This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed
in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-5376C

# A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems

Dimitrios Sikeridis*, Ali Bidram*, Michael Devetsikiotis*, and Matthew J. Reno¶
*Department of Electrical and Computer Engineering, The University of New Mexico, Albuquerque, NM, USA
¶Sandia National Laboratories, Albuquerque, NM, USA
{dsike, bidram, mdevets}@unm.edu, mjreno@sandia.gov

***Abstract*—Distribution and transmission protection systems are considered vital parts of modern smart grid ecosystems due to their ability to isolate faulted segments and preserve the operation of critical loads. Current protection schemes increasingly utilize cognitive methods to proactively modify their actions according to extreme power system changes. However, the effectiveness and robustness of these information-driven solutions rely entirely on the integrity, authenticity, and confidentiality of the data and control signals exchanged on the underlying relay communication networks. In this paper, we outline a scalable adaptive protection platform for distribution systems, and introduce a novel blockchain-based distributed network architecture to enhance data exchange security among the smart grid protection relays. The proposed mechanism utilizes a tiered blockchain architecture to counter the current technology limitations providing low latency with better scalability. The decentralized nature removes singular points of failure or contamination, enabling direct secure communication between smart grid relays. We also present a security analysis that demonstrates how the proposed framework prohibits any alterations on the blockchain ledger providing integrity and authenticity of the exchanged data (e.g., real-time measurements/relay settings). Finally, the performance of the proposed approach is evaluated through simulation on a blockchain benchmarking framework with the results demonstrating a promising solution for secure smart grid protection system communication.**

***Index Terms*—Smart Grid, Cyber-Physical Security, Adaptive Protection Systems, Blockchain Technology**

## I. Introduction

Power system protection is a key grid component responsible for detecting and clearing faults on different equipment, e.g., generators, lines, and transformers [1]. Its key elements are protection relays which are responsible for fault detection and isolation on their protected equipment. A protection system is expected to ascertain requirements for sensitivity (i.e., the ability of timely detecting and isolating faulted regions to avoid damaging other equipment), and selectivity (i.e., the intelligent isolation of faults to minimize the number of customers experiencing power outage). The 2003 Northeast blackout, the world's second most widespread blackout, highlights how a well-coordinated protection system could have prevented the spread of cascading power outages [2]. Also, the 2018 assessment of North American Electric Reliability Corporation reports that 9% of the total grid interruptions in the last five years are related to relay misoperations [3].

The design of protection systems includes physical components coupled with communication-enabled intelligence to implement the protection logic resulting in large scale cyber-physical formations. Due to the the infrastructure's critical role, security is paramount especially since the rapid automation of the grid leads to completely digital protection components with increased capabilities in terms of computing power, embedded storage, and communications. This shift to smart industrial devices, introduces vulnerabilities pertaining to the cyber fabric of the installations that can in turn affect physical components, which is an important national security threat in case critical loads are targeted [4], [5].

### A. Related Work

Conventional protection systems utilize fixed settings for protective relays which are well-tuned only for the normal operating conditions [6], and do not account for extreme events, e.g., hurricanes, where the system is prone to multiple simultaneous faults and line outages, and the power system undergoes drastic topology changes. Moreover, the coordination of the conventional protection system can be affected by the large number of distributed energy resources (DER) due to their different fault current levels and potential for reverse power flow [7]. To tackle these challenges, adaptive protection schemes have been proposed to modify the protective actions according to system condition changes, as in [8], where authors utilize numerical directional overcurrent relays coupled with commercial mathematical programming tools and optimization solvers.

Focusing on the cyber layer, power systems automation infrastructure often utilizes centralized communication network with a central substation controller for monitoring data and sending control/protection signals [9]. Such centralized data aggregation creates security challenges as parts of the infrastructure are in risk of being paralyzed in case of an attack on the control center (e.g. 2016 attack against Ukraine's substation [5]). In addition, the emerging digital nature of protection components makes them vulnerable to a series of modern security threats including false data injection attacks [10], grid command tempering (e.g., in Puerto Rico [5]), Aurora attacks, and privacy leaks [5].

Recently, towards enhancing the security of power systems infrastructure, the emerging Blockchain technology [11] has been utilized to achieve build-in privacy, integrity, authenticity, and confidentiality of the exchanged data and control signals. In [12], the authors propose a blockchain-based scheme for

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

smart meter data aggregation within the smart grid to preserve the electricity consumption data privacy by grouping users of the same blockchain network and utilizing pseudonyms for identity protection. However, the final data aggregation is facilitated by traditional means through a wide area network. Wan et. al. in [13] introduce a Bitcoin-based Industrial Internet of Things (IIoT) architecture for smart factories, and automated production platforms. Their design retains confidentiality, integrity, and availability through state machine and transition models, while the IIoT security is enhanced through asymmetric encryption and whitelisting. Finally, in [14] the authors introduce a bitcoin-based data protection mechanism for smart grid meters, that utilizes a single tier architecture (all meters included in the same blockchain), and present a discussion of successful attack probabilities through different scenarios. While the proposed solutions offer security and privacy advantages, they require nodes with high computational and memory capabilities, and come at a cost on network scalability, and achievable throughput [11], [15].

### *B. Contributions and Outline*

In light of the above, this work introduces an Adaptive Protection Platform (APP) coupled with a blockchain-inspired network architecture for data aggregation and relay setting dissemination. The main contributions of this paper are summarized as follows:

1) A scalable APP is proposed for distribution systems to effectively adjust the protection relays' settings in real-time considering the uncertainties in the power distribution system.

2) A multi-tiered decentralized blockchain architecture is adopted to facilitate secure information exchange within the APP. The modular architecture increases the throughput of the local relay to relay communication, while leading to better scalability, and low node storage requirements.

3) An analysis of the overall security of the distribution protection system demonstrates how the blockchain-inspired architecture meets various security requirements for measurement aggregation and control signaling.

4) An experimental performance evaluation demonstrates that the proposed holistic blockchain-based communication architecture can conclude to a promising solution for future smart grid protection systems.

The remainder of the paper is structured as follows. The proposed APP is described in Section II, while Section III discusses the blockchain-inspired APP communication architecture along with the specific design goals. A safety and security analysis of the holistic APP design is presented in Section IV. Finally, Section V presents the performance evaluation of the proposed mechanism, while Section VI concludes this work.

## II. Adaptive Smart Grid Protection Platform

The proposed APP is shown in Fig. 1. The APP is directed by the so-called APP management system (APPMS) that communicates to the Intelligent Electronic Devices (IEDs) through a communication hub. IEDs can include protection relays as well as DERs located on the distribution circuit. Through the communication hub, APPMS receives the latest circuit status and measurements, calculates, and sends the proper settings and commands to the IEDs located on its supervised region. The APPMS is envisioned to be implemented in the distribution feeder substation and is supervised by the distribution system operator (DSO). The APPMS consists of four main modules namely the adaptive circuit model management, the short circuit study, the protection coordination study, and setting calculation modules. The three latter modules build up an advanced protection analyzer (APA) that updates the settings of protection relays in real-time. Note that the APPMS is performing updates to the protection system and not providing the fault detection and location itself. This means that the communication requirements for speed, latencies, and update rates in the APPMS are more relaxed than for communication-assisted protection schemes. The APPMS modules include:

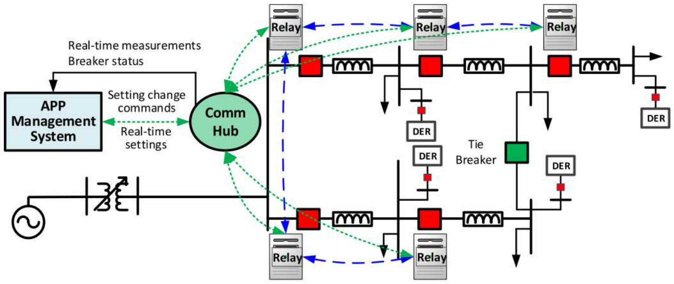

Fig. 1: Adaptive protection platform

*1) Adaptive Circuit Model Management:* This module carries the most updated power flow and short circuit model of the power system. Also, the most recent protection devices data including their status and settings are stored in this module. This module continuously monitors the received data and sends a flag to APA once a change (e.g., generation level of DERs or status of circuit and grid-tie breakers) is detected.

*2) Short Circuit Study Module:* The short circuit study module acts as the first stage in APA to provide the required short circuit analysis data for coordination studies and recommending new settings. This module incorporates different categories of short circuit studies including symmetrical and asymmetrical faults as well as high-impedance and open-conductor faults based on short circuit model received from adaptive circuit model management module. Short circuit study module utilizes an industry-approved short circuit simulation software package to simulate sequential faults and facilitate event-based fault analysis.

*3) Protection Coordination Study Module:* The purpose of the coordination study module is to identify potential relay miscoordinations given the latest status of the power system based on a set of pre-defined protection coordination rules. The most important rule is to ensure that there is a minimum acceptable time interval between the operating time of protection devices which is referred to as acceptable coordination time interval (CTI). The coordination studies will include system normal as well as N-1 contingencies and highlight the contingencies that violate the predefined acceptable CTI as coordination violations. The contingencies can consider the

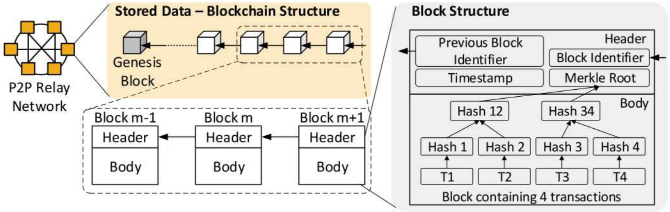

Fig. 2: Blockchain Data Structure

outage of neighboring branches, distribution transformers, and DERs.

*4) Setting Calculation Module:* This module uses the coordination study results to recommend new settings for the protection devices. Any flagged relay misoperation or CTI violation in the coordination study results is taken into consideration. This module identifies the misoperating protection devices and recommends new settings based on a set of predefined protection rules. These protection rules are electric power utility specific and determine the acceptable protection practices and setting ranges for the protection devices.

## III. Blockchain-based APP Network Architecture

### *A. Blockchain Preliminaries and Considerations*

Blockchain relies on a purely distributed and peer-to-peer (P2P) networking topology and can be described as a distributed and transparent public ledger (data structure) replicated and shared among the P2P network entities. Participating nodes, utilize a private public key encryption model to issue transactions (any data exchange) between them. Peer nodes verify the transaction signatures and data before appending them in records termed “blocks” that have specific capacity and consist of a header and a body. The block’s body stores the data transactions while the blockchain maintains blocks chronological order by cryptographically chaining them to their predecessors through the header. The blockchain’s first block is known as “genesis” block. Each block’s header contains its identifier, that is derived through a cryptographic hash of the included transactions, the previous block’s identifier, and a publish timestamp. In addition, the header includes a Merkle tree root that is created by hashing the included transactions’ IDs in pairs building a hash tree. Fig. 2 shows the structure of a blockchain P2P network’s components.

Newly created blocks are permanently added to the blockchain using an established set of rules termed distributed consensus protocol that ensures the agreement among the independent nodes of a common global blockchain-data state (transaction content, and order). A variety of distributed consensus algorithms has been proposed (highly active research topic) with diverse impact on the scalability and performance of Blockchain implementations [16]. At a higher level, depending on the specific application and consensus approach, blockchain systems can be either public (permissionless, e.g., Bitcoin) or private (permissioned). In public blockchains any node can take part in the network, issuing transactions, validating and publishing new blocks while maintaining a full copy of the ledger. They usually accommodate large number of nodes and utilize Proof-of-Work (PoW)-based consensus protocols where a miner node collects transactions into a block and only after successfully solves a computationally hard puzzle can append the block into the chain. The aim is to create an environment tolerant to pseudo identities, and malicious behaviour by making any tampering of block contents extremely costly. To the contrary, in private blockchains each node has to be authenticated and strictly identified. Since they admit tighter control on participants and synchronization, they utilize more conventional Byzantine Fault-Tolerant protocols and voting mechanisms to reach consensus without computationally expensive proofs [16].

Given the above, the incorporation of blockchain architectures into smart grid systems poses challenges. Their design and consensus protocol functionality that provides decentralization, and fault tolerance come at a cost on scalability, and achievable throughput. In addition, blockchain implementations that rely on puzzle solving are power consuming and require nodes with high computational capabilities. Finally, since the distributed ledger continuously grows with new entries, a single blockchain containing all relay nodes would consume more local storage space with poor scaling. Our proposed design aims to mitigate these challenges while considering the specific communication needs of grid protection systems where (a) geographically close or neighboring relays need to exchange measurements or settings, (b) measurements should be periodically reported to the substation, while (c) the latter can convey setting updates to the desired relays.

### *B. Modular APP Network Design and Operation*

For the considered protection system infrastructure, we will utilize a private blockchain logic which provides extra security through strict node authentication, higher transaction throughput, and the ability to utilize a computationally-light consensus mechanism. In addition, while all relay nodes maintain routing functionalities for transaction propagation and verification, our design utilizes nodes of two roles, namely “light-client” and “full-client”. Full-client relays maintain a complete and updated replica of the blockchain, are able to issue and verify transactions, and are able to publish new blocks changing the state of the chain. Relays acting as light-client spend less computational resources and retain locally only a copy of each block’s header. While they can issue and validate transactions (using the headers’ copy), they cannot add new blocks.

In addition, in order to improve the system’s scalability and efficiency, we adopt a tiered design where geographically close relays, acting as “full-clients”, form separate “sidechains” and select a “Leader” node responsible for adding new blocks to the internal ledger. These sidechains are part of a greater central blockchain, termed “mainchain” that connects them with substation nodes which act as “full-clients” of the mainchain keeping a full record of the data and operating as mining nodes. In order to reduce the storage requirements of the “Leader” nodes, they participate to the mainchain as “light-client” members. The use of sidechains enables relays to retain measurements only from neighbors locally, while avoiding val-

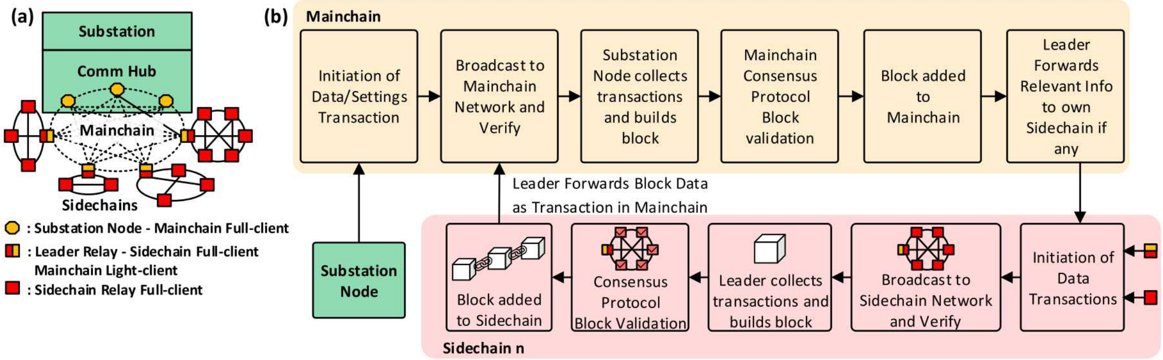
(a)
Substation
Comm Hub
Mainchain
Sidechains
●: Substation Node - Mainchain Full-client
▨: Leader Relay - Sidechain Full-client Mainchain Light-client
🟥: Sidechain Relay Full-client
(b)
Mainchain
Initiation of Data/Settings Transaction
Broadcast to Mainchain Network and Verify
Substation Node collects transactions and builds block
Mainchain Consensus Protocol Block validation
Block added to Mainchain
Leader Forwards Relevant Info to own Sidechain if any
Leader Forwards Block Data as Transaction in Mainchain
Substation Node
Block added to Sidechain
Consensus Protocol Block Validation
Leader collects transactions and builds block
Broadcast to Sidechain Network and Verify
Initiation of Data Transactions
Sidechain n

Fig. 3: Multi-tiered Blockchain-based APP Network: (a) Architecture, (b) Workflow Overview

idating transactions occurring on a totally different sidechain (i.e., physical location). The modular network architecture is depicted in Fig. 3-a. Through the mainchain, the substation is able to collect relay data and issue setting updates in the form of separate transactions towards the sidechain leader. The overall framework's workflow is shown in Fig. 3-b.

In what follows, we focus on the mechanisms that facilitate the data (same for measurements or settings) exchange and overall blockchain functionality in a singe chain:

*1) Relay measurements/settings exchange:* First, all relays and substation nodes in the tiered blockchain network are assigned a public and private key. Transmitting relay's measurements are initially encrypted using the receiver's public key. Following that, the transmitting relay creates a digital signature by using a secure hash algorithm (SHA) on the transaction data and encrypts the outcome to create a digital signature. The outgoing transaction of measurements/settings contains the encrypted payload and includes the digital signature on its header. The transaction is then broadcasted to the rest chain participants. For relay to substation communication the transaction is addressed initially to the sidechain Leader relay, that is in charge of forwarding the message to the mainchain once it is locally verified. The same logic is utilized for setting transactions initiated by the substation nodes. Leader relays retain and forward setting messages to relays inside their sidechain. In all cases, the receiving node begins verifying the contents by decrypting the digital signature using the issuer's public key before decrypting the transaction message data using its own private key. By hashing the received data and comparing the output with the hash inside the digital signature, the transaction is finally verified.

*2) Consensus and Block Generation:* Focusing on the framework's consensus, all participating chains utilize the classic Practical Byzantine Fault Tolerance (PBFT) algorithm [16] to achieve agreement among relays on the blockchain content. The process requires three stages, namely:

a) The pre-prepare phase where the chain Leader assembles transactions in a specific order into a block.

b) Next, during the prepare phase, the Leader broadcasts this block to the P2P network for validation. The block validating relays extract hashes of this block and rebroadcast them.

c) Finally, over multiple rounds the validating relays observe the hashes from the rest participants which are essentially votes for the candidate block's validity. During this final commit phase, relays wait until more than $2/3$ of the rest chain nodes are in favor of the block under consideration. When this happens the relays cryptographically add it to the blockchain copy as demonstrated in Section III.

Assuming a network of $N$ relays, the algorithm has a communication bound of $O(N^2)$ to achieve consensus in the condition of Byzantine failures, requiring $N \geq 3m+1$ relays to tolerate $m$ failing ones. Despite the voting overhead, PBFT consensus provides low latency, and achieves high throughput rates.

## IV. Security Considerations

*1) Authentication and Trust:* In our proposed model relay authentication is inherently preserved since a public-private signature scheme is utilized in the data exchange procedure. Man-in-the middle, and impersonator attacks can be easily detected by the relay upon transaction reception. Due to the decentralized nature of the framework, protection system nodes do not need to trust the substation (i.e., the centralized entity) to strictly handle their data. This prevents unauthorized third parties from accessing sensitive measurements if desirable.

*2) Integrity and Immutability:* There may be cases where a malicious attacker, after intercepting a transaction message, can challenge its integrity via falsifying measurements or setting commands. However, upon decryption on the receiving relay, the content verification will fail due to the disagreement between the hash of the modified data with the hash inside the sender's digital signature. In addition, the blockchain itself, as a distributed ledger containing all previous records of applied relay settings or aggregated measurements, is resistant to any kind of censorship or tampering attempt. More specifically, tampering a block's transaction in a compromised relay would produce different hashes in the Merkle tree's branch, leading to instantaneous detection. Also, altering the measurements or settings residing on a block would change its hash-based identifiers and therefore cause a domino effect on the cryptographic links between blocks. To avoid that an attacker has to (a) alter all the headers of the blocks that follow, and (b) make those alterations to at least 2/3 of the network relays to hijack the consensus process. Evidently, since both are highly demanding tasks from a computational and communication perspective, the smart grid protection system is shielded against false-data injection attacks or command manipulations [5].

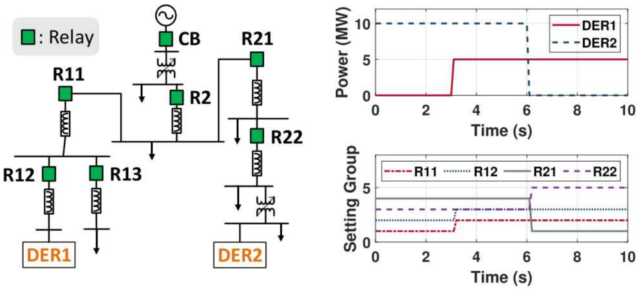

Fig. 4: (a) Simulated Power System and (b) APP Operation

*3) Fault Tolerance:* The utilized distributed consensus protocol introduces identification of Byzantine failures and achieves agreements between relays despite the possible existence of malicious behaviour of dishonest nodes. Also, all participating relays or substation nodes retain identical replicas of the shared chains. Thus, any node can identify measurement or setting leakages and mitigate them autonomously. Finally, the distributed nature of the ledger and its existence in multiple locations ensures resiliency in case of multiple relay malfunction, and rapid infrastructure recovery which is a crucial attribute of distribution and transmission protection systems.

*4) Impact and Consequences:* While intercepting protection relay measurements poses relatively minor privacy concerns, the major risks are impacts to the sensitivity (tripping when there is a fault) and selectivity (not tripping when there is not a fault) of the protection system. Modifying data flowing from the relays or settings communicated by the substation could decrease the protection system's dependability. For example, by clearing settings on the relays, fault may go undetected for long periods of time and damage equipment. On the other hand, forcing breakers to operate could cause blackout for sections of the system. It is also important that the APPMS only has access to the required settings in the relays to mitigate risks like malicious firmware updates.

Moreover, the addition and synchronization of new relays into the sidechain is easily facilitated, with each Leader being responsible for the relay's authentication as a legitimate, non-malicious participant. Finally, the underlying secure communication architecture enables the automatic and secure execution of protection system maintenance tasks with relay rekeying being a case in point. This can be a cost efficient alternative to the manual rekeying of thousands relays that includes labor costs and is prone to security holes, while blockchain-based dynamic key management is already considered as a viable solution for cyber-physical systems [17].

## V. Performance Evaluation

This section presents a numerical evaluation of the proposed solution in terms of overall communication efficiency. Our simulations consider a distribution circuit whose single line diagram is shown in Fig. 4-a. Each relay is simulated on a separate virtual node within our network hosted by machines with E5-1620 3,6 GHz CPUs, and 16 GB RAM. To closely imitate relay hardware specifications each node is assigned a single processor core with 2 GB RAM, running Ubuntu 18.04.

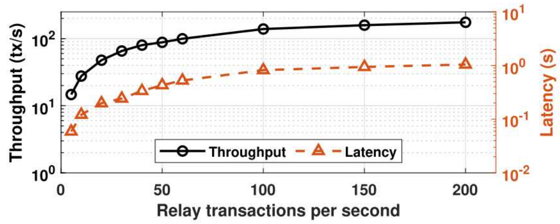

Fig. 5: Performance vs. increasing relay transaction rates

First, we demonstrate the functionality of the adaptive protection system with a sample simulation that focuses on adopting new setting groups for relays after the generation level of DERs are changing drastically. It is assumed that R11, R12, R21, and R22 are microprocessor relays with multiple predefined setting groups selected interchangeably through the adaptive protection system. Fig. 4-b (top) shows the real-time active power measurement of DERs that are sent to APPMS through the blockchain-based communication system. As seen, DER1 and DER2 generation change drastically at $t$ = 3 sec and $t$ = 6 sec, respectively. These changes are detected by the APPMS, and in response the APA (see Section II) chooses new setting groups for protection relays R11, R12, R21, and R22 to ensure protection system's coordination after the active power changes are satisfied. Impacted relay setting group changes are shown in Fig. 4-b (bottom).

Second, we focus on the communication framework and evaluate its performance in terms of transaction throughput, i.e., the number of transactions successfully included into a block and attached to the ledger per second, and latency, i.e., the elapsed time between a transaction generation and the confirmation reception (response time per transaction). Based on the power system of Fig. 4, our topology consists of two sidechains with four nodes, i.e., {R11, R12, R13, DER1}, and {R2, R21, R22, DER2}. For the blockchain simulation we deployed a modified version of the BLOCKBENCH tool [15], with a Hyperledger Fabric backend. Also, in order to imitate adjustable load generation by the relay clients, we will utilize the YCSB workload [18] which supports different ratios of read/write operations on the blockchain ledger.

In our experiments, the two sidechains operate simultaneously, and consist of three transaction issuers and the Leader. For the performance measurements we monitored their performance for 10 minutes, while each relay sends transactions with an increasing rate. Fig. 5 shows the achievable transaction throughput and latency as averaged for the elapsed 10 minutes and for the two sidechains as the request rate of each relay increases. As relays generate more messages per second, the Leader attempts to publish an increasing amount of blocks, creating extra network traffic due to the consensus protocol's voting mechanism. This saturates the throughput and increases latency for more demanding data exchange. However, this cost is countered by the inherent security characteristic that the blockchain architecture introduces to the protection system.

Next, we fix the transaction generation rate of each relay at 20 tx/sec and examine how the sidechain size impacts the system's performance. Fig. 6 shows the average throughput

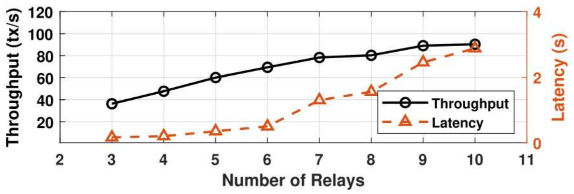

Fig. 6: Performance vs. increasing number of relays

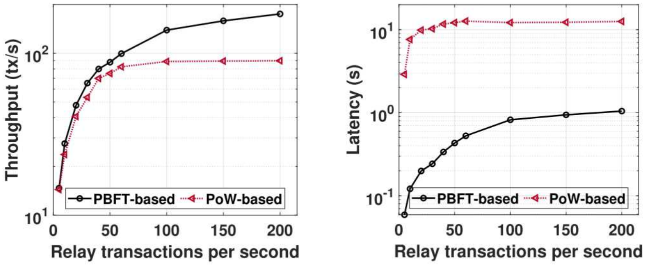

Fig. 7: PBFT vs. PoW Consensus: (a) Throughput, (b) Latency

and latency as the number of participating relays increases. Evidently, the increasing amount of local network resources needed to propagate transactions and blocks to more relays leads to scalability limitations in terms of performance for a single-tier blockchain. Since throughput and latency are significantly better when less nodes are involved, the modular architecture of our proposed solution allows for further partition of overpopulated relay installations to increase the overall system's communication efficiency.

Finally, we present a comparative evaluation of the impact of the consensus algorithms on our private blockchain relay network. For the aforementioned topology we tested a deployment based on Ethereum which utilizes a PoW-based consensus. Fig. 7 shows the comparison with our proposed system in terms of average achievable throughput and latency as each relay's transaction rate increases from 5 to 200 tx/sec. PBFT consensus outperforms PoW as the latter is computationally bound and block mining is more time consuming for the Leader with its difficulty being at 3 seconds per block [16]. In addition, over the 10 minute test period, the average CPU utilization of the virtual node was at 20% for the PBFT-based approach, and over 70% for the PoW one. Therefore, the use of the latter would put extra stress on the relay nodes, taking up resources from the circuit protective monitoring tasks.

## VI. Conclusions

In this paper, we outline an adaptive protection platform for modern smart grid infrastructures and design a blockchain-based communication framework to facilitate integrity, authenticity, and confidentiality of the exchanged data. The proposed solution counters the technology limitations in terms of achievable throughput and scalability, via the use of multi-tiered architecture that consists of relay sidechains interconnected with the substation through a central mainchain. The security characteristics of the resulting architecture are discussed and the framework was evaluated in terms of transaction throughput and latency on a blockchain testbed. Part of our future work aims for extension towards two directions: (a) Develop alternative consensus protocols for smart grid blockchains towards reducing the system's latency and (b) incorporate the proposed framework into a real-work protection relay network and use realistic data streams to test its performance and resilience against different cyber-physical attack scenarios.

## Acknowledgment

This work was supported by the National Science Foundation under the New Mexico SMART Grid Center - EPSCoR cooperative agreement Grant OIA-1757207. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

## References

[1] A. Ahmed *et al.*, "Cyber physical security analytics for anomalies in transmission protection systems," in *2018 IEEE Industry Applications Society Annual Meeting (IAS)*. IEEE, 2018, pp. 1–8.

[2] NERC Steering Group *et al.*, "Technical analysis of the august 14, 2003, blackout: What happened, why, and what did we learn," *report to the NERC Board of Trustees*, 2004.

[3] NERC, "State of reliability 2018 - nerc.com," 2018. [Online]. Available: https:www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_2018_SOR_06202018_Final.pdf

[4] V. K. Singh, A. Ozen, and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," in *2016 North American Power Symposium (NAPS)*. IEEE, 2016, pp. 1–6.

[5] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[6] H. F. Albinali and A. S. Meliopoulos, "Resilient protection system through centralized substation protection," *IEEE Transactions on Power Delivery*, vol. 33, no. 3, pp. 1418–1427, 2018.

[7] J. Seuss, M. J. Reno, R. J. Broderick, and S. Grijalva, "Determining the impact of steady-state pv fault current injections on distribution protection," *Sandia National Laboratories, SAND2017-4955*, 2017.

[8] M. N. Alam, "Adaptive protection coordination scheme using numerical directional overcurrent relays," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 64–73, Jan 2019.

[9] V. Venkataramanan *et al.*, "Enhancing microgrid resiliency against cyber vulnerabilities," in *2018 IEEE Industry Applications Society Annual Meeting (IAS)*. IEEE, 2018, pp. 1–8.

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[12] Z. Guan *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[13] J. Wan, J. Li, M. Imran, D. Li *et al.*, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, 2019.

[14] 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 Transactions on Smart Grid*, 2018.

[15] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[16] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu, and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv preprint arXiv:1805.02707*, 2018.

[17] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[18] B. F. Cooper, A. Silberstein, E. Tam, R. Ramakrishnan, and R. Sears, "Benchmarking cloud serving systems with ycsb," in *Proceedings of the 1st ACM symposium on Cloud computing*. ACM, 2010, pp. 143–154.