A systematic survey of blockchain application in Smart Grid

Santosh Desai*, *Student Member, IEEE,* Amit Dua†, *Member, IEEE,* Ranadive Sahil‡, Neeraj Kumar§, *Senior Member, IEEE*
Ashok Kumar Das¶, Joel J. P. C. Rodrigues‖, *Senior Member, IEEE*
* † ‡ Department of Computer Science and Information Systems, BITS Pilani, Pilani, India
§ Computer Science & Engineering Department, Thapar University, Patiala (Punjab), India
¶ Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India
‖ National Institute of Telecommunications (Inatel), Brazil;
Instituto de Telecomunicações, Portugal; University of Fortaleza (UNIFOR), Brazil
E-mails:* santoshdesai12@hotmail.com † mail.amitdua@gmail.com ‡ f2016097@pilani.bits-pilani.ac.in § neeraj.kumar@thapar.edu
¶ ashok.das@iiit.ac.in ‖ joeljr@ieee.org)

***Abstract*—Smart grid are supposed to provide an efficient means for energy trading using blockchain technology. They are implemented to address the problems related to security and privacy in transactions. Smart grids may aim to handle the pricing of energy, the computation of the amount of energy used or both in a secure and private manner. However there exist several implementations of smart grids that are decentralized using blockchain technology such as those using consortium blockchains, multi signatures and ethereum smart contracts. The concept of smart meters and charging pile sharing to improve load distribution on the grid are also discussed. In this paper we aim to identify the advantages and challenges that the various implementations of blockchain in smart grids present to the users and the energy market.**

I. Introduction

A Smart grid is a semi-manual system of interconnected and networked components which use bi-directional communication devices for trading energy. Energy flows in one direction and the compensation for the energy supplied flows in the other direction. Each device that is a part of smart grid is either a consumer, an entity that only consumes energy or a prosumer, an entity that both produces and consumes energy. The energy that is widely distributed is tracked through a connected network of smart meters that are used to both track the consumption and hence for the estimation of the requirement. These smart meters enable the consumers to send requests for energy to the grid whenever required. This request may be accepted by a mediator who finds a prosumer to supply energy to the user who sent in the request. The identities of both the parties remains undisclosed and information about amount of energy supplied or used is maintained only by the mediator. Due to the anonymous nature of the transaction, we need to maintain authenticity of transactions occuring on smart grids. The method discussed here is one using blockchain technology.

Blockchain technology refers to a distributed ledger of multiple transactions where the total amount of cash or tokens is fixed. It is monitored universally by a relay of hashed transactions that can be verified and re-iterated by those who are joining the system in a later period of time. The blockchain technology has been in use and news for its application in cryptocurrency systems. However, in a more recent set of applications, it is being used for maintaining and book keeping anonymous transactions across difefrent industries. Several people and organizations are actively trying to introduce BlockChain technology to Smart Grid systems.

A. Disclaimer

In this paper, we are analysing different technological and implementational details to opine on the overall feasibility of execution. The reader is requested to read through all the cited papers to get an exposure on authors' perspectives for themselves. We highlight and quote the papers, only for the purposes of context and analysis.

B. Terminology

In this section we iterate the most commonly used phrases and terms to describe components and events in blockchain for smart grids.

1) *Blockchain* : Blockchain is a series of connected blocks of data that contain information about transactions occuring on a network. This chain of blocks is created by adding blocks whenever new information is generated. The process of adding blocks to blockchain involves sending out a request for the said transaction after which users of the blockchain verify the authenticity of the transaction using a method called consensus. Once consensus is reached the block of information is added to the blockchain. Blockchain presents us the unique feature of being immutable. It means that once a transcation is added to the chain, it can't be changed by any malicious user. Another advantage of blockchain is that there is no central authority governing it meaning that it is decentralized and no single entity has the authority to change anything in the blockchain.

2) *Smart Contracts* : One way to use the blockchain is by developing a smart contract which specifies the needs and demands of the counterparties.[5] Once the aforementioned parties reach an agreement, a smart contract can be authored which can sent to the consumer in exchange of currency. The new blockchain network developed by Ethereum that is blockchain 2.0 is one that supports smart contracts and allows users to deploy their own contracts using their personal blockchain called a testnet. Platforms like truffle and solidity can be used to initialize the code for smart contracts whereas the front end can be develped on platforms such as Node.js. Adding a smart contract to a blockchain follows the same concept as adding data to a block on a blockchain once the transaction is verified by consensus.[6] Ethereum has introduced certain changes in the structure of a block to accomodate a smart contract. Apart from the difficulty level, nonce and hash value corresponding to the merkle tree of the blockchain, a block here contains the terms gas and gasLimit. These terms determine the reward to the miner by simply taking the product of the computation power appied and the gas per unit specified in the block. If this product is greater than the gasLimit then the transaction cannot be added to this block and has to find another block to which it can be added. A block is like a piece of land and a spot on that piece of land comes at a price which is the reward that a miner earns.

3) *Consortium Blockchain* : A consortium blockchain [4] is a blockchain where the consensus process is controlled by a pre-selected set of nodes. We choose the consensus according to requirement and not according to preset rules.

4) *Tokenized Energy* : From the prosumer's point of view, it is not their concern who uses the energy they are selling. As long as they generate one unit of energy they should get paid for it. Let's say the fundamental unit of energy currency in blockchain for smart grid be energyCoin. The blockchain enables payments by rewarding say 1MW of energy produced by one token of the energyCoin which can traded on the energy currency market.

5) *Workforce Abundance* : For any technology to be built, we need both of thinkers and workers. They constitute the workforce. The proportionality of thinkers is more than workers where the role of strategy in the technology is dynamic. On the contrary, the workers are needed more for construction and maintenance of the technology.

   Similarly, the level of expertise is broader and specific. For example, if we have more Java developers than Python developers, an Android project can be made more easily. However, if we have more Python developers than Java developers, text mining could be done competently. Workforce Abundance talks about the proportionality of workforce requirement in the market vs workforce availability and the proportionality of thinkers and workers in the available workforce. Ideal workforce abundance means to have workforce that meets the requirements with required proportionality of thinkers and workers.

C. Motivation

There exist several implementations of smart grids using blockchain technology, each with its own perks and shortcomings. In order to have some semblence of techniques that might be used in the future to implement smart grids, we need to know the conditions in which a particular technique may be applied. This enables us not only to locate chances of improvement but also the degree and choices that we can make during execution and deployment. Having varied opinions over a topic is always welcome but nomenclature, hypothesization and organization of components, events, triggers and pitfalls can help us prioritize different aspects of a common goal. There is always a gap between knowledge and experience, theory and implementation, ideality and practicality. One of the scientific ways of approaching the problem of deployability is domain based study.

Smart cities are the objective of the future and to successfully develop a smart city, one must have the knowledge of the ways in which energy may be supplied in the smart city. Smart grids provide a solution to the problem of energy supply in smart cities, may it be the operation of electric vehicles or home appliances. V2G networks are an alliance of smart grid technology that work under the co-domain of smart-cities and smart grids but are also the fore-runners of VANETS. Successfully handling the load on the city's power grid is one function of the underlying blockchain technology. Another functionality provided by the blockchain network would be the security and privacy in transactions of energy. Anonymity and trustlessness are the added benefits offered by the blockchain technology. In the end the vehicles form a huge demand and actively work as a consumer more than a prosumer. So in order to keep up with the demands of the future a study on the various implementations of smart grids is necessary.

D. Research Contributions

In this paper, we introduce the reader to the fundamental concepts of various aspects of smart grids, blockchains and the cross-domain functionality and feasibility of these entities in real world.

E. Organization

The rest of the paper is outlined as follows. In Section Blockchain ChoicesII, we present the different schemes of block chain deployment in smart grids. We present the proof mechanisms in Section Choices in ProofsIII The next section Alternatives to Blockchain IVexplores the scalability aspects of blockchain and feasibility, should we choose to move on from the blockchain system. The paper concludes in final sectionV.

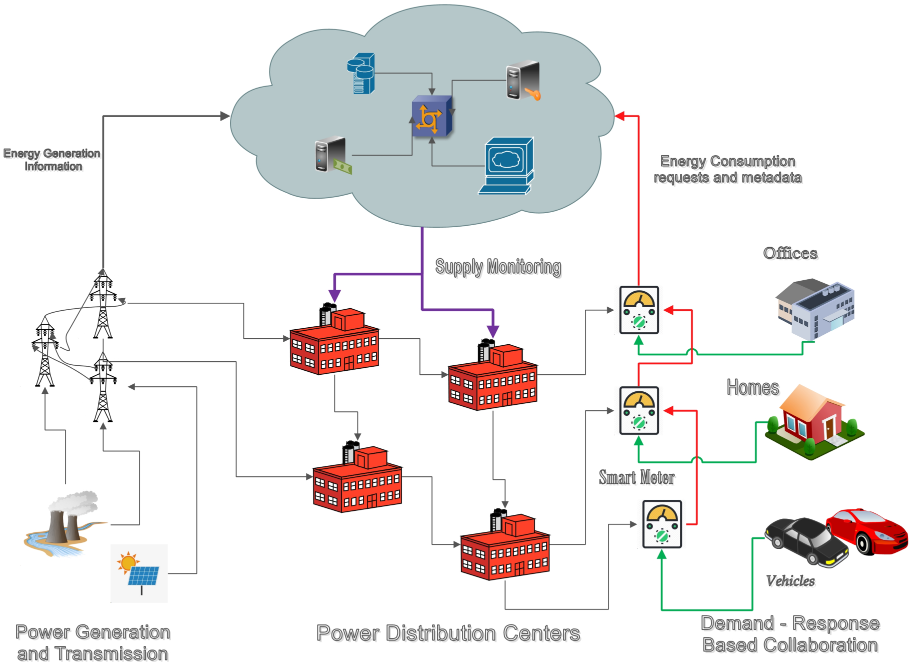
Energy Generation Information
Energy Consumption requests and metadata
Supply Monitoring
Offices
Homes
Smart Meter
Vehicles
Power Generation and Transmission
Power Distribution Centers
Demand - Response Based Collaboration

Fig. 1. Smart Grid

II. Blockchain Choices

In this section, we shall discover the early attempts at smart grid communication and blockchain integration.
Several early attempts were made by computer scientists based on distributed database systems and cloud enabled stream monitors for record keeping and transanction monitoring.**??** The proposed ideas in this approach are compatible with existing sources of infrastructure and workforce abundance is ideal but are also centralized and not universally auditable. There are pressing concerns about privacy and anonymity.
The blockchain based model guarantees immutability, non-repudiation and decentralization. Hence we have different models of blockchain to consider for smart grids.

1) GridMonitoring technology using a sovereign blockchain.[2]
2) PriWatt technology using multisignature schemes.[3]
3) PETCON using consortium blockchain.[4]

A. Sovereign Blockchain

In this system, the ledger is a sophisticated, secure and sovereign blockchain of transactions. It contains an ordered list of transactions with unique and indisputable timestamps.

1) Overview: [2]

(a) Each component is given a unique id in the network. They are functionally distributed into processing nodes and consensus nodes. There are multiple threads of blockchain in the network, with each identified uniquely using a consumers identity.
(b) The processing and consensus nodes are entirely responsible for processing events into blocks and broadcasting blocks into the sovereign blockchain network.
(c) 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.
(d) While monitoring the blocks, parent and side ones included, nodes alert the system when breaches to the agreed use of data occur.
(e) The paper proposes using public key encryption system. It consists of consumer private key, consumer public key and authenticator contract key for smart contracts.

2) Advantages of the approach: The paper proposes a set of new ideas for the deployments.

(a) *Layered Structure* : The most applaudable feature of this approach is the layered structure of the proposed idea. Multiple independent and pluggable resources can be used to swap out and swap in the given system. It gives the architecture, a room to improve and scale in the future. The general hierarchy described in the paper allows for a cross-layer diagnostics and cross-domain functionality.
(b) *Parent and Side blocks* : The description of the parent and side blocks in this paper inspires us to level the granularity. The clear and pointed description of the diversity and versatility of blocks helps in creation of data

objects and control objects in the coding environment. The object-oriented approach and given the immutable nature of transactional records can help us quickly diagnose abnormalities. Furthermore, estimation of memory and bandwidth can be planned in advance.

(c) *Smart Contracts Algorithm* : The algorithm proposed in the paper is one of the few concrete examples in favor of deployability and execution of the blockchain. The algorithm has a small memory footprint with respect to packet sizing, code size and is more event driven. This is in favor of applying the idea for a V2G network inside a smart city.

3) Shortcomings of the approach:

(a) *Scalability and Access Control* : The approach highlighted is restricted in terms of scalability. The existence of smart contract database with single signature is not in accordance with distributed computing. The history of cryptocurrency systems are full of insider jobs, anonymous thefts which are publicly claimed to be external manipulations and compromises. Coming back to scalability aspect, it is not possible to append every transaction with a sign of approval from the organization. If we were to trust a single authenticator, there are security concerns as we see next. We need to be vigilant against malicious workforce.

(b) *Security and Single point of Failure* : At its core, the cryptocurrency like system is flawed due to the existence of single private key. It may lead to single point of failure. If we were to allow signatures of authenticator, we need to have multiple signatures for authenticator and frequent rotation and randomization of said signatures. Generating keys offline is a possible solution but it is favorable to avoid such misdirections (possible lack of randomness in key generation induced by malicious insider) in the power grid systems for maximum security. We need to guard against signature foregeries inside authenticating systems in a trustless escrow. One possible solution here is multi-sig.

B. PriWatt's MultiSignature

In this system, the blockchain can be any implementation, so long as it supports anonymous message/transaction streams, ownership transfers and infrastructure for multisignature encryptions.

1) Overview: [3]

(a) It is a completely trustless system although a semi trustless flavor can also be implemented.

(b) It supports microtransactions and works with any system of pre-existing blockchain technology.

(c) The blockchain is controlled through collective voting of anonymous nodes. Hence the system demands an additional feature of nested blocks.

(d) There exists a support for transaction revocation and refund.

(e) The paper proposes using proof of work based system.

2) Advantages:

(a) *Prevention of double spending*: One of the well known ways of prevention of double spending is checking the transactions along the blockchain. In PriWatt too, the conventional checking mechanism is present. However, there are two forms of attack, that are ppossible : double-spending of energy token T from the customers side and double-spending ownership of an amount of energy from the suppliers side. PriWatt uses nested blocks and locking mechanisms to prevent double spending.

(b) *Support for microtransactions*: The systems of payments in installments and credit require a feature of microtransactions. The most significant contribution of this paper is the suggestion of structure and design of a microtransactional system. This enables quick access to energyCoin in small amounts and as a continuous deterministic event as opposed to single event perspective.

(c) *Support for ownership transfer and multisignatures* : The multisignatures allow for more security. The paper discusses in detail how different types of attacks can be mitigated. All those are majorly a consequence of multisignature based system. Ownership transfers enable the system to handle dispute management and refunds more efficiently.

(d) PriWatt forces users to generate new messaging addresses for each new trade negotiation in order to preserve anonymity.

(e) The Attack tree in the paper takes care of most of the well known security threats.

3) Shortcomings of the approach:

(a) *Complex data replication procedure and scalability* : The system is too complicated in terms of data replication at requirement and in multiple sites. This becomes worse as the data to be replicated increases due to multiple organizational factors in the proposed system.

(b) *Workforce issues and self healing* : The requirement of technically adaptive workforce is a relative shortcoming in the proposed system. Any breakdown of the system despite the continuous monitoring requires a team of people to diagnose the issues as there is no in place mechanism for self healing. The system itself is complex to build in the first place and needs constant vigilance during deployment.

C. PETCON : Consortium Blockchain

Let us now explore the feasibility of Consortium blockchain in the domain of Smart Grids. PETCON stands for P2P Electricity Trading system with COnsortium blockchaiN (PETCON).

1) Overview: [4]

(a) It expands the knowledge and domain of Smart Grid culture to V2G systems. The plug-in Hybrid Electric Vehicles (PHEVs) are the point of focus. The efficient utilization and conservation of energy in mobile stations is a pressing concern that needs to be addressed.

(b) The PHEVs can charge up their batteries at social hotspots such as parking lots and charging stations (analogs to petrol pumps). However, they can also be incentivised to discharge for cash or other credits at these junctions.

(c) The PHEVs play different roles in localized Peer-to-Peer electricity trading at hotspots: charging PHEVs, discharging PHEVs, and idle PHEVs. Each PHEV chooses its own role according to current energy state and driving plan.

(d) Each charging pole with a built-in smart meter calculates and records the amount of traded electricity in real time. The charging PHEVs pay to the discharging PHEVs according to the records in the smart meters.

2) Advantages:

(a) *Completely trustless system* : The system is robust and reliable due to the implementation details being transferred fast without relying on a single trusted party for authentication. Due to the iterative double auction mechanism, PHEVs only submit bid prices to the auctioneer without private information during trading. It is inarguably the most significant feature of this system.

(b) *Duality in transaction* : The novel idea of conversion of energyCoins to energy and vice-versa hints at a larger expansion role of this technique analog to how bitcoin works for cryptocurrency. It makes for an increased potential for execution in real world.

(c) *Accounting for more coins* : The conventional bitcoin type prefers a closed system of coins which reduces inflow of cash as necessary and doesn't account for any kind of inflation and deflation in currency. The energyCoin described by this scheme accounts for more inflow of cash. This means that the miners of the energyCoin can be constantly or incrementally incentivized for creating blocks and verification.

3) Shortcomings of the approach:

(a) The influx of new energyCoins opens up a different set of problems previously undiscovered in the cryptocurrency system. We don't have sufficient information on this kind of system. The current establishment of cryptocurrency increases or decreases the value of existing bitcoin while the proposed idea demands inclusion of new coins. It is not shortcoming of the approach but in general, makes the approach relatively distant from implementation

(b) The double auctioning system is a compromise between reliability and efficiency. Until a better system is found, the implementations are limited by the potential of the computational device involved.

(c) The system doesn't account for the amount of energy used for mining the data. Currently the blockchain based systems are not energy efficient. If the given system can accomodate on the energy requirements of mining process, that could make the system proposed into a closed circuit of energy expenditure.

III. Choices in Proofs

In this section we shall explore the different aspects of using blockchain proof systems and their feasibility in Smart Grid systems.

A. Proof of Work

In the section before, we had discussed various blockchain mechanisms for security of Smart grid systems. In all of these systems, Proof of Work (PoW) is the common mechanism to ensure the verification. In proof of work style of contribution, every miner is required to find a hash to the block that they have created using a nonce. The restriction on hash could be a fixed number of zeroes as prefix. Generating the hash with required number of zeroes as prefix takes a lot of trial and error with nonces.

The question is how will it help for the security of the system. The work done by a miner helps in creating a delay which is random. With a difference in finding success by creating hashes, the miner gets to prove his work for the mining incentive. Since hashing is a one way function with an avalanche effect, getting a block with a nonce that hashes upto given restriction on hash is randomized in probability. These techniques have proven to be helpful in dealing with denial of service attacks, maintaining integrity of the blockchain and as seen before in II-C, avoiding double spending.

The primary disadvantage of proof of work style is that the computation made during hashing are as useless as watching paint dry on a wall. The amount of energy and memory spent on proof of work could have been spent on anything more productive.We cannot simply introduce proof of work into smart grid systems on account that energy grid needs to spend a significant amount of energy for miners or risk integrity and security. Although some variations such as PrimeCoin help the system to investigate on new primes with a specific property.

The next big problem using proof of work is the 51% attack. Here if 51% of the existing userbase is compromised, then the whole grid will be compromised. Since energy hotspots are likely to be targets of malicious attackers, deploying this sort of system in a public system is disastrous in consequence. The attackers would be able to prevent any and all new transactions being verified, control the transfers in the grid and allow themselves to double-spend.

B. Proof of Stakes

As aforementioned in III-A, the energy required for mining (verification of a block) is extremely energy inefficient. According to recent estimates, the cost of mining one block is as much as 1.55 times of energy consumed in American household per day. In terms of smart grid, a user might be in dilemma and less likely to mine given the cost leading upto what is commonly referred to as tragedy of commons. To avoid this problem, proof of stakes is introduced.

In Proof of Stakes, the miner is restricted to mine a portion of transactions that is indicative of their stakes in ownership. This reduces the chance of fifty-one percent attack. The main focus of 51% attack is to compromise the system and gain advantage over the system. For an entity with 51% in PoS based systems, it needs to own 51% of the shares. It is not in the interest of the owner of 51% shares to attack the system due to their commitment of stakes.

The major disadvantage of Proof of Stakes is that we can never be sure about consensus. Proof of Stakes, at its core, doesn't guarantee consensus. People committing to a coin stake can vote for multiple forks of a blockchain, mine easily to their advantage and occassionally double spend. In Proof of Work, voting for multiple forks is disadvantageous due to the fact that it reduces the probability of finding a hash. Although, in real life, the lifetime of a fork is very less, implying that consensus is being practically achieved. In theory, since consensus is not guaranteed, we must be cautious nonetheless.

Proof of Stakes brings up a distribution problem in that in the strategy, the money can get accumulated in one person's wallet and that will lead to shut down of the system. In terms of smart grids, this would mean that if played strategically, a person can single handedly control all the energyCoins and never release them. Even if the energy is generated, this person has highest bids to own it all creating a surplus of money or energy in one single location.

C. *Proof of Activity*

Proof of Work allows 51% attack and Proof of Stakes allows hoarding of energyCoins. Proof of Activity tries to being best of both previous attempts and reduce energy costs. In Proof of Activity, the mining starts out as any flavor of Proof of Work where miners are equally competent and competitive to outpace each other in creating and appending a new block to the blockchain. Once a block is successfully mined, the system switches to Proof of Stakes approach, where each block has miner's reward address and a header. In the next round, based on the header details, a new set of validators from the blockchain network are chosen who are required to verify and validate the newly created block. The more energyCoins a user owns, the higher the probability of them getting chosen as a validator in the system. In smart grid system, they may be supplied additional energy for mining. The block is added to the chain only when all the validators agree.

The major problem in this approach is that it uses same if not more energy used by Proof of Work approach.

There exist several flavors of aforementioned protocols to sustain a smart grid. In this paper, our goal is only to introduce and analyze different implementable ideas. The reader is encouraged to explore these flavors per necessity.

IV. Alternatives to Blockchain

One of the pressing hurdles of Blockchain is its portability. Every miner and user needs to have a complete record of all of the blockchain. As of third quarter of 2018, the size of Bitcoin has reached 184 GB. This shouldn't be much of a hassle for limited userbase but for potential application to large populations such as India or Brazil, this is definitely a concern that needs to be addressed. The chain will grow with a higher order of number of users and number of transactions. Even the higher amount of energy demand is pointing us towards finding an alternative especially when extending the smart grid to accomodate V2G and IoT networks where there are mobile entities like vehicles and drones with possibly multiple ownerships.

One of the more recent advances that can help us mitigate the disadvantages of blockchain is moving from blockchain itself. Tangle™[8] is a new innovative idea that shrinks computational space by allowing multiplicty of children for given block. A tangle is the name given to a directed acyclic graph as opposed to a linear chain used by blockchain. In a tangle, each transaction validates at least two other transactions. We need to emphasize on the minimum requirement of at least two transaction sites because if we restricted it to just one, the system would default to a blockchain with transactional capacity of one. Such a system would be extremely inefficient. When a new transaction is added by a vehicle by validating two existing transaction but before it gets validated by any transaction, it will be called a cache tip. The addition of tips actually validates at least two previous tips, which means the cache speeds up as more vehicles join the system. This is especially convenient for blocks that are created by a mobile entity and needs to be verified quickly.

Another alternative is EOS based model. EOS concentrates on creating a custom operating system and environment necessary for the cryptocurrency like ledger based formats. As of August 2018, the project is open source and is under incubation period. It is too early to predict the advanatages and ramifications of such system and its impact on smart grid systems.

V. Conclusion

In this paper, we have discussed different aspects and research initiatives, contributions and shortcomings in those aspects. We expect that we have provided sufficient introduction to the user about the implementation and challenges of introducing blockchains in smart grid. We recommend the reader to explore the cited papers themselves and choose the approaches according to the requirements.

References

[1] 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. 483488.

[2] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, G. Dong,"GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid",Special Section on Cloud and Big Data based Next Generation Cognitive Radio Networks, 2018, pp. 9917-9915.

[3] N. Z. Aitzhan, D. Svetinovic,"Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 15, NO.5, 2018, pp.840-812.

TABLE I
SUMMARY OF BLOCKCHAIN CHOICES

Parameter	Grid Monitoring	PriWatt	PETCON
BlockChain Mechanism	Sovereign Blockchain	Flexible	Consortium BlockChain
Security	Public Key Encryption	Trustless, PoW and Attack chart based	Semi-Closed system and double auctioning systems
Layered Architecture	Yes	Restricted	No
Scalability	Semi-scalable	Not scalable	Scalable
Domain	Closed grid V2G systems	Microtransactional systems	Open grid V2G systems
Advantages	Block variation and Object Oriented Model	Ownership and multisig system	Transactional duality
Disadvantages	Rigid Access Control and Single Point of Failure	Complex data replication procedure and auditing model, weak self healing	Fluctuating record of energyCoin

[4] J. Kwang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain,”Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchain”, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL.13, NO.6, 2017, pp.3154-3164.

[5] A. F. Castellanos J, D. Coll-Mayor, J. A. Notholt,”Cryptocurrency as Guarantees of Origin: Simulating a Green Certificate Market with the Ethereum Blockchain”,5th IEEE Conference on Smart Energy Grid Engineering, 2017, pp. 367-372

[6] C. Lio, K. K. Chai, X. Zhang, E. T. Lau, Y. Chen,”Adaptive Blockchain Based Electric Vehicle Participation Scheme in Smart Grid Platform”, IEEE Vol 6, 2018, 25657-25665.

[7] Y. Hou, Y. Chan, Y. Jiao, J. Zhao, H. Ouyang, P. Zhu, D. Wang, Y. Liu,”A Resolution of Sharing Private Charging Piles Based on Smart Contract”, 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, 2017, pp. 3004-3008.

[8] S. Popov , ”The Tangle version 1.4.3”, IOTA™, 30 April 2018.