IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 7, 2018, accepted February 6, 2018, date of publication February 27, 2018, date of current version March 15, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2806303

GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid

JIANBIN GAO[1], KWAME OMONO ASAMOAH[2], EMMANUEL BOATENG SIFAH[2], ABLA SMAHI[2], QI XIA[3], HU XIA[2,4], XIAOSONG ZHANG[3], AND GUISHAN DONG[2,5]

[1]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[3]Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu 611731, China
[4]Youe Data Co. Ltd., Beijing 100071, China
[5]National Engineering Laboratory for Big Data Application on Improving Government Governance Capabilities, Guiyang 530000, China

Corresponding author: Qi Xia (xiaqi@uestc.edu.cn)

This work was supported in part by the applied basic research programs of Sichuan Province under Grant 2015JY0043, in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2015J154, Grant ZYGX2016J152, and Grant ZYGX2016J170, in part by the programs of International Science and Technology Cooperation and Exchange of Sichuan Province under Grant 2017HH0028, in part by the Key Research and Development Projects of High and New Technology Development and Industrialization of Sichuan Province under Grant 2017GZ0007, in part by the National Key Research and Development Program of China under Grant 2016QY04WW0802, Grant 2016QY04W0800, and Grant 2016QY04WW0803, and in part by the National Engineering Laboratory for Big data application on improving government governance capabilities.

ABSTRACT Electricity is the commonest commodity for most businesses in our world today. The use of electricity has been a breakthrough for the discovery of new technologies and has become the main driving force behind several innovations. With the introduction of smart grid systems, there have been improvements in how utility companies interact with their customers with regards to electricity use. However, since the readings are done via the Internet, there is the tendency for the data to be compromised when it gets into the hands of the wrong people. Moreover, customers mostly do not know why they pay huge amounts and which appliances use more electricity, since they are not privy to the readings. The sovereign blockchain technology, which provides transparency and provenance, is utilized in this paper to mitigate these above mentioned problems. A smart contract, which executes laid down procedures to provide a trust-based system between participants on the network is also implemented. Our system proves very efficient as the user can monitor how the electricity is used, and it also provides a platform where there is no manipulation from either party.

INDEX TERMS Sovereign blockchain, smart meter, smart grid network, electricity, event.

I. INTRODUCTION

In modern times, the use of electricity is perceived to be the critical underpinning component that enables the discovery or development of new technologies [1]. Electricity as a commodity has become the main driver of technology and without it, most technologies are limited or unusable [2], [3]. Its use has spawned and supported technologies in several spheres of human activity. Transportation, communication, computing, etc. are areas where electricity has enabled several innovations [4]–[6]. Its portability and subsequent commonplace usage attract the interest of several research institutions to look into various means that can better support its efficient distribution and monitoring of use. The smart grid is one result of such interests [7].

Smart grid as a technology introduces a two-way communication between utility companies and their customers and enables better integration of newer energy generation technologies such as wind and solar energy supporting the growing plug-in charging of electric vehicle [8]–[10]. The smart home communicates with the smart grid by logging and sending data to the smart grid through a smart meter and thus enables consumers to better manage their electricity consumption [11]–[13]. By measuring a homes electricity usage levels more efficiently through a smart meter, utility companies can provide their customers with better information to manage and inform how much they pay for the service.

In a smart grid system, electrical data recorded from the smart home onto the grid system is done on real-time basis through the internet and is processed and stored in databases for billing the consumers and also for research purposes by various research institutions [14]–[16]. The data which is recorded and transferred to the smart grid system via the

internet can be compromised when it falls into the hands of malicious actors. The compromise of such data often leads to situations where the consumer is required or induced to pay amounts not commensurate with the service received at the end of the billing period, usually month. This may result in overpaying by the customer or loss of revenue by the utility company. In addition to the problem stated above, details of billing are not revealed to consumers so they don't know which electrical appliances consume more power, a knowledge which can inform consumers behavior and optimize the use of such appliances to lower costs [17].

Several methods have been proposed to address the problems arising from the use of smart grids in the past years. Gngr *et al.* [18] pointed out the problems with todays power distribution systems. A lack of automated analysis, poor visibility, mechanical switches causing slow response times, lack of situational awareness etc. were some of the deficiencies they found with current power distribution systems. They went further to suggest the smart grid as a solution to address these problems. The various communication technologies associated with the smart grid were also spelled out. These include ZigBee, wireless mesh, cellular network communication, powerline communication and digital subscriber lines. Also, the various requirements and standards of smart grid were elaborated.

Rusitschka *et al.* [19] proposed a cloud computing model for managing the real-time streams of smart grid data. Their model is a platform for the collaboration and information exchange between users, retailers, virtual power plant operators of highly distributed generation as well as network operators. Their emphasis was on the specific features associated with cloud computing that lead to an internet-scale platform which can facilitate the data-intensive needs of the smart grid.

Metke and Ekl [20] proposed security technology for smart grid networks based on public key infrastructure technologies (PKI) which binds public keys with user identities through the use of digital certificates. They proposed the development of PKI standards for use by critical infrastructure industry and these standards are to be used to establish requirements on PKI operations of energy service providers.

Mylrea and Gourisetti [21] proposed blockchain for smart grid resilience. This is a model that uses blockchain and smart contracts as intermediaries between electricity consumers and electricity producers to help cut down cost, increase the speed of transactions and also strengthen the security of the transaction data generated. In their model, whenever a transaction takes place, there is a blockchain-based meter that updates the blockchain by creating a unique timestamp block for verification in a distributed ledger. At the distribution level, system operators charge the customers based on the data recorded on the blockchain.

In order to allow utility companies have maximum security control over the data that are generated and to let the Internet Communication (ICT) framework handle more clients, Ye *et al.* [22] proposed an identity-based (ID based) security scheme. The core of this scheme is an ID-based syncryption (IBSC) scheme. This scheme performs the functions of digital signature and encryption simultaneously. Their scheme makes use of public key cryptography and is computed based on the ID of each client together with a given time after which computation of the public key is not permissible by the system.

Nonetheless, the sovereign blockchain can be seen as a technology that can provide a suitable remedy in addressing the problems stated previously through its attractive characteristics of immutability, non-repudiation and decentralization [23]–[25]. In this paper, we propose a sovereign blockchain-based solution coupled with smart contracts for creating a tamper-proof system for protecting consumer data recorded and transferred onto the smart grid system. The sovereign blockchain will be used to create an immutable data structure where data recorded and transferred onto the system cannot be altered. The smart contract will be used to set the rules between consumers and utility companies and thereby introduce algorithmic enforcement of contract terms in case any entity is found culpable of foul play.

II. PRELIMININARIES

In this section, we explain the preliminaries employed in our secure sovereign blockchain-based monitoring on smart grid. We describe the sovereign blockchain network with side blocks as individual components and we also give a brief layout of the supposed cryptographic behavior needed in the system. It should be noted that the smart grid network and the sovereign blockchain network refers to the same structure and are therefore used interchangeably.

A. SOVEREIGN BLOCKCHAIN NETWORK

The sovereign blockchain is a distributed database that contains an ordered list of records linked together through chains on blocks [26], [27]. The blocks on the chain can be defined as individual components that contain information pertaining to a specific transaction. A typical example of this information can be logs on a single event. A sovereign blockchain network maintains an ever growing list of records which cannot be changed [28]–[30]. This allows systems built on sovereign blockchain technology to achieve secure distribution of assets among mutually distrustful entities.

In our secure sovereign blockchain-based monitoring on smart grid, the processing and consensus nodes are entirely responsible for processing events into blocks and broadcasting blocks into the sovereign blockchain network. Forms are generated by the processing and consensus nodes pertaining to any event that is transferred onto the sovereign blockchain network and are developed into blocks and later broadcast on the sovereign blockchain network. The above action gives the completion of a block and allows the broadcast of the block into the sovereign blockchain network. There are multiple threads of blockchain in the network, with each identified uniquely using a consumers identity. Threading side blocks to their parent blocks are used to maintain a contiguous log

of well-ordered logs developed from requests by different consumers.

Structuring the network this way enables us to point to the fact that each block in a particular string represents different instances of events that have occurred. These are indexed and updated by the smart contracts in a particular child-block appended to the parent block as a side block. The significance of implementing side blocks is to keep an effective log and efficient fetching of blocks with emphasis on querrying and investigation for the occurrence of breach of terms by consumers and utility companies.

The content of the side blocks appended to their parent blocks are reports from the smart contracts that are indexed thereby maintaining accuracy on identical reports with violations stored concurrently in the smart contract database. The structure of generating multiple threads for our sovereign blockchain network and generating side blocks on parent blocks aggregates to a comprehensive collection of reports.

As pointed out earlier, a block is developed from a form which is generated from an event. An entire block is made up of a single event which spans from when it was created till the time it becomes available to the smart grid system. The processing and consensus nodes are the only entities which have direct access to the sovereign blockchain network. While monitoring the blocks, parent and side ones included, nodes alert the system when breaches to the agreed use of data occur.

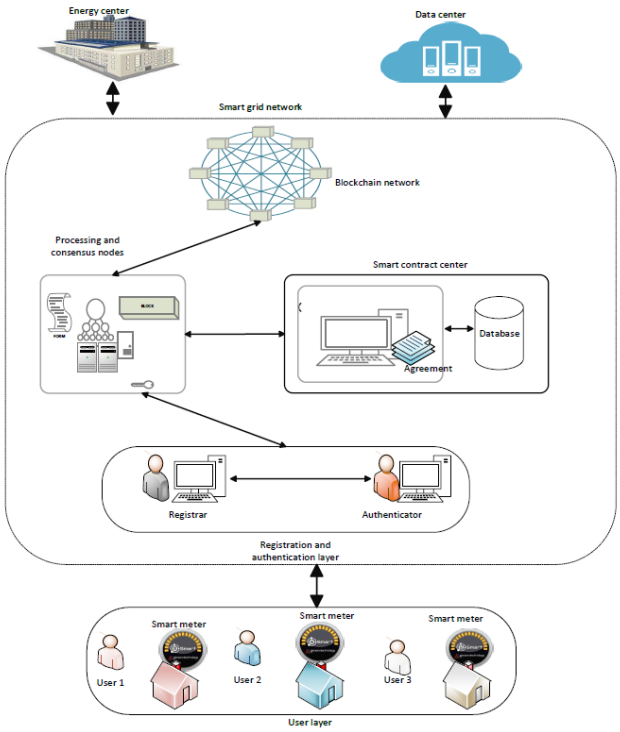

FIGURE 1. System model with the various layers.

B. CRYPTOGRAPHIC KEYS

In our system, cryptographic keys are employed to execute specific tasks relating to system and data security. For the secure sovereign blockchain-based monitoring on smart grid, we show the keys needed to achieve confidentiality for transactions between consumers and the respective utility companies. These keys enable us to achieve a high level of security of our system.

In our system, there is the need to adopt cryptographic primitives for the secure transfer of data from the smart home onto the smart grid to prevent the interception and modification of data in transit by malicious actors. We describe the primitives and keys that best suit our system below. These keys include:

- **Consumer private key**: This is generated by the consumer and used to digitally sign requests for data access.
- **Consumer public key**: This is a key generated by the consumer and sent to the authenticator on the smart grid network and it is used to verify the identity of the consumer for data access. The public key is also used to encrypt data to be sent out to the consumer by the authenticator.
- **Authenticator contract key**: This is a key pair generated by the authenticator and attached to a smart contract in a package used to encrypt reports from the consumers system to the smart grid network and vice versa.

For a consumer who wants to access the records of electrical consumption, the consumer generates a key pair (consumer private key and public key), stores the private key and shares the public key with the smart grid network. The consumer then creates requests, signs them using the consumer private key and sends them to the smart grid network. Upon reception, the authenticator confirms the request by verifying the signature with the consumer public key. Results of computations on data requested are placed in tags added to the data and further processed on the smart grid network by the appropriate entities. This processed data is encrypted with the authenticator contract key and is then sent to the consumer. Upon reception, the consumer decrypts the encrypted package and reads the data. To adequately secure the transfer of data from the consumer to the smart grid network, the reporting of actions and events generated from the use of cryptographic functions and the flags raised on the data are encrypted using the authenticator contract key tagged to the contracts which has already been generated by the data originator. This is consequently sent to a secure database.

III. DESIGN FORMULATION

In this section, we explain the various entities that we employ in our system.

A. SYSTEM STRUCTURE

We formulate a data transfer mechanism used by the secure sovereign blockchain-based monitoring on the smart grid between consumers and utility companies for data security and transparency. *Figure 1* describes our system model.

1) USER LAYER

The User Layer comprises all the entities who access electricity from the given utility company for the initiation and running of processes that are necessary for their purposes. This layer directly interfaces with the registration and authentication layer on the smart grid network and allows users to register to be part of the system. Users register on the system by visiting this interface and provide the necessary information. This information is submitted onto the smart grid network and it is received and processed at the registration and authentication layer. Examples of users can be individual users in homes or offices, schools, healthcare facilities, corporations etc.

2) DATA PROCESSING AND MONITORING LAYER

This layer consists of individual components that help in processing all the data sent to the smart grid network. This particular layer also performs computations on the data and also tags the data with functionalities that help in monitoring every action performed in the entire system. On this layer, algorithms are implemented to automatically report any illegal actions performed in the system and also triggers an action to automatically deny access to the usage of electricity. The reported illegal actions are tagged with the unique ID of the corresponding user and are securely stored in a database. Results of every action that is sent to the system is broadcast onto network which helps to guarantee trustless and fair auditing. Lastly, this layer has the responsibility of authenticating every action and request for data access in the entire system.

3) REGISTRATION AND AUTHENTICATION LAYER

This layer comprises of the registrar and the authenticator. The data of a user who registers on the system is first received by the authenticator. The request is processed and a unique ID is generated for the user. This unique ID identifies every user on the system. Anytime a user logs onto the system, he is authenticated by the authenticator using this unique ID.

4) SMART CONTRACTS

These are specifically designed functions that are activated and executed upon the reception of an action [31]. The smart contracts generated on this system have been embedded with cryptographic keys and this enables the contracts to encrypt the reports generated from the activation of actions. The main function of the smart contracts is to identify malicious usage of electrical power and electrical data and to report such actions into a database. The smart contracts revoke access to electrical power whenever there is any malicious usage of electrical power by a user. The smart contract alerts a user whenever there is malicious manipulation of electrical data of that particular user.

5) SMART CONTRACTS DATABASE

This is a report violation storage and action center on the sovereign blockchain network. The violations are received from the smart contracts upon the inspection of requests and actions. The smart contract database stores lists of actions agreed on between consumers and utility companies to be carried out when there is a violation of contract terms. It also stores receipts for each action and thus provides consistency of data for accountability and auditing when required.

6) ENERGY CENTER

This layer directly interfaces with the processing and monitoring layer and it generates the electrical power and transfers it to the processing and monitoring layer upon request by the processing and consensus nodes. The power is later distributed to clients on the network based on tariffs paid per month.

7) DATA CENTER

The data center also directly interfaces with the processing and monitoring layer and it receives copies of the data that are processed onto the sovereign blockchain and are stored for research purposes.

IV. DESIGN APPROACH

This section describes the various processes involved in the design of our secure sovereign blockchain-based monitoring on the smart grid.

A. REGISTRATION AND AUTHENTICATION LAYER

On this layer, a user requests access to energy by visiting the user layer and entering the required information. The information is sent to the registration and authentication layer on the sovereign blockchain network. The data is received by the registrar and then a unique identification number which serves as the user's meter ID is generated and the data is shared with the authenticator. The authenticator forwards the data to the processing and monitoring layer. When the data is received by a processing and a consensus node, the corresponding area code of where the user resides is added and then the data is linked to a smart meter to be installed in the residence of the user. After a successful installation of a smart meter in the home of a user, the unique ID that is the meter ID of the user is sent to the smart grid network by the smart contract where it is received by the authenticator for verification. When a user is verified successfully, the user is given access to electricity.

B. SMART METER

A smart meter is a new type of electricity and gas meter which uses wireless technology to digitally send meter readings on real time basis from a users home to energy supplier for more accurate energy bills [22]. It comes with an in-home display screen that shows exactly how much energy a user is consuming in real time. In this work, we employ smart meters to digitally send meter readings from the home of a consumer to the sovereign blockchain network. The meter readings received on the sovereign blockchain network via the smart meter are processed into blocks and later added to

the sovereign blockchain after they have been verified and accepted by majority of processing and consensus nodes. We also create smart contracts protocol between the smart meter and the sovereign blockchain network. The smart contracts are triggered and executed based on the activity detected whether there is a malicious activity on the meter or an appropriate action is taken.

C. PROCESSING AND CONSENSUS NODES

The processing and consensus nodes handle the processing of power usage data from clients, including requests and access granted. This is recorded in blocks on the network. Power is requested from the energy center and is distributed to the clients according to the status of the agreed to monthly subscription. A processing and consensus node receives the energy request details of a consumer and then adds the corresponding meter ID, house number and area code of the consumer and processes them into a temporary form. This form is later converted into a block which is handed to other nodes for verification and acceptance. When the block is verified and accepted by majority of the processing and consensus nodes, it is added to main sovereign blockchain. On the other hand, if it is not accepted it is sent back to the originator for reconsideration. Copies of the form are sent to the data center for storage. The data stored in the data center are used by the utility company and research agencies for forecasting and research purposes respectively.

D. DATA PROCESSING ON THE SMART GRID NETWORK

Data processing on the smart grid network by the processing and consensus node is very crucial for the proper and secure functioning of the transaction among the untrusted participating parties. Data processed by the processing and consensus nodes pertaining to power usage must maintain high integrity and values inhibiting the reliability of the system's data, processes and entities ability to stand scrutiny are removed by the careful design and structuring of data processing and sharing methods.

The data corresponding to the transaction of power usage of consumers is processed by the processing and consensus node on the smart grid network. The consensus node creates a package out of it. The package created contains a payload and a unique ID of the node responsible for processing the data along with meter ID of the corresponding user. This data is processed into a form which is later converted into a block through processing. The processed data is made available to a second processing and consensus node for further validation of the work done by the first consensus node. Responses for successful validation of newly processed data are sent back to the originating node. The consensus node records all the timestamps on the blocks which the activities on a particular transaction happened.

After the original processing and consensus node has received the data, the node sends a request to the smart contract center which is received by the smart contract generator. The smart contract generator produces a script and transmits it to the node. The script, together with the timestamps, is then attached to the current processed state of the data. This data is converted into a block and it is joined to the main chain of blocks.

The smart contracts are linked to the smart meters installed in the homes of consumers such that it is able to send data from the smart grid network to the smart meter and vice versa. The data recorded by the smart contract on the smart grid network is stored in a smart contracts database. This is later retrieved by the processing and consensus nodes and processed into a side block which is attached to the parent block of the corresponding data.

V. SMART CONTRACTS AND SOVEREIGN BLOCKCHAIN DESIGN

In this section, we explain the processes taken to design the sovereign blockchain and the smart contracts in our system.

A. SMART CONTRACTS DESIGN

Smart contracts can be described as finite state machines which execute laid down instructions when predefined conditions are met or specified actions have taken place. We employ smart contracts in this work to report the state of data on the smart meter and violations which happen on both the smart meter and on data on the smart grid network. This improves the reliability of the monitoring environment for both consumers and utility companies since the entire data transferred on the system is monitored in a secure environment.

Data transferred to the smart grid network are processed, indexed and broadcast into a sovereign blockchain network. Violations on consumer data that happens on the smart grid network are also processed, indexed and broadcast into a sovereign blockchain and the consumer is then alerted via the smart meter. We write the sets of rules that are applied to the state of the smart meter and also on consumer data on the smart grid network. These rules when in force trigger the smart contracts to send reports to the smart grid network. They also leave alert messages on the screen of the smart meter for the consumer.

After a successful installation of a smart meter in the home of a consumer, the smart contract generates a private key and public key automatically and shares the public key on the smart grid network. The smart contract encrypts a report with its private key and sends it to the smart grid network. This is either a success or a failure message and the content is known upon the decryption of the message. Consumer data being manipulated maliciously on the smart grid network triggers the smart contract to send an encrypted message to the smart meter which is decrypted by the smart contract on the smart meter and displayed on the screen on the smart meter to the consumer. At a point in time when a consumers power gets to the minimum value, the smart contract on the smart grid sends an encrypted message to the smart meter which is decrypted by the smart contract on the smart meter and displays it on the screen to the consumer. When a consumers

power gets used up, the smart contracts on the smart meter are activated and shut down the electrical power and sends an encrypted message to the smart grid network indicating a system shutdown of that particular consumer's meter. A smart meter that is tampered with automatically triggers the smart contract to send an encrypted message to the smart grid network and shuts down the power system that corresponds to the tampered meter. All these messages are stored in a smart contract database which are processed into side blocks and are appended to their corresponding parent blocks on the sovereign blockchain.

B. PARENT BLOCK STRUCTURE

In a sovereign blockchain, a block has a format which uniquely identifies it from all others. The format is followed by the block size which contains the size of the whole block. The next structure after the block size is the block header. The block header is hashed with sha256(sha256()) as done in the Bitcoin headers. The block header plays a very crucial role in the sovereign blockchain network in terms of ensuring immutability. When an attacker wants to modify a block header, the attacker should be able to modify all block headers starting from the genesis block in order to falsify the record of the block. This helps in ensuring a higher level of security on the network since there is a maximum assurance of an impossibility in achieving this task. In the case of malicious activity, a block mismatch will alert the system of a suspicious event which triggers data forensics. The data version of a block is contained in the block header and this indicates the validation rules to follow for a particular data type. The data version of a block specifies the properties and the type of data being accessed.

The block header contains the hash of the previous block which is a sha256(sha256()) hash and the function of this is to make it impossible to change a previous block header without changing the preceding block headers. The Merkle root hash forms part of the header by making sure that none of the blocks in the sovereign blockchain network can be changed without changing the header. This is achieved by taking the hashes of all the events in the sovereign blockchain network and appending the output to the current block. This results in a sha256(sha256()). The header also contains a timestamp and this indicates when the block was created. There is a target difficulty in the header and this is a value which shows how processing is achieved by the processing and consensus nodes. This value is unique to the system to make processing difficult for malicious nodes but efficient and solvable by verified consensus nodes in the system. Finally, there is a nonce in the header which is an arbitrary number the processing and consensus nodes generates to modify the header hash in order to produce a hash below the target difficulty.

The block has an action counter and this records the total number of violations which have been applied on the accessed data in the entire block. The next component is the transactions which have been grouped into two parts, that is, timestamps and the data. The timestamps are made up of time to

Algorithm 1 Smart Contracts Algorithm

```
Class ContractMeterRule{
public meterID ;
public power.flow ;
public state.tamper ;
public threshold.value ;
public data.tamper ;
public power.finished ;
public meter.instance ;
public normal.flow ;
public key ;
public signature ;
function comment() {
if meter.instance == power.flow then
   comment ="Installation successful";
else if meter.instance == state.tamper then
   comment = "Meter with " || meterID || "has been
   tampered with";
else if meter.instance == threshold.value then
   comment ="Power running down, top up";
else if meter.instance == data.tamper then
   comment == "You are being over charged";
else if meter.instance == power.finished then
   comment ="Meter with " || meterID || "has no power,
   system shutdown";
else {meter.instancee == normal.flow;}

end if
}
function encrypt(key, signature) {
retrieve key ;
retrieve signature ;
encrypt comment() ;
}
function main() {
if meter.value <= threshold.value then
   encrypt(key, signature) ;
else if meter.value = 0 then
   encrypt (key, signature) ;
else {return null;}

end if
if meter.instance == normal.flow then
   encrypt(key, signature) ;
else if meter.instance == state.tamper then
   meterinstance = power.cut;
   encrypt (key, signature) ;
else {return null;}

end if
if meter.data <= data.tamper then
   encrypt(key, signature) ;
else {return null;}

end if
}
```

purchase power (TTP), time to process the transaction (TPT), time power starts reading (TPR), time power reaches threshold value (TPRT), time power gets finished (TPF). The data part comprises of meter ID (MID), house number (HN), amount of power purchased (APP), processing node ID (NID) and signature of processing node (Nsig). Finally, the entire block is defined by a structure called blocklocktime. This is a timestamp that records the last entry of transactions as well as the closure of a block. When conditions for this field are met, the block is ready to be broadcast into the sovereign blockchain network. The blocklocktime generally signifies the time the block enters the sovereign blockchain. *Figure 2* describes the structure of our parent block.

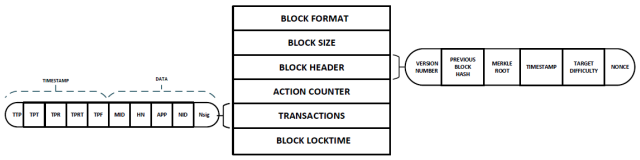

FIGURE 2. Parent block structure.

C. SIDE BLOCK STRUCTURE

A side block is made of a format and this format is derived by appending a section of the main blocks ID to an ID generated by consensus nodes to the side block. The block format is followed by the block size which is the entire size of the block. The side block has headers which is made up of six entities. These entities are the version number and this uniquely identifies the reports used to create the side block, previous side block hash, merkle root of all side blocks for a particular parent block, timestamp, target difficulty and a nonce. These entities have same properties as their parent block but relate to the side blocks.

The side block also has an action counter and this is for the recording of the violations on the smart meter and data on the smart grid network and the state of the smart meter. The next component is the transaction counter which is made up of the timestamp of violation (TSV), timestamp of state of smart meter (TSM), meter ID (MID), house number (HN), type of violation (TVLN), processing node ID (NID), and processing node signature (Nsig). The block is then timelocked and broadcast to the blockchain by appending it to the parent block. *Figure 3* describes the structure of our side block.

VI. DISCUSSION

In this section, we talk about comparison of our work with existing systems and the metrics chosen for the comparison.

The first metric considered was information sharing and this refers to the ability of utility companies to make data generated available to third parties for research purposes. The next metric considered is efficient data manageability and this refers to the ability of data owners to have full control over their data shared with third parties. The Sovereign blockchain provides a well robust platform where data

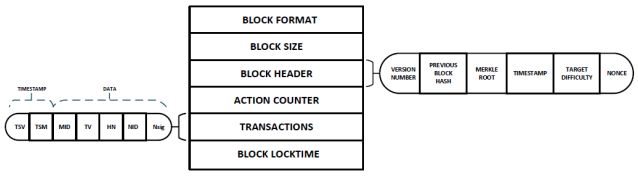

FIGURE 3. Side block structure.

TABLE 1. Comparison between proposed system and other related systems.

Metric	[19]	[20]	[21]	[22]	GridMonitoring
Information sharing	Y	N	Y	Y	Y
Efficient data manageability	Y	N	N	N	Y
Data immutability	N	N	Y	N	Y
Customer utility control	N	N	N	Y	Y
Data integrity	Y	Y	Y	Y	Y
Data confidentiality	Y	Y	Y	Y	Y
Data provenance and auditing	N	N	Y	N	Y

owners can have full control over their data. Data immutability was also considered. Data immutability refers to the data being unalterable. Sovereign blockchain provides this property and makes it infeasible to change or modify data on a sovereign blockchain without detection. Again, we considered customer control over utility and this metric refers to customers being able to control their power usage. Smart meters allow customers to monitor daily power consumption of their devices. Data integrity, or the ability to detect unauthorized modifications to data, was also considered. The Sovereign blockchain achieves this property by making data on the platform secure against unwarranted changes. We considered data confidentiality, how secure generated data on a system is against intrusion. Again, the Sovereign blockchain employs a tamper-proof structure and therefore prevents external attackers from having access to the data without permission. Data provenance and auditing which refers to data users being able to account for data usage was also considered. The Sovereign blockchain, coupled with smart contracts ensures this property by due to every action performed being recorded and sent to an appropriate destination.

Results on the comparison of our work with the existing systems based on the metrics previously discussed in this section is displayed in table 1.

VII. CONCLUSION

In this paper, a sovereign blockchain-based system which has the properties of ensuring transparency, provenance and immutability is implemented on a smart grid system. This is due to the fact that there are numerous inconsistencies between electricity companies and consumers, regarding electricity usage and bills. With the incorporation of smart meters, consumers can actually know the amount of wattage being consumed and also which appliances consume them the most. The utilization of smart contracts in this model

enhances the transparency, as penalties are applied to defaulters in any transaction. This platform in the large scale ensures security. Comparison of our work with other models prove ours to be efficient. In the future work, we hope to implement the system and obtain feasible results.

REFERENCES

[1] D. Newbery, G. Strbac, and I. Viehoff, "The benefits of integrating European electricity markets," *Energy Policy*, vol. 94, pp. 253–263, Jul. 2016.
[2] A. S. G. Andrae and T. Edler, "On global electricity usage of communication technology: Trends to 2030," *Challenges*, vol. 6, no. 1, pp. 117–157, 2015.
[3] E. Brynjolfsson, P. Hofmann, and J. Jordan, "Cloud computing and electricity: Beyond the utility model," *Commun. ACM*, vol. 53, no. 5, pp. 32–34, 2010.
[4] S. D. Manshadi, M. E. Khodayar, K. Abdelghany, and H. Uster, "Wireless charging of electric vehicles in electricity and transportation networks," *IEEE Trans. Smart Grid*, to be published. [Online.] Available: http:// ieeexplore.ieee.org/document/7837718/
[5] M. Salahuddin and K. Alam, "Information and communication technology, electricity consumption and economic growth in OECD countries: A panel data analysis," *Int. J. Elect. Power Energy Syst.*, vol. 76, pp. 185–193, Mar. 2016.
[6] P. Sadorsky, "Information communication technology and electricity consumption in emerging economies," *Energy Policy*, vol. 48, pp. 130–136, Sep. 2012.
[7] U. S. Department of Energy, "The SMART GRID," *Communication*, vol. 99, p. 48, 2010. [Online]. Available: https://energy.gov/oe/technology-development/smart-grid/smart-grid-primer-smart-grid-books
[8] F. Li *et al.*, "Smart transmission grid: Vision and framework," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 168–177, Sep. 2010.
[9] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2011.
[10] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, 2011.
[11] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016.
[12] J. Zheng, D. W. Gao, and L. Lin, "Smart meters in smart grid: An overview," in *Proc. IEEE Green Technol. Conf.*, Apr. 2013, pp. 57–64.
[13] X. Hao *et al.*, "Smart meter deployment optimization for efficient electrical appliance state monitoring," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun., (SmartGridComm)*, Nov. 2012, pp. 25–30.
[14] M. Jaradat, M. Jarrah, A. Bousselham, Y. Jararweh, and M. Al-Ayyoub, "The Internet of energy: Smart sensor networks and big data management for smart grid," *Procedia Comput. Sci.*, vol. 56, no. 1, pp. 592–597, 2015.
[15] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 425–436, Feb. 2016.
[16] K. S. Reddy, M. Kumar, T. K. Mallick, H. Sharon, and S. Lokeswaran, "A review of integration, control, communication and metering (ICCM) of renewable energy based smart grid," *Renew. Sustain. Energy Rev.*, vol. 38, pp. 180–192, Oct. 2014.
[17] C.-I. Fan, S.-Y. Huang, and W. Artan, "Design and implementation of privacy preserving billing protocol for smart grid," *J. Supercomput.*, vol. 66, no. 2, pp. 841–862, 2013.
[18] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.
[19] S. Rusitschka, K. Eger, and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 483–488.
[20] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.
[21] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Proc. Resilience Week*, 2017, pp. 18–23.
[22] F. Ye, Y. Qian, and R. Q. Hu, "An identity-based security scheme for a big data driven cloud computing framework in smart grid," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1–6.
[23] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
[24] J. Basden and M. Cottrell, "How utilities are using blockchain to modernize the grid." in *Harvard Business Review Digital Articles*. Brighton, MA, USA: Havard Business Review, 2017, pp. 2–5.
[25] B. Zhang, C. Jiang, J.-L. Yu, and Z. Han, "A contract game for direct energy trading in smart grid," *IEEE Trans. Smart Grid*, to be published. [Online.] Available: http://ieeexplore.ieee.org/abstract/document/7725484/
[26] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.
[27] J. Ni, K. Zhang, X. Lin, Q. Xia, and X. S. Shen, "Privacy-preserving mobile crowdsensing for located-based applications," in *Proc. ICC*, May 2017, pp. 1–6.
[28] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "BlockChain technology: Beyond bitcoin," *Berkley Eng.*, no. 2, p. 35, 2016.
[29] J. Ni, X. Lin, Q. Xia, and X. S. Shen, "Dual-anonymous reward distribution for mobile crowdsensing," in *Proc. ICC*, 2017, pp. 1–6.
[30] T. Mcconaghy *et al.*, "BigchainDB: A scalable blockchain database (DRAFT)," BigchainDB, Berlin, Germany, White Paper, 2016, pp. 1–65.
[31] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.

JIANBIN GAO received the Ph.D. degree in computer science from the University of Electronic Science and Technology of China (UESTC) in 2012. He was a Visiting Scholar with the University of Pennsylvania, Philadelphia, PA, USA, from 2009 to 2011. He is currently an Associate Professor with UESTC.

KWAME OMONO ASAMOAH received the B.Sc. degree in computer science from the Kwame Nkrumah University of Science and Technology, Ghana, in 2014. He is currently pursuing the master's degree in computer science and technology with the University of Science and Technology of China. His current research includes blockchain technology and big data security.

EMMANUEL BOATENG SIFAH received the B.Sc. degree in telecommunications engineering from Ghana Technology University College, Ghana, in 2014, and the M.Sc. degree in computer science and technology from the School of Computer Science and Engineering, University of Electronic Science and Technology of China, in 2017, where he is currently pursuing the Ph.D. degree in computer science and technology. His current research interests include blockchain technology and privacy and big data security.

ABLA SMAHI received the B.Sc. and M.Sc. degrees in computer science from Tahri Mohammed University Bechar-Algeria, in 2013 and 2015, respectively. She is currently pursuing the Ph.D. degree in computer science and technology with the University of Electronic Science and Technology of China. Her current research includes blockchain technology privacy preserving data mining and big data security.

QI XIA received the B.Sc., M.Sc., and Ph.D. degrees in computer science from the University of Electronic Science and Technology of China (UESTC) in 2002, 2006, and 2010, respectively. She was a Visiting Scholar with the University of Pennsylvania, Philadelphia, PA, USA, from 2013 to 2014. She is currently the PI in cyber security with the National Key Research and Development Program of China. She is also the Vice Dean with the Center for Cyber Security and currently an Associate Professor with UESTC. He has authored or co-authored over 20 papers. She was a recipient of the National Scientific and Technological Progress Second Prize in 2012.

HU XIA received the Ph.D. degree from the University of Electronic Science and Technology of China in 2012. He was a Visiting Scholar with the University of Minnesota, Twin cities, USA from 2010 to 2011. He is currently an Associate Director with the National Engineering Laboratory of Big Data application to improving the Government governance capacity in China. He is currently an Associate Research Fellow with the University of Electronic Science and Technology of China.

XIAOSONG ZHANG received the B.S. degree in dynamics engineering from Shanghai Jiaotong University, Shanghai, in 1990, and the M.S. and Ph.D. degrees in computer science from the University of Electronic and Technology of China (UESTC), Chengdu, in 2011. He has worked on numerous projects in both research and development roles. He is currently an Associate Director with the National Engineering Laboratory of Big Data application to improving the Government governance capacity in China.

He is also a Professor in computer science with UESTC. He is the Dean with the Center for Cyber Security of UESTC. He has coauthored a number of research papers on computer network security. His current research involves software reliability, software vulnerability discovering, software test case generation, and reverse engineering.

GUISHAN DONG born in 1974. He received the Ph.D. degree in computer science from the University of Electronic Science and Technology of China (UESTC). He is currently an Associate Director with the National Engineering Laboratory of Big Data application to improving the Government governance capacity in China, and a Chief Expert in network security with CETC Group. His main research areas include network security, cloud computing, big data, and network trust system. He was a recipient of the State Council Special Allowance Winner in 2016.