity.

ACKNOWLEDGEMENT

This work was supported by the National Science Foundation under Grant ECCS-1744129.

REFERENCES

[1] M. Shahidehpour and Y. Wang, *Communication and Control in Electric Power Systems*. NJ, USA.: Wiley-Interscience, 2003.

[2] S. F. Bush, *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid*. John Wiley & Sons, 2014.

[3] R. J. Campbell, "Electric grid cybersecurity," Congressional Research Service, Tech. Rep. R45312, Sep. 2018.

[4] B. Hill, S. Chopra, and P. Valencourt, *Blockchain Quick Reference*. Packt Publishing, 2018.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[6] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Resilience Week*, Sep. 2017, pp. 18–23.

[7] R. Skowronski, "On the applicability of the GRIDNET protocol to smart grid environments," in *Proc. IEEE Smart Grid Commun.*, Oct. 2017, pp. 200–206.

[8] I. Kotsiuba, A. Velykzhanin, O. Biloborodov, I. Skarga-Bandurova, T. Biloborodova, Y. Yanovich, and V. Zhygulin, "Blockchain evolution: from bitcoin to forensic in smart grids," in *Proc. IEEE Big Data*, Dec. 2018, pp. 3100–3106.

[9] T. Tesfay, M. Jamei, A. Scaglione, M. Khorsand, K. Hedman, and R. Bazzi, "AVAIL: Assured volt-ampere information ledger," in *Proc. IEEE Smart Grid Commun.*, Oct. 2018, pp. 1–6.

[10] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[11] M. Pipattanasomporn, S. Rahman, and M. Kuzlu, "Blockchain-based solar electricity exchange: Conceptual architecture and laboratory setup," in *Proc. IEEE ISGT*, Feb. 2019, pp. 1–5.

[12] M. Fan and X. Zhang, "Consortium blockchain based data aggregation and regulation mechanism for smart grid," *IEEE Access*, vol. 7, pp. 35 929–35 940, Apr. 2019.

[13] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25 657–25 665, Jun. 2018.

[14] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[15] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, Mar. 2018.

[16] K. Nakayama, R. Moslemi, and R. Sharma, "Transactive energy management with blockchain smart contracts for P2P multi-settlement markets," in *Proc. IEEE ISGT*, Feb. 2019, pp. 1–5.

[17] J. Lin, M. Pipattanasomporn, and S. Rahman, "Comparative analysis of blockchain-based smart contracts for solar electricity exchanges," in *Proc. IEEE ISGT*, Feb. 2019, pp. 1–5.

[18] P. Danzi, M. Angjelichinoski, C. Stefanovic, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," in *Proc. IEEE Smart Grid Commun.*, Oct. 2017, pp. 45–51.

[19] J. Horta, D. Kofman, D. Menga, and A. Silva, "Novel market approach for locally balancing renewable energy production and flexible demand," in *Proc. IEEE Smart Grid Commun.*, Oct. 2017, pp. 533–539.

[20] P. Danzi, S. Hambridge, C. Stefanovi, and P. Popovski, "Blockchain-based and multi-layered electricity imbalance settlement architecture," in *Proc. IEEE Smart Grid Commun.*, Oct. 2018, pp. 1–7.

[21] C. Dang, J. Zhang, C. Kwong, and L. Li, "Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market," *IEEE Trans. Smart Grid*, 2019, in press.

[22] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang, "Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles," *IEEE Trans. Emerg. Topics Comp. Intell.*, vol. 3, no. 3, pp. 205–216, Jun. 2019.

[23] C. Lazaroiu and M. Roscia, "Smart district through IoT and blockchain," in *Proc. IEEE ICRERA*, Nov. 2017, pp. 454–461.

[24] M. T. Devine and P. Cuffe, "Blockchain electricity trading under demurrage," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2323–2325, Mar. 2019.

[25] O. Saukh, F. Papst, and S. Saukh, "Synchronization games in P2P energy trading," in *Proc. IEEE Smart Grid Commun.*, Oct. 2018, pp. 1–6.

[26] J. Guerrero, A. C. Chapman, and G. Verbic, "Decentralized P2P energy trading under network constraints in a low-voltage network," *IEEE Trans. Smart Grid*, 2018, early access.

[27] M. N. Kurt, Y. Yilmaz, and X. Wang, "Secure distributed dynamic state estimation in wide-area smart grids," *IEEE Trans. Inf. Foren. Sec.*, 2019, in press.

[28] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*. Kluwer Academic Publishers, 1999.

[29] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Adv. Crypt.* Springer Heidelberg, 1988, pp. 369–378.

[30] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[31] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *J. ACM*, vol. 27, no. 2, pp. 228–234, April 1980.

[32] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comp. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[33] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. ACM Symp. Operating Syst. Princ.*, March 2017, pp. 51–68.

[34] M. Baudet, A. Ching, A. Chursin, G. Danezis, F. Garillot, Z. Li, D. Malkhi, O. Naor, D. Perelman, and A. Sonnino, "State machine replication in the Libra blockchain," The Libra Assn., Tech. Rep., 2019.

[35] S. Popov, "The tangle," The Iota Foundation, Tech. Rep., 2018.

[36] H. F. Korth, "Consensus in enterprise and financial blockchains: Assumptions and challenges," in *Proc. First Workshop on Blockchain and Distributed Ledger*, 2019.