Seamless Grid: an off-chain model proposal for scalable P2P electricity markets and grids management

Fabrizio Bruno Armani, Francesco Grimaccia, Sonia Leva, Marco Mussetta
Department of Energy
Politecnico di Milano
Milan, Italy
fabriziobruno.armani@polimi.it, francesco.grimaccia@polimi.it, sonia.leva@polimi.it, marco.mussetta@polimi.it

***Abstract* — The increasing interest shown in Blockchain Technology in recent years has involved also the electric energy sector which is seeking new solutions to manage the rising penetration into the grid of Distributed Energy Resources (DERs) and Demand Response (DR) users and their secure operational integration into the electricity markets. The participation of small distributed resources to a Peer-to-peer (P2P) electricity market running without the intermediation of a trusted third party represents an additional challenge for which the research has addressed Blockchain as a possible game changer solution. This work aims to propose a model based on Bitcoin Blockchain and the Lightning Network - an off-chain second layer protocol - in order to manage fast and secure transactions of electricity in a prototype 3 nodes grids. This model represents a novel solution that, even based on a solid blockchain system, can overcome the intrinsic trustlessness versus scalability limits that affects traditional public blockchains.**

***Keywords*—Blockchain, Distributed Energy Sources (DERs), Lightning Network (LN), Off-chain, Peer-to-Peer electricity market**

I. Introduction

Blockchain paradigm – begun with the introduction of Bitcoin in 2008 [1] – represents one among the most actual and promising technology in computing science. From a definition point of view, a Blockchain is a distributed ledger constituted by an append-only data structure organized in blocks. Each block is cryptographically bonded to the previous one through a chain of hashes and contains cryptographic messages called transactions. The blockchain is managed by a client program installed in each node device and which communicates with the other node of the network through some communication protocol (usually – but not limited to - the Transmission Control Protocol/Internet Protocol (TCP/IP).

Each node performs – in an independent way from the other nodes – three main tasks:

- Communicate and forward transactions and blocks to the other connected nodes forming the Peer-to-Peer (P2P) network.
- Enforce the rule of the protocol on which the blockchain is based regarding transactions and blocks. Transactions and blocks which don’t comply with the protocol rule of the node are rejected and not broadcasted to the other connected nodes.
- Store a complete and updated copy of the blockchain including the most recent and compliant blocks.

In particular, each node enforces a so-called Consensus Rule through which it can decide what is the most updated blocks of the chain and thus the complete history of all transactions from the beginning of system operation. This rule guarantees that, within some finite time interval, all the nodes enforcing the same protocol, independently, reach a consensus on a single history of the transactions. Several mechanisms have been conceived to guarantee the distributed consensus: among the most important ones we can find Proof of Work (PoW) [2] adopted in Bitcoin which is based on competitive computation between nodes (mining), and Proof of Stake (PoS) which is based on the quantity of underlying availability of assets owned by each node. The consensus rule together with the other properties of the blockchain enables multiple parties to transact or do business without needing a third intermediary party which is usually appointed to check transaction for double spending.

As in many other industrial sectors, also the energy field have been deeply considered for potential blockchain applications and case studies. Recently in [3] a use of Blockchain for self-consumption and local energy communities is proposed to support the energy transition and the development of renewable energies. The paper introduces a blockchain-based solution tailored for solar energy sharing to manage the exchanges according to a set of community rules. The system needs smart metering infrastructures installed by the Distribution System Operator (DSO), considered as the trusted party for energy data.

978-1-5386-4722-6/19/$31.00 ©2019 IEEE

As the need for RES integration is becoming more and more essential, energy trading platforms are being developed and established in the microgrid framework. In this light microgrids have introduced a variety of applications and innovative solutions for efficient system maintenance. In [4] for example a blockchain-based smart home is proposed in order to manage data and information flows. In the last year other attempts in supporting the blockchain potential in energy transaction management have widely explored also in vehicles charging, carbon credits and digital networks [5-8].

In [9] an Ethereum Blockchain is proposed to be used as a platform for tokenized Guarantees of Origin (GoO) trading for variable pricing strategy in future electric market. The energy market in fact represents one of the most suitable contexts for an effective use of blockchain paradigm and P2P trading mechanisms [10-12].

Among all possible applications envisaged in the last years' literature, due to its innovative design as a distributed and decentralized information system, blockchain see its greater potential in contexts where prosumers participate in local electricity markets, microgrid systems or smart city frameworks using the internet technology [13-15], [24-26].

As an additional feature, blockchains allow to have distributed networks where non-trusting members can interact in a peer-to-peer manner without a trusted intermediary, using smart contracts or scripts that are built-in in the blockchain itself, allowing the automation of multi-step processes and potentially exploiting the future IoT services [16].

This paper aims to describe a new proposal that exploits a quite recent development of Bitcoin technology, namely the Lightning Network (LN), and to propose a suitable additional layer to manage secure electricity transactions and payments of electric energy, possibly enabling P2P electricity market models. The adoption of Lightning Network technology is used in order to overcome the intrinsic scalability problem of the Bitcoin Blockchain. Morevoer this model exploits the features based on a digital scarce asset working as a backbone for transaction according to a *management through payment* approach.

II. BLOCKCHAIN SCALABIITY , DECENTRALIZATION AND INTRINSIC VALUE TRADE-OFFS

Two important and intrinsic properties of blockchains should be focussed before addressing to the main topic of this paper. The first one is represented by the scalability of the blockchain model and the second one by the nature of the cryptographic messages brought by each transaction, namely digital intrinsic value in case of cryptocurrencies or a representation of some other asset (e.g. an electric kWh).

A. *Scalability versus trustlessness*

Starting from the first topic, the size of the blockchain is determined by the maximum size of the blocks allowed to be constructed by validating nodes then checked and appended by each node to its local blockchain copy. This property has an immediate and clear impact on the number of transactions that each block can store. In addition, the average time of confirmation between blocks is kept fixed in most of blockchain models (e.g. 10 minutes on average in Bitcoin) and controlled, for example, through mining difficulty adjustment updates in PoW blockchains. This fact clearly contrasts with the scalability of the blockchain itself i.e. the number of transactions that the protocol can process per unit time in a complete way from broadcast to inclusion in blocks. For example, looking at electricity market applications, where the potential P2P transaction rate between prosumers is going to grow several orders of magnitude and the speed of ancillary services requirements is high, this property represents a really stringent limitation (taking as an example the maximum 7 transactions per second as standard for Bitcoin Blockchain).

Actually, depending on the kind of blockchain, this issue can be addressed differently. In public blockchains - where anyone is free to join the various distributed activities that the protocol allows - the great exposition to external source of attack, the complexity to implement widely accepted modification on the protocol hard rules, and – definitely – the intrinsic decentralization, prevents these systems from sudden and deep changes and thus easy scalability. Indeed, hard modifications such as the change of block size or confirmation time could endanger the whole security model and thus the complete trustlessness of the blockchain. In particular, any modification of the code aimed at the increase of the blockchain size can burden the nodes with limited computational performances and definitely leading to more centralization of the blockchain. Any high impact modification on the blockchain protocol instead should be carefully evaluated, tested and agreed upon the broader community of users, developers and miners.

On the other hand, the so called private/permissioned blockchains can achieve almost unparalleled time efficiency and scalability performance as well as flexibility in code modification according to present and future needs of the use case they are built for. However, these features are achieved at the cost of relying upon a trusted third party - also in the form of a group of *federated users* - that is entitled to choose the rules of the blockchain, to select which trusted node can join and/or validate the blockchain, and basically to decide upon every aspect of the blockchain governance and development. Potentially the trusted third party can even reverse the history of the transaction up to some point or impose some other changes without the agreement of the network. In general, this kind of systems run in an environment that doesn't need to be completely trustless anymore and can be categorized under the wider group of Distributed Ledger Technologies (DLTs).

B. *Intrinsic value incentive mechanism*

A second major issue to consider regards the intrinsic value that can be carried by the blockchain. Indeed, in public PoW blockchains, which are based on cryptocurrencies, the scarce digital value exchanged in transactions provide a well-designed economic incentive scheme based on feedback that allows the blockchain to safely operate. This incentive scheme runs through the role of the following groups of actors:

- *Developers' community* writes code and maintain blockchain node client implementation according to the protocol rules (for one of the most used implementations in Bitcoin see [17]): they solve bugs and possibly add new features to the blockchain thus creating a robust environment for users and miners.
- *Users*, by using wallet software, sign and broadcasts transactions trusting the decentralized nature of the blockchain as a medium for exchange digital value in a trustless way.
- *Miners*, following the coded protocol rules, collect transactions and put them into blocks trough competitive process based on computational effort. They are rewarded trough transaction fees and minting of new cryptocurrency (block reward) up to the maximum quota hard-coded in the protocol; in a second time this reward can be injected in the economic system as a new value to pay goods and services, including electricity.

The intrinsic digital value operates as a real fuel for the proper and honest operation of the whole system and of its security model based on the Consensus Rule: well written and maintained codes push the adoption of the blockchain by a greater number of users which, in turn, need their transaction to be secured by miners. In PoW blockchains, miners use physical electricity to feed their computation hardware in a competitive environment validating blocks proportionally to their computational power. If a miner behaves in a dishonest way, for example trying to double spend some transactions or creating malformed blocks, the P2P network will reject its blocks by not including them in the updated blockchain local copy of each node, thus preventing him from collecting block rewards.

From an economic point of view, it is clear that an attempt to attack the network results in wasting of electricity and missing in recovering hardware capital costs. On the other hand, if a greater attack is carried by more than half of the computational power in a combined way (51% attack) [18], the security of the chain could be compromised in the long term, and users and developers will soon abandon the use of the blockchain leading to a sharp decrease of value of the cryptocurrency. In fact this outcome is realized at a very high cost by attacker miners.

It is worth nothing how the electricity consumption acts as a bridge between a physical world scarcity and the virtual scarcity of a digital assets enforced by the protocol rule in addition to hardware costs: these constraints lead rational economic actors to follow the Consensus Rule thus enhancing the security of the chain, boosting development effort and adoption in a circular way. On the other hand, when a blockchain carries a completely digital representation of another asset, the economic incentive to follow the Consensus Rule is not straightforward anymore - especially in an adversarial environment - and must rely on other form of trust. In this case, private blockchains are immune of this kind of issue; nevertheless, the representation of a digital assets is possible through embedding data information in a cryptocurrency blockchain transaction, for example through notarization or with smart contracts which exploit the security mechanism of the underlying blockchain.

It is useful to resume the main points discussed before:

- Digital scarcity achieved through robust protocol rules and a scarce underlying digital value connected to a scarce physical good provide economic incentives to run resilient blockchains exposed to public access and thus adversarial environment guaranteeing security and trustlessness.
- These features lead to a very heavy and rigid structure which is difficult to scale-up and increase in size at the cost of compromising consensus and security model.

As in any field of science, we always face an unavoidable trade-off driven by physical limitation: in this case scalability represents a trade-off with respect to security and trustlessness issues.

In accordance with these properties we decided to focus on the Bitcoin Blockchain thanks to its high degree of resilience, decentralization and trustlessness demonstrated during almost ten year of continuous activity. Nevertheless, the discussed scalability issues prevent the direct use of Bitcoin Blockchain for fast electric energy application as those of P2P market. However we need to exploit the payment of electricity services through bitcoin payments which are embedded into the blockchain mechanism and not directly trade kWh or other forms of energy assets.

In order to overcome public blockchains trade-offs we will make use of a system that is built on-top of Bitcoin. This kind of solutions, known as off-chain systems, is bonded to the security of the first blockchain layer (L1) but is decoupled from it regarding many cryptographic operations such as routing of messages and instant digital value transferring. In Bitcoin, one of these second layer (L2) systems has been named as the Lightning Network.

III. THE BITCOIN LIGHNING NETWORK

Lightning Network (LN) represents one of the most promising attempts the Developer Community has addressed to overcome scalability limits of Bitcoin Blockchain [19]. This second layer protocol [20] provides the possibility to achieve nearly immediate and multiple transactions between two parties without the need to wait for their inclusion in blockchain blocks. This achievement is realized through a client node software – a LN client, available in different implementations [21-23] – which provides the possibility to create a particular transaction that locks a fixed amount of bitcoins between two parties. These funds - locked through a blockchain transaction between the nodes' parties called opening transaction - constitute a so-called *bidirectional payment channel* (see [24] for a detailed overview on the topic) that tracks how many funds each party has committed in this shared account: basically, a payment channel can be considered as a smart contract written on Bitcoin Blockchain.

After channel opening, the two nodes can subsequently transact the bitcoins contained in the channel between them.

However, in this case they don't need any more to register each transaction into the blockchain, but - respecting the amount committed at channel opening - they can update the channel balance (the so-called channel state) by modifying the amount each party is virtually in possession off. The off-chain payment is performed through a system of cryptographic messages called payment requests or receipts: receipts are issued by the payee party and signed by the payer and contain cryptographic signatures, quantity of bitcoins transacted, nodes address information and a freely completable field identified as *memo field*.

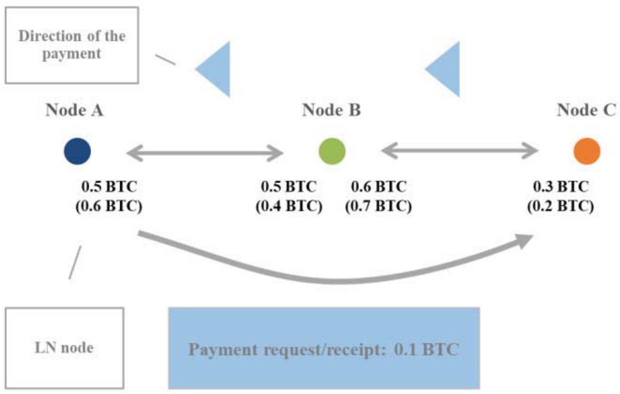

Figure 1. Representation of a LN multi-hop payment forwarded through two channels. 1 bitcoin (BTC) has been committed in channel A-B: 0.5 BTC put by each side, while channel B-C locks 0.9 BTC (0.6 from node B and 0.3 from node C). If node C accept to pay the payment request issued by node A the payment move the channel balances accordingly to the numbers in round brackets.

After several off-chain transactions, the two parties can eventually decide to close the payment channel by sending a closing transaction to the blockchain. The transaction contains the last channel state that is agreed upon the party and which represents the final settlement of all payments that took place between the two parties. An important security property of LN provides protection against the attempt to reverse channel updates, for example trying to broadcast old states as closing transaction. In this case, the damaged party has the possibility to punish the malicious party by depleting all the funds committed into the channel with a closing "punishment" transaction whose application is encoded within the protocol.

However, the real groundbreaking feature of the protocol resides in the possibility to forward payment through nodes not directly connected by a channel. In greater detail: if two nodes are not directly connected by a channel, LN protocol provides the possibility to route payments through a chain of channels (if available) connecting the two nodes preventing the possibility that an intermediate node can steal the founds in the route. In practice, each channel balance is moved towards the direction of the payment as shown in Fig.1. If only one intermediate node fails in routing the payment, the whole operation doesn't take place: this feature is known with the term *atomicity* and represents the base of these kind of off-chain value transfers. These kind of payments, named *multi-hop payments* are guaranteed by the cryptography which is hard-coded in the protocol of the Lightning Network. As a last economic incentive feature, each node through which a multi-hop payment is routed, can charge a freely chosen fee: indeed, several payment routes could be theoretically available and the chosen route could be the one that provides the lower total fee cost.

IV. THE SEAMLESS GRID MODEL PROPOSAL

Following this theoretical framework of blockchains, intrinsic constraints and potential solutions to those limitations, we can proceed with the description of a Proof of Concept (PoC) model suitable to be applied for P2P electricity market and grid management: we will call it *Seamless Grid*.

For the sake of simplicity, this model has been conceived for a 3 node behind-the-meter microgrid (see [25-26] for more complex microgrids systems and related analysis) which is constituted by three entities (Fig.2):

- Production node (e.g. a PV plant);
- Consumption node (e.g. a domestic load);
- Point Of Delivery (POD) connected to the Distribution Grid.

We will describe the operation of the model following a step-by-step method starting from scratch.

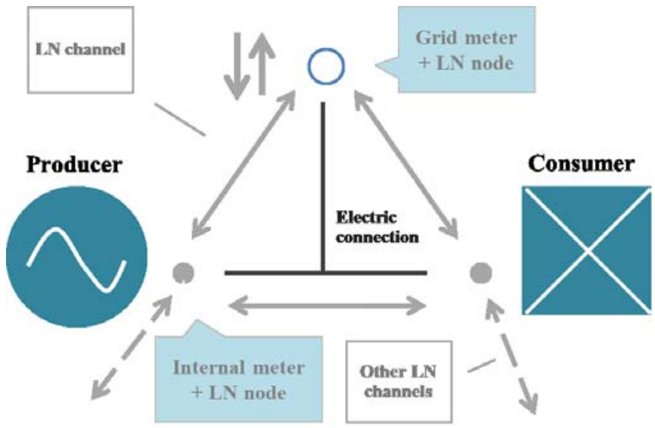

Figure 2. The representation of Seamless Grid model applied to a test 3 nodes microgrid. The other LN channels are necessary for channel rebalancing purposes.

As a first step, every node of this 3 node microgrid is provided with a LN node coupled with a meter: the production and consumption nodes are provided with an internal energy meter, while the POD is provided with a standard grid meter. The meter and its respective LN node are linked by a communication protocol enabling the possibility to register real energy flows and settle them with the payment activity of the LN node.

Each LN node opens a payment channel with its neighbour committing some fractions of bitcoin into the channel. At this regard, it is worth noting that the topology of the LN channels overlays the topology of the underlying physical electric connection. In this way we can guarantee that electricity flows are duly monitored at the lowest possible level.

After channels opening (i.e. the opening transaction is registered into the Bitcoin Blockchain) the system is ready for operation. As an example, we assume that the microgrid need to transact some quantities of energy to be produced and withdrawn in the following day with an hourly granularity (a miniaturize day-ahead market). The idea is that trough a layer 3 protocol (L3) to be designed, some particular Lightning Network (L2) payment requests are broadcasted starting from the production node and reflecting its availability to inject energy into the grid.

The payment requests, besides the cryptographical information of a standard LN receipt such as the bitcoin quantity, the LN node ID and cryptographic signatures, will carry in the memo field some relevant information regarding energy to be produced:

- Quantity of energy (kWh) / power profile (kW)
- Time of delivery
- Issuer grid node ID

Basically, the system is designed in order to "quantize" energy in form of payments requests. These receipts are used only to sell quantity of energy that will be delivered in a future time window according to a *production driven model*. In this way, the uncertainty of the last kWh of production (especially important for RES) is reflected within the receipt and thus made available as a further information to the participants of the market.

Following our test microgrid environment, payment requests are then broadcasted from the production node - that has issued them - to the consumption node following the path of LN channels previously opened. At this point the consumption node is able to chose among two possibilities:

- Sign, thus pay the receipt with the only constraint that each receipt, if payed, has to be accepted atomically (i.e. receipts cannot be accepted partially).
- Discard the receipts it receives forwarding them to the other connected nodes (in this case only the POD node).

The accepted receipts constitute an Over The Counter (OTC) like transaction between the two nodes providing both a price signals and a unit commitment signal (Fig. 3). The payment is made instantaneous by the LN network and correspond to a new balance within the payment channel opened between producer and consumer. At the same time, the signed receipts, stored locally in each node, constitute a smart contract obliging the two parties to inject and withdraw that precise quantity of energy at the delivery time indicated by the receipts. The whole process takes place in a seamless way until the energy delivery time: before delivery the production node can issue any amount of receipts that sells the additional energy of its updated production profile. At the same time, the consumption node will pay or discard receipts issued by the producer in order to match its consumption profile and, as well, it can issue some receipts that sell its excess profile. As an interesting features encoded in the LN protocol, receipts carry an expiration time after which the not accepted requests are no longer valid for payment thus allowing producer to replace them with new ones.

The POD node, on the other hand, has the ability both to issue and to pay receipts that have been discarded or issued directly by the other connected nodes. In this way each node (including production node), through subsequent issuance and payment of receipts, is able to fulfill its real-time profile reducing imbalances as much as possible according to the updated production/consumption forecasts. It is worth noting that, at least in theory and in advance respect to delivery time, each node has also the ability to short-sell some quantity of electricity. At delivery time, all the accepted receipts are evaluated and compared to the real energy flow measured at the meter: the imbalances could be then treated according to a common rule established in the grid. In our PoC a possible solution could be represented by an imbalance receipt issued by the POD meter reflecting the real-time energy price of the ancillary services market. Basically the POD node represents a collector and a last resort source of receipts, balancing the energy flows and thus their payment with the rest of the grid.

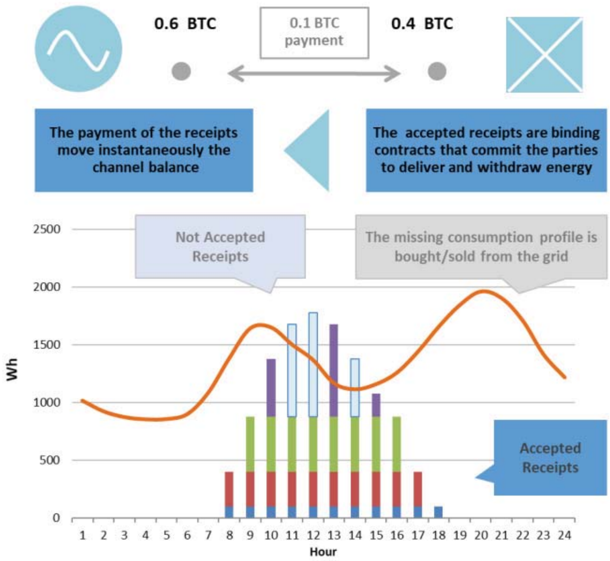

Figure 3. Management through Payment mechanism within the model. The orange line represents the forecast of the consumer's load. Each accepted receipt moves the channel balance from consumer to producer. Not accepted receipts could be broadcasted by the consumer node to the POD node.

Looking to a wider picture, if other nodes at DSO level share the same L3 system, the discarded receipit of our POD behind-the-meter node could be broadcasted and potentially accepted (and reissued as well) by other nodes at this grid level. It is easy to immagine how aggregator nodes, for example those provided with a storage system or those connected with the High Voltage Grid, can continuosly accept and issue new receipts, shifting and re-modulating energy across each hour of the day. Of course the receipts accepted at this grid level would be characterized by a multi-hop payment scheme routed through the chain of channels built among the LN nodes coupled with the electric nodes of the grid. In principle, such LN nodes could burden the energy payments with fees representing a sort of grid charge that may takes also into account the level of energy losses. It is worth nothing that this PoC model fosters the consumption of electricity as close as possible to the production node: above of all self-consumed behind-the-meter electricity.

V. CONCLUSION

The recent growing interest in blockchain technology has involved also the energy sector in applications mainly related to RES integration management, microgrids and new electricity market models. Nevertheless, as treated in this paper, every blockchain system face a scalability vs trustlessness trade-off that cannot be easily overcome by a pure Layer 1 solution.

The Proof of Concept herein proposed, exploiting Bitcoin Lightning Network off-chain protocol features, represents an attempt to manage fast and secure transactions of electric energy through cryptocurrency payment. The combined features of the model can enable DERs and Consumers to transact energy in an effective P2P way exploiting OTC like smart contracts without the interaction of a trusted third party and allowing the couterparties to be protected from credit risk.

The model adoption in complex behind-the-meter microgrids, such as those of the Energy Communities, could be implemented in a straightforward way with an additional software solution which is able to read energy flows directly from the meter. It is worth noting that the multi-hop feature of the energy receipts envisaged by the model can easily and quickly scale its application to wider grid networks.

Finally, following the PoC design described here, the electrity grid can be seen as a "highway" of liquidity that can be used to route also non-energy payments: the only difference would be in the attributes associated to receipts issued and routed from time to time by the nodes.

REFERENCES

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: https://bitcoin.org/bitcoin.pdf, 2008.

[2] A. Back, "Hashcash - a denial of service counter-measure," [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf, 2002.

[3] C. Plaza, J. Gil, F. de Chezelles and K. A. Strang, "Distributed Solar Self-Consumption and Blockchain Solar Energy Exchanges on the Public Grid Within an Energy Community," in *Proc. 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, Palermo, 2018, pp. 1-4.

[4] E. S. Kang, S. J. Pee, J. G. Song and J. W. Jang, "A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid," in *Proc. 2018 3rd International Conference on Computer and Communication Systems (ICCCS),* Nagoya, pp. 472-476.

[5] Y. Wang, Z. Su, Q. Xu and N. Zhang, "Contract Based Energy Blockchain for Secure Electric Vehicles Charging in Smart Community," in *Proc. 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress,* Athens, pp. 323-327.

[6] V. Sharma, "An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV)," in IEEE Communications Letters, vol. 23, no. 2, pp. 246-249, Feb. 2019.

[7] M. J. Ashley and M. S. Johnson, "Establishing a Secure, Transparent, and Autonomous Blockchain of Custody for Renewable Energy Credits and Carbon Credits," in IEEE Engineering Management Review, vol. 46, no. 4, pp. 100-102, Fourthquarter, Dec. 2018.

[8] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, G. Sciumè and G. Zizzo, "An Energy Blockchain, a Use Case on Tendermint," in *Proc. 2018 IEEE 2018 EEEIC / I&CPS Europe*, Palermo, 2018, pp. 1-5.

[9] J. A. F. Castellanos, D. Coll-Mayor and J. A. Notholt, "Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum Blockchain," in *Proc. 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE),* Oshawa, ON, 2017, pp. 367-372.

[10] K. Mannaro, A. Pinna and M. Marchesi, "Crypto-trading: Blockchain-oriented energy market," in *Proc. 2017 AEIT International Annual Conference,* Cagliari, pp. 1-5.

[11] M. Hinterstocker, C. Dufter, S. von Roon, A. Bogensperger and A. Zeiselmair, "Potential Impact of Blockchain Solutions on Energy Markets," in *Proc. 2018 15th International Conference on the European Energy Market (EEM),* Lodz, pp. 1-5.

[12] M. Sabounchi and J. Wei, "Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism," *in Proc. 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2),* Beijing, pp. 1-5.

[13] B. Richter, E. Mengelkamp and C. Weinhardt, "Maturity of Blockchain Technology in Local Electricity Markets," in *Proc. 2018 15th International Conference on the European Energy Market (EEM),* Lodz, pp. 1-6.

[14] L. Xue, Y. Teng, Z. Zhang, J. Li, K. Wang and Q. Huang, "Blockchain technology for electricity market in microgrid," in *Proc. 2017 2nd International Conference on Power and Renewable Energy (ICPRE),* Chengdu, pp. 704-708.

[15] S. Li, "Application of Blockchain Technology in Smart City Infrastructure," in *Proc. 2018 IEEE International Conference on Smart Internet of Things (SmartIoT),* Xi'an, pp. 276-2766.

[16] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

[17] "Bitcoin Core – Bitcoin Blockchain client", [Online]. Available: https://bitcoin.org/en/bitcoin-core/

[18] See https://en.bitcoin.it/wiki/Majority_attack

[19] J. Poon and T. Dryja," The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[20] "Lighnting Network Specification RFC – Basis Of Lighnting Technology BOLT", [Online]. Available: https://github.com/lightningnetwork/lightning-rfc

[21] "Lightnin Network Daemon - LND – LN client", [Online]. Available: https://dev.lightning.community/

[22] "c-lighnting – LN client", [Online]. Available: https://github.com/ElementsProject/lightning

[23] Eclair – LN client – available at: https://github.com/ACINQ/eclair

[24] C. Burchert, C. Decker, and R. Wattenhofer, "Scalable funding of bitcoin micropayment channel networks", in *Proc. 2017 International Symposium on Stabilization, Safety, and Security of Distributed Systems* , pp. 361–377.

[25] A. Dolara, E. Donadoni, S. Leva, G. Magistrati, G. Marchegiani, "Performance analysis of a hybrid micro-grid in Somalia", in *Proc. 2017 IEEE Manchester PowerTech*, Manchester (GB), pp. 1-6.

[26] S. Polimeni, L. Meraldi, L. Moretti, P. Raboni, G. Manzolini, S. Leva, "Numerical and experimental testing of predictive EMS algorithms for PV-BESS residential microgrid", in *Proc. 2019 IEEE Milan PowerTech,* Milano (IT), pp. 1-6.