

# Privacy-Preserving P2P Energy Market on the Blockchain

Alain Brenzikofer  
Supercomputing Systems AG  
alain.brenzikofer@scs.ch

Noa Melchior  
Supercomputing Systems AG

**Abstract**—*Quartierstrom* creates a peer-to-peer marketplace for locally generated solar power. The marketplace is implemented as a smart contract on a permissioned blockchain governed by all prosumers. Two privacy-by-design concepts are presented which guarantee that the users individual load profile is not leaked to any third party despite using a blockchain. The first approach leverages UTXO based coin mixing protocols in combination with an account-based on-chain smart contract. The second approach relies on an off-chain smart contract running in trusted execution environments.

## I. INTRODUCTION

Renewable electrical energy is increasingly produced locally in a decentralized fashion. Self-consumption of this produced energy is incentivized in many legislations in order to improve the profitability of renewables. However, most prosumers currently have no possibility to influence the level of remuneration for the energy they sell nor are they allowed to sell directly to their neighbors. The *Quartierstrom* project [1] implements a transactive energy system that manages the exchange and remuneration of electricity between consumers, prosumers and the utility in the absence of intermediaries. Blockchain [2] technology was chosen to implement the decentralized peer-to-peer market that does not rely on a trusted third party (TTP). Both prosumers and consumers can indicate a price at which they are willing to sell or buy locally produced solar energy without the intermediation of a utility or any other TTP. Utilities still enjoy a lot of trust in most European countries [3]. However, this trust mainly regards their integrity, not their competence in information security matters nor the absence of their curiousness regarding personal data.

Blockchain solutions have the potential to guarantee transparency and integrity of the process along with confidentiality and information security. Moreover, the absence of any single point of failure improves resiliency. Finally, blockchain technology is a natural choice to endorse the bottom-up community spirit, attractive to many customers engaging in decentralized energy production.

### A. Decentralized Energy Market

*Quartierstrom* implements a double auction with discriminatory pricing as its market mechanism. For both, consumers and prosumers, the smart meters transmit bids containing the price limit determined by the individual household and the electricity demand or supply measured by the meter. An order book collects all bids during discrete intervals of 15 minutes and sorts them by price: Sell bids with a lower sell price

are prioritized, and buy bids with a higher price, respectively. Discriminatory pricing means that for each trade, the price is derived as the mean between the buyer's and seller's price.

Befitting the idea of decentralization, the auction is implemented as a smart contract on the blockchain. *Quartierstrom* is built upon a Tendermint BFT consensus [4] with nodes running on embedded devices [5] at the metering points in the grid.

### B. Privacy Challenge

The aggregated power consumption of each individual household is sampled every 15 minutes and placed on the market as a bid by means of a blockchain transaction. Linking bids for a particular participant reveals his usage profile, which is to be considered personal data. A Nakamoto blockchain [2] guarantees pseudo anonymity by representing each demand and production smart meter as a public key (the public key can be thought of as an account number in the traditional banking sense). No association between the public key and the household's address or occupant's identity is published on the blockchain at any point in time. However, third parties may be able to gain insights about consumer behavior, household characteristics or occupancy patterns from market orders. Because of this linkability risk, the European Blockchain Observatory considers public keys personal data under GDPR [6].

### C. Goal

*Quartierstrom* therefore aims at breaking the linkability among subsequent market orders. The *Quartierstrom* marketplace features a public order book, therefore price and amount of all orders are public. This transparency is desired so every observer can verify the market's integrity. However, the identity of a bid's originator does not need to be public as long as the market can enforce settlement of successfully cleared bids. Leveraging blockchain features, a cryptocurrency can be used to supply the necessary funds along with a bid using an atomic transaction. Such a cryptocurrency needs to feature private transactions to avoid linkability of bids. As the group of users on a market is bound by the physical dimensions of the respective grid, k-anonymity [7] can be achieved at best, k being the number of participants per grid region. This paper presents two fundamentally different approaches that were evaluated as candidates for privacy enhancements of the *Quartierstrom* system. Section II approaches the problem with cryptography, while section III leverages trusted execution environments.

arXiv:1905.07940v1 [cs.CR] 20 May 2019

## II. TRANSPARENT-BID AUCTION WITH SHIELDED BID ORIGINATORS

*Quartierstrom* implements a double auction by means of a smart contract. The business logic behind this marketplace is not further explored here. Instead, the focus is put on user privacy in a transparent market on blockchains in general.

Orders contain a price in [cts/kWh] and the amount of energy in [kWh] consumed or produced during the last 15 minutes. As the order is sent to the market as a blockchain transaction, the sender has to sign the order with her private key. Therefore, her public key is tied to the order, which leads to unwanted information leakage as subsequent orders can be linked to the same public key, thereby revealing consumptional behavior.

On a blockchain, the bidder can directly supply the maximum value of her order together with the bid, in the form of cryptocurrency. If her order is cleared at a lower price, the change can be returned to the sender address. Supplying the necessary value along with the order is the first step to unlink orders because it makes every order binding by itself and the market contract can settle all trades directly without knowing the identity or an account number of the originator. However, even if one may now use a different address for every order, one still has to fund these addresses, thereby linking them. As shown in [8], tracing blockchain transactions can easily reveal a sender's identity.

We propose to use shielded addresses to break linkability between orders. Shielded addresses are shadow identities unlinkable to the main addresses, which can be used to transfer tokens without revealing the originators, the transaction amount or beneficiaries. As a consequence the traceability of blockchain transactions is prevented. Hence, shielded addresses are able to perform coin mixing [9]. Currently, the two largest blockchains (measured by market capitalization) implementing shielded addresses are Zcash [10] and Monero [11]. While Zcash leverages zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs), Monero employs linkable ring signatures (LRS) along with one-time public addresses.

Fig. 1 shows the proposed generic transaction flow.  $0x001$  may be a public address, possibly funded by an exchange and therefore linkable to an identity. The user *Bob* sends funds to a shielded address  $0x002$ , thereby breaking the link to his identity. For each order, Bob sends the necessary value to a fresh unshielded address  $0x003$ , which in turn is used to call the smart contract to register his order.

Both Zcash and Monero use unspent-transaction-outputs (UTXO) [2] but they don't feature smart contracts. Ethereum [12] on the other hand does feature smart contracts but uses account-based transactions. Therefore, it is known who called a smart contract as only the payload of the contract call can be encrypted.

Quorum [13] built a hybrid blockchain featuring a modified Zerocoin protocol along with smart contracts. While our proposed concept is expected to work on Quorum, zk-SNARKS are computationally heavy and applying such a protocol to embedded applications like our blockchain-smart-meter appears unreasonable today. However, recent advancements in the

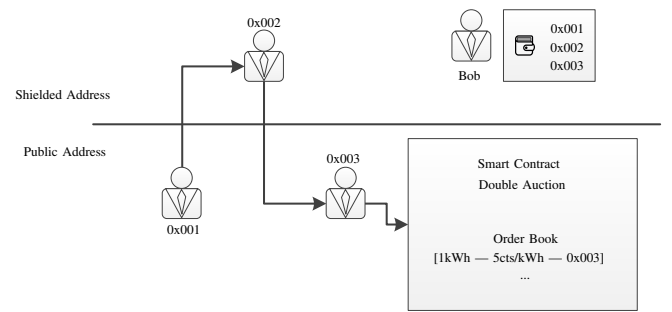


Fig. 1. Shielded transactions break linkability among successive orders to preserve user privacy.

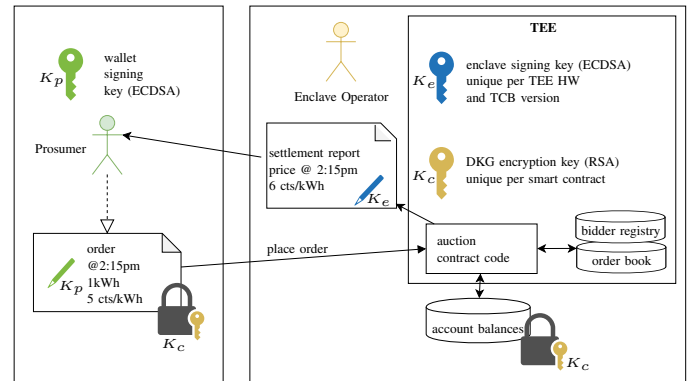


Fig. 2. Basic auction setup with a single trusted execution environment acting as trusted auctioneer.

field of cryptographic primitives led to the release of JubJub [14] enabling faster zero-knowledge proof generation with less RAM usage.

The CryptoNote protocol [11] is considered to be more suitable for embedded applications because no heavy computation is involved. If implemented on top of Tendermint, shielded transactions can be combined with smart contracts.

Both Zerocoin and CryptoNote risk leaking private information when using light clients. For both protocols, every user has to scan every block for transactions concerning himself. If a light client queries a full node for his account balance, the full node learns the user's individual public keys. For *Quartierstrom* this is a drawback, as pure consumers who do not sell excess energy are equipped with cheaper light client devices.

## III. OFF-CHAIN AUCTION WITH TRUSTED EXECUTION ENVIRONMENTS

Trusted execution environments (TEEs) allow confidential code execution inside an enclave that is secured by hardware. Such TEEs convince third parties of the integrity and confidentiality of a computation by means of remote attestation by the hardware manufacturer. [15], [16], [17] and [18] proposed protocols for private blockchain transactions based on Intel SGX [19]. For embedded devices, ARM TrustZone [20] could be leveraged. Keystone [21] develops an open source RISC V CPU featuring a TEE which, unlike the former two, will be formally verifiable. In any of these cases one has to trust the device manufacturer.

Fig. 2 shows the proposed architecture for a confidential double auction, where confidentiality is ensured by TEEs. A prosumer’s smart meter creates an order based on the energy measurement for the last 15-min-slot and the customer’s price preference. It signs the order with a wallet key  $K_p$ , allowing the auction enclave to access his pre-paid funds. The prosumer encrypts his order with an encryption key  $K_c$  provided by the auction enclave. Therefore, no one except the auction enclave can decrypt the order and learn about its content or originator.

The auction enclave collects all orders in its order book and clears the market. The auction enclave maintains a ledger with all pre-paid account balances and settles the market immediately. A public settlement report, signed by the enclave key  $K_e$ , is finally broadcast to all bidders to provide price transparency.

So far, this does not involve a blockchain at all. The described concept could be applied using a central enclave operator. The central operator would not be able to read any orders or account balances. It could even manage account refills supporting standard payment options. To gain a customer’s trust, the operator should allow remote attestation by the TEE manufacturer and the auction enclave code would have to be open sourced and would have to be built deterministically so anyone can build the trusted computing base (TCB) and compare its hash to the remote attestation’s quote.

This centralized *trusted computing* approach already comes with privacy benefits if compared to today’s standard meter-to-cash process, because confidentiality and integrity of the market are enforced by hardware. However, *Quartierstrom* aims to provide a *decentralized* market for local communities. Decentralizing the described market involves allowing anyone to act as enclave operator and the settlement layer may not rely on a trusted third party.

Fig. 3 shows a setup leveraging blockchain for a decentralized registry of attested enclaves: (i) A TEE operator registers an auction enclave by supplying a remote attestation (RA) quote to the enclave attestation registry (ER) (on-chain). (ii) The ER validates the RA quote and updates its registry. (iii) All registered enclaves generate a new distributed key pair  $K_c$  (see III-B).

#### A. Trusted Auctioneer Integrity

Integrity of computation is guaranteed by the TEE manufacturer. However, successful side-channel attacks have been shown in [22] compromising not only confidentiality but also integrity. To mitigate such attacks, we suggest to diversify by running a pBFT consensus [23] among multiple TEEs from different manufacturers. [18] proposes an incentive scheme to balance power among different manufacturers.

#### B. Trusted Auctioneer Confidentiality

If more than one TEE may act as auctioneer, a shared secret needs to be established, known to all registered enclaves but no one else. [16] suggests to use a distributed key generation (DKG) protocol published in [24]. Such a shared secret can then be used to derive the encryption key pair  $K_c$  in Fig. 2. Frequent renewal of the shared secret is recommended to improve forward-secrecy in the case of future TEE vulnerabilities.

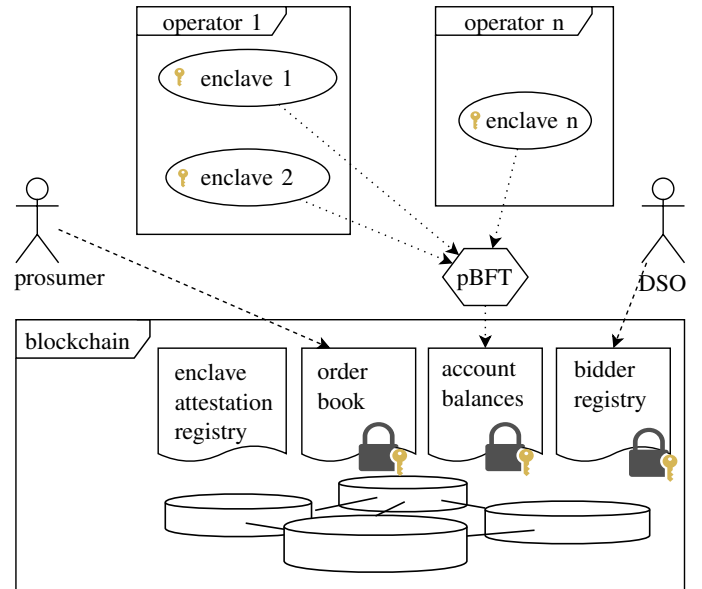


Fig. 3. Blockchain setup with off-chain TEEs who register with a registry contract. A DSO registers prosumers allowed to trade. Prosumers send their orders to the blockchain in encrypted form. The enclaves may perform token transactions on behalf of prosumers to settle the market.

#### C. Settlement

An auction enclave must be able to settle the market without any interaction with the prosumer. It therefore is a custodian of a prepaid balance on behalf of the latter. In our decentralized scenario there is no single operator that could offer a prepaid account topup service to the prosumers as in the case of a centralized auctioneer. A practical approach would be that utilities are permitted to issue IOUs (“I owe you”) denominated in fiat currency on behalf of prosumers topping up their balance. A more decentralized way would be to introduce bridges to cryptocurrency blockchains along the ideas presented in [25].

#### D. Permissioned Bidder Registry

There is no way around the natural monopoly of a distribution system operator (DSO). Only the DSO knows which prosumers are connected to the same low-voltage grid and should therefore be able to trade energy on their local market as envisioned by *Quartierstrom*. The DSO also knows who actually operates a real PV plant and of what size. Therefore, decentralization faces its natural limits when touching physical givens, represented by the bidder registry.

## IV. RELATED WORK

The methods presented in Section II extend and concretize the ideas of [26]. While [26] performs computations off-chain and uses the blockchain as a log, our approach uses completely on-chain computations for the shielded auction.

Eکیدen [16] is a platform for confidentiality-preserving, trustworthy and performant smart contracts built on TEEs. It is a universal platform built on Tendermint and a possible option for an implementation of a prototype.

Strain (Secure auctIons foR blockchAInS) [27] proposes a sealed-bid auction for blockchains, leveraging zero-knowledge proofs. The protocol, however, relies on a semi-trusted judge.

## V. CONCLUSION

We have introduced the privacy challenges when implementing a decentralized auction for electrical energy on a blockchain. Two concepts have been presented that provide confidentiality of personal data while still delivering transparency of the auction process. The first approach breaks the linkability among subsequent orders by means of either zero-knowledge proofs or ring signatures. The second approach leverages trusted execution environments to guarantee both confidentiality and integrity of the auctioneer. Both approaches can be applied to centralized and decentralized systems alike, enhancing privacy with or without leveraging blockchain.

## ACKNOWLEDGMENTS

The *Quartierstrom* project is co-funded by the Swiss Federal Office of Energy (SFOE). The consortium consists of Wasser- und Elektrizitätswerke Walenstadt WEW, bits to energy lab ETHZ, Bosch IoT Lab HSG, Hochschule Luzern, Supercomputing Systems AG, Cleantech 21, Sprachwerk, Planar, SwiBi, BKW.

## REFERENCES

- [1] A. Brenzikofer, A. Meeuw, S. Schopfer, A. Wörner, Ch. Dürr, *Quartierstrom: A Decentralized Local P2P Energy Market Pilot on a Self-Governed Blockchain*, CIRED proceedings article in press, 2019
- [2] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. <http://bitcoin.org/bitcoin.pdf>. 2008.
- [3] Ipsos-London Economics-Deloitte consortium, *Second consumer market study on the functioning of the retail electricity markets for consumers in the EU*, Fig. 39, 2016
- [4] E. Buchmann, J. Kwon, Z. Milosevic. *The latest gossip on BFT consensus*. ArXiv180704938 Cs. 2018.
- [5] Meeuw et al., *Experimental bandwidth benchmarking for P2P markets in blockchain managed microgrids*, Energy Procedia, Article in press, 2019
- [6] The European Blockchain Observatory. *Blockchain and the GDPR*. 2018.
- [7] P. Samarati. *Protecting Respondents' Identities in Microdata Release*. IEEE Transactions on Knowledge and Data Engineering archive Volume 13 Issue 6. 2001.
- [8] Fergal Reid. *An Analysis of Anonymity in the Bitcoin System, Security and Privacy in Social Networks*. 2012.
- [9] Maxwell, G.: *CoinJoin: Bitcoin privacy for the real world. Post on Bitcoin Forum*, <https://bitcointalk.org/index.php?topic=279249>, 2013
- [10] E. Ben-Sasson et al. *Zerocash: Decentralized Anonymous Payments from Bitcoin*. Proceedings of the IEEE Symposium on Security & Privacy (Oakland), 459-474, IEEE. 2014.
- [11] N. van Saberhagen. *CryptoNote v 2.0*. <https://cryptonote.org/whitepaper.pdf>. 2014.
- [12] Vitalik Buterin. *Ethereum: A next-generation smart contract and decentralized application platform*. <https://github.com/ethereum/wiki/wiki/White-Paper>. 2014.
- [13] JP Morgan Chase. *Quorum*. <https://github.com/jpmorganchase/quorum>.
- [14] Zcash. *JubJub Prototype*. <https://github.com/Electric-Coin-Company/jubjub-prototype>. 2017.
- [15] *Hyperledger Sawtooth Private Data Objects*. <https://github.com/hyperledger-labs/private-data-objects>. 2018.
- [16] Raymond Cheng et al. *Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution*. arXiv:1804.05141. 2018.
- [17] J. Lind, I. Eyal, P. Pietzuch, E. Gün Sirer. *Teechan: Payment Channels Using Trusted Execution Environments*, arXiv:1612.07766, 2017
- [18] Brenzikofer A., *encounter - An Ecological, Egalitarian and Private Cryptocurrency and Self-Sovereign Identity System*, <https://encounter.org>, 2018
- [19] V. Costan, S. Devadas. *Intel SGX Explained*. Tech. rep. Cryptology ePrint Archive.
- [20] *Introducing ARM TrustZone*. <https://developer.arm.com/technologies/trustzone>.
- [21] Dayeol Lee. *Keystone Enclave: An Open-Source Secure Enclave for RISC-V*. RISC-V Summit, Santa Clara. 2018.
- [22] Jo Van Bulck et.al. *Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution*. 2018.
- [23] M. Castro and B. Liskov. *Practical byzantine fault Tolerance*. OSDI '99 Proceedings of the third symposium on Operating systems design and implementation. 1999.
- [24] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. *Secure distributed key generation for discrete-log based cryptosystems*, International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 295310. 1999.
- [25] I. Bentov et al., *Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware*, IACR Cryptology ePrint Archive, 2017
- [26] A. Laszka, A. Dubey, S. Eisele, M. Walker, and K. Kvaternik. *Design and Implementation of Safe and Private Forward-Trading Platform for IoT-Based Transactive Microgrids*. arXiv:1709.09614. 2018.
- [27] Erik-Oliver Blass and Florian Kerschbaum, *Strain: A Secure Auction for Blockchains*, Cryptology ePrint Archive, Report 2017/1044, 2017