Privacy-Preserving Netting in Local Energy Grids

Preprint version, to appear at IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020)
May 3-6, 2020, Toronto, Canada

Jacob Eberhardt, Marco Peise, Dong-Ha Kim, Stefan Tai
Technische Universität Berlin
Information Systems Engineering (ISE)
Berlin, Germany
{je, mp, st}@ise.tu-berlin.de
dong-ha.kim@campus.tu-berlin.de

***Abstract*—The production of renewable energies by individual households typically is small-scale and not profitable without public subsidies, yet a critical factor in preventing further global warming. Unlike market-based peer-to-peer trading solutions, which require households to engage in costly peer-to-peer trading activities, we propose a community-based approach where households in a local distribution grid share the energy they produce in a netting process to maximize internal consumption. The technical instantiation of this idea in real-world energy grids comes with several challenges. Households within a community do not necessarily trust each other or electric utilities. Furthermore, energy consumption data is highly sensitive and must be protected. Further idiosyncrasies of national energy markets, regulatory frameworks, and current grid infrastructure exist. Addressing all these challenges, we propose a blockchain-based system that leverages zero-knowledge off-chain computations to facilitate automated energy sharing within a community in a trustless and privacy-preserving way. We provide a proof-of-concept implementation using the ZoKrates framework for verifiable off-chain computations and the Ethereum Blockchain. To support our claims, we provide evaluation results obtained in the context of a major German national research project on blockchain-based energy networks.**

***Index Terms*—Energy Trading, Blockchain Privacy, ZoKrates, Off-chaining**

I. Introduction

Climate change is one of the greatest challenges of the century. To prevent further global warming, it is of paramount importance to reduce consumption of fossil energy sources. Increasing production from renewable energy sources is a crucial factor in this transition towards a more sustainable form of energy production.

Today, however, economic incentives for the small-scale production of renewable energies are not aligned. The costs of maintaining solar panels, for example, often exceed expected sales profits without government intervention.

A line of work addresses this problem by enabling households to trade energy they produce with each other or on public markets. Several proposals for blockchain-based peer-to-peer energy trading fall into this category [1]–[7].

However, these proposals deliberately do not consider the idiosyncrasies of the energy market and today's physical energy grids to a sufficient degree: Load profiles of individual households are hard to predict, which limits their ability to trade future energy flows [8]. Furthermore, market-based peer-to-peer trading approaches take a greenfield approach and do not consider existing restrictions and peculiarities [7], [9], [10]: Establishing a global, large-scale trading system where arbitrary pairs of households could engage in peer-to-peer trading would be disruptive on a technical and legal level and, therefore, hard to instantiate and deploy.

Therefore, to make an impact today, we propose a localized and community-oriented approach where households in a shared local distribution grid maximize their internal consumption: As of now, individual prosumers maximize the use of their own energy production, i.e., they only purchase the amount of energy from an Electric Utility that they do not produce themselves. In our approach, we expand this idea to a group of households in the same local distribution grid. Together, they form a community that shares the energy produced internally, and the Utility serves as a gateway providing or purchasing the residual load for that community. The locality of prosumption can unlock further economic benefits, e.g., reduced network charges or tax exemptions. Our approach considers the idiosyncrasies of the current energy grid, making it inclusive and realistic to deploy. Neither does it require changes to the physical energy grid, nor household production planning, or a change in participant's behavior.

The instantiation of this approach comes with several technical challenges: A community needs to reliably keep track of its internal production and consumption of energy. From this data, the residual load which needs to be purchased from a Utility to balance the grid can be calculated. We refer to this process of calculating community-internal net production and consumption values as *netting*. For this calculation, households in a community should neither have to trust each other, nor the Electric Utility. However, they can not rely on their calibrated and trusted metering infrastructure either as the netting of energy in a community does not reflect physically. Additionally, energy consumption data is highly sensitive, which further complicates this processing. This data allows detailed insights on household behavior [11] and hence must not be shared within a community.

As our core contribution, we propose a system design to address the challenges previously stated, i.e., we enable the calculation of nettings for a community in a trustless and privacy-preserving way: We leverage the ZoKrates language and toolkit [12] to calculate a netting for a community on blockchain-external resources while maintaining the blockchain's trustlessness property. The blockchain verifies this computation's correctness without ever learning the sensitive consumption data, which is hidden through ZoKrates computation's zero-knowledge property. Furthermore, we provide a characterization of desirable netting results for a community as well as an algorithm to compute such nettings efficiently.

Abstracting from the peculiarities of the specific use case, we provide a more fundamental result: We show how ZoKrates-based off-chain computations can be combined with a commitment scheme to execute a calculation in a group of mutually distrusting members with blockchain-properties and privacy-protection at the same time.

To assess the viability of our design, we implemented an open-source prototype[1] of the proposed system for the Ethereum Blockchain using the ZoKrates framework. We conducted an extensive evaluation in the context of *BloGPV*, a German national research project on renewable energy production.

II. Background

To set the scene, we provide necessary background on physical energy grids as well as energy markets and a prosumer's economic perspective. Our description is based on the German energy grid but stays sufficiently abstract so that our insights hold for other countries as well.

A. Energy Grid Organization

The energy grid is a physical network that enables the delivery of energy from producers to consumers. It can most easily be described by the responsibilities of its building blocks:

- **Generation**: Power plants and other producers generate energy they supply to the grid.
- **Transmission**: The transmission grid is responsible for long-distance energy transmission
- **Distribution**: The distribution grid takes care of stepping down energy, so it is usable by consumers and delivery to the location of consumption.
- **Consumptions**: Households and other consumers use the energy provided through the distribution grid.

For the remainder of this paper, we focus on local distribution grids, which we define as subsets of the distribution grid. Figure 1 show an example of a local distribution grid in which a Utility-controlled gateway and several households are directly connected.

[1] https://github.com/JacobEberhardt/decentralized-energy-trading

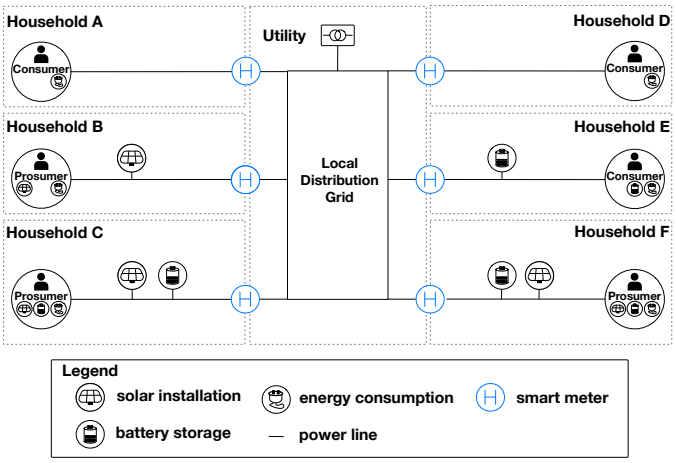

Fig. 1. Local Distribution Grid formed by Households and Utility.

B. Energy Market Organization

The energy market is the virtual place where compensation for utilization of the energy grid is organized. We can identify five logical groups of actors that fulfill distinct roles and participate in this market:

- **Utilities**: Enter contracts with Prosumers in order to buy and sell energy and balance residual loads in distribution grids.
- **Energy Exchanges**: Trading platforms where Utilities trade energy futures.
- **Prosumers**: Produce or consume energy in the grid.
- **Infrastructure System Operators**: Supply and maintain the physical infrastructure for energy transmission. They can be categorized by the layers of the energy grid described in Section II-A, e.g., Transmission System Operators. For their services, they are compensated by the other groups of actors.
- **Meter Operators**: Supply, maintain, and provide access to metering infrastructure and ensure that regulatory requirements are fulfilled. For these services, they are compensated by Utilities.

To illustrate the relationship between these actors involved in the energy market, we provide an overview of the communication and compensation flows in Figure 2.

C. Prosumer Economics

In the current, established model of energy supply, an electric Utility provides energy to consuming households through a local distribution grid. To ensure that the Utility cannot —intentionally or accidentally— bill the consumers for the incorrect amount of consumed energy, calibrated electricity meters are installed in households. In the context of this work, these are Smart Meters, i.e., electronic devices that collect measurements digitally and have communication and processing capabilities. Such a device serves as an independent reference point: Both consumers and suppliers can refer to it in case of disputes with regards to the amount of consumed energy.

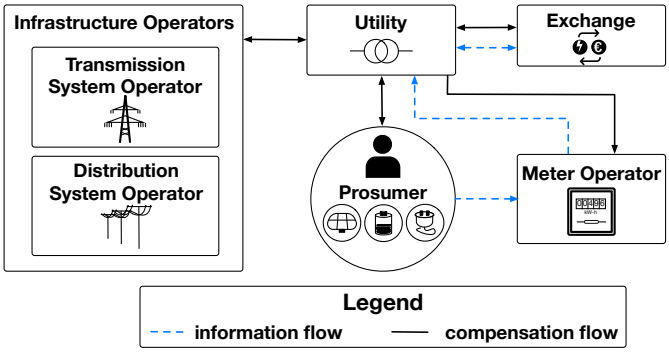

Fig. 2. Actors and their Relation in the Energy Market

For energy consumed, households pay a fixed price p_{buy}, which is contractually agreed on with the Utility in advance. Households that produce energy can sell it to the Utility at price p_{sell}. The Utility company sets these prices in a way that it makes a profit. We can express the relation between both prices as $p_{buy} = p_{sell} + \Delta_{margin}$. By netting consumption and production within a community, this margin can be internalized and benefit the participating households.

III. Related Work

In this section, we present results from literature that are relevant in the context of this paper and discuss their relation to our contributions. To structure this discussion, we classify related work in three categories: blockchain-based energy trading, privacy in smart grids, and privacy in blockchain-based energy trading.

A. Blockchain-based Energy Trading

There exists an extensive body of research in the context of blockchain-based energy trading. Numerous proposals have been surveyed by academia [13]–[15] and industry [16], [17]. Mengelkamp et al. [1] introduce a blockchain-based local energy market, where households trade future energy flows. Several other proposals suggest a comparable ex-ante auction mechanism to support peer-to-peer energy trading among households [4], [7]. Munsing et al. [3] propose a blockchain-based mechanism for microgrid balancing and control of distributed energy resources. Mihaylov et al. [9], [18] represent renewable energy production as cryptocurrency tokens called NRGcoins. These tokens can be traded and are used in a Utility-controlled pricing model to incentivize balancing local grids.

While similar in motivation, these market-based approaches require hard-to-predict future load profiles for individual households and do not consider privacy challenges in their design.

B. Privacy in Smart Grids

Privacy is recognized as a crucial property in Smart Grids as energy usage data can reveal household behavior and thus represents personally identifiable information [11], [19]. With the evolution of Smart Grids, privacy of consumer data became a key concern within the energy domain and was addressed by research before the advent of peer-to-peer trading [20], [21]. Solutions vary from zero-knowledge proofs [22], [23], hiding & anonymization techniques [24], [25], spatial and temporal aggregation [26], [27], homomorphic encryption, multi-party computations, and differential privacy [28] to simply adding noise.

Unlike our approach, these proposals attempt to hide information from Utilities and Meter Operators. In contrast, we primarily focus on the protection of personally identifiable information from other peers in a blockchain network. Hence, both lines of work should be combined for optimal privacy protection as they address different concerns.

C. Privacy in Blockchain-based Energy Trading

More closely related to our approach, there are some efforts to incorporate privacy requirements into blockchain-based designs for energy trading. Dorri et al. [29] propose an off-chain routing method to agree on prices for energy tokens and then execute the actual trade on-chain through an atomic swap which does not reveal participating smart meters. The work is conceptual and there is no implementation and evaluation available. In another token-based approach, Aitzhan et al. [5] propose *PriWatt*, a Bitcoin-based energy trading system that uses Bitmessage for anonymous messaging. While privacy is presented as a property of the proposed system, this does not reflect in the architecture or protocol design. Gai et al. [2] address linking attacks in blockchain-based energy trading by introducing noise in combination with dummy accounts. Laszka et al. [30] propose privacy-preserving energy transactions (PETra), a mixing-based approach to hide the ownership of energy tokens. Bergquist et al. [6] discuss potential improvements of this approach through anonymous routing and advanced mixing techniques.

In summary, these projects attempt to hide on-chain token ownership and transfer history, while in our approach, we never publish this information on the blockchain in the first place.

IV. System Design

In this section, we introduce a blockchain-based system design for trustless and privacy-preserving automatic netting to maximize a community's internal consumption.

Hereby, we proceed in two steps: First, we address the trust issue by proposing a blockchain-based system architecture. We add privacy protection for households through zero-knowledge off-chain computations in a second step.

A. A Blockchain-based Architecture

In the current energy market, without energy sharing in a community, consumers do not have to trust other actors. A Smart Meter measures the net produced or consumed energy for a household in a given time interval. The meter's balance is directly used for accounting by the Utility, which is the only trading partner. If there should ever be a dispute with the

Utility, the calibrated Smart Meter acts as the single source of truth.

This changes when a community of households uses a netting algorithm, as described in depth in Section VII, to maximize their internal consumption by reducing trading volume with the Utility as much as possible. In that case, meter readings are no longer sufficient: They do not report community-internal re-allocation of energy. This information cannot be measured, because energy transfers between households are purely virtual, i.e., happen on a logical level solely for accounting purposes. The virtual transfers do not reflect physically in the local distribution grid. Due to this loss of a trusted reference point, households would not be able to dispute invalid electricity bills. Hence, the Utility can no longer be in charge of accounting. Not can any other single party as the households mutually distrust each other.

To address this trust issue and thereby enable our netting-based approach to community-internal consumption maximization, we propose a blockchain-based system design. The core idea is to calculate the netting function in a Smart Contract deployed to a blockchain-network formed by households in a local distribution grid and the Utility. This design ensures decentralized, censorship-resistant, and agreed-on processing that does not require trust among the participants. Together, the calibrated electricity meters and our blockchain-based netting system re-establish a trusted reference point in a world with peer-to-peer energy sharing.

As depicted in Figure 3, the architecture comprises three main components: Smart Meters, Household Processing Units, and a Blockchain supporting Smart Contracts. The process of performing a trustless netting in the network is as follows:

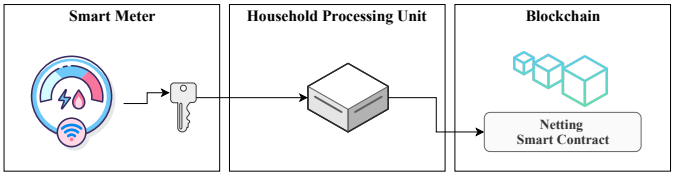

Fig. 3. Conceptual Architecture without Privacy Protection.

The *Smart Meter* periodically measures the energy consumption and production within a household through a set of internal sensors. It aggregates the sensor data to a net production value for a time interval h_t, i.e., the inputs to the netting Algorithm. h_t is measured in energy units, e.g., kWh or Ws, and has positive values for producers and negative values for consumers. The Smart Meter signs h_t and sends it to the Household Processing Unit (HPU).

Acting as a bridge, the *Household Processing Unit* receives $(h_t, sig(h_t))$ from the Smart Meter and registers it in the netting Smart Contract through a Blockchain-transaction. As the reported data is signed by the Smart Meter, the HPU cannot manipulate it without detection through the receiving Smart Contract. Being able to participate in the netting process provides a strong economic incentive always to report data. Withholding is possible but leads to opportunity costs.

The *Blockchain* is formed by the households and the Utility in a local distribution grid. It contains a *Netting Smart Contract* that is responsible for tracking energy consumption and execution of the *Netting Algorithm* N, which is triggered periodically and calculates $N(\vec{h}_t)$ (see Section VII). After a netting has successfully been performed on the Blockchain, the HPU retrieves its netting result $N(h_t)$ and the set of virtual transfers the household was involved in.

B. Adding Privacy

While successfully automating the netting process and addressing the trust challenge, the system design introduced in the previous section suffers from weak privacy guarantees. Potentially very sensible consumption data is shared between all participants in the Blockchain-network. All households can see each other's consumption due to the transparent processing within the Netting Smart Contract. Hence, in a second step, we improve on this system by strengthening households' privacy guarantees through leveraging verifiable zero-knowledge off-chain computations.

Zero-knowledge verifiable off-chain computations were proposed in [12] as a means to address privacy challenges in blockchains. Verifiable Off-chain computations [31] allow the execution of computations on blockchain-external resources, but retain blockchain's trustlessness through enabling the on-chain verification of the computation's correctness cryptographically. Zero-knowledge verifiable off-chain computations [32] allow information to be used in the off-chain computation without revealing it with the attestation of correctness. This property enables verifiable statements on private data, a property that we leverage in the design subsequently introduced.

To ensure privacy, households' consumption data must never be published on the Blockchain. The Netting Algorithm, however, does require access to that data. There seems to be a fundamental conflict: The netting needs to be calculated in a trustless way —which motivated a Blockchain-based design in the first place— and at the same time, the data necessary cannot be written to the Blockchain.

We resolve this conflict by introducing a new blockchain-external component, the *Netting Entity*, which executes the Netting Algorithm as a zero-knowledge verifiable off-chain computation. This modification allows the blockchain to verify that the computation happened correctly without requiring access to sensitive data. Still, the households need to be convinced that the correct input data was used for the off-chain computation, and the result they learn from the Netting Entity is the actual output and not some arbitrary data. We address this by binding participants to input and output values on the blockchain through cryptographic commitments [33], [34].

The architecture resulting from this extension is shown in Figure 4. Subsequently, we describe this novel privacy-preserving trustless netting process:

As in the previous design, the *Smart Meter* provides signed net production values $(h_t, sig(h_t))$ to the HPU. Additionally,

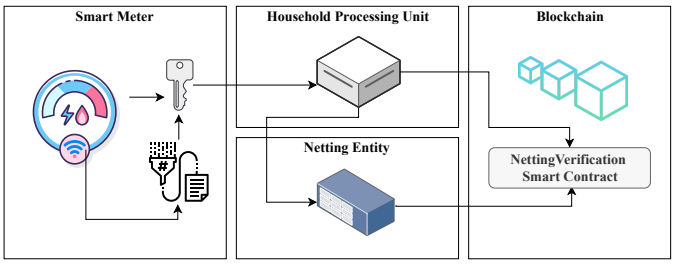

Fig. 4. Conceptual Architecture with Privacy Protection.

it now calculates $(comm(h_t), sig(comm(h_t))$, a signed commitments to these values and also sends it to the HPU.

The *Household Processing Unit*, on receipt, forwards the signed production values $(h_t, sig(h_t))$ to the new Netting Entity. It publishes $(comm(h_t), sig(comm(h_t))$, the production value commitments, to the NettingVerification Smart Contract on the Blockchain.

The new core component, the *Netting Entity*, contains a program which can be executed as a zero-knowledge verifiable off-chain computation and comprises the following three steps:

1) Calculate a netting result $N(\vec{h}_t)$ for the inputs $\vec{h}_t$ by executing a Netting Algorithm, but keep it private through the zero-knowledge property.
2) Calculate the commitments for the inputs $comm(\vec{h}_t)$.
3) Calculate the commitments for the netting results $comm(N(\vec{h}_t))$.

Executing this program produces the output $o_t = (\pi, comm(\vec{h}_t), comm(N(\vec{h}_t)))$, where π is the cryptographic attestation of correctness. After receiving production values $\vec{h}_t$ from the HPUs, the Netting Entity runs the program. The resulting output o is sent to the NettingVerification Smart Contract.

The *Blockchain* hosts a *NettingVerification Smart Contract*. This contract is no longer responsible for executing a Netting Algorithm directly. Instead, it stores commitments to inputs $comm(h_t)$ and verifies the correctness of netting computations by the Netting Entity. This verification comprises three steps:

1) Verify the cryptographic attestation π.
2) Verify the input commitments $comm(\vec{h}_t)$, i.e., check that the inputs to the Netting Algorithm used by the Netting Entity were the actual net production values previously committed to by the HPU.
3) Store the commitments to outputs $comm(N(\vec{h}_t))$.

To learn about the netting result, the HPU retrieves $N(h_t)$ and its virtual trades from the Netting Entity. It recalculates the commitment $comm(N(h_t))$ and compares it to the value stored in the NettingVerification Smart Contract. If equal, the HPU is convinced that the Netting Entity reported the netting result honestly.

This proposal enables the trustless and, at the same time, privacy-preserving netting of energy production in a local distribution grid. If the netting process fails for some reason, the system defaults to today's behavior where the Utility sells and purchases all energy. Note that while the netting entity is not trusted regarding the correctness of the netting, it is trusted with regards to privacy: A malicious netting entity could leak consumption data. This concern can be addressed by having the Meter Operator, which has access to all smart meter data by design, run the Netting Entity.

V. Implementation

In this section, we describe our proof-of-concept implementation of the system proposed in Section IV. The overall architecture is depicted in Figure 5. Our prototype is open-source and available on GitHub[2].

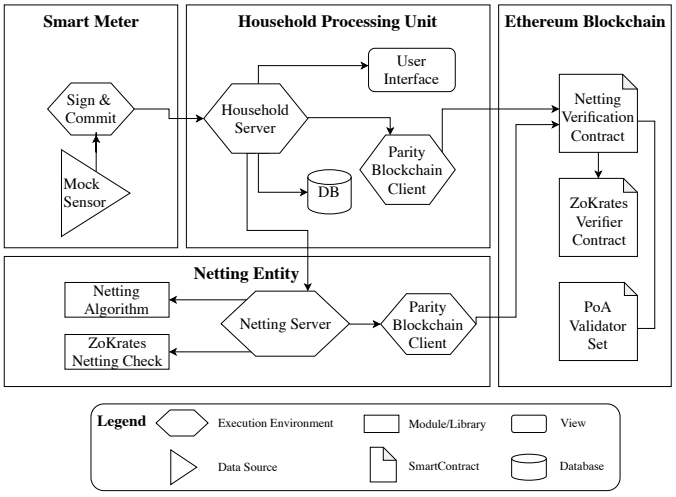

Fig. 5. Proof-of-Concept Implementation Architecture.

A. Smart Meter

In our prototype, we simulate the *Smart Meter* component through a lightweight `Node.js`[3] daemon. This allows testing and benchmarking of other components without depending on physical meters. A *Mock Sensor* draws data from a load profile generator[4] which realistically simulates energy consumption for households [35]. Signatures of and commitments to the data are calculated and then forwarded to the HPU together with the raw data. As a commitment scheme $comm$, we chose $comm(v) = sha256(v||r)$, where v is the value committed to and r is a random number.

B. Household Processing Unit

Our implementation of the *Household Processing Unit* comprises four sub-components: a Household Server, a Database, a User Interface, and a Blockchain Client. The implementation of the HPU is designed to run on resource-constrained devices, e.g., on Raspberry Pies that are attached to the Smart Meters in the *BloGPV*[5] research project's field test environment. Built with `Node.js`[3], the Household Server's main tasks is communication with the Netting Entity and the Blockchain

[2]https://github.com/JacobEberhardt/decentralized-energy-trading
[3]https://nodejs.org
[4]https://github.com/loadprofilegenerator/automation
[5]https://blogpv.net/

according to the description in Section IV. Additionally, it serves a *User Interface* for end-users, which displays energy consumption over time, lists peer-to-peer transfers, and shows relevant network statistics. We provide a screenshot in Figure 6. The UI is implemented with `React`[6] and the displayed data is retrieved from the household server through a REST-API, where it is persisted in a MongoDB[7] instance. To connect the HPU to the Blockchain, we chose a Parity Ethereum Client[8].

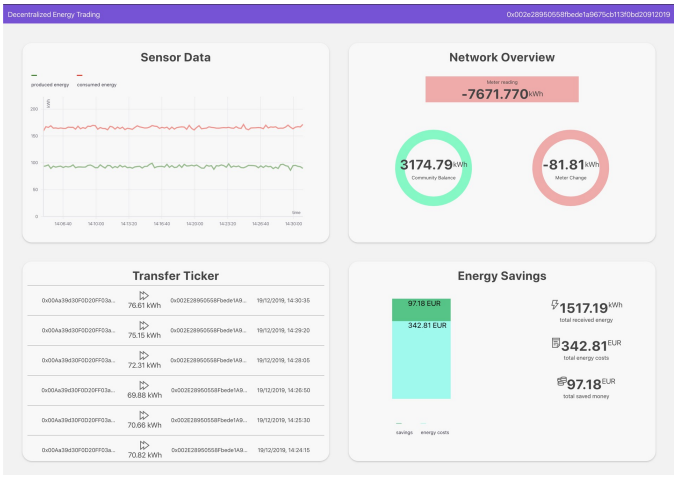

Fig. 6. User Interface presented to a Household.

C. Netting Entity

The *Netting Entity* consists of a *Netting Server* implemented in `Node.js`[3] that triggers the Netting Algorithm and invokes a ZoKrates Netting Check, as well as a Parity Ethereum Client.

Here, the implementation is slightly different from the design introduced in Section IV: Instead of directly encoding Algorithm 1 in a ZoKrates program, we run the algorithm in a *Netting Algorithm* component implemented in `JavaScript`. In a second step, a ZoKrates program called *ZoKrates Netting Check* checks and proves that *Consistency*, *Pareto Efficiency* and *Proportional Fairness* as introduced in Section VII hold for the previously calculated netting result. To account for rounding in the netting algorithm implementation, we tolerate an error ϵ for the *Proportional Fairness* property. We do this for efficiency, as ZoKrates programs involve overhead: Computing a netting is more complex than asserting a set of desirable properties for a given netting result. However, checking and proving these properties is sufficient, so that the netting itself can be computed in a low overhead execution environment. This approach is similar to how NP-complete problems are described: an NP-complete algorithm is hard to compute, but a given solution is easy to verify. A further advantage is that this design allows the Netting Algorithm to be changed without any other modifications in the system, as long as the invariants hold

[6]https://reactjs.org/
[7]https://www.mongodb.com
[8]https://www.parity.io/ethereum/

D. Blockchain

For our prototype, we chose Ethereum as an established state-of-the-art Smart Contract–enabled Blockchain. Furthermore, ZoKrates natively supports Ethereum and generates Smart Contracts for proof verification. We assume the Ethereum Blockchain to be deployed as a private network that connects households and the Utility in a local distribution grid. As a consensus algorithm, we chose Proof-of-Authority (PoA). In our deployment, calibrated Smart Meters represent authorities and sign transactions on behalf of HPUs which run blockchain clients. These authorities are registered in the *PoA Validator Set Contract* that stores a list of validators allowed to sign blocks as part of the PoA Consensus. In this setup, each household independently validates and votes on all blockchain transactions, thereby establishing a trustworthy reference point. Due to the close proximity of nodes in a local distribution grid in combination with PoA, high transaction throughput can be achieved, i.e., block intervals can be short and block gas limits high. The registry of Smart Meters in the local distribution grid in the PoA Validator Set Contract serves a second purpose: It allows the Netting Verification Contract to ensure that commitments to household net production values actually come from a calibrated Smart Meter. The *ZoKrates Verifier Contract* is generated by the ZoKrates toolchain and acts as a library, which supports checking an attestation of netting correctness' validity. It is called by the *NettingVerification Contract* as introduced in Section IV.

As a summary, we provide an overview of the netting process in Figure 7.

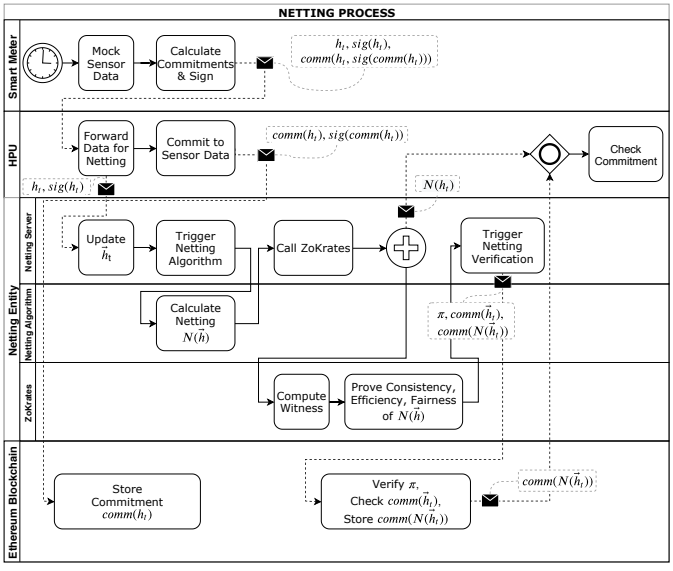

Fig. 7. Overview of the Netting Process.

VI. Evaluation

In the field test within the *BloGPV* research project, we assume a netting interval of 15 minutes and a local distribution grid comprising 100 households. This netting interval defines

the upper bound for the time it can take to calculate the netting and then prove its *Correctness*, *Pareto Efficiency*, and *Fairness* in a ZoKrates program within that netting interval. The other component implemented as part of our prototype are very lightweight and fulfill their tasks for a netting interval within microseconds, even in resource-constrained environments. Therefore, we can limit our performance evaluation to the Netting Entity. Here, the calculation of the netting algorithm completes in microseconds and is hence negligible.

In Figure 8, we show benchmarks for program execution and proof generation time. The benchmarks were performed on a consumer laptop with an Intel Core i7-6920HQ @2.9 GHz processor, 16 GB RAM, and a 1 TB SSD. Together, program execution and proof generation take 14 min without optimizations. Hence, the overall netting time stays below the set 15-minute goal. Thus, we leave optimizations for future work. We expect significant speedups from optimizations in the ZoKrates code, e.g., the use of Pedersen commitments [36] instead of our hash-based commitment scheme. Furthermore, the process could be accelerated through more powerful hardware.

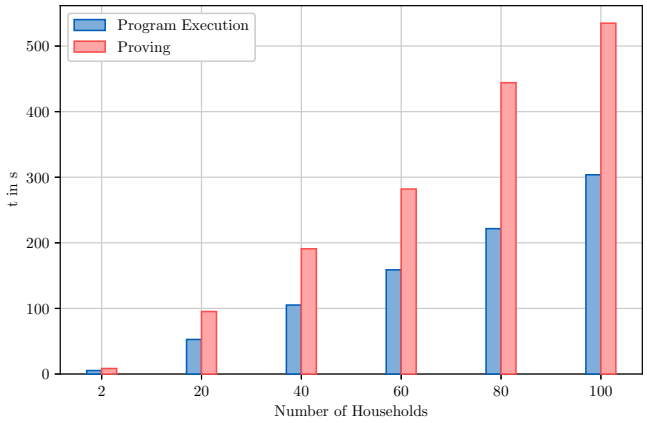

Fig. 8. Program Execution and Proving Time for the ZoKrates Program.

We provide an overview of the gas cost required for the verification of a netting result in the NettingVerification Smart Contract in Figure 9. As the private blockchain employed in the field test is formed by participants of the local distribution grid with low network latencies, the required gas-throughput is easily achieved.

VII. Netting

To incentivize the production of renewable energies, we propose a community-oriented trading model where households maximize the use of energy within their community. This re-allocation among households minimizes the amount of energy traded with Utilities. A Utility only sells or buys the residual load, i.e., the net amount of energy prosumed in a local distribution grid. Hence, we refer to this approach as *netting*.

Unlike related work (see Section III-A), which commonly seeks to bring together future demand and supply, we take

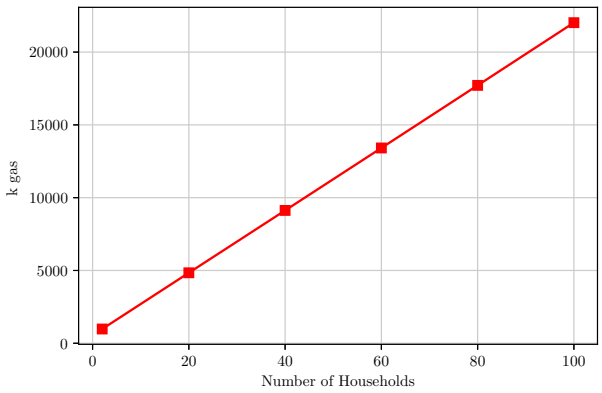

Fig. 9. On-chain Verification Cost of a Netting Result.

an ex-post perspective: For a given time interval, energy is produced and consumed. After the interval passed, we observe the amount of energy that was produced and consumed within the local distribution grid. Based on that data, we calculate a netting, which introduces transfers that happen within a community and thereby minimizes the energy traded with the Utility. Essentially, this approach only affects accounting. The physical energy flow is not affected.

Compensation for the transfers within a community can happen but does not have to. Households are never worse off after a netting, so they may be satisfied by occasionally receiving and giving away energy for free.

A. Characterizing Desirable Netting Results

As described before, the netting process comprises the creation of virtual transfers between households so that only residual load is traded with the Utility. However, there are many possible ways to allocate these energy flows to households in the network. In this section, we define desirable properties of netting results and formulate characterizing invariants. These properties should be considered during the design of netting algorithms.

Let $\vec{h} = \left(h_1, h_2, \ldots, h_n\right)^T \in \mathbb{R}^n$ be the grid energy trading balance as a vector of net energy sales of $n \in \mathbb{N}$ households to the Utility for a given time interval. These values are denoted in energy units, e.g., kWh or Ws, and are positive for sellers and negative for buyers. The total amount of energy bought from the Utility $e_b \colon \mathbb{R}^n \to \mathbb{R}$ and the total amount of produced energy sold to the Utility $e_s \colon \mathbb{R}^n \to \mathbb{R}$ are defined as:

$$e_b(\vec{h}) = \sum_i^n min(h_i, 0), \quad e_s(\vec{h}) = \sum_i^n max(0, h_i)$$

For convenience, instead of writing $e_b(\vec{h})$ and $e_s(\vec{h})$, we write e_b and e_s. We define a netting algorithm as a function $N \colon \mathbb{R}^n \to \mathbb{R}^n$, which calculates the new and reduced net trading volume with the Utility $\vec{h}_{net}$.

Let N be an arbitrary netting algorithm. We now define the invariants as follows:

1) Consistency: After a successful netting, the total energy balance within the grid remains unchanged, i.e., energy is never artificially lost or introduced into the system.

$$e_b(\vec{h}) + e_s(\vec{h}) = e_b(N(\vec{h})) + e_s(N(\vec{h}))$$

While this invariant is the weakest of all, it is also the most fundamental which characterizes all valid netting algorithms.

2) Pareto Efficiency: No household should ever be worse off after participating in a netting. This property is captured through the following invariant:

$$|N(\vec{h})_i| \leq |\vec{h}_i| \quad \forall i \in \{1, \ldots, n\}$$

Pareto Efficiency indicates that after a successful netting, no producing household sells more energy to the Utility, and no consuming household buys more energy from the Utility than before.

3) Fairness: Fairness characterizes how the benefits that can result from netting should be allocated to participating households. There are many different ways to define fairness, e.g., lower participation threshold or equal distribution. We introduce the notion of *Proportional Fairness* as a specific type of fairness that suits our use case.

In a proportionally fair netting, the benefits gained from minimizing trading volume with the Utility are allocated to households in proportion to their prosumption. We distinguish two cases depending on the between e_b and e_s:

1) $e_b \geq e_s$: In this case, households consumed at least as much energy as they produced. All energy produced by households is allocated to consuming households in proportion to their consumption:

$$N(\vec{h})_i = \begin{cases} h_i + e_s \cdot \frac{h_i}{e_b}, & h_i < 0 \text{ (consumer)} \\ 0, & \text{otherwise} \end{cases}$$

2) $e_b < e_s$ In this case, households produced more energy than they consumed. All consumed energy can be supplied from within the community directly, and the residual production is sold to the Utility. Here, the share a producer transfers to consuming households is proportional to its share of the overall production:

$$N(\vec{h})_i = \begin{cases} h_i + e_b \cdot \frac{h_i}{e_s}, & h_i > 0 \text{ (producer)} \\ 0, & \text{otherwise} \end{cases}$$

B. A Fair and Constructive Netting Algorithm

After characterizing desirable netting results, we now introduce an algorithm to compute a netting that fulfills these properties. This algorithm reduces the amount of energy traded with the Utility and instead maximizes trading volume between households. It is *constructive*, i.e., it computes and records virtual trades between households in the process.

Algorithm 1 computes a netting result which fulfills *Consistency*, *Efficiency*, and *Proportional Fairness* up to a rounding error ϵ. Let $\vec{h} = (\vec{h}_s, \vec{h}_b)$ be the grid energy trading balance ordered by selling and purchasing households, e_s, e_b the total amount of energy sold to and bought from the Utility, as defined in Section VII-A.

Algorithm 1 Proportional Netting

procedure NET(e_s, e_b, $\vec{h}_s$, $\vec{h}_b$)
  if $|e_s| < |e_b|$ **then**
    $\vec{h}_{from}, e_{from}, \vec{h}_{to}, e_{to} \leftarrow \vec{h}_s, e_s, \vec{h}_b, e_b$
  else
    $\vec{h}_{from}, e_{from}, \vec{h}_{to}, e_{to} \leftarrow \vec{h}_b, e_b, \vec{h}_s, e_s$

  for all $h_t \in \vec{h}_{to}$ **do**
    $e_{allocate} \leftarrow \left\lfloor e_{from} * \frac{h_t}{e_{to}} \right\rfloor$
    for all $h_f \in \vec{h}_{from}$ **do**
      if $e_{allocate} \neq 0$ **then**
        if $|e_{allocate}| \leq |h_f|$ **then**
          $h'_f, h'_t \leftarrow transfer(h_f, h_t, e_{allocate})$
          $e_{allocate} \leftarrow 0$
        else
          $h'_f, h'_t \leftarrow transfer(h_f, h_t, h_f)$
          $e_{allocate} \leftarrow e_{allocate} - h_t$
        $\vec{h}_{from}[index(h_f)] \leftarrow h'_f$
        $\vec{h}_{to}[index(h_t)] \leftarrow h'_t$
  return $\vec{h}_{from}, \vec{h}_{to}$
procedure TRANSFER(h_{from}, h_{to}, e)
  record $(index(h_{from}), index(h_{to}), e)$
  $h_{from} \leftarrow h_{from} - e$
  $h_{to} \leftarrow h_{to} + e$
  return h_{from}, h_{to}

The computed netting function $N\colon \mathbb{R}^n \to \mathbb{R}^n$ reassigns the new energy balances of each household as a state transition:

$$N(\vec{h}) = \begin{cases} min_i(h_i + \left\lfloor e_s \cdot \frac{h_i}{e_b} \right\rfloor, 0 + \frac{\epsilon}{n}), & \text{if } |e_b| \geq e_s \\ max_i(0 + \frac{\epsilon}{n}, h_i + \left\lfloor e_b \cdot \frac{h_i}{e_s}) \right\rfloor, & \text{otherwise} \end{cases}$$

where min_i and max_i are the element-wise min and max functions.

VIII. Conclusion

In this paper, we introduced a blockchain-based and privacy-preserving system design for energy sharing within a community through ZoKrates-based verifiable off-chain computations. We described our open-source proof-of-concept implementation and its extensive evaluation within the *BloGPV* research project. More generally, we show how ZoKrates-based off-chain computations can be combined with on-chain commitments to execute algorithms in a group of distrusting members with blockchain-properties while preserving privacy.

Acknowledgment

We thank Paul Etscheit, Julia Holz, Simon Huber, Pablo Osinaga, Myron Rotter, Umar Siddiq, Duy Minh Vo, and Daniyal Warsi for their contributions to the implementation.

A part of the work in this paper was performed in the context of the BloGPV-Blossom project. BloGPV-Blossom is partially funded by the Germany Federal Ministry for Economic Affairs and Energy (BMWi) under grant no. 01MD18001E.

REFERENCES

[1] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science - Research and Development*, vol. 33, no. 1-2, pp. 207–214, Feb. 2018. [Online]. Available: http://link.springer.com/10.1007/s00450-017-0360-9

[2] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8613816/

[3] E. Munsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *2017 IEEE Conference on Control Technology and Applications (CCTA)*. Mauna Lani Resort, HI, USA: IEEE, Aug. 2017, pp. 2164–2171.

[4] J. Horta, D. Kofman, D. Menga, and A. Silva, "Novel market approach for locally balancing renewable energy production and flexible demand," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2017, pp. 533–539.

[5] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7589035/

[6] J. Bergquist, A. Laszka, M. Sturm, and A. Dubey, "On the design of communication and transaction anonymity in blockchain-based transactive microgrids," in *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers - SERIAL '17*. Las Vegas, Nevada: ACM Press, 2017, pp. 1–6. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3152824.3152827

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

[8] M. Chaouch, "Clustering-based improvement of nonparametric functional time series forecasting: Application to intra-day household-level load curves," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 411–419, 2013.

[9] M. Mihaylov, I. Razo-Zapata, R. Rădulescu, S. Jurado, and A. Avellana, Narcisand Nowé, "Smart grid demonstration platform for renewable energy exchange," in *Advances in Practical Applications of Scalable Multi-agent Systems. The PAAMS Collection*, Y. Demazeau, T. Ito, J. Bajo, and M. J. Escalona, Eds. Cham: Springer International Publishing, 2016, pp. 277–280.

[10] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8234700/

[11] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*. ACM, 2010, pp. 61–66.

[12] J. Eberhardt and S. Tai, "ZoKrates - Scalable Privacy-Preserving Off-Chain Computations," in *IEEE International Conference on Blockchain*. IEEE, 2018.

[13] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143 – 174, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032118307184

[14] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Oct 2017, pp. 6153–6158.

[15] N. U. Hassan, C. Yuen, and D. Niyato, "Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges and Solutions," *arXiv e-prints*, p. arXiv:1909.02914, Sep 2019.

[16] BDEW, "Blockchain in the energy sector - the potential for energy providers," BDEW, 2018, 2018, available at: https://www.bdew.de/media/documents/Studie-Blockchain-englische-Fassung-Dez.2018.pdf, Accessed: 2019-11-27.

[17] DENA, "Blockchain in the integrated energy transition," https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2019/dena-Studie_Blockchain_Integrierte_Energiewende_EN2.pdf, 2019, accessed: 2019-11-27.

[18] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowé, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *11th International Conference on the European Energy Market (EEM14)*, May 2014, pp. 1–6.

[19] F. Pallas, "Beyond gut level–some critical remarks on the german privacy approach to smart metering," in *European Data Protection: Coming of Age*. Springer, 2013, pp. 313–345.

[20] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2820–2835, Fourthquarter 2017.

[21] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344 – 1371, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613000042

[22] M. Jawurek, M. Johns, and F. Kerschbaum, "Plug-In Privacy for Smart Metering Billing," in *Privacy Enhancing Technologies*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, S. Fischer-Hübner, and N. Hopper, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, vol. 6794, pp. 192–210. [Online]. Available: http://link.springer.com/10.1007/978-3-642-22263-4_11

[23] A. Rial, G. Danezis, and M. Kohlweiss, "Privacy-preserving smart metering revisited," *International Journal of Information Security*, vol. 17, no. 1, pp. 1–31, 2018.

[24] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in *2010 First IEEE International Conference on Smart Grid Communications*. Gaithersburg, MD, USA: IEEE, Oct. 2010, pp. 232–237.

[25] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *2010 First IEEE International Conference on Smart Grid Communications*. Gaithersburg, MD, USA: IEEE, Oct. 2010, pp. 238–243.

[26] T. Dimitriou and G. Karame, "Privacy-friendly tasking and trading of energy in smart grids," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. ACM, 2013, pp. 652–659.

[27] A. Ahadipour, M. Mohammadi, and A. Keshavarz-Haddad, "Statistical-based privacy-preserving scheme with malicious consumers identification for smart grid," *CoRR*, vol. abs/1904.06576, 2019. [Online]. Available: http://arxiv.org/abs/1904.06576

[28] G. Ács and C. Castelluccia, "I Have a DREAM! (DiffeRentially privatE smArt Metering)," in *Information Hiding*, T. Filler, T. Pevný, S. Craver, and A. Ker, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, vol. 6958, pp. 118–132. [Online]. Available: http://link.springer.com/10.1007/978-3-642-24178-9_9

[29] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak, and Z. Y. Dong, "Spb: A secure private blockchain-based solution for energy trading," 2018.

[30] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," in *Proceedings of the Seventh International Conference on the Internet of Things*, ser. IoT '17. New York, NY, USA: ACM, 2017, pp. 13:1–13:8. [Online]. Available: http://doi.acm.org/10.1145/3131542.3131562

[31] J. Eberhardt and S. Tai, "On or off the blockchain? insights on off-chaining computation and data," in *European Conference on Service-Oriented and Cloud Computing*. Springer, 2017, pp. 3–15.

[32] J. Eberhardt and J. Heiss, "Off-chaining models and approaches to off-chain computations," in *Proceedings of the 2Nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, ser. SERIAL'18. New York, NY, USA: ACM, 2018, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/3284764.3284766

[33] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *ACM SIGACT News*, vol. 15, no. 1, pp. 23–27, 1983.

[34] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[35] N. Pflugradt. Load profile generator. https://www.loadprofilegenerator.de/. Accessed: 2019-11-29.
[36] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Annual International Cryptology Conference*. Springer, 1991, pp. 129–140.