On the Performance of Consensus Mechanisms in Privacy-Enabled Decentralized Peer-to-Peer Renewable Energy Marketplace

Roman-Valentyn Tkachuk*, Dragos Ilie*, Remi Robert**, Victor Kebande*, and Kurt Tutschku*
*Department of Computer Science, Blekinge Institute of Technology, Karlskrona, Sweden
Email: roman-valentyn.tkachuk@bth.se, dragos.ilie@bth.se, victor.kebande@bth.se, kurt.tutschku@bth.se
**Ericsson Research, Stockholm, Sweden , Email: remi.robert@ericsson.com

***Abstract*—This work defines a decentralized blockchain-based peer-to-peer (P2P) energy marketplace which addresses actors' privacy and the performance of consensus mechanisms. The defined marketplace utilizes private permissioned Ethereum-based blockchain client Hyperledger Besu (HB) and its smart contracts to automate the P2P trade settlement process. Also, to make the marketplace compliant with energy trade regulations, it includes the regulator actor, which manages the issue and generation of guarantees of origin and certifies the renewable energy sources used to generate traded electricity. Finally, the proposed marketplace incorporates privacy-preserving features, allowing it to generate private transactions and store them within a designated group of actors. Performance evaluation results of HB-based marketplace with three main consensus mechanisms for private networks, *i. e.*, Clique, IBFT 2.0, and QBFT, demonstrate a lower throughput than another popular private permissioned blockchain platform Hyperledger Fabric (HF). However, the lower throughput is a side effect of the Byzantine Fault Tolerant characteristics of HB's consensus mechanisms, *i. e.*, IBFT 2.0 and QBFT, which provide increased security compared to HF's Crash Fault Tolerant consensus RAFT.**

***Index Terms*—Renewable Energy Marketplace; Blockchain Technology; Peer-To-Peer Energy Trading; Hyperledger Besu; Data Privacy;**

I. Introduction

Energy distribution systems play a vital role in modern societies. The dependency on electricity supply transcends every aspect of a society's operation, making it a necessity. However, the electricity production conducted by power plants that work on fossil fuels results in atmosphere carbonization. In order to make electricity generation cleaner, renewable energy sources (RES), *e. g.*, solar panels, were introduced as an alternative to fossil fuel ones. Consequently, the introduction of RES opened opportunities for electricity prosumers, *i. e.*, producers/consumers, to become a part of the grid as a distributed energy resource (DER) [1]. This allows prosumers to not only consume energy as a conventional node but also to produce and output it to the energy grid [2]. Further, prosumers can also trade the produced electricity through the energy marketplace, which incentivizes the installation of RES and the production of green electricity. However, today's energy markets face a number of challenges when it comes to management and operation. The first is the *inflexible pricing model* of today's marketplaces, where the prosumer is limited to selling the generated electricity to a single buyer without any other options. In addition, the generated electricity is sold at a price set by the buyer through a governmental body, *e. g.*, country's energy agency regulates the margins for the RES-produced electricity selling and leaves no room for negotiation [3]. The second is *inaccurate consumption information*, *i. e.*, buyers receive unreliable information about the sources of the electricity they consume. Nowadays, the information about RES-produced electricity is recorded in the *guarantee of origin* (GO). GO is proof to the buyer that a given quantity of electricity was produced by the RES [4]. However, due to the inflexibility of energy distribution systems, *e. g.*, unavailability of RES in close proximity to consumers, they still end up using the electricity produced by fossil fuel energy sources while having the GO [5].

These limitations can be alleviated by introducing the *peer-to-peer* (P2P) *electricity trading*, which is an automated sale process for renewable energy between market participants using a contract with pre-determined conditions [4]. A P2P energy trade settlement allows prosumers to trade electricity directly with each other, enabling them to control when, where, and for what price the electricity is bought or sold. The ultimate goal of P2P energy trading is the widespread adoption of RESs, resulting in the decarbonization of the energy distribution systems [6].

Today's marketplaces are built as centralized systems. Thus, a *trusted third-party* (TTP) (typically a prosumer's energy provider) has to be present to guarantee that the predetermined conditions of a P2P energy trading contract are followed. *However, trust issues are raised, when it comes to scaling the marketplace to more than one energy provider*. Energy providers want to keep their operations private to maintain a competitive advantage in the electricity market. This requires the introduction of an external TTP that can be trusted by all energy providers within the marketplace [7], *i. e.*, allowing individuals belonging to different energy providers to trade with each other. To remediate these limitations, a *decentralized marketplace architecture* can be used to distribute control over the marketplace operations to multiple energy providers. However, all organizations require an efficient and robust consensus-reaching mechanism that provides guarantees that P2P trade settlement conditions are followed while maintaining actors' data privacy. Such capabilities can be provided by blockchain technology [8]. Blockchain provides

marketplace participants with distributed storage, *i. e.,* the ledger, and brings such benefits as provenance, accountability, transparency, and privacy to all data processed in a system. It also acts as a consensus-reaching platform, allowing initially non-trusting energy providers and prosumers to establish a trusted relationship and conduct P2P trade settlements without needing a single TTP acting as a middleman [9].

Based on the challenges discussed above, the main contributions of this study can be summarized as follows. This study defines a decentralized blockchain-based P2P energy marketplace that utilizes *Hyperledger Besu* (HB) [10] as the blockchain platform. The proposed marketplace utilizes HB's *smart contracts* (SCs) to automate P2P energy trade settlement and issue and consume GOs. To make the marketplace compliant with energy trade regulations, it incorporates the *regulator* actor, which manages the issue and consumption of GO and certifies the RES used to generate traded electricity. Further, the marketplace utilizes Tessera private transaction manager to ensure actor data privacy. The following methodology was used to define the proposed marketplace. First, with advice from an energy provider, we define a set of regulatory and operational requirements. Further, we define the marketplace's architecture and detail its implementation. Next, we present the performance evaluation with the SC tailored for P2P energy trading. We investigate in-depth the performance of the main Proof of Authority (PoA) consensus mechanisms supported by HB, *i. e.,* QBFT, IBFT 2.0, and Clique. Finally, we provide a summary of observations on the mechanisms that lead to secure consensus while preserving actors' data privacy.

The remainder of the paper is structured as follows. Section II describes the actors for the proposed marketplace, details its blockchain platform, and implementation. Section III details the performance evaluation process and results. Section IV describes related work on energy marketplaces and their performance evaluation. Finally, Section V draws a summary of the proposed marketplace and provides an outlook.

II. Blockchain-based Energy Marketplace

The energy marketplace is subject to several regulatory constraints, which must be met to satisfy current P2P energy trade regulations, *i. e.,* GOs and an automated trade contract. Thus, the proposed marketplace requirements are aligned with regulations described in D2018/2001 of the European Parliament [4] regarding the issuing, trading, and consumption of GOs. To align with D2018/2001, we introduce a *regulator* role in the proposed marketplace. The regulator is an actor that manages the issue and consumption of GOs, which are required to execute a trade settlement contract. Further, the regulator certifies the RES used to generate traded electricity. To the best of our knowledge, none of the other energy marketplace studies are taking into consideration such governmental regulatory requirements in conjunction with actors' data privacy. Finally, the marketplace actors and requirements were defined in collaboration with the authors' local energy provider, which has DERs as a part of their grid infrastructure.

A. Marketplace Actors

Energy marketplace actors and their respective places in the grid infrastructure are depicted in the *Physical Layer* in Figure 1. The *prosumer* represents a DER in an energy grid with an installed RES. The prosumer's main interest in becoming a part of the marketplace is to control the conditions of energy trade settlement, *e. g.,* to sell electricity at a better price. Further, prosumers want to get GO for the electricity they produce within the marketplace's automated system.

The *energy provider* is an actor that manages the energy grid to which the prosumer is connected. As a local central point in the energy distribution scheme, the energy provider collects data on electricity consumption fluctuations to optimize distribution and conduct an accounting of the electricity and money flows in its network. Further, energy providers want to expand their DER infrastructure to meet customer demand for RES-generated energy delivery.

The *regulator* is the representative of governmental authority who manages the issue and consumption of GOs. The GO acts as proof that the electricity was generated with RES and has to be presented during the trade transaction by the prosumer-seller. Further, the regulator is the entity that certifies prosumers' RES and ensures the correct mapping between the generated and marketplace-traded electricity.

B. Blockchain Platform

To enable marketplace actors' to conduct P2P trade settlement, the blockchain platform has to be chosen. Considering the privacy requirements, the proposed marketplace utilizes a private permissioned blockchain platform. Permissioned blockchain network has an identity and access management (IAM) [11] mechanism that defines a set of entities, *i. e.,* collaborating organizations and users, which are allowed to access the network. Further, permissioned blockchain requires that after entering the network, the entity has to be authorized to execute new transactions and add them to the global ledger. Finally, private blockchains enable data privacy and better address the demands of the business use-cases [12]. *Hyperledger Besu* (HB) [10] is representative of private permissioned blockchain platform. It is an open-source Ethereum [13] client that was first developed by Pegasys and later handed over to the Hyperledger Foundation. From the beginning, the Ethereum blockchain was designed as a public permissionless platform, *i. e.,* opened for everyone to join and generate transactions. HB can be considered an adaptation of the original public Ethereum blockchain to the private context. Here, HB implements the *Enterprise Ethereum Alliance Protocol* to enable such functionality as private transactions, IAM, and permissioning. In the HB network, the *validator* nodes order, execute and verify transactions in the blockchain network. However, validator nodes cannot be used to initiate transactions. All transactions in the HB network are initiated by *user accounts*, which represent a public and private key pair that can be generated off-chain. The smart contract (SC) defines functions a user account can call to operate on the data in the ledger. First, SC has to be installed in the

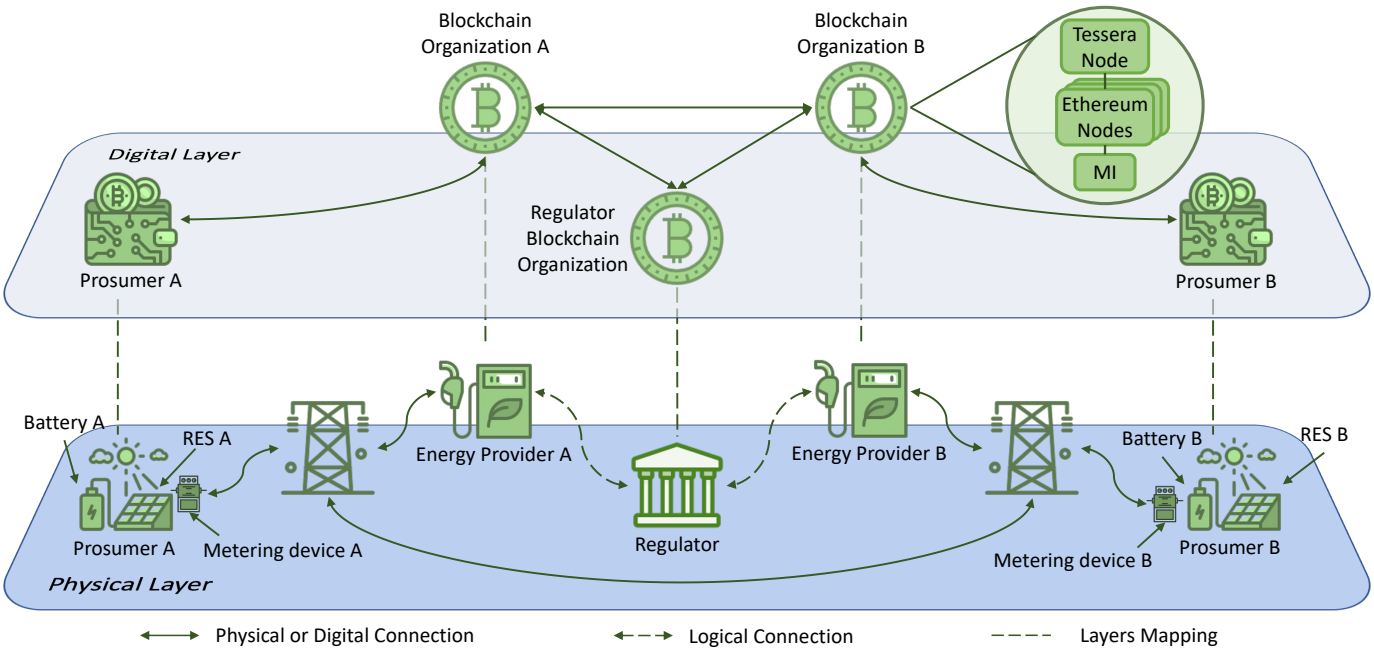

Fig. 1: Energy Marketplace. *(Physical layer, i.e., energy grid, is mapped to a digital blockchain-based layer, where the electricity trade operations are executed).*

blockchain network. Once installed, it serves as a predefined trade settlement contract where fixed, agreed-upon rules are enforced during every execution.

C. Data Privacy

In HB, private data is stored in transactions that are disclosed only to a subset of network participants (further referred to as privacy group (PG)). The private transactions in HB are handled by the *Tessera* private transaction manager. Each organization in HB must have a Tessera node to participate in private transactions. When a new private transaction is generated, it is passed from the Ethereum node to the Tessera node associated with it. Further, the Tessera node encrypts the transaction and distributes it to the PG. Recipient Tessera Nodes from PG decrypt the transaction and pass it to their Ethereum Nodes. Further, the rest of the nodes outside of PG receive the record confirming that the private transaction was executed. This record is written into the global ledger. Such an approach may result in limited auditability of private transactions. Since the nodes outside of PG receive only the record about transaction execution and not the hash of the transaction itself, *i. e.*, supported in Hyperledger Fabric (HF) [14], there is no way to verify the integrity of private transaction data in case it has to be disclosed.

In the public Ethereum network, *gas* is required to execute a transaction. In contrast, privacy-enabled HB Ethereum networks allow disabling gas spending to execute both ordinary and private transactions. This requires a certain level of trust among the blockchain network transacting nodes, *i. e.*, none of the participants will act maliciously and perform a denial of service (DoS) attack by flooding the network with transactions. Thus, privacy-enabled networks must have off-chain trust-enabling mechanisms, including smart contract deployment recommendations and legal consequences for malicious activity.

D. Consensus Mechanisms

The consensus mechanism defines an algorithm by which all nodes in the network can agree on the validity of transaction order in the block. While proof of work (PoW) [8] worked in a public blockchain, it was unsuitable for private deployment, *i. e.*, low transaction throughput and high energy consumption to mine new blocks. Hence, a new approach was followed in private Ethereum called proof of authority (PoA). The blocks in PoA consensus mechanisms are not mined but signed by the designated pool of validators, *i. e.*, avoid wasting energy by delegating block creation to the trusted nodes.

Within the available consensus mechanisms, some are identified as Byzantine Fault Tolerant (BFT) and/or Crash Fault Tolerant (CFT) [15]. CFT consensus mechanisms are protected from node failures, *i. e.*, if less than 50% of the nodes fail, the network can operate successfully. If consensus is BFT, it is both CFT and can operate in the presence of adversaries, *e. g.*, nodes that manipulate transactions. The improved security of BFT consensus mechanisms may come at the cost of decreased performance compared to CFT ones.

The consensus mechanisms supported by the HB are PoW (Ethash), Proof of Stake (PoS), and PoA (Clique, IBFT 2.0, and QBFT). This study concentrates on PoA consensus mechanisms used in private HB networks. When comparing consensus mechanisms, such characteristics as *immediate finality*, *quorum (minimum number of validators)*, *liveness*, and *throughput* have to be considered. Immediate finality refers to the ability to avoid forks, *i. e.*, alternative blockchains or chain reorganizations. Quorum refers to the minimum number of validator nodes in the blockchain network. Liveness refers to

how many failed validators it can sustain and continue normal operation. Throughput refers to the maximum possible write or read transactions, *c.f.,* Section III. The characteristics of each investigated consensus mechanism are discussed next.

Clique is a PoA consensus algorithm that was first proposed in the Ethereum Improvement Proposal (EIP) [16]. In Clique, a designated node pool of trusted *validators* creates and adds new blocks to the ledger. Clique consensus does not have immediate finality due to the possibility of proposing two different blocks at a time. Next, since Clique is not BFT, the minimum number of signers for Clique to operate is two. Finally, Clique's liveness is up to 1/2 of failed validators.

IBFT 2.0 [17] is the Istanbul Byzantine Fault Tolerant PoA consensus mechanism. Similarly to Clique, IBFT 2.0 also has a designated list of *validators*. IBFT 2.0 achieves immediate finality, *i.e.,* prevents chain forks. However, the minimum number of validators for IBFT 2.0 increased to four. Thus, it achieves quorum and is BFT only if up to *(n-1)/3* validators are malicious, where *n* is the total number of validators. Finally, IBFT 2.0's liveness is up to 1/3 of failed validators.

QBFT or Quorum BFT [18] is the latest PoA consensus mechanism for HB private networks. It was proposed as a solution to the liveness and safety concerns of IBFT 2.0, *i.e.,* blockchain network DoS when two legitimate validators lock on different blocks. QBFT is similar to IBFT 2.0 regarding immediate finality, quorum, and liveness. However, the difference is that in QBFT, if validators do not achieve consensus before a certain, predefined time expires, the validation round will reset, triggering a new consensus attempt. QBFT is recommended by HB developers as the enterprise-grade consensus protocol for private networks.

E. Marketplace Implementation

The marketplace is shown in the digital layer in Figure 1. Each energy provider and regulator are represented within the marketplace as a *blockchain organization* (BO). Each BO must operate at least one validator node. Further, each BO has a dedicated Tessera node to enable private transaction execution in the network. Finally, each BO has a marketplace interface (MI) that is utilized by the prosumers to conduct P2P trade settlements.

Following this setup, HB provides the participants in the blockchain network, *i.e.,* the electricity providers and regulator, with two types of guarantees: *1)* the guarantee that the data stored in the ledger cannot be tampered with and *2)* the guarantee that it can only be modified following the rules implemented in the SC. These guarantees can be leveraged to fulfill the marketplace requirements. Firstly, by storing the GO in the ledger and encoding the rules governing their lifecycle in an SC, *i.e.,* issue and consumption, it is possible to automate their management in a transparent fashion and guarantee that the legislation is followed. Secondly, the same principles can be applied to the management of electricity production, consumption and trade settlement. By encoding the state of all the entities of the marketplace in the ledger, *i.e.,* prosumer, RES, and order, the marketplace ensures that there is always a consensus among all participants regarding the status of the marketplace as a whole. Further, by describing all the processes in the marketplace as a set of operations transforming this data and implementing these operations in the SC, it is possible to ensure that all the operations in the marketplace respect the agreed upon rules.

One limitation of blockchain technology is that it can only provide guarantees after storing the data in the ledger. In other words, it cannot verify the validity of the data inserted in the ledger. In that regard, HB can only provide traceability for the data, recording which actor provided the information. The other marketplace actors either need to trust that actor to provide correct information or rely on external processes to verify its validity. Within the marketplace, the regulator is trusted with the insertion of the GO, the certification of the prosumer-owner RES, and the energy providers are trusted with the report of the energy production. The SC guarantees that the implemented rules are followed for all the other operations. In that case, the challenge is ensuring that the SC implementation matches the legislation. Another limitation appears when designing a system respectful of the privacy of the actors. In that case, the complete state of the system can no longer be publicly stored and shared with all the actors. Instead, it needs to be split, and different parts are then stored in different PGs depending on which actor needs to access the data. Beyond weakening the tamper resistance guarantees, this also introduces additional complexity in the design and implementation of the SC, making it more challenging to ensure that the implementation correctly matches the legislation.

In the marketplace implementation, prosumers are represented as user accounts. Prior to the registration, the prosumer-owned RES must be certified by the regulator. Further, the RES is saved as a data record within PG which includes the energy provider and regulator. During prosumer registration in the marketplace, the previously created RES record is attached to the prosumer record. In addition, the prosumer receives a personal wallet record where both fiat currency and bought electricity are stored. The energy provider registers the prosumer-generated electricity in the marketplace if the prosumer's RES is marked as certified. While trading, the prosumer utilizes an ordering system where buy or sell orders can be fulfilled according to a predefined marketplace SC.

Each record in HB is saved as *<key, value>* pairs. *Key* is a unique data identifier and must not repeat within a ledger. *Value* contains data associated with a specific key and all fields that the data record consists of. An underlying data structure is required to manipulate data in trade settlement transactions.

TABLE I: Prosumer Blockchain Data Record

Field Name	Type	Description
ID	*String*	Prosumer's record unique identifier
Electricity	*Double*	Amount of generated electricity *(kWh)*
WalletID	*String*	Prosumer's Wallet identifier
RESID	*String*	Prosumer's RES identifier

1) Marketplace Data Structure: The *prosumer* record is described in Table I. It is private for the PG which includes the

energy provider and regulator. This record contains prosumer unique *ID*. The ID represents the *key* in *<key, value>* pair and contains a user blockchain identity *Address*. The *Electricity* field is updated by the energy provider and regulator based on the data from the prosumer's metering device. Further, it contains a respective wallet and RES IDs. The prosumer record intentionally does not contain any personally identifiable information (PII) to comply with General Data Protection Regulation (GDPR) [19]. All PII needed for legal purposes can be saved in the conventional DB outside of the blockchain.

TABLE II: Wallet Blockchain Data Record

Field Name	Type	Description
ID	*String*	Wallet's unique identifier
Currency	*Double*	Amount of fiat currency, *e. g.*, USD, EUR
Electricity	*Double*	Amount of prosumer bought electricity *(kWh)*

The *wallet* record is described in Table II. The *Currency* is the amount of fiat currency the prosumer has. It is used for trade settlement execution. The *Electricity* shows the amount of bought electricity. The wallet record *Electricity* and the prosumer record *Electricity* are separated to ensure that the bought electricity is not resold twice. The wallet record is visible to all energy providers to conduct cross-provider trade settlements.

TABLE III: GO Blockchain Data Record

Field Name	Type	Description
ID	*String*	GO unique identifier
OwnerID	*String*	GO owner ID
RegulatorID	*String*	Issuer of GO
ElectricityAmount	*Double*	Amount of electricity *(kWh)*
IsConsumed	*Boolean*	Set *True* when electricity is sold

The GO record is described in Table III. It is a significant asset without which trade settlements cannot be executed. The GO records are public for the entire blockchain network. Further, the GO record contains the respective ids of the prosumer who owns it and the regulator who issued it. Further, *ElectricityAmount* contains the amount of electricity certified by the regulator for further trading. Finally, when the energy is sold, the *isConsumed* field is set *True*.

TABLE IV: Order Blockchain Data Record

Field Name	Type	Description
ID	*String*	Order unique identifier
Type	*String*	Order Type *(Sell or Buy)*
Price	*Double*	Price for the entire amount sold
ElectricityAmount	*Double*	Amount of electricity *(kWh)*
GOID	*String*	GO unique identifier
SellerWalletID	*String*	Seller wallet identifier
BuyerWalletID	*String*	Buyer wallet identifier

The *order* record is described in Table IV. *Type* shows what kind of order it is, *i. e.*, sell or buy. Further, the *Price* and *ElectricityAmount* contain the respective amounts of resources required from both parties. The *GOID* links a particular GO to the order. In *buy* order, the *GOID* is left empty to be filled by the seller. The *SellerWalletID* and *BuyerWalletID* fields contain identifiers of prosumer wallets. Depending on the type of the order, when it is created, one of the wallet identifiers is left empty, *i. e.*, *SellerWalletID* is empty for a buy order, and *BuyerWalletID* is empty for a sell order. When the order is fulfilled, it is private for prosumers and energy providers participating in trade settlement.

Algorithm 1 Fulfill Sell Electricity Order

```
function BuyElectricity(Order, GO, BuyerWallet, SellerWallet)
    if BuyerWallet.Currency ≥ Order.Price then
        if GO.IsConsumed == False then
            Order.BuyerWalletID ← BuyerWallet.ID
            SellerWallet.Currency ← SellerWallet.Currency +
            Order.Price
            BuyerWallet.Currency ← BuyerWallet.Currency −
            Order.Price
            BuyerWallet.Electricity ← BuyerWallet.Electricity+
            Order.ElectricityAmount
            Commit
        else
            return Invalid GO Attached to the Order.
    else
        return Insufficient Buyer Currency.
Buyer energy provider executes FinalizeOrder(Order, GO)
function FinalizeOrder(Order, GO)
    GO.IsConsumed ← True
    Delete(Order)
    Commit
```

2) Trade Settlement Smart Contract: The marketplace SC contains operations that actors require to operate, *i. e.*, electricity registration, order creation, and trade settlement. Due to space limitations, this study includes a trade settlement SC function that fulfills the *sell* customer electricity order, *c. f.*, Algorithm 1. The trade settlement operation execution has two stages. In the first stage, a buy electricity settlement is executed. It is done due to SC's inability to modify private and public data in a single transaction. The *BuyElectricity* function takes a sell order posted by a prosumer-seller. Further, the algorithm checks if the GO is consumed and if the buyer has enough currency in the wallet. Finally, the resources are exchanged between the buyer and seller, *i. e.*, electricity and currency. This transaction is private for PG which includes trading prosumers' energy providers. In the second stage, the *FinalizeOrder* function is executed by buyer's energy provider, *i. e.*, the actor interested in preventing electricity double spending. First, this function takes the GO, sets its *IsConsumed* value to *True*, and saves it in the public ledger. Further, it marks the fulfilled order as deleted. It is not visible in the order chart but can be seen in the ledger history.

III. Performance Evaluation

The throughput of public transactions, *i. e.*, visible to the entire private network, has already been investigated by the authors of [20]. The main aim of this study is to measure the performance of private transaction execution with the SC tailored to the energy marketplace needs. The performance evaluation was conducted on the test infrastructure described

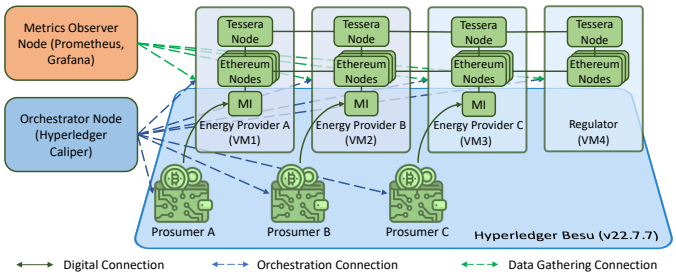

Fig. 2: Implemented Energy Marketplace.

in Figure 2. The infrastructure consists of 4 virtual machines (VMs), where each VM size is 16 vCPUs, 64 GB RAM, and 256 GB high throughput (150MB/s) disk space. Energy providers A, B, and C run VM1, VM2, and VM3, respectively, while the regulator runs VM4. All VMs are connected with a 10Gbit/s network interface. In our experimental implementation, we use HB version 2.7.7 and Tessera 22.1.7 without modifying the core code. All nodes within the infrastructure are deployed as docker containers. To collect reliable and correct performance evaluation data, *Prometheus*, *Grafana*, and *Hyperledger Caliper* (HC) tools are utilized. The *Prometheus* is used as the main blockchain operation data collector. The *Grafana* is used as a data visualization tool. The *HC* performance evaluation tool is used as a transaction load generation.

Several performance metrics are considered in this study. First, the *throughput* is the number of successful transactions (TPS) or reads (RPS) executed per second. The *latency* is the time it takes to finalize transaction execution and write it to the ledger or return a reply with the query result. The *scalability* is the behavior of the network with an increasing number of nodes. Also, it is the behavior of increasing the size of PG.

TABLE V: Performance Evaluation Parameters

Parameter	Value
Transaction Send Rate (Write)	10, 20 → 300 with step of 20 *(fixed-rate in duration of 5 minutes)
Block Period Seconds (BPS)	1 → 6 with step of 1
Transaction Send Rate (Read)	100, 300 → 3000 with step of 300 *(fixed-rate in duration of 5 minutes)
Validator Nodes	4 → 24 with step of 4
Privacy Group Size	2, 3, 4
Consensus Mechanism	Clique, IBFT 2.0, QBFT

This study manipulated several configurable metrics within HB to investigate the maximum throughput. These metrics were selected based on the performance tests conducted by the HB developers and research studies [20]. The *Block Period Seconds* (BPS) metric defines the time validators accept transactions to add to the new block. When the BPS time is up, the block is cut and embedded into the ledger. Further, horizontal scalability is investigated by changing the number of validator nodes and PG size. To investigate write transaction throughput, 5-minute tests were executed with a constant send rate. To investigate read throughput, the 4KB asset was read from the local HB database, *i. e.*, state database, with

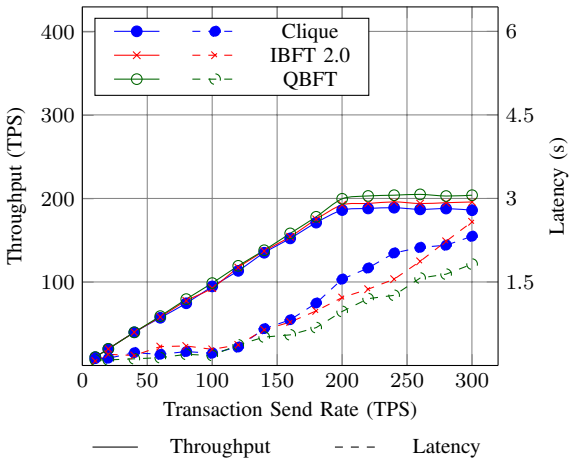

Fig. 3: Transaction Throughput and Latency (*Block Period Seconds = 1s, Validators = 4, PG size = 2*).

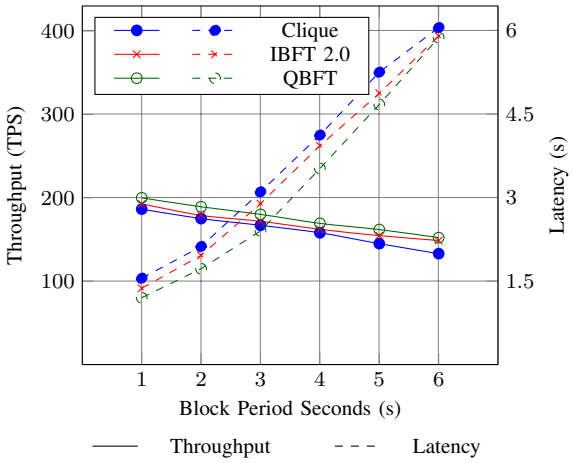

Fig. 4: Throughput and Latency with varying *Block Period Seconds* (*200 TPS send rate*).

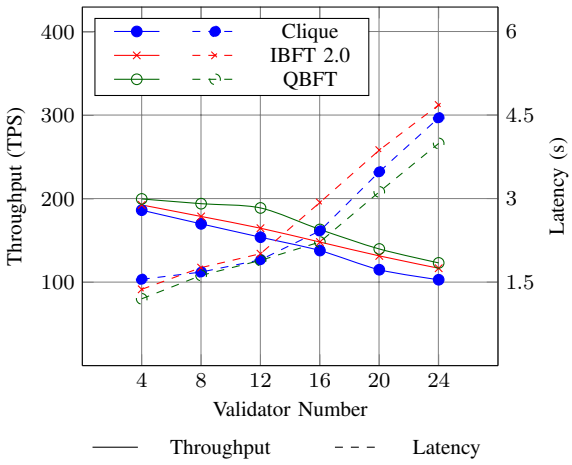

Fig. 5: Throughput and Latency with varying *Validator Nodes* number (*Block Period Seconds = 1s, 200 TPS send rate*).

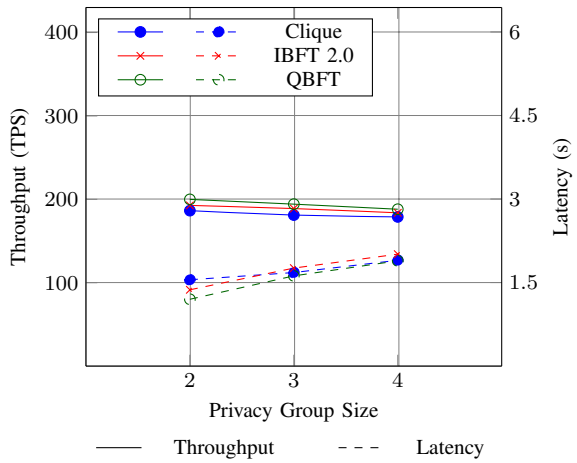

Fig. 6: Throughput and Latency with varying *PG Size* (*Block Period Seconds = 1s, Validators = 4, 200 TPS send rate*).

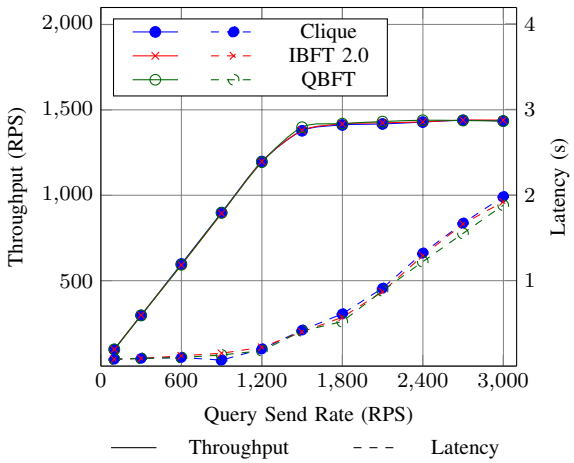

Fig. 7: Read Throughput and Latency (*4KB asset*).

varying query send rates. The entire performance evaluation parameters configuration is summarized in Table V.

1) Write - Trade Settlement Execution: In this study, an Algorithm 1 was executed as an SC function to test maximum write TPS. To write a transaction to the ledger, a respective consensus mechanism, *i. e.*, Clique, IBFT 2.0, or QBFT, must be executed. First, we test the baseline HB configuration, which included the minimum necessary setup to operate, *i. e.*, four validators, Block Period Seconds = 1s. The PG size is 2, *i. e.*, energy providers A and B. The throughput measurement results are shown in Figure 3. All consensus mechanisms show the similar performance of approximately 200 TPS. However, QBFT demonstrated the best latency. The baseline test demonstrates the maximum sustainable network load of around 200 TPS. Thus, further tests are conducted with a fixed send rate of 200 TPS.

Next, the maximum TPS with a varying BPS was investigated, *c.f.*, Figure 4. The results demonstrate that the BPS affects the maximum throughput of the HB network, *i. e.*, the BPS increase results in a steady throughput decrease. Further, the latency rises significantly, *e. g.*, up to approximately 6s latency for BPS = 6s. Here all investigated consensus mechanisms show similar performance under varying BPS, where QBFT is the best performer.

The horizontal scalability was investigated with varying validators number and a PG size. The results of the validator scalability investigation are shown in Figure 5. Here, the number of validator nodes significantly affects the maximum network throughput. It represents a significant performance bottleneck resulting in approximately 115 TPS throughput with 24 validators. Here, all investigated consensus mechanisms demonstrate similar performance, with QBFT having the highest TPS. In addition, QBFT demonstrates the best scalability by maintaining 190-200 TPS up to 12 validators.

The results of PG size scalability are shown in Figure 6. The investigated PG sizes are under four due to each BO can operate only one Tessera node, *i. e.*, the infrastructure limitation. The PG size increase does not result in a significant throughput decrease. However, the latency increases approximately by a half second for all investigated consensus mechanisms with PG size equal to four. Here, the performance of consensus mechanisms is similar, with QBFT showing the best results.

The performance evaluation results demonstrate that the maximum possible throughput depends significantly on BPS and network size, *i. e.*, the best throughput is achieved with BPS = 1s and 4 Validators configuration. Further, the QBFT has the best throughput, latency and scalability characteristics out of all investigated consensus mechanisms. Finally, the performance evaluation shows that HB-based marketplace demonstrates an approximately two times lower throughput and higher latency than HF-based marketplace investigated in [21]. However, HF uses RAFT consensus mechanism which is only CFT, *i. e.*, does not protect from malicious nodes.

2) Ledger Data Read: The read throughput is shown in Figure 7. The query request does not execute consensus mechanism to get the requested data. Thus, is the block or network configuration does not affect the read throughput. Here, it is the *asset size* that affects RPS. To investigate read throughput the query was constructed to read 4KB of data from RockDB world state database. The results demonstrate the maximum throughput of approximately 1440 RPS for all investigated consensus mechanisms.

IV. Related Work

Hyperledger Foundation has created a number of projects which employ different blockchain architectures, *i. e.*, public and private, to address industrial and business use-cases [22]. Thus, private blockchains like HF and HB became the main energy marketplace implementation and investigation tools. Authors of [23] define actors and requirements for the P2P energy marketplace. However, their marketplace does not include a regulator role, GO usage, and data privacy requirements intrinsic to energy market systems. In [24], authors propose an HB-based P2P marketplace to conduct energy trading and payment settlement. The marketplace was evaluated with data from the Western Australian energy market. According to the authors, their marketplace demonstrates better throughput and latency than PoW and Ethereum Clique. The authors of [23]

propose an HF-based P2P energy marketplace for tokenized energy assets. Such assets are traded within the marketplace, where each actor can benefit monetarily depending on its role. The authors claim that their implementation achieved a throughput of 448.3 TPS. However, the authors do not consider private transactions. In [20], authors conduct an in-depth performance evaluation of the HB platform and its three main consensus mechanisms for private blockchain, *i. e.,* Clique, IBFT 2.0, and QBFT. They evaluate the throughput, latency, and scalability of public transaction execution in a private HB network. Authors claim that QBFT consensus has the best performance results. Authors of [25] propose an automated blockchain-based P2P energy marketplace based on a multi-agent system paradigm. Permissioned blockchain allows for reduced transaction costs, enables marketplace micro-transactions, and eliminates a single point of failure. According to the authors, blockchain technology enables prosumer self-sovereignty while allowing the marketplace to comply with current data regulations. In [26], authors propose an HB-based framework for P2P energy trading. The proposed marketplace uses a flexible permission ascription scheme that utilizes HB permissioning scheme. Authors claim that the proposed framework provides an efficient scheme for P2P energy trading compared to other solutions.

V. Summary and Outlook

This work proposes a decentralized blockchain-based P2P energy marketplace that addresses actors' privacy and the performance of consensus mechanisms. The main aim of the marketplace is to automate the P2P trade settlement process while preserving actors' privacy. The novelty of the proposed marketplace is its alignment with the current energy trade regulations defined in D2018/2001 of the European Parliament. In detail, our marketplace incorporates the *regulator* actor. The regulator represents a governmental authority that controls renewable energy trading via GO issue and price regulation. In addition, the regulator certifies the RES used to generate traded electricity. Hence, with current regulations, the marketplace is partially centralized around the regulator actor but still improves the automation of energy trading.

Performance evaluation results of an HB-based marketplace private transaction execution with three main consensus mechanisms, *i. e.,* Clique, IBFT 2.0, and QBFT, demonstrate a throughput of approximately 200 TPS with baseline configuration. The QBFT consensus mechanism shows the best throughput and latency. Further, QBFT demonstrates the best scalability by maintaining 190-200 TPS throughput for up to 12 validators. However, HB's QBFT consensus mechanism demonstrates lower throughput than another popular private permissioned blockchain platform HF. This is a side effect of BFT and, thus, increased computations of QBFT. In contrast, HF executes the RAFT consensus mechanism, which is CFT, *i. e.,* more centralized and it is not secured against malicious nodes. However, the inherent centralization around the regulator mitigates this issue, making HF better suited for such a use case.

Future work will focus on investigating possible improvements for consensus mechanisms in terms of scalability, performance, and security.

Acknowledgment

The work was partly sponsored by the Swedish Knowledge Foundation through the project *Symphony - Supply-and-Demand-based Service Exposure using Robust Distributed Concepts* where project partners are Ericsson AB (Stockholm, Sweden) and Affärsverken Energi AB (Karlskrona, Sweden).

References

[1] Y. Yang *et al.*, "Optimal design of distributed energy resource systems coupled with energy distribution networks," *Energy*, Jun 2015.
[2] B. Jasim and P. Taheri, "An Origami-Based Portable Solar Panel System," in *2018 IEEE IEMCON*, Nov 2018.
[3] C. Pop *et al.*, "Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids," *Sensors*, Jan 2018.
[4] EU Parliament, "Directive (EU) 2018/2001," 2018. [Online]. Available: http://data.europa.eu/eli/dir/2018/2001/2022-06-07
[5] Ákos Hamburger, "Is guarantee of origin really an effective energy policy tool in Europe?" *Society and Economy*, Dec 2019.
[6] B. Hertz-Shargel *et al.*, *Assessing Blockchain's future in transactive energy*, 2019.
[7] T. Kollmann *et al.*, "Toward a renaissance of cooperatives fostered by Blockchain on electronic marketplaces: a theory-driven case study approach," *Electronic Markets*, Jun 2020.
[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[9] J. Singh and J. D. Michels, "Blockchain as a Service (BaaS): Providers and Trust," in *2018 IEEE EuroS&PW*, Apr 2018.
[10] "Hyperldger Besu Ethereum client," 2022. [Online]. Available: https://besu.hyperledger.org/en/stable/
[11] R.-V. Tkachuk *et al.*, "A Survey on Blockchain-based Telecommunication Services Marketplaces," *IEEE TNSM*, 2021.
[12] M. Liu *et al.*, "How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain," *Current Issues in Auditing*, Sep 2019.
[13] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014. [Online]. Available: https://gavwood.com/paper.pdf
[14] E. Androulaki et al., "Hyperledger fabric," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, Apr 2018.
[15] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," *Lecture Notes in Computer Science*, 2016.
[16] P. Szilágyi, "EIP-225: Clique proof-of-authority consensus protocol," 2017. [Online]. Available: https://eips.ethereum.org/EIPS/eip-225
[17] R. Saltini *et al.*, "Ibft 2.0: A safe and live variation of the ibft blockchain consensus protocol for eventually synchronous networks," Sep 2019.
[18] H. Moniz, "The istanbul bft consensus algorithm," Feb 2020. [Online]. Available: http://arxiv.org/abs/2002.03613
[19] GDPR, "General Data Protection Regulation (GDPR) – Official Legal Text," pp. 1–99, 2016. [Online]. Available: https://gdpr-info.eu/
[20] C. Fan *et al.*, "Performance analysis of hyperledger besu in private blockchain," *2022 IEEE DAPPS*, Aug 2022.
[21] R.-V. Tkachuk *et al.*, "Towards Efficient Privacy and Trust in Decentralized Blockchain-Based Peer-to-Peer Renewable Energy Marketplace," Oct 2022, Submitted for publication. [Online]. Available: dx.doi.org/10.2139/ssrn.4255555
[22] D. Li *et al.*, "A Survey on Blockchain for Enterprise Using Hyperledger Fabric and Composer," *International Conference on DSA*, Jan 2020.
[23] N. Karandikar *et al.*, "Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure," *Sensors*, May 2021.
[24] J. Abdella *et al.*, "An architecture and performance evaluation of blockchain-based peer-to-peer energy trading," *IEEE TSG*, Jul 2021.
[25] Y. Mezquita *et al.*, "Towards a blockchain-based peer-to-peer energy marketplace," *Energies*, Apr 2022.
[26] N. R. Pradhan *et al.*, "A flexible permission ascription (fpa)-based blockchain framework for peer-to-peer energy trading with performance evaluation," *IEEE Transactions on Industrial Informatics*, Apr 2022.