On the applicability of the GRIDNET protocol to Smart Grid environments

Rafal Skowronski
Department of Computer Science
Poznan University of Technology, Poland
rafal.skowronski@cs.put.poznan.pl

***Abstract*— The blockchain technology seems to be regarded by many, as a revolution, on the scale comparable to the advent of the Internet. The blockchain by itself is a rather simple data structure. The cryptocurrency design details account for the security of the underlying system. In this work, we present the design of our cryptographic system for use in Smart Grid environments. The mechanism is to incentivize distribution of greenfield energy, but also, to handle and encourage the required data transmission and storage. In our design, value of the cryptocurrency, as well as, of the energy itself, is determined *solely* by forces of supply and demand. Our design is unique in that, Smart Meters are the only trusted actors. We stress the importance of features required by, such a system; to be regarded as secure, distributed and indeed - decentralized. We advocate, that a smart-meter is the only element required to be trusted; and that should hold true only in regard to making energy measurements. We show, why a cryptocurrency based system, which we have designed, is particularly suitable for energy-distribution scenarios, especially in limited-trust environments, where anonymity and security of data transmission are of the essence. Our hereby proposed system provides a fully distributed market for prosumers, costumers, power line owners and any other entities involved in both energy and data distribution. In this paper we focus on the architectural design.**

Keywords*— *smart grid systems; decentralized systems; consensus; cryptography; blockchain; communication; GRIDNET

I. INTRODUCTION

When it comes to communication infrastructure, we believe, that relay nodes are a backbone of every distributed packet-switched type of computer networking and if they are to participate on their own will, providing a proper incentive to cooperate is of crucial importance. In game-theoretic terms, cooperation in any type of wealth distribution - where relay nodes are considered to be autonomous while not having clearly defined benefits from participation in the exchange; poses a dilemma. Taking computer networking as an example; different authorities may manage nodes, having different priorities. To save battery, bandwidth and processing power, nodes should not forward information to others. If, however - a significant number of nodes adopts such a strategy, quality of network degrades vastly, for all. Similar assumptions hold true for Smart Grid environments. In game-theoretic terms, a prosumer, shall not distribute energy to others for free. He or she needs to be paid. In order to support the development of green energy, government subsidies are being provided to prosumers. It is of an importance to simplify such practices and to ease the exchange of required information.

Our design supports a liberalized market structure. It is unique, in that, to best of our knowledge, it is the only design, so far, which allows energy to be traded solely on the basis of almost-live local market bids/offers, while not introducing any trusted actors beside Smart Meters. Although, previous works proposed the free market based approach, they did relay on trusted intermediaries in the form of Distribution System Operators (DSOs)[12]. In our design, although DSOs still play a significant role, they are able to influence energy production/consumption and synchronization only[1] by means of self-commenced market forces. Second, previous approaches did not propose an architecture which would provide *incentive* for data dissemination inside of Smart Grid environments. Since we consider fully autonomous grid systems, proper and secure, *incentivized* distribution of information shall be, also, - of the essence. By undertaking such an approach, we can achieve a self-sustaining environment, in which, both energy and information distribution are effectively encouraged and incentivized by market forces. Therefore, our research and proposal shifts heavily the nature of power distribution from monopolistic to a liberalized, competitive nature of services.

II. LIBERALISED MARKET STRUCTURE

We argue that market based coordination is indeed technologically feasible. The blockchain data structure is a perfect candidate for ensuring open trade and transparency of all of the transactions. With careful design the technology can provide anonymity, while also enable for data-mining for the purpose of scheduling wholesale transactions on the side of DSOs. Our hereby proposed design allows for the benefits of economies of scale (DSOs can still offer good price to prosumers and customers due to the already existing

[1] DSO in emergency, or in case of congestion, can send appropriate information to smart meters in a given area.

infrastructure), while enabling a transparent environment, where data is stored in a single distributed location.

III. RENEWABLE ENERGY TRADE

In our architectural design, anyone can distribute energy to anyone else. The amount of energy has its numerical representation and is paid for by anyone else willing to accept the price. Energy can be bought from prosumers by a DSO, or it can be transferred directly to another customer. To ease transmission between the current architecture, we fully do support the existence of DSOs, however, in our design, these do not need to implement price functions and do not need to be concerned with resource scheduling *inside* of a given grid in the sense of ensuring fair trade. When it comes to emergency situations, and/or congestion avoidance, the role of DSO is still clearly visible. For these purposes, we implement emergency commands. The DSO would send such a command to prosumer's device to cut it off from the network, to stop energy production etc. In any case, such data packets should have only an informative function, with the ability to be overridden by a Smart Meter's owner on his responsibility.

Implementation of various price functions makes the protocol less agile, for, each change to these requires a fork to the entire network; unless we do not need actions of the DSOs to be verified by others; but then – users need to put their trust into DSOs. We believe in an open market and that market forces shall allow for an equilibrium price to settle. As for this matter, we focus on providing an automated match between prosumer and consumer based on bids and offers. Having price functions implemented on the side of DSOs would make the system centralized, with DSOs having power of controlling access to energy and being able to promote certain prosumers more than others. According to [18]; - DSOs "*must not discriminate between system users or classes of system users, particularly in favor of its related undertakings*".

In our design, DSOs play a role of market brokers, indeed, participating in an open-market system. They might be able to mediate between wholesale energy markets and local autonomous grids. At the same time, however, when it comes to ability of buying and selling energy they do not differ from other prosumers. Although unrealistic, every prosumer can make a buy offer at a higher price than a local DSO and energy shall be offered to him. Customers can decide whether to buy electricity from a given prosumer or not based on price. If market forces drive energy offered by DSOs to be more expensive than from prosumers, green energy from later shall be preferred. Due to the number of Green Energy sources being relatively low; DSOs would still be playing a significant part in our ecosystem for the foreseeable future to come. The important part of our design is that all of the transactions and energy utilizations, are visible in an open ledger, - and so, if a government decides to promote green energy, their support could be easily integrated by introducing explicit cryptocurrency subventions directly to prosumers' accounts based on their verifiable production levels. Government could also promote green energy by aiding DSOs which in turn could offer higher bids on the open energy market to prosumers. The platform allows for any sort of market interactions.

IV. COMMUNICATION

Let us begin with the information-centric part of our design. The GRIDNET architecture incorporates a fully distributed communication system, which rewards intermediaries based on the amount of data they help to disseminate. The communication system lacks any kind of a trusted third party, while providing mechanism for protection against various kinds of impersonation attacks and hideous behavior. At the very core, end-to-end encryption is maintained at all times.

FD-GRIDNET protocol [17] is the first fully distributed communication system to reward intermediaries with a universal wealth. It incorporates a distributed ledger database, also termed colloquially as a '*blockchain'*. We utilize the concept *of proof-of work*, as well as, *proof-of-stake*. *Proof-of-work* mechanism has already been used by various cryptocurrencies and popularized initially by *Bitcoin* [6], which in turn, paved the path for others. Bitcoin was the first to use the concept of *proof-of-work* to reach consensus on the state of a distributed ledger database containing transactions between users. When considering a communication system which is to provide a fair spread of rewards for the intermediaries, we inevitably need to keep track of data packet deliveries. In a *Fully-Distributed GRIDNET* architecture, every data flow is tracked and resolved through a distributed ledger database. No communicated data is ever stored anywhere and communication identifiers are completely anonymous. Therefore, we do not see need in generating new identification addresses for each transaction. In case of a misbehavior - such users could be easily marked as malicious by an 'authority'[2]. In our protocol, full-nodes verify communication flows and *relay tickets*. The byproduct of the process, being a virtual currency, spread among relay nodes in accordance to their contributions. Every participant in our network is tight to a stake. The *proof-of-stake* mechanism is used to thwart hideous incentives. Each and every user needs to perform a certain *proof-of-work* related to one's identity before being able to participate inside of the network. This proof would then serve as a stake. When a node begins to cheat, the stake would be lost

V. FORMULATION OF A PROBLEM

We formulate the problem as follows; description of constraints shall follow along. We want a Smart Grid participant *A* to be able to trade energy with participant *B*, through an arbitrary number of intermediaries (ex. Power distribution line owners, aggregators). We must allow for energy transaction and communication participants to agree on the terms of a contract. Every deal shall be based on live, open market assumptions. For this to happen, we want node *A*, to be able to, communicate with node *B*, through an arbitrary number of intermediaries. These intermediaries, in game-theoretic terms, need to be incentivized

[2] Here, an authority is an entity which can, but does not need to be trusted by other

to mediate between *A*, *B* and any other necessitated parties. Only designated nodes shall be able to read encrypted data. No single intermediary nor data receiver shall be able to get to know the path traversed while data in transit. Intermediaries shall not be able to cheat the incentive system, for example, by adding an arbitrary number of intermediaries to the datagram, for the purpose of, increasing profit. It should be unworthy, in game-theoretic terms, for a given intermediary to be willing to create additional artificial intermediaries, so as, to maximize profit. One should not be able to remove any previous intermediary from the list of nodes traversed, so as to steal or maximize profit. The system shall payout credits only after a successful delivery of data and/or energy. The system should prevent double spending attacks. The system must provide means of rewarding numerous power distribution intermediaries, such as, power line owners. All of the actors beside[3] smart meters, owned by actors[4], are considered to be untrusted. Finally, even though being completely decentralized, the system should provide facilities for punishing individuals for acting against the rules proclaimed by the majority of users.

VI. Storage of Information as Part of a Distributed Blockchain, Merkle Trees, Reaching Consensus

In our system, every crucial information is being stored as part of a distributed ledger. Be it the reward for data communication intermediaries or a contract between a power-line owner and a prosumer. In a Smart Grid environment, such resolution tremendously lowers investments in data aggregation and data trade. Anonymous, from technical perspective, data regarding every transaction is publicly available. In the distributed ledger database, termed colloquially a 'blockchain', each entry is called a block. Blocks are bound together. Each following block contains a hash value of a previous one. The more blocks, the harder it is for an attacker to replace a given block. The difficulty lies in a required computational power; This is mainly due to a fact that data contained inside of a block needs to encapsulate a hash which meets a certain *difficulty criterion* i.e. - it needs to be below a particular value. Full nodes – the ones which store the entire blockchain, rival among each other, to find a proper nonce – a single value inside of a block. Its target value results in block's hash to be below a difficulty cap. Block with a higher difficulty wins - it is accepted by other nodes and added to the blockchain. That is how consensus among different *mining nodes* is reached. Attacking the scheme would require an immense computation power. The more blocks on top, the more secure transaction.

As for the Smart Grid environment, there is no need for energy-industry to invest into the full-nodes infrastructure. These can be operated by any people and organizations. In our design, the very decentralization ensures security of the entire eco-system.

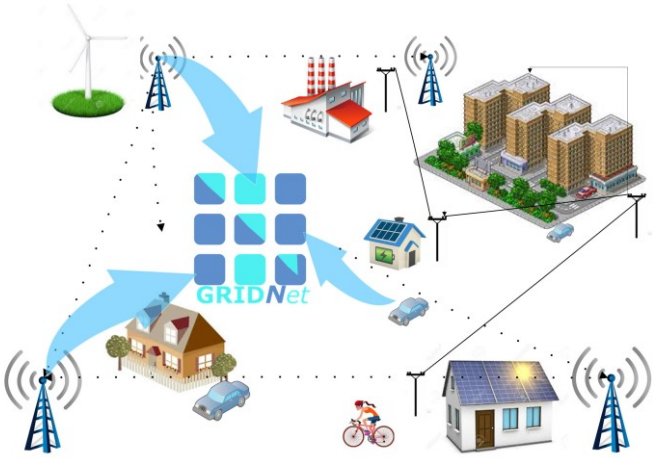

Figure 1: Actors are incentivized to participate in data exchange by earning cryptocurrency. Anonymous metadata is stored inside of the blockchain which opens doors for data mining possibilities and ensures open, safe trade.

VII. Proof-of-Work and Proof-of-Stake

In our proposal, the incentive behind data and energy propagation is cryptocurrency, which's limited supply, in turn, is governed by the laws of physics. Special nodes, - full nodes, need to consume time and energy, in the form of electricity, to come up with an appropriate *Proof-of-Work* for a given transaction block. When one earns cryptocurrency, he can *consume* it for the purpose of generating a *Transmission Token (TT)*. *TT* allows intermediaries to verify sender's willingness to cover data propagation fees. *It* can be thought of as a financial bond without holders specified until the wealth is delivered. Every intermediary however can verify bond's authenticity and hope to receive its fraction by cooperating.

In game-theoretic terms one should not risk more than the expected return from investment. That is where the *Proof-of-Stake* comes into play. Every node needs to compute a *proof-of-work* of their identifier. This *PoW* consists of a hash value which's numerical representation needs to be under a certain threshold defined as *work difficulty*. It is coupled by a *nonce* - an integer value which results in a hash of the address to be under a given threshold. In case of a nonce overflow, the address is concatenated with itself until success. The result serves as a *Proof-Of-Stake*. It is stored in the blockchain together with one's address and is also attached to every datagram generated by a given address. In case of a lack of payouts from the data originator or due to its misbehavior an unfair node can lose its stake – he would lose the initial proof-of-work attached to his *address*.

[3] Even though, smart-meters are considered as trusted; it is still possible to mark transactions resulted from measurements of a given meter as compromised. This could done by a respected third party; such as police or smart meter manufacturer.

[4] A Smart Meters can be owned by a DSO what is important is that the owner is in its control and that he is responsible for handling of his private key. The manufacturer of the Smart Meter shall be responsible for correct reading of the device, as the amount of energy produced is signed by the manufacturer's private key to which the owner shall have no access to.

VIII. State-full and state-less channels

The throughput of a proof-of-work based blockchain infrastructures is usually considerably limited. The amount of possible transactions in a time frame θ can be calculated as $\tau = \left(\frac{\frac{\beta}{\mu} * \rho}{\theta}\right)$; where τ represents achievable transaction throughput, μ stands for size of an average transaction; β -size of a single block, ρ- block creation interval. Taking Bitcoin as an example, the possible amount of transaction per second as of year 2017 cannot exceed the amount of seven, for transactions happening directly on the blockchain. There has been incentive, recently, to move intermediate transactions 'off the chain'.

The term *state channel* was proposed first by Jeff C. in his blogpost [12]. Inheriting from the concept, we propose definitions of a *state-full*, as well as, of a *state-less* channel. In our nomenclature, state-full channels represent state channels proposed by Jeff C.

In this sense, after [12], steps required to create a *state-full channel* are as follows: 1) Part of the blockchain state is locked through a contract on which participants must agree on. 2) Participants update the state among themselves, by constructing and signing transactions that could be submitted to the blockchain, but instead are merely held onto for now. Each new update outdoes previous updates. 3) Finally, participants submit the state back to the blockchain, which closes the state channel and unlocks the state again (usually in a different configuration than it started with). In the second step, an unlimited number of updates can be rapidly made without the need to involve the blockchain at all.

Proposed by us, *state-less channels* differ from *state-full channels*, in that, there is no state being a priori locked inside of the blockchain. Instead, there is a form of partially known, registered, secret/puzzle; - answer, to which, is being steadily revealed. Participants can verify whether the next part of a secret is correct and by whom it has been issued. The steps to create a state-less channel are as follows: 1) A given party registers a multi-stage puzzle, - it might know the answers to; inside of the blockchain, by sacrificing a certain amount of currency; It also specifies payout ratio for correct answers. 2) Another party releases signed answers to the puzzle. 3) Anyone can verify whether the answers are correct just by looking at the puzzle and a given answer. Each unique disclosure gives right to a certain amount of previously consumed currency. The number of times second step can be performed is determined by the number of unique answers to a puzzle.

Both state-full and state-less channels aim to improve scalability of 'blockchain' conceives. State-full channels are useful when it is possible to define contracting participants by some properties and include them inside of the blockchain a priori. State-less channels, on the other hand, are convenient when the participants and their unique attributes remain beforehand unknown. State-less channels can be used in situations where it is impossible or not feasible to verify or predict identities of actors, who can perform desired tasks.

In our hereby proposed architecture, we employ state-less channels for the purpose of incentivizing propagation of data; - since the intermediaries might be beforehand unknown. On the other hand, we use state-full channels for the purpose of defining a contract between concrete energy-transaction participants. Updates to these contracts are then delivered through a stale-less channel. Full end to end encryption is maintained at each step.

Thanks to such design decisions we achieve a very scalable solution. In our eco-system, even unknown third parties can be incentivized to perform readings from smart meters; for example, in very distant rural areas. There is then no need to employ or sign contracts with specific third parties; everything happens automatically and is entirely information-centric.

IX. Data Transmission

In *FD-GRIDNET* there is no *PKI* infrastructure. Distributed blockchain serves as a global source of trust, with its integrity guarded by a proof-of-work mechanism. Users are identified by their addresses. Addresses are derived from user's public keys. Private keys are kept secret and shared with no one. Each datagram contains an anonymous sender's address.

In a scenario where there is no access to a full node i.e. to a blockchain, intermediaries of data transmission are assured to some degree by a *proof-of-work* attached to sender's identity. Initiating a payout is associated with a fee calculated as a fraction of a *Transmission Reward*. Therefore, a recipient might prefer to initiate clearance not too often for a single sender. This minimizes size of the blockchain and allows recipients and intermediaries to make profit. FD-GRIDNET can operate as an overlay protocol over IPv4/IPv6, preserving privacy of each intermediary (addresses of each one are encrypted inside of an onion, with each layer encrypted to a public key of a given intermediary).

X. The notion of Transmission Tokens and Transmission Token Pools

There are three important unique concepts to the GRIDNET protocol. Token Pools, Transmission Tokens, Transit Pools and Smart Contracts. For the sake of clarity, and due to space limitations, here, we will touch upon the main ideas. More specific implementation details can be found in [17]. In a nutshell, a token pool is a data structure which is represented by a hash chain. A single token pool is defined by *part* of a cryptographically secure hash function (*hash-seed* value), the number of hashes present in a hash chain and a final ceiling value of a given hash-chain.

Hash pool is computed by a person sacrificing coins, and so, the person is the only one with knowledge of hash values in

between the partial-hash-seed and the final ceiling hash. Initial seed-hash, in its entirety, remains a secret until depleted. Final hash can and needs to be known to the public. Coins sacrificed to generate a *token pool* are not ultimately lost however.

A *token pool* is generated by consuming[5] a certain amount of currency. Each hash from a token pool represents a share in a consumed amount of currency. In other words, by sending currency to an unredeemable address, one exchanges coins for hashes in a hash pool. Value of a single hash in a given hash-pool can be calculated as $\frac{\text{NumberOfConsumedCoins}}{\text{NumberOfHashesInAHashPool}}$.

Every single hash, or a range of hashes from the hash-chain can be used to create a single *Transmission Token (TT)*. By specifying the amount of revealed hashes, data originator can proportion priority of a datagram or data bundle. The higher the *TR*, the higher incentive for intermediaries to store and forward information for longer periods of time. The lower the *payrate* fraction inside of *TT*, the sooner the encouragement deceases. The diminishing profit for further intermediaries, as a side effect, prevents network from being flooded by old irrelevant datagrams. This facilitates a *Time-To-Live* mechanism, one guarded by forces of supply and demand.

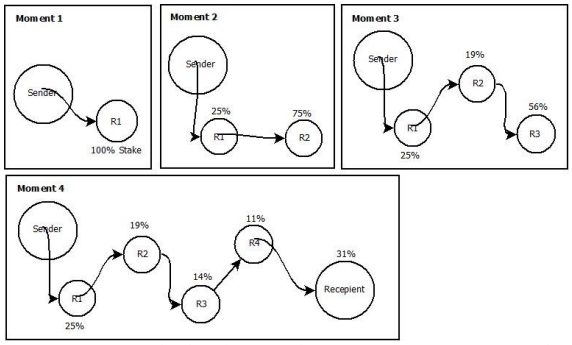

Figure 2: Spread of Token Pool resources among intermediaries via a Transmission Token. The sample payrate fraction is set to 0.75.

Figure 2 shows how transmission reward is spread among intermediaries. When a datagram reaches first intermediary, the first intermediary owns a full share in a *TR*. When a current node decides to retransmit to another node, the current one hands over a *payrate* fraction of its current share to next node. *The scheme repeats*. This way, it is unworthy for a current node to add artificial, owned by itself, payout addresses to a *hop-list,* since, it already owns everything it can. On the other hand, each node knows that, most probably, it needs to pass the data on, as coming into a direct contact with a target node might not be probable enough. Time is also of the essence. Data originator might be wealthy enough to have hired multiple initial messengers. Nodes constituting a given path, would receive credits, but only after a successful delivery. The hop-list is protected against tempering [17].

Taking note inside of the blockchain of every data packet among millions of users would require an infeasible amount of storage space. In order to overcome this problem, we introduce the notion of *Transit Pools*. With thanks to these, we can efficiently track particular data packets in large data streams. *Transit Pools* are formed by the data receiver when the connection ends. These are created by concatenating the last Transmission Token with the list of intermediaries. The higher stability of connection-link the lower number Transit Pools, the lower number of payouts inside of the blockchain, the lower transmission fees. Data receivers are incentivized to create largest Transit Pools possible; so as to increase their profits.

Smart Contract are means of ensuring that concrete, a priori defined energy transaction participants, receive their share. Every participant agrees on his share/payout-ratio inside of a contract. In our scenario, the consumer agrees on a certain price per kWh, further, the power line owner agrees on his reward per transmitted kWh. There can be multiple entities involved. Each contract participant needs to sign a particular contract with his private key. Updates to contracts are delivered by means of a state-less channel.

As can be seen, in our design, we take use of both state-full and state-less channel. State-full channels take a form of smart contracts, which are delivered through a state-less channel. First instance of a contract is uploaded to a blockchain so everyone can verify and see if its valid. Subsequent deliveries of updates to contract's state (updates to everyone's balance) happen, off the chain.

XI. Transmission of Energy

In the hereby proposed design, a Smart Meter is the only trusted appliance. It needs to be trusted, as there needs to be an entity which measures energy delivered from solar panels, wind turbines, etc.

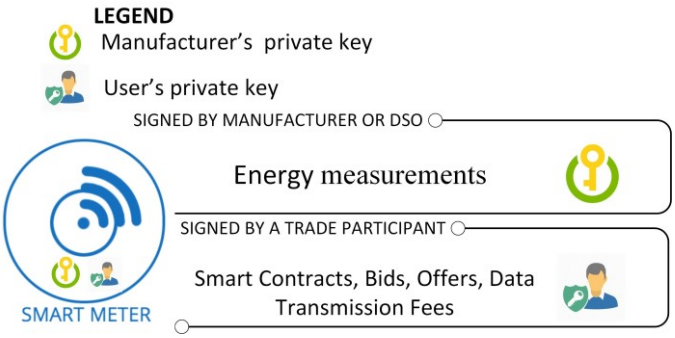

Figure 3: Energy measurements are signed by a DSO's or manufacturer's private key while everything else is signed by the user.

Every period of 15 minutes the smart meter releases the amount of green energy produced, signed by the meter. The meter itself is registered inside of the blockchain to a given proof-of-stake and identity-token. In case of any accusations by a well-established authority, registered inside of the blockchain, the stake would be considered as lost, - by those who trust the authority. A well-established authority such as police, smart-

[5] Currency is not consumed i.e. destroyed, but deposited for future intermediaries.

meter company, etc. could publish their public key and if such an authority notices tempering with a given smart meter etc. they could mark it as compromised. To increase confidence for others, some of the prosumers might choose to couple their identity tokens with a stake.

In our design, the amount of energy and the asked-for price serve as an input to an algorithm running on a customer's device. The customer can be either a DSO or any other buyer. The customer needs to verify the authenticity of a signature presented by the seller. If seller's signature is authentic i.e. it has been registered inside of the blockchain by another trusted entity, then the buyer might agree to receive the energy and tap into its stream. Note however, that there is no Trusted Authority in a strict cryptographic sense, besides, - the Smart Meter. Individuals choose, whether to trust a given entity, or not. Consumers can choose by their own will manually, or they can include certain public keys into a smart contract inside of their energy supply unit so to allow for autonomous decisions without their interaction.

The following diagram illustrates energy transaction and transmission process.

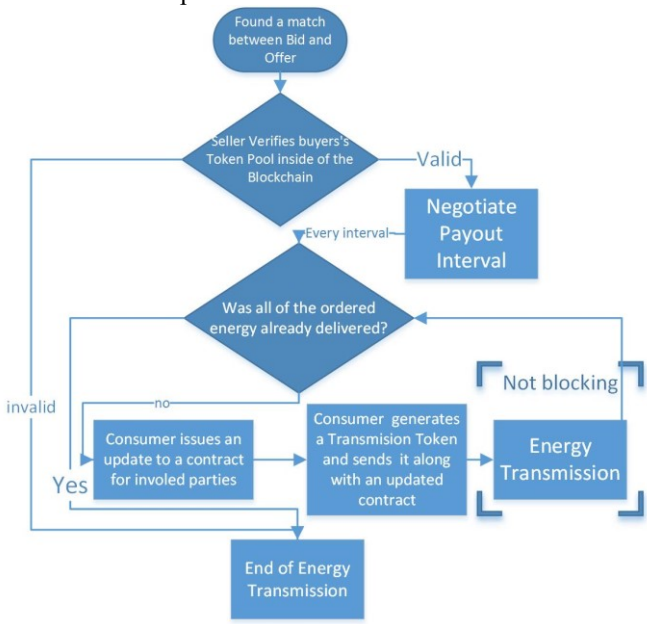

Figure 4: Energy transaction and transmission process.

The energy transmission could begin anytime, however, the sooner the involved parties begin to receive updated states of a contract, the sooner they are assured of being rewarded with cryptocurrency. Confrères may initiate payout anytime, however, initiating a payout involves cost. The cost is imposed mainly to ensure storage efficiency inside of the blockchain. Every transaction finalization has a consequence of inflicting an entry inside of it.

XII. Our Distributed Energy Trade Model

Microgrids constitute a well-known approach to management of Distributed Energy Resources (DERs). Microgrids are defined as autonomous partitions of the physical infrastructure. These contain a single Point of Common Coupling (PCC), which is to help distribute resources between a micro-entity and the hosting grid. This would implicate centralization on the side of PCCs, which need to be trusted. In our design, DSOs play an important role, however, their actions are fully determined by market forces and contracts between individual prosumers and customers.

Though business models are out of the scope of this work, markets have proven to be a suitable mechanism for resource allocation and control of autonomous selfish parties and have already been tested for Distribution Grid Energy Management in the US, following the Transactive Energy approach [13], and in Europe under several projects involving microgrids [14] [15].

In our design, in contrast with [12], substations do not implement reward mechanisms. Transactions can be performed directly between individuals, in real-time. Due to a potential blockchain storage overhead, we do not implement matching of bids/offers inside of it. Instead, every electricity buy/sell offer is broadcasted to other concerned parties. Here, the very cryptocurrency itself constitutes a market-defined cryptocurrency, which's price itself is determined on crypto-currency exchange markets and is prone to fluctuations. The representation of the amount of energy is detached from the representation of cryptocurrency. Amount of energy is represented solely by a numerical value in kWh and is cryptographically signed by a Smart Meter.

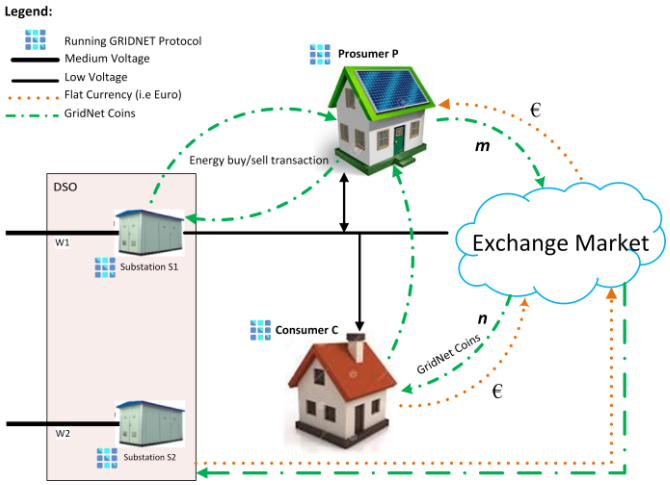

Figure 5: Illustration of the Trading Model.

Every transaction is made in cryptocurrency. In our design, fiat money is used on exchange markets to either buy it or sell the former. There can be multiple exchange markets, owned by various third parties, just like fiat currency exchange markets. As of 2017, foreign exchange markets which offer exchange between fiat and multiple cryptocurrencies already exist.

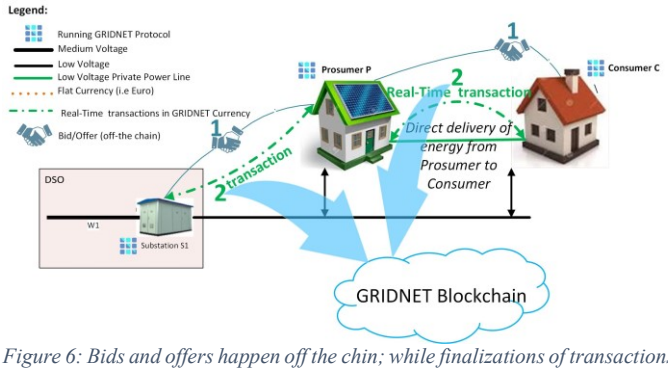

Figure 6: Bids and offers happen off the chin; while finalizations of transactions are included inside of it.

Bids and offers are delivered through multicast transmissions to parties of interest. There is nothing stopping the substation from acting as a communication hub, after all, it would automatically receive provision for participation in the data exchange. Communication happens off the chain, through a state-less channel, while transactions (contracts and updates to a contract) - are uploaded inside of it.

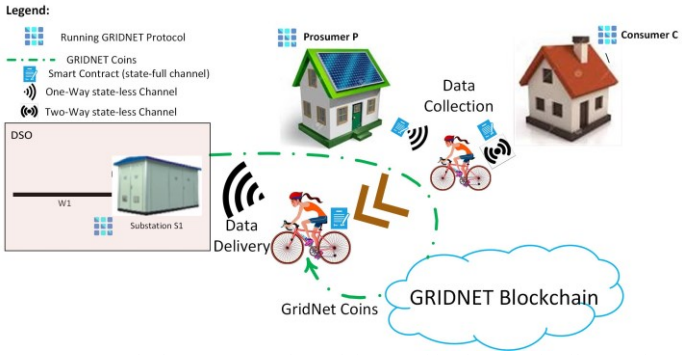

Figure 7: Bicycle driver passing through her neighborhood and collecting data bundles; effectively creating an information centric environment.

In the most exotic imaginable situation, even a bicycle driver could drive through her neighborhood and wirelessly collect data-bundles containing signed and updated contracts. What is worth to notice, is that only one way communication would suffice, while still ensuring that the bicycle driver is rewarded.

XIII. Previous works

Previously, rewarding energy exchange with a token-based mechanism, but not a cryptocurrency, was proposed by [12]. A comprehensive survey on the possibilities of utilizing Blockchain technology in the energy industry was presented in [20]. Ideas of incorporating proof-of-stake mechanism for solar energy trade were shown in [21].

XIV. Summary

In this paper, we have proposed a fully distributed architecture for use in Smart Grid environments. Our design is unique in that, it creates an eco-system for incentivizing both energy and data distribution. It rewards service providers, consumers, but intermediaries of the trade, as well. Thanks to a careful design, we have achieved a proposal which maintains a high level of security, due to an end-to-end encryption and anonymity thanks to anonymous identifiers. One of the interesting aspects of our proposal is the openly available distributed database, which opens doors for data mining opportunities. Additionally, when it comes to security of such a distributed ecosystem we have showed that a proof-of-stake mechanism could be used to thwart attempts of malicious behavior. Our design presents a very liberalized infrastructure, the technology allows of a very high level of anonymity. Still, due to an openness of the platform, there exist numerous possibilities of ensuring obedience with laws present in a given country.

References

[1] Self-Policing Mobile Ad-Hoc Networks by Reputation Systems, Sonja Buchegger, Jean-Yves Le Boude
Qi He Dapeng Wu, Pradeep Khosla
[6] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
[7] Mitigating Routing Misbehavior in Mobile Ad Hoc NetworksSergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker Department
[8] U.S Government, Gold Reserve Act, January 30th, 1934
[9] History of Telecommunications Technology, Christopher H. Sterling, George Shiers
[10] Gellman, Barton; Poitras, Laura (June 6, 2013). "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program". The Washington Post. Retrieved June 15, 2013.
[11] Braun, Stephen; Flaherty, Anne; Gillum, Jack; Apuzzo, Matt (June 15, 2013). "Secret to PRISM Program: Even Bigger Data Seizures". Associated Press. Retrieved June 18, 2013
[12] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. Magrans de Abril and A. Nowé,"NRGcoin: Virtual Currency for Trading of Renewable Energy in Smart Grids", in Proc. of the 11th International Conference on the European Energy Market (EEM), Krakow, Poland, 2014.
[13] S. Widergren, C. Marinovici, T. Berliner, and A. Graves, "Real-time pricing demand response in operations," in Power and Energy Society General Meeting, 2012 IEEE, July 2012, pp. 1–5.
[14] J. Kumar and A. Jayantilal, "Models of distributed energy resources markets in distribution grid operations," in Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on, Dec 2011, pp. 1–6.
[15]C. Block, J. Collins, and W. Ketter, "Agent-based competitive simulation: Exploring future retail energy markets," in Proceedings of the 12th International Conference on Electronic Commerce: Roadmap for the Future of Electronic Business, ser. ICEC '10. New York, NY, USA: ACM, 2010, pp. 68–77.
[17] R.Skowronski, "Fully Distributed GRIDNET protocol, with no trusted authorities" in Proc. of the 31st International Conference on Information Networking (ICOIN), IEEE,Vietnam, 2016
[18] Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003
[19] P. Koutstaal, J.Lenstra, R.Haffner et.al, "The role of DSOs in a Smart Grid, Amsterdam/Rotterdam, 23 April 2014,report for the European Commission
environment
[20]C.Burger, J.Weinmann et.al "Blockchain in the energy transition. A survey among decision-makers in the German energy industry.", DENA German Energy Agency
[21] A.Islam, J.Zitoli, N.Gogerty, "Connecting the Blockchain to the Sun to Save the Planet"