Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network

Ahmet Önder Gür[1], Şafak Öksüzer[1], Enis Karaarslan[1]
Department of Computer Engineering, Muğla Sıtkı Koçman University
Muğla, Turkey

***Abstract*—Measurement of energy especially electricity consumption becomes an issue in big cities. Electricity usage monitoring is becoming more crucial and there is a need for the instant view of active energy usage. Solutions like smart grids are possible. Smart grids give a view in macro-level, there is also a need of a micro-level view. We mean a small region's or customer's usage when we mean micro-level view. The privacy of the personal data and the user's trust in the system should also be considered in these scenarios. This study aims to propose such an alternative system which uses blockchain technology and Internet of Things (IoT) devices for the metering and billing of the customer for the electric network. The trust and privacy issues are aimed to be solved. Blockchain can provide safer and more transparent solutions with its decentralized structure. Raspberry Pi is used to simulate metering, Hyperledger Fabric is selected as a blockchain system. A scalable and energy efficient energy tracking system with blockchain and IoT devices is proposed. A prototype system is formed and the possible usage scenario is simulated on the prototype.**

***Index Terms*—blockchain, IoT, privacy**

I. Introduction

Big cities involve many electricity consumers, measurement and planning of the electricity network becomes an issue. Transactions between distributors and consumers are far from automation and there is no transparency in traditional energy billing and distribution systems. Current consumption levels can not be monitored in most implementations as most of the metering systems still rely upon manual consumption meter readings. These metering process also cost a lot of money and time[1]. Analysis of the data is insufficient because of the collection method. There can be trust issues as these systems are non-transparent and centralized, customers are not aware of the process and their personal data can be vulnerable to attacks or misuse.

There is a need for a system where all users reach the current usage levels, all users trust the system and the privacy of their personal data is preserved. The usage levels can be analyzed and used to solve technical problems before any possible problem gets critical. Blockchain and IoT technologies can be used as a solution[2].

Blockchain technology offers an immutable distributed ledger to store transactions. Participants of the blockchain network can make transactions without trusting each other or some other third party[3]. Privacy of personal data can be assured by using cryptographic algorithms. The decentralized architecture of the blockchain system will make the network safer against Cyber threats. IoT devices can be modified to measure energy consumption automatically and work with the blockchain system. An economic, scalable, secure and energy efficient solution can be developed[4].

In the next section, the fundamentals of blockchain, Hyperledger, Internet of Things (IoT) technologies, security services and the privacy need in a digitalized world will be given. In section 3, related works is given. In section 4, the proposed system is described. In section 5, implementation is explained. Finally, results and discussion are given.

II. Fundamentals

A. Blockchain

Blockchain technology helps to keep a secure and transparent/private list of records where the data blocks are linked together using cryptography techniques. The name of the registry used is called the ledger. Ledger is kept in various devices which are connected to each other within the P2P network. Blockchain technology uses distributed devices and provides a decentralized system[5]. It uses consensus protocols that guarantee co-decision in the system without making an authority.

Bitcoin as digital currency was the first Blockchain implementation in 2008[6]. Later there were several applications such as Ethereum, Ripple, and Neo. There are also different blockchain systems such as Hyperledger that offer enterprise solutions. Hyperledger project is an open source project that is managed by the Linux Foundation[7].

There are different blockchain types according to the way nodes join the network and the visibility of the ledger. The types change according to the anonymity of the validator (node) and the trust in it as it is shown in Figure 1.

The blockchain type that is described in Satoshi's paper[6] about Bitcoin and used in many crypto currencies is Public/Permissionless blockchain. This network is open to join without requiring permission or reference. As anyone can be a node, the trust in the validator is low. The number of nodes

978-1-7281-1315-9/19/$31.00 ©2019 IEEE

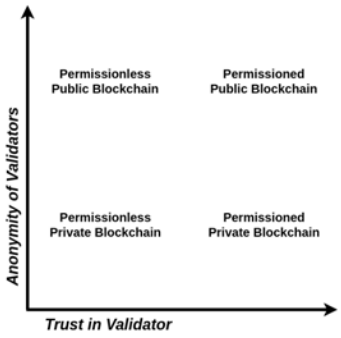

Fig. 1. Anonymity/Trust of Validators

is needed to be increased to provide enough security to the system. As these systems use a prize method for adding block, fair node selection needs high energy and time consuming consensus protocols like PoW. Transparency is provided as all participants in the network can access all the transaction data. As no part of the data can be made private, this type is not suitable for most enterprise applications[8]. Privacy issues in Bitcoin is investigated in [9]. However, the needs of the enterprise applications and privacy measures are different.

Private/permissioned blockchain is developed for the applications where a level of control and management is required. The reliability of the nodes are ensured by applying several conditions. The terms for participation in the network are ruled by the network initiator. The nodes who satisfy the conditions are added to the network as participants. A digital currency or token-like structures is not needed as an incentive in most cases. Data sharing type is predetermined by who provides the data. It is not a completely decentralized structure as it is clear which peers store the data[3]. Consensus protocols used in this type consume less energy and time[8, 10]. Hyperledger Fabric and R3 Corda can be given as examples to this type of blockchain systems[11].

Hyperledger Fabric which is available in the Hyperledger Project is chosen for this study as it fulfills the requirements of an enterprise application. Data sharing can be managed between parties. Less energy and time-consuming consensus protocols can be used. Hyperledger Fabric has a modular architecture that enables the configuration of smart contracts (chaincode) by setting inter-participant roles and rules. Each node in the network has limited authority and nodes can create groups (channel) among themselves and implement different consensus protocols within the group. Each participant has its own certificate authority so that the owner of each transaction can be identified[7]. Hyperledger Fabric can be used as a distributed operating system. It has an extensible architecture that allows modular construction. Chaincode can run within the Docker container so high-level Object-Oriented languages (Java, Go etc.) can be used. Creating a new chaincode or changing the one does not take much time. The privileges of the participants can be restricted by the rules in the chaincode[12]. A business network can also be created with the virtual computers on the cloud.

B. Internet of Things

Internet of Things (IoT) devices are small computing equipment that collects data via various sensors. These devices communicate with other devices mostly over wireless connections. They have the low processing power and memory capacity that makes them affordable. Electricity, water, and natural gas meters started to change with the smarter IoT versions. IoT smart meters can be configured to connect to the distribution network and provide data (almost) in real time. This will allow the users of the system to monitor the distribution network efficiently[13].

C. Security Services

Enterprise applications need the authenticity of the node and the confidentiality of the data. The confidentiality of the data is provided with cryptology. The main problem in encryption/decryption process is the key distribution. The key distribution problem is solved with asymmetric encryption. Asymmetric encryption is mainly used to distribute the key which will be used in the symmetric encryption[14]. Each side of the communication will only need the public key of the other for the encryption/decryption process. A public key can be distributed freely without endangering the encryption process. Certificate authorities (CA) can be used to ensure the authenticity of the public key by using digital certificates[12].

D. Privacy Need in a Digitalized World

Privacy is a human right. Data privacy should be a primary consideration in any data processing system which includes personal data. Data from various sources are being collected as big data and it can be used to violate the privacy of an individual. For this reason, any data can be described as personal data[15].

The governments started to give more focus on protecting their citizens' data with privacy regulations all around the world. Any company which involves processing the citizen data must respect the regulation of the citizen's nation. Personal data is protected with KVKK (Personal Data Protection Law) in the Republic of Turkey[16] and GDPR (General Data Protection Regulation) has started to be regulated in the European Union[17]. These regulations states that; personal data cannot be processed without the explicit consent of the person concerned and he/she is allowed to withdraw the consent. Encryption and pseudonymization are required for compliance as a start but is not sufficient.

There are personal data in the bills of the current systems, and these data are reachable by people such as company employees and neighbours. A system designed with privacy in mind and the automation of the system with smart contracts (chaincodes) can provide privacy that is needed. Smart contracts can be designed to prevent unauthorized people from seeing the personal data.

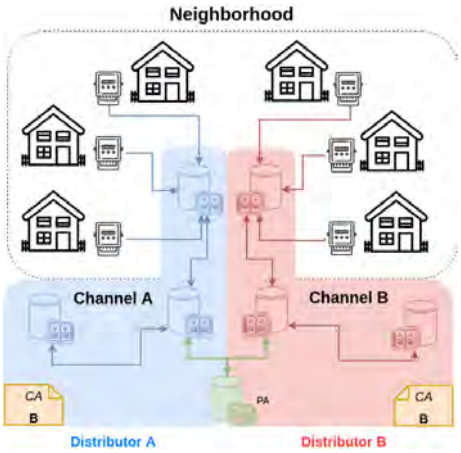

Fig. 2. Major actors of the system

III. RELATED WORKS

The industry is forming alliances for integrating blockchain and IoT to the energy sector and establishing standards. These are Energy Web Foundation, Enterprise Ethereum Alliance and Trusted IoT Alliance. A growing number of companies like Grid Singularity, Power Ledger, and LO3 are developing their own standards and applications. There are also new startups who want to promote their altcoins or tokens (crypto coin) for their proposed systems like WePower[18] and Restart Energy[19]. Most applications focus on microgrids and energy sharing [20].

There are also some patents which propose solutions to the energy market. The differences of our work from the similar patents are shown in Table 1. Patent P2 is for the renewable energy only. The main difference in our work is focusing on the end-user (consumer) side and personal data privacy.

TABLE I
COMPARISON OF THIS WORK WITH THE SIMILAR PATENTS

	Patent 1 [20]	Patent 2 [21]	This Study
Target Market	Smart Grid	End-User	End-User
Token	Token	Token	X
Measurement	✓	✓	✓
Billing	X	X	✓
Privacy of Personal Data	Not Mentioned	Not Mentioned	✓

In a recent study[23], the authors presented a marked design and simulation for a decentralized local energy market using blockchain technology. The preliminary economic evaluation is also presented. A recent master thesis[24] is about the digital identity management for the open model energy system by using blockchain. The security and privacy issues in decentralized energy trading are discussed in a recent work[20].

IV. SYSTEM PROPOSAL

The proposed system aims to solve the cost, privacy and security problems of measurement and billing systems by using a decentralized system. Major actors of the system is shown in Figure 2. CA is the certificate authority. This system has four major actors:

- Users: People who want to receive service from distributors.
- Distributors: Energy distribution companies.
- Smart Meter (IoT) Devices: Device with internet connection for sending energy consumption measurements.
- Public Authority (PA): This can be any governmental institution which wants to get the current view of the system, such as the current load of the electricity grid in a neighborhood, district or a city.

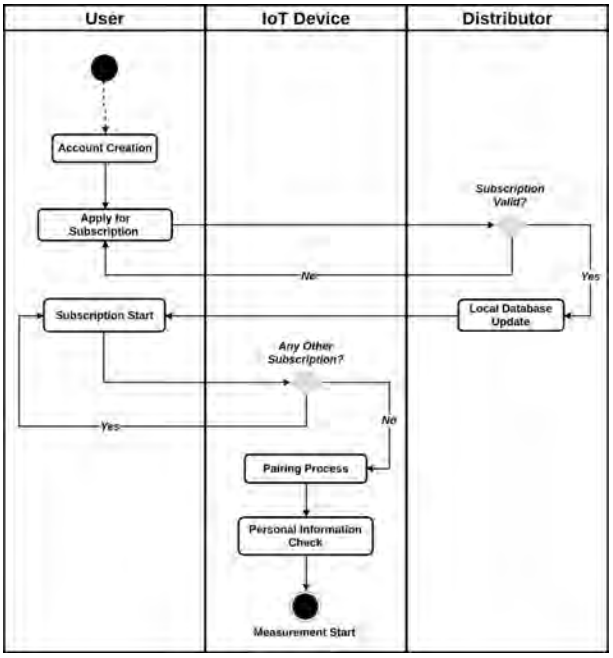

Fig. 3. The steps taken by a user to receive services

A. Phases of The Users

The start phase of a user to receive services are shown in Figure 3. There are four phases of the user application:

a) Account Creation: The user installs the user interface application of the system on a smart mobile device and creates a local account. The personal data that is required for the service is entered through the interface. The application generates a Session Key during this process and encrypts the personal data with the Session Key and stores in the smart meter.

b) Subscription Start: The user sends a subscription request to the distributor. Once the distributor has approved the request, the subscription phase starts. The session key is encrypted with the public key of the distributor and sent encrypted to the distributor. The distributor gets the session key which will be used during the subscription.

The user uses the mobile application to pair the account with an IoT device to receive the service. Encrypted personal data

is copied to the IoT device during this pairing. The IoT device informs the blockchain network and sending measurements to the blockchain network starts afterward.

c) Subscription: IoT device sends the measurements to the blockchain network at predefined intervals which are set by the distributor. These measurements are kept in the blockchain encrypted with the Session Key. Only the distributor and the public authority in the channel can see these measurements. The subscriber can reach his/her own consumption statistics and can see the amount to be paid.

No personal data is kept in the blockchain, only a SubscriptionID which the distributor sets is kept as an identification. If the distributor or the public authority need to reach personal the data of the subscriber for bureaucratic purposes, a request is created in the system. This request and its reason are also stored on the blockchain. If the requester knows the session Key of the user, the smart contract enables to reach the data which is stored in the IoT device of the user.

Sending measurement data frequently to the blockchain system can also put the subscribers' privacy in danger[25]. There are solutions for this problem as specified in [26] but these issues are left as future work.

d) Subscription End: The session key is valid for the duration of the subscription. If the subscription is canceled by the user or expired, the session key is regenerated and personal data is encrypted with this new key. The privacy of the personal data is ensured this way. Measurements that are encrypted with the previous session key will still be available to the previous distributor but not the personal data of the user. The user can subscribe to any other distributor after leaving one and gets service again.

V. Implementation

A prototype simulation is implemented in Hyperledger Fabric 1.3 as a proof of concept on an ordinary PC with 12 GB RAM, 240 GB SSD, and an i7 Intel 3.5 GHz CPU. Version 1.3 is preferred for its new features such as peer channel-based event services and stabilization. Implementation technologies that are used in the system are shown in Figure 4. Hyperledger Fabric is run as a virtual machine on the Virtualbox. Vagrant Tool is used to accessing the virtual machine. Peers are run on Docker containers which were created by using official Hyperledger Fabric Docker images. Two channels are created and one peer is added to each for validating and storing the data. A database is installed for each peer to keep transaction logs and the current state of assets. Assets are used to define tangible or intangible values and are kept in JSON or binary form. Assets are defined in the chaincodes. CouchDB was chosen as it allows complex queries which will be used during generating reports. Different Certificate Authorities are used for each channel. Membership Service Provider (MSP) is a part of the Hyperledger Fabric which is used for validating certificates and user authentication.

Hyperledger Composer Tool is used as a coding and testing platform. The codes can be generated on the programmer's

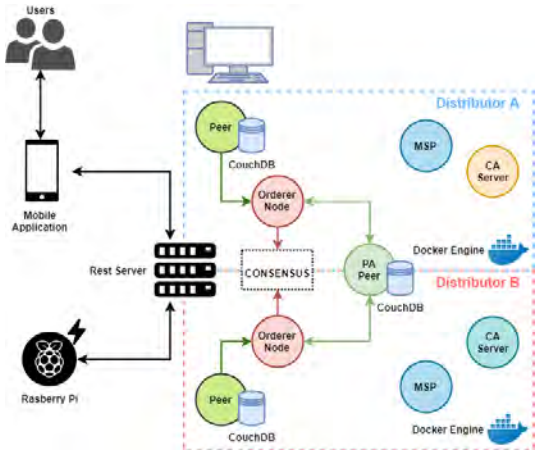

Fig. 4. Implementation Technologies Used in the Prototype

machine. Simple chain codes are coded with JavaScript. Several sample rules are generated for the participants, such as rules which grant view access to only their data.

Business Network Archive (BNA) was created to deploy the chaincode into the business network. In deploying, SOLO consensus protocol is chosen for testing. Rest Server is used to generate APIs of the written chaincode to use on the sample user interface application.

Raspberry Pi 3 Model B v1.2 is used as an IoT device to simulate smart meter of the end user. Random measurements are generated with python code. The device is connected to the blockchain network with the API of the Hyperledger Fabric.

VI. Results and Conclusion

A scalable and energy efficient energy tracking system with blockchain and IoT devices is proposed in this study. The cost of the measurement methods can be decreased with this system. The system will be less vulnerable to the cyber attacks because of the decentralized architecture.

Hyperledger Fabric environment was preferred as its suitable for enterprise solutions. The environment is complex and still evolving. It wasn't easy to find enough information on it at first but the community is developing new content and solutions. The environment became more stable after version 1.3.

Privacy of the personal data was the main focus of this study. A system is proposed in which the user keeps its own personal data on his/her own device and only shares the data when necessary. Personal and measurement data is only shared with the company during the subscription period. A shared key is used to encrypt the data during the subscription.

Using smart contracts, making all energy tracking procedures automated will help in reducing the rate of wrong manual measurements. Certificate Authorities will show the validators of the the transactions.

The prototype simulation with smart contracts was tested by using different IoT devices. Preliminary findings showed that the rest server usage reduces the software development

time but there is a need of additional security procedures on identity management.

Future works will include working on privacy enhancing and testing. As the quantum computers will become more widespread, post-quantum cryptography can be studied and added to the process. New methods should be used instead of the asymmetric encryption methods.

REFERENCES

[1] S. Albrecht, S. Reichert, J. Schmid, J. Strüker, D. Neumann, and G. Fridgen, “Dynamics of Blockchain Implementation - A Case Study from the Energy Sector,” Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.

[2] M. Friedlmaier, A. Tumasjan, and I. M. Welpe, “Disrupting Industries With Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures,” SSRN Electronic Journal, 2016.

[3] K. Wust and A. Gervais, “Do you Need a Blockchain?,” 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018.

[4] M. Mylrea and S. N. G. Gourisetti, “Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security,” 2017 Resilience Week (RWS), 2017.

[5] E. Karaarslan and M. F. Akbas, Blokzinciri Tabanlı Siber Güvenlik Sistemleri [Blockchain-based Cyber Security Systems], Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, vol. 3, no. 2, pp. 16-21, 2017.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] C. Cachin, "Architecture of the hyperledger blockchain fabric," Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, 2016.

[8] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” International Journal of Web and Grid Services, vol. 14, no. 4, p. 352, 2018.

[9] Conti, M., Kumar, E.S., Lal, bC. and Ruj, S., 2018. A survey on security and privacy issues of bitcoin. IEEE Communications Surveys Tutorials, 20(4), pp.3416-3452.

[10] Q. Nasir, I. A. Qasse, M. A. Talib, A. B. Nassif, "Performance analysis of hyperledger fabric platforms," Security and Communication Networks, 2018.

[11] M. Valenta, P. Sandner, Comparison of Ethereum Hyperledger Fabric and Corda, Frankfurt:Frankfurt School Blockchain Center, Jun. 2017.

[12] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains", Proceedings of the 13th ACM SIGOPS European Conference on Computer Systems, 2018.

[13] Iu Hua, Zhang Junguo, Lin Fantao, "Internet Of Things Technology And Its Applications In Smart Grid", vol. 12, no. 2, 2014.

[14] C. Kaufman, R. Perlman, M. Speciner, Network Security. Private Communication in a Public World, NJ, Englewood Cliffs:Prentice-Hall, 1995.

[15] G. Zyskind, O. Nathan, and A. sandy Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” 2015 IEEE Security and Privacy Workshops, 2015.

[16] Kişisel Verileri Koruma Kanunu [Personal Data Protection Law] , Kanun numarası: 6698, Resmi Gazete Sayı: 29677, 2016, [online] Available: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119:1–88, April 2016.

[18] "WePower Green Energy Network” white paper, version 0.81, 2019. [Online]. Available: https://wepower.network/media/WhitePaper-WePower_v_0.81.pdf. [Accessed: 21- Jan- 2019].

[19] “Restart Energy”, [Online]. Available: https://restartenergy.io/. [Accessed: 21- Jan- 2019].

[20] N. Z. Aitzhan, D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures blockchain and anonymous messaging streams", IEEE Trans. Depend. Sec. Comput.

[21] Steven Lewis S., Biermann M., Pattnaik S., (2017), WO 2017/066431 A1, World Intellectual Property Organization International Bureau

[22] Mayne T., Umasky S., (2017), WO 2017/199053 A1, World Intellectual Property Organization International Bureau

[23] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets" in Computer Science—Research and Development, Berlin, Germany:Springer, pp. 1-8, Aug. 2017, [online] Available: http://link.springer.com/10.1007/s00450-017-0360-9.

[24] S Kikitamara, M van Eekelen, DIJP Doomernik, “Digital Identity Management on Blockchain for Open Model Energy System”, Masters Thesis, 2017

[25] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, M. Nojoumian, "Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems", Future Generation Computer Systems, 2017.

[26] L. Sankar, S. R. Rajagopalan, S. Mohajer, H. V. Poor, "Smart meter privacy: A theoretical framework", IEEE Trans. Smart Grid.