Blockchain Support For Time-Critical Self-Healing In Smart Distribution Grids

Befekadu G. Gebraselase*, Charles M. Adrah*, Tesfaye Amare†, Bjarne E. Helvik* and Poul E. Heegaard*
*Department of Information Security and Communication Technology,
NTNU, Norwegian University of Science and Technology, Trondheim, Norway
†Sintef Energy AS, Trondheim, Norway
Email: {befekadu.gebraselase, charles.adrah, tesfaye.zerihun, bjarne, poul.heegaard}@ntnu.no*/@sintef.no†

***Abstract*—Smart distribution grids have new protection concepts known as fault self-healing whereby Intelligent Electronic Devices (IEDs) can automatically reconfigure the power circuits to isolate faults and restore power to the relevant sections. This is typically implemented with IEDs exchanging IEC 61850 Generic Object Oriented Substation Event (GOOSE) messages in a peer-to-peer communication network. However, a self-healing application may be faced by challenges of emerging cyber-physical security threats. These can result in disruption to the applications' operations thereby affecting the power system reliability. Blockchain is one technology that has been deployed in several applications to offer security and bookkeeping. In this paper, we propose a novel concept using blockchain as a second-tier security mechanism to support time-critical self-healing operations in smart distribution grids. We show through a simulation study the impact of our proposed architecture when compared with a normal self healing architecture. The results show that our proposed architecture can achieve significant savings in time spent in no-power state by portions of the grid during cyber-physical attacks.**

***Index Terms*—Smart Distribution Grid, Cybersecurity, Blockchain, IEC 61850, Self-healing**

I. Introduction

The transition from the traditional power grid to the smart grid has enabled more reliable, efficient, and secure services [1]. The traditional grid enables a unidirectional power flow from generation plants to the consumers, whiles the smart grid enables electricity and information exchange in both directions as well as the integration of distributed energy resources (DERs) [2]. The IEC 61850 standard for power utility automation defines the communication between Intelligent Electronic Devices (IEDs) within a substation as well as wide-area protection and control application services [3].

The fifth generation mobile network (5G) is defined over three types of connected services known as Enhanced mobile broadband (eMBB), Massive Machine Type Communication (mMTC), and Ultra-reliable low latency communications (URLLC) [4]. 5G URLLC services will support time-critical operations such as remote surgery, emergency response, autonomous driving, and smart grid with strict latency (1ms) and reliability (99.999%) requirements [5]. Hence, a 5G URLLC solution will be deployed for Smart Distribution Grid (SDG) applications bringing benefits of guaranteed quality of service, as well as reducing capital and operational expenses.

One such application is fault self-healing in SDGs. Fault self-healing refers to automatic control measures to eliminate or isolate the fault and restore service using modern communication, computer, automatic control and power electronics technologies [6]. Self healing, also known as Fault Location, Isolation, and Service Restoration (FLISR) is a key SDG application which is implemented using peer-to-peer (P2P) IEC 61850 Generic Object Oriented Substation Event (GOOSE) communication. FLISR enables utilities to significantly reduce outage time to the end customers and improve their distribution network reliability.

When GOOSE messages are used in such self-healing applications, communication between the IEDs is usually not encrypted due to performance reasons since the messages are time-critical [7]. This makes the information exchange between participating IEDs susceptible to man-in-the-middle attacks, denial-of-service (DoS), and repeat messages attacks [8]. Moreover, self-healing applications can involve multi-actors of producers, consumers and prosumers in the grid which may bring the challenge of trusting the information exchanges among the IEDs from these actors. Furthermore, there is no specification on how the messages exchanged between actors can be stored as immutable records and to be used in future investigations.

In this paper we propose a GOOSE and 5G based self-healing architecture utilizing blockchain to address the challenges of security and immutability of records. Our architecture uses blockchain as a second-tier security layer to validate time-critical messages in a smart grid FLISR application. As a second-tier security layer, our blockchain architecture does not affect the time-critical GOOSE message exchanges but can reverse actions of these time-critical messages when they are invalidated at some future time. The architecture also provides a secure decentralized bookkeeping that can be used to probe and track both internal and external actor activities.

The rest of the paper is organized as follows: Section II presents our proposed blockchain second-tier security archi-

This paper has been funded by Prodig - Power system protection and control in digital substations, (under KPN-project ENERGIX, 295034/E20), and CINELDI - Centre for intelligent electricity distribution, an 8 year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway, and the other partners of Prodig and CINELDI.

978-1-6654-8032-1/22/$31.00 © 2022 IEEE

tecture for a self-healing application. In section III, we explain how blockchain information is organized and distributed in our architecture. In Section IV, we present a simulation evaluation of the proposed architecture. Finally, we give concluding remarks in Section V.

II. Blockchain-Based Second-Tier Security Architecture

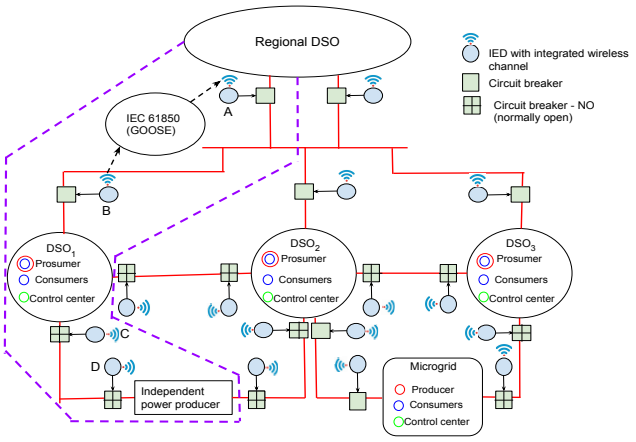

Fig. 1. Self-healing in a smart distribution grid

A. Smart Grid Use Case

Figure 1 presents a self-healing application in an SDG topology consisting of a Regional Distribution System Operator ($R-DSO$), three Distribution System Operators (DSO_1, DSO_2 and DSO_3), an Independent Power Producer (IPP) from a distributed energy resource, and a micro-grid. We assume the DSOs are independent with their own administrative domains. The IPP can be connected to DSO_1 or DSO_2 while the microgrid can be connected to the main grid through DSO_2 or DSO_3. All the feeder lines have circuit breakers and IEDs. The IEDs serve as control units for the circuit breakers in the feeder lines and are mainly used to localize fault outages.

The self-healing activities entail Fast fault clearing, Locate the fault, Isolation, Selectivity and Reconfiguration (FLISR). The IEDs use P2P communication to exchange GOOSE messages with the self-healing logic residing in the IED. FLISR operates autonomously without the need of a control centre. However, all actions taken during a self-healing carried out will be communicated immediately to the control centre which can be located at the $R-DSO$, to keep the grid operation status up-to-date.

B. Architecture

Figure 2 shows the proposed architecture which combines the FLISR application and blockchain over a 5G communication system. 5G is introduced to provide the P2P communication mechanism among the interacting IEDs as well as to the control center. This can be realized by a virtual bus in 5G edge cloud. In this work, we considered that URLLC provides the network communication service. As such, the time-critical low latency requirement is guaranteed according to URLLC specifications [9]. We also assume a network slice that provides the URLLC service for the application traffic.

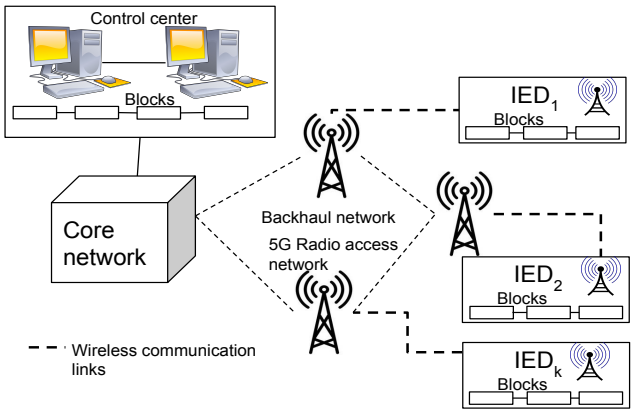

Fig. 2. Blockchain-based second-tier security architecture in self-healing smart distribution grid

In our proposal, the FLISR system still operates to autonomously isolate and restore faults as previously explained. However, whenever an event occurs such as a GOOSE message is published or is received by a subscribing IED, an independent corresponding blockchain transaction is also generated and broadcasted to the other IEDs in the network. This generated transaction propagates to a full node or miner to be validated or invalidated.

If an IED validates the transaction, it adds the transaction to its' valid log file. The self-healing action taken based on the GOOSE message from that now validated transaction is kept and maintained as true. Subsequently new blocks may be created from the valid transactions and added to the ledger for bookkeeping purposes. On the other hand, if an IED invalidates the transaction received, the self-healing action taken based on the GOOSE message from the invalidated transaction will then be discarded or reversed. The invalid transaction will be added and stored to its invalid log file.

The blockchain communication will run over the URLLC network slice, which will make the transaction propagation delays smaller than running on traditional networks. The block generation intensity depends on the event that leads to self-healing handling. The IED node generates a block of valid transactions inside when self-healing handling happens. Nevertheless, the block generation intensity can be adjusted to keep the bookkeeping with the GOOSE message delay requirement. When the IEDs create a block, they add transactions from the backlog to the block and push it to the neighbor nodes. We assume the IEDs to have computation and storage capacity to run blockchain nodes.

The block generation depends on the type of consensus protocol used. In this work, we consider Practical Byzantine Fault Tolerance (PBFT) which is a computationally-light consensus mechanism compared to other consensus protocols such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) [10, 11]. CPU utilization of a node using PBFT was 20% and over 70% using

PoW [10]. In addition, PBFT can process more transactions in the order of 1000 transactions per second compared to PoW (2 transactions per second) and PoS (50 transactions per second) [10].

C. Interactions between self-healing and blockchain events

In this section, we demonstrate through sequence activities, the interactions between the self-healing events and the blockchain events in normal operation and when there is a malicious attack. We illustrate this using a simplified self-healing application involving $\mathtt{R-DSO}$, $\mathtt{DSO_1}$ and an IPP in Figure 1 (i.e., section is framed by violet line)

In the normal operation, $\mathtt{DSO_1}$ is fed power from the $\mathtt{R-DSO}$ (i.e., circuit breakers, $\mathtt{CB_A}$ and $\mathtt{CB_B}$ are closed). When a fault occurs on the feeder line between $\mathtt{R-DSO} \leftrightarrow \mathtt{DSO_1}$, the $\mathtt{IED_A}$ and $\mathtt{IED_B}$ communicate the event change (i.e., by publishing GOOSE messages) to $\mathtt{IED_C}$ and $\mathtt{IED_D}$. $\mathtt{CB_A}$ and $\mathtt{CB_B}$ become opened whiles $\mathtt{CB_C}$ and $\mathtt{CB_D}$ which are normally open will then close to allow power to be fed from the IPP. When the fault is cleared between $\mathtt{R-DSO} \leftrightarrow \mathtt{DSO_1}$, the event change is again communicated to $\mathtt{IED_C}$ and $\mathtt{IED_D}$ which then open $\mathtt{CB_C}$ and $\mathtt{CB_D}$. $\mathtt{CB_A}$ and $\mathtt{CB_B}$ also close and power feed is restored to $\mathtt{DSO_1}$ from the $\mathtt{R-DSO}$, as in the normal operation.

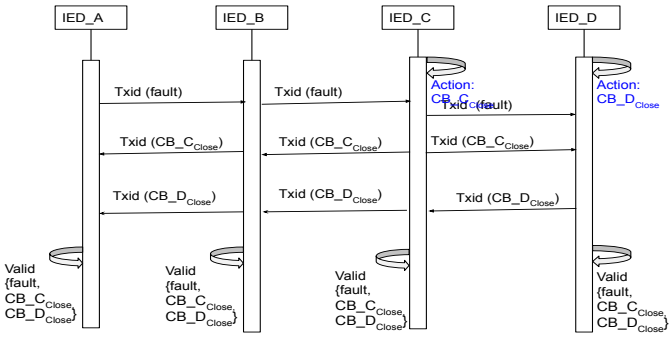

Fig. 3. Blockchain activity sequence for self-healing in normal operation

The activity sequence of self-healing with blockchain process is shown in Figure 3. At the instance when a fault occurs and $\mathtt{IED_A}$ and $\mathtt{IED_B}$ publish $\mathtt{GOOSE_{fault}}$ messages, blockchain transactions are also generated by $\mathtt{IED_A}$ and $\mathtt{IED_B}$. These transactions, named $\mathtt{Txid(GOOSE_{fault})}$, are broadcasted to all other IEDs to be validated. $\mathtt{IED_C}$ and $\mathtt{IED_C}$, will execute an action (.i.e, close $\mathtt{CB_C}$ and $\mathtt{CB_D}$), and will also at this instant generate blockchain transactions $\mathtt{Txid(CB-C_{Close})}$ and $\mathtt{Txid(CB-D_{Close})}$. Both transactions will reach all other IEDs in the network and be validated. The transactions having been validated as true will necessitate no further actions at this point. Note that similarly, the actions $\mathtt{CB-A_{Open}}$ and $\mathtt{CB-B_{Open}}$ can also generate blockchain transactions that can be independently validated.

In Figure 4, we show an activity sequence of self healing with blockchain process under malicious attack. Here, the $\mathtt{GOOSE_{fault}}$ message is published into the network from $\mathtt{IED_X}$, a malicious user that tries to compromise the information exchanges between the other IEDs. However, $\mathtt{IED_X}$ is not part of the blockchain network since unknown nodes can not join the private network without approval by the other nodes. $\mathtt{IED_C}$ and $\mathtt{IED_D}$ being subscribers to this message will immediately execute actions of closing their normally open circuit breakers (i.e., $\mathtt{CB-C_{Close}}$, $\mathtt{CB-D_{Close}}$) and also generate blockchain transactions based on the actions taken. $\mathtt{Txid(CB-C_{Close})}$ and $\mathtt{Txid(CB-D_{Close})}$ are broadcasted to be received by all other IEDs. These transactions will go through the validation process. $\mathtt{IED_C}$ and $\mathtt{IED_D}$ will invalidate these transactions, as will all other legitimate IEDs in the network. At this time, the previous actions executed by $\mathtt{IED_C}$ and $\mathtt{IED_D}$, $\mathtt{CB-C_{Close}}$ and $\mathtt{CB-D_{Close}}$, will be reversed based on the invalidated transactions.

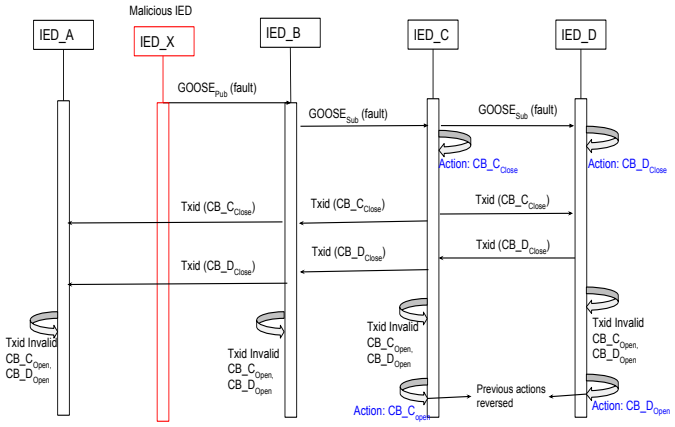

Fig. 4. Blockchain activity sequence for self-healing under malicious attack

III. Blockchain Information Organization in the Proposed Architecture

This section presents how blockchain collects transaction information from the GOOSE messages, organizes and stores this information, distributes the new updates to the neighbor devices, and generates a report for further investigation.

A. Acquire transaction information

GOOSE is usually sent as Layer 2 multicast and hence used within the substation (i.e., intra-substation). GOOSE can be routed into the wide area network using layer 2 tunneling or transport over layer-3 routers with UDP/IP headers [12]. Figure 5 shows a typical GOOSE packet frame. The variable portions is contained in the Application layer. The GOOSE Application Protocol Data Unit (APDU) has 12 unique fields that is used to organize its message.

When a change of event occurs and an IED publishes a GOOSE message, some fields (`gocbRef`, `goId`, `t`, `stNum`, `confRev`, `allDaTA`) in the GOOSE APDU can be changed into transaction inputs. A generated transaction by the IED will then contain these inputs together with either the Media Access Control (MAC) or Internet Protocol (IP) source and destination addresses for record keeping.

GOOSE messages are published spontaneously into the network when an event change occurs or periodically to repeat

```
Frame 1: 165 bytes on wire (1320 bits), 165 bytes captured (1320
bits)
Ethernet II, Src: SuperMic_3d:2e:9f (00:25:90:3d:2e:9f), Dst: Iec-
Tc57_01:28:50 (01:0c:cd:01:28:50)
GOOSE
   APPID: 0x0001 (1)
   Length: 151
   Reserved 1: 0x0000 (0)
   Reserved 2: 0x0000 (0)
goosePdu
    gocbRef: SERVER-GOOSELDevice1/LLN0$GO$CB_Goose_TRIP1
    timeAllowedtoLive (msec): 1000
    datSet: SERVER-GOOSELDevice1/LLN0$Goose_TRIP1
    goID: Goose_TRIP1
    t: May 13, 2016 13:30:28.228710949 UTC
    stNum: 2
    sqNum: 0
    test: False
    ConfRev: 1
    ndsCom: FALSE
    NumDataSetEntries: 2
allData
    bitString: BITS 0000-0015: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
    boolean:  TRUE
```

Fig. 5. GOOSE packet after event

the same event state. However, to reduce the number of transactions generated by an IED, only transaction generation from specific events leading to self-healing action need to be added to the blockchain. The corresponding blockchain transaction input, which we call Txid(GOOSE), that can be generated is shown in Figure 6.

```
Goose_to_Transaction
{
    "Txid": "2fef4b992c1f88e33b43647b98fccda8f5cc670exxxxx",
    "Src":  "SuperMic_3d:2e:9f (00:25:90:3d:2e:9f)",
    "Dst":   "Iec-Tc57_01:28:50 (01:0c:cd:01:28:50)",
    "size": 165,
    "gocbRef": SERVER-GOOSELDevice1/LLN0$GO$CB_Goose_TRIP1,
    "goID": Goose_TRIP1,
    "t": May 13, 2016 13:30:28.228710949 UTC,
    "stNum": 2,
    "ConfRev": 1,
    "allData": 0000-0015: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0,TRUE
}
```

Fig. 6. Txid(GOOSE): a GOOSE packet translated into blockchain transaction

B. Organize, store and distribute transaction information

Each IED acts as an independent blockchain node that participates in adding and validating a block. A GOOSE message with an event change published into the network by an IED (i.e., GOOSE(Pub)), will instantly generate a new Txid(GOOSE) transaction into the network. Similarly, an IED that receives a subscribed GOOSE message (i.e., GOOSE(Sub)), and executes an action will also generate a new transaction, Txid(Action) into the network.

When new transactions arrive at an IED, the IED validates and then stores the new arrivals at a backlog until block creation occurs. At the same time, the IED also maintains an internal reference or mapping between the GOOSE message it has either published or subscribed to, and the transactions generated. GOOSE(Pub) $\leftrightarrow$ Txid(GOOSE) and GOOSE(Pub) $\leftrightarrow$ Txid(Action)). Hence, it is possible to reverse actions when transactions have been invalidated. Figure 7 shows the internal mapping in an IED between GOOSE frames (published/subscribed) and transactions generated which are stored in the backlog as valid or invalid.

The blocks are connected through cryptographic hash and stored according to a timestamp creation and confirmation order. This makes it easier to extract relevant information at any point in the network. Both GOOSE and blockchain rely on broadcast communications to publish or propagate the latest event updates, hence the subscribing or participating entities receive the new updates autonomously.

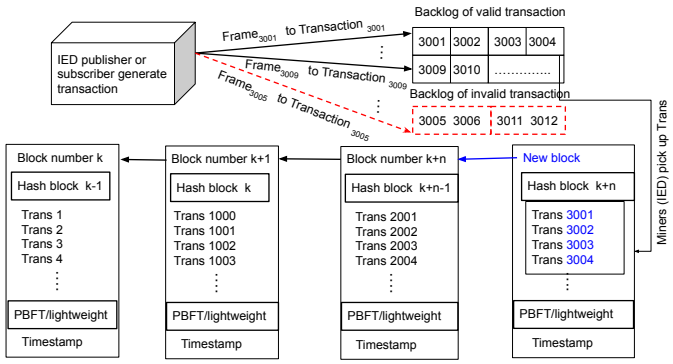

Fig. 7. Mapping in IED for GOOSE frames and blockchain transactions

IV. Simulation Study

In this section, we carry out a simulation study of the proposed architecture. The architecture is modeled with Stochastic activity network (SAN) models using the Möbius tool [13]. SAN is a general and modular stochastic modelling formalism, which is built from atomic block models. We use the simplified self-healing application in Figure 1 in our simulation study.

A. Model

We develop three atomic models consisting of the power system network, 5G communication system, and the blockchain transactions process. Firstly, a model is developed for the power system network made up of R − DSO, DSO_1, IPP, two feeder lines and the four circuit breakers. Secondly, a model is also developed for the 5G based communication of the four IEDs. Finally, a model is developed for the blockchain transactions in the network. The overall system is modelled by connecting the atomic sub-models using the Join formalism in Möbius. The reward model functionality in Möbius is used to collect statistics of interest. We describe below a summary of the atomic models used in our simulation study:

1) Power system: Figure 8 shows the atomic model for the power system network of the self-healing application. It has 6 places. Power_line_Ok represents the initial state of feeder 1 while feeder 2 has initial No_Power state. Bother feeder lines can be in Power_line_Failed state. The Breaker place represents the state of the 4 circuit breakers. The Customer_OK and Customer_No_power states represent the power supply states for DSO_1.

2) Communication model: Figure 9 shows the atomic model of the communication between the four IEDs in the network. The communication is based on IEC61850 publisher-subscriber multicast mechanism whereby IEDs publish a change of state of their breaker state (i.e., failed or OK) to the other IEDs (e.g., Goose_A_broadcast). An IED receiving GOOSE messages will initiate a self healing activity to execute

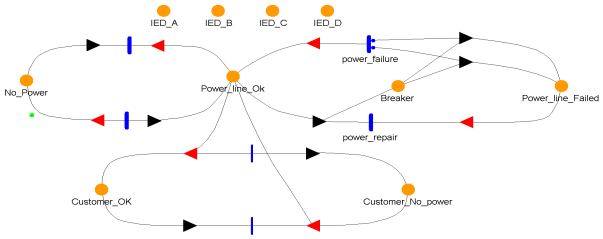

Fig. 8. Power system atomic model

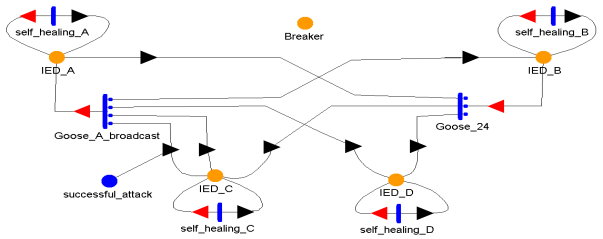

Fig. 9. 5G communication atomic model

a predefined action on its breaker (e.g., `self_healing_C`). In addition, the atomic model shows a scenario whereby there is a man-in-the-middle cyber attack on the communication between `IED_A` and `IED_C` with a probability of success. In a successful attack, the communication of a failed breaker state (e.g., breaker status = open) from `IED_A` is altered to an OK state (breaker status = closed).

3) Blockchain model: The atomic model of the blockchain transactions process is shown in Figure 10. The IEDs with blockchain nodes form an overlay network topology, in which we assume nodes forming a ring topology. If a feeder line fails and the breaker state changes to open, an IED publishes GOOSE messages to the other IEDs in the network and at the same time generates a blockchain transaction corresponding to the GOOSE message. This transaction propagates to the other IEDs in the network with each receiving IED validating the new arrival. The validation requires arrival of the blockchain transactions from all IEDs connected to the IED. Once the transactions are validated, a corrective actions (i.e., `self_healing_A`) will be executed on the IED if the validated state is different from the initial state received from the GOOSE multicast message. Block generation process is an independent process that was not considered in this atomic model. This is because block generation events do not affect the overall performance of our study model. It is a process that collects valid transactions into a block and pushes the new block to the neighbor nodes for bookkeeping.

TABLE I
DELAY / SERVICE TIME

Component	Circuit breaker	IED	Communication (5G)	Blockchain transactions
Delay / Service time [msec]	1000	10	10	1000

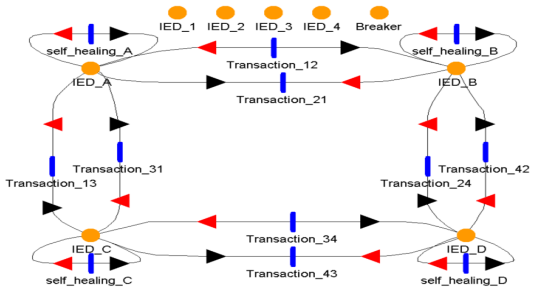

Fig. 10. Blockchain transactions interaction process atomic model

B. Case Study

In the case study, we evaluate the downtime and unavailability of power supply to $\texttt{DSO}_1$ in a normal self-healing architecture and the proposed blockchain self-healing architecture. We study the impact of cyber attacks on the 5G-based communication between the IEDs by modeling a man-in-the-middle attack between `IED_A` and `IED_C`. We conduct a sensitivity measure of cyber attacks with varying attack probability of success and its impact on the $\texttt{DSO}_1$ power unavailability.

The delay and service times assumed for the circuit breaker, IEDs, 5G communication and blockchain transactions are shown in Table I while the failure rates and repair time for the feeder lines are shown in Table II.

TABLE II
FAILURE AND REPAIR RATES

Component	Failure rate [/year]	Repair rate [hours]
Feeder lines	0.01	4

C. Results

1) The impact of attack success probability: Figure 11 shows the downtime and unavailability experienced by $\texttt{DSO}_1$ with increasing probability of successful attack for the normal self healing architecture and the proposed self-healing with blochchain support. The x-axis represents the probability of successful attack, p, and the y-axis indicates the down time in seconds per year, t_U. As can be observed from the figure, self healing with blockchain support has a significant reduction in the downtime on $\texttt{DSO}_1$ compared to the normal self healing operation. Furthermore it is observed for both architectures, the downtimes increase with increasing attack probability. For the normal self healing architecture, With probability $p = 0.1$, the downtime of $\texttt{DSO}_1$ is $t_D = 2676.39$ [seconds/year] (44.6 minutes/year) for normal architecture while downtime $t_D = 4.8$ [seconds/year] with blockchain support architecture. With probability of successful attack increased to $p = 0.8$, the downtime for $\texttt{DSO}_1$ is $t_D = 20659.2$ [seconds/year] (344.3 minutes/year) for normal architecture while downtime 8.6 seconds/year with blockchain support architecture.

For the normal self healing, when there is a successful attack on the communication between `IED_A` and `IED_C`, IPP can not

supply power to $\mathtt{DSO}_1$. Hence, $\mathtt{DSO}_1$ remains in a no power state until the feeder 1 ($\mathtt{R-DSO} \leftrightarrow \mathtt{DSO}_1$) is repaired. On the other hand, with our proposed architecture, the blockchain transactions act as second-tier security mechanism which enable the actions of a successful attack between IED_A and IED_C to be reversed. Hence, $\mathtt{DSO}_1$ will remain in no power state for sometime until the blockchain transactions invalidate the successful attack actions. Power is restored to $\mathtt{DSO}_1$ with feeder 2 ($\mathtt{DSO}_1 \leftrightarrow$ IPP). We assume here that the blockchain transaction processing time per IED is 1 second.

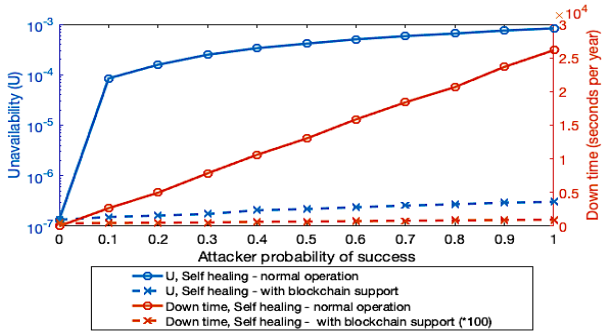

Fig. 11. Downtime and unavailability of $\mathtt{DSO}_1$ for normal self healing architecture and proposed self healing architecture with blockchain support

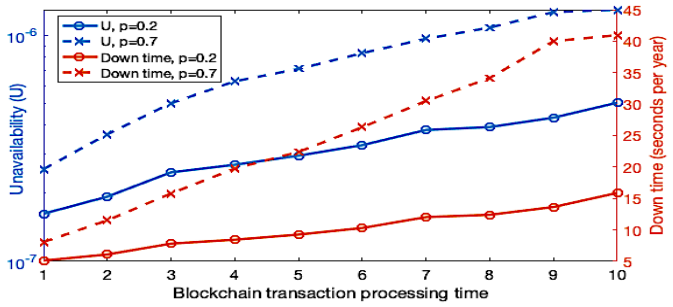

Fig. 12. Downtime and unavailability of $\mathtt{DSO}_1$ for proposed self healing architecture with blockchain support considering varying blockchain transaction processing time per IED

2) Effect of blockchain transactions processing time: Figure 12 shows the downtime and unavailability observed at $\mathtt{DSO}_1$ when we consider different blockchain transaction processing times per IED for our proposed architecture. We evaluate based on two attack probabilities. It was observed that for all values of blockchain transaction processing time considered, the downtime was higher for probability of successful attack, $p = 0.7$ compared to $p = 0.2$. The downtime increases linearly with the transaction processing time, t_p, while the unavailability (U, increases exponentially (note the log-scale on the axis).

In the cases evaluated, even though the downtime increases due to increasing blockchain processing times, the blockchain support architecture still achieves a much larger savings in the downtime observed as compared to the normal operation with a 4 hour feeder repair time.

V. Conclusion and Future Work

Self healing applications among distributed entities such as DSOs, microgrids and IPP having their own administrative domains require building trust between the participating units. However, due to the time-critical nature required in self-healing operations, there is the challenge of security mechanisms to deploy in order not to affect speed of operations. This paper has proposed an architecture based on blockchain as a second-tier security layer to validate the time critical messages in a self-healing application. The architecture provides security for the real-time application in that actions may be reversed after invalid transactions are detected, while the ledger maintains the bookkeeping. A simulation study was conducted and it was shown that our architecture results in less downtime (no power state) for the DSO considered when compared to a normal self healing.

The proposed architecture can address the impact of cyber-physical security for real-time self-healing in the SDG thereby increasing the grid immunity towards cyber-physical attacks. In the future work, we plan to further study the impact of blockchain in providing support for self-healing operations.

References

[1] Jinju Zhou et al. "What's the difference between traditional power grid and smart grid? — From dispatching perspective". In: *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*. 2013, pp. 1–6.

[2] Pratik Kalkal and Vijay Kumar Garg. "Transition from conventional to modern grids: Modern grid include microgrid and smartgrid". In: *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*. 2017, pp. 223–228.

[3] IEC. *IEC standard for communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations*. Tech. rep. IEC, 2010.

[4] Petar Popovski et al. "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View". In: *IEEE Access* 6 (2018), pp. 55765–55779.

[5] Haiyu Ding et al. "Use Cases and Practical System Design for URLLC from Operation Perspective". In: *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2019, pp. 1–6.

[6] Tianyou Li and Bingyin Xu. "The self-healing technologies of smart distribution grid". In: *CICED 2010 Proceedings*. 2010, pp. 1–6.

[7] IEC 62351. "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850". In: (2020).

[8] Juan Hoyos, Mark Dehus, and Timthy X Brown. "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure". In: *2012 IEEE Globecom Workshops*. 2012, pp. 1508–1513.

[9] Liang Zhu et al. "Priority-Based uRLLC Uplink Resource Scheduling for Smart Grid Neighborhood Area Network". In: *2019 IEEE International Conference on Energy Internet (ICEI)*. 2019, pp. 510–515.

[10] Dimitrios Sikeridis et al. "A blockchain-based mechanism for secure data exchange in smart grid protection systems". In: *2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*. 2020, pp. 1–6.

[11] Yaqin Wu and Fuxin Song Wang. "Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain". In: Apr. 2020, pp. 18–23.

[12] IEC. "IEC standard for communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasors information according to IEEE C37.118 IEC 61850-90-5 TR Ed 1.0. Technical report". In: (2012).

[13] Shravan Gaonkar et al. "Performance and Dependability Modeling with Möbius". In: *ACM SIGMETRICS Performance Evaluation Review* 36 (Mar. 2009), pp. 16–21. DOI: 10.1145/1530873.1530878.