Blockchain-enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things

Meng Li, *Member, IEEE,* Donghui Hu, *Member, IEEE,* Chhagan Lal*, *Member, IEEE,* Mauro Conti, *Senior Member, IEEE,* Zijian Zhang, *Member, IEEE*

***Abstract*—Energy trading in Industrial Internet of Things (IIoT), a fundamental approach to realize Industry 4.0, plays a vital role in satisfying energy demands and optimizing system efficiency. Existing research works utilize a utility company to distribute energy to energy nodes with the help of energy brokers. Afterwards, they apply blockchain to provide transparency, immutability, and auditability of peer-to-peer (P2P) energy trading. However, their schemes are constructed on a weak security model and do not consider the cheating attack initiated by energy sellers. Such an attack refers to an energy seller refusing to transfer the negotiated energy to an energy purchaser who already paid money. In this paper, we propose FeneChain, a blockchain-based energy trading scheme to supervise and manage the energy trading process towards building a secure energy trading system and improving energy quality for Industry 4.0. Specifically, we leverage anonymous authentication to protect user privacy, and we design a timed commitments based mechanism to guarantee the verifiable fairness during energy trading. Moreover, we utilize fine-grained access control for energy trading services. We also build a consortium blockchain among energy brokers to verify and record energy trading transactions. Finally, we formally analyze the security and privacy of FeneChain and evaluate its performance (i.e., computational costs and communication overhead) by implementing a prototype via a local Ethereum test network and Raspberry Pi.**

***Index Terms*—Industry 4.0, Industrial Internet of Things, energy trading, security, privacy, blockchain.**

I. Introduction

IIoT, as a realization approach towards Industry 4.0 [1], has become a highlight in both academics and industries, which will be an important ingredient of future industrial systems [2], [3], [4]. While IIoT brings correlation and intelligence to industrial systems with continuous progress in scale and performance, it is facing a great challenge to meet the ever-expanding energy demands of IIoT applications [3]. To address this issue, P2P energy trading[1] among IIoT nodes, such as smart meters and vehicles, has been presented with the integration of promising technologies, e.g., energy harvesting, and vehicle-to-grid [5]. In particular, the IIoT nodes can sell their spare energy to other nodes to meet energy needs, make profits, and improve overall energy efficiency for structuring a sustainable system for Industry 4.0 where all energy transactions require a secure and fair environment.

A majority of current energy trading infrastructures [6] are centralized around a utility company and a trusted authority, which handles energy distribution and entity registration, respectively. Such centralized infrastructures suffer from single point of failures and privacy leakage [7]. In recent years, grid incidents happen frequently, and they cause some devastating consequences. Here are two examples. On December 17, 2015, hackers attacked an electric transmission station in Kiev, Ukraine, and it was judged the first real-world malware that struck an infrastructure since Stuxnet [8]. The attack blacked out a part of the city equivalent to a fifth of its total power capacity. On August 10, 2019, a major power cut caused by two power stations failing affected nearly a million people in the UK and many people were stuck in the tunnel and train stations [9]. All the incidents manifest that a secure energy system is of prime importance to a normally functioning society.

To support a transparent, immutable, and auditable managing of grid transactions, some recent research studies [10], [3], [7], [11] have resorted to blockchain technology [12], [13], [14], [15], [16], [17], [18], [19], while addressing some security and privacy (S&P) issues [20], [21], [22], [23]. S&P are one of the most significant concerns in energy trading, considered that the IIoT infrastructures are faced with different threats. First, adversaries with different agendas try to bypass user authentication and control industrial resources (e.g., communication channel, and terminal). Meanwhile, outsiders may request energy services (e.g., home electricity, and vehicle charging) even if they are not granted corresponding attributes or they are unqualified after being punished for some mischievous behaviors or misconduct. Second, curious entities seek to collect energy data and extract sensitive information (e.g., identity, and transaction) via analyzing the collected data. For instance, readings of a smart meter can expose which appliances are being used, indicating the owner's indoor activities [24]. If trading behaviors are linked by an adversary, it will reveal the energy status of traders.

Unfortunately, existing works did not consider the fairness issue [25] during P2P energy trading. For example, when *Alice* purchases some energy from *Bob* by paying him 50 in advance. The mischievous *Bob* breaks the deal and refuses to transfer the energy to *Alice* since there is no fairness guarantee. Such a malicious attack would bring disastrous consequences to

Meng Li and Donghui Hu are with Key Laboratory of Knowledge Engineering with Big Data (Hefei University of Technology), Ministry of Education; and with School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230601, China. (e-mail: {mengli,hudh}@hfut.edu.cn)

Chhagan Lal (Corresponding Author) is with Simula Research Laboratory, Norway (e-mail: chhagan@simula.no).

Mauro Conti is with the Department of Mathematics, University of Padua, 35131 Padua, Italy (e-mail: conti@math.unipd.it).

Zijian Zhang is with School of Computer Science and Technology, Beijing Institute of Technology, China and School of Computer Science, University of Auckland, New Zealand. (email: zhangzijian@bit.edu.cn)

[1]https://www.ft.com/content/6d62b494-209a-11e9-b126-46fc3ad87c65

the energy trading system and eventually push away energy purchasers. The intuitive of solving this problem would be designing a mechanism for anonymous energy traders who do not trust each other to transact in a P2P environment. Such a mechanism should exhibit strong security guarantee: regardless of how sellers act, honest purchasers will never get cheated. In other words, honest purchasers are assured that the trading will end fairly [25]. Therefore, it is urgent to construct a fair trading environment for energy purchasers.

To address the above problems, we have designed and implemented a decentralized energy trading system named FeneChain to provide privacy protection, verifiable fairness, and access control. FeneChain is built upon consortium blockchain [12], [14], [15], anonymous authentication [26], timed commitments [25], and fine-grained access control [27], enabling IIoT nodes to conduct energy trading transactions in a privacy-preserving and fair manner. As we anticipate, the proposed FeneChain aims to provide a privacy-preserving, secure, and verifiable energy trading system for improving energy quality and then achieving more functionalities and goals at the higher level for Industry 4.0. If data is not protected adequately in Industry 4.0, data breaches could result in degrading of trust leading to further losses and entities could be faced with court proceedings[2]. In particular, we make the following contributions:

- We propose FeneChain, a blockchain-based energy trading management scheme, to better supervise and manage the energy trading process in IIoT with transparency, unforgeability, and verifiability. Concretely, we utilize anonymous authentication [26] to verify users' identities to protect their privacy, we design a timed commitments based mechanism [25] to guarantee the verifiable fairness during energy trading, we leverage fine-grained access control [27] for energy trading services, and we build a consortium blockchain to record all the energy trading transactions for a transparent, immutable, and verifiable management of energy trading data.
- We are the first to address the fairness issue during P2P energy trading. FeneChain aims to protect the energy purchasers' rights. We construct a stronger security model for P2P energy trading. Particularly, we adopt the honest-but-curious security assumption for most of the entities, and we include some malicious energy sellers who can launch cheating attack and unauthorized trading attack. Finally, we prove the security and privacy properties of FeneChain scheme.
- To demonstrate the practicability and efficiency of FeneChain, we implement it on an Ethereum platform [3] and Raspberry Pi 3, and evaluate its computational costs and communication overhead.

The remaining of this paper is organized as follow. We discuss related work in Section II. In Section III, we introduce the system model, security model, and design goals. Some preliminaries are reviewed in Section IV. We present the proposed FeneChain scheme in Section V, followed by a security analysis and performance evaluation in Section VI and Section VII, respectively. Section VIII discusses our work. Finally, we conclude our work in Section IX.

[2] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

[3] https://www.ethereum.org

II. Related Work

Mihaylov et al. [28] proposed a method NRG-X-Change for trading locally produced renewable energy in smart grid that do not depend on any energy market. In the NRG-X-Change, the consumers are billed by the distributed system based on their actual usage and rewarded according to their energy provision. But they only considered basic security mechanisms to resist tampering with the smart meters.

Xiao et al. [29] proposed dynamic energy trading (DET) for wireless powered communication networks (WPCNs) that allows local devices with variations in their energy harvesting procedure to transact exchange energy. DET has several benefits, such as enabling energy devices to provide surplus energy and improving the reliability of the energy supply for WPCNs, and allowing energy exchange and improving the energy utilization efficiency for WPCNS. Lin et al. [30] built a mixed-integer linear programming (MILP) model to reduce energy waste by optimizing the charging/discharging decisions. Their system model consists of end-user, energy storage, electric vehicle, and energy trading platform in the Internet of Energy (IoE). It enables the end-user to buy and sell energy. However, the two schemes are concentrating on the utility of energy trading while not considering security.

Lin et al. [10] proposed a blockchain-based scheme (called BSeIn) for mutual authentication with access control. In B-SeIn, both blockchain and attribute signatures are used to authenticate users anonymously, and the message authentication code is used to authenticate gateways. Meanwhile, the multi-receivers encryption is used to guarantee that only authorized users can access the plaintext of broadcasted messages. Smart Contracts (SC) are designed for the entire request process. Also, Li et al. [3] proposed a consortium blockchain-based energy trading scheme (called EneBloc). The blockchain is engineered for general scenarios of P2P energy trading comprised of energy sellers, purchasers, and aggregators.

Aitzhan et al. [7] focused on offering transaction security for distributed smart grid energy trading without a trusted party. They designed an energy trading scheme (called Pri-Watt) based on Bitcoin system, P2P message authentication, and delivery system Bitmessage, allowing users to negotiate energy prices and perform trading transactions in a secure and privacy-preserving way. Recently, Gai et al. [11] proposed a consortium blockchain-based scheme (called BETS) to tackle the privacy leakage problem in smart grid. They presented a noise-based privacy-preserving method to hide the trading distribution tendency. BETS also include a privacy-preserving method to achieve differential privacy which leverages dummy/dividing accounts to change the feature of transactions while not affecting performance. However, [11] claimed that privacy in data transmissions was not a significant concern. Furthermore, they did not consider the fairness issue.

The above mentioned first three schemes are only focusing on the utility of energy trading, while the later four schemes are designed with specific S&P goals needed in the industry

domain, thus, these four are more related to our work. In this paper, we focus on the authentication, access control, privacy, and verifiable fairness in designing a blockchain-based energy trading scheme. We prove that when compared with the state-of-the-art schemes, only FeneChain provides all the design goals, especially the verifiable fairness.

It is worth noting that verifiable fairness is a crucial security feature for energy trading in Industry 4.0, which confronts with multiple attacking surfaces in a closely collaborating environment. Without it, energy trading will be difficult to carry out since customers lose faith in obtaining fair energy services. If the underlying energy infrastructure collapses, then the services and mechanisms in Industry 4.0 based on it will no longer work.

III. Problem Statement

A. System Model

The system model of FeneChain is demonstrated in Fig. 1. Key notations are described in Table I.

Energy Nodes (ENs): include energy purchasers and energy sellers. They are IIoT nodes (e.g., electric vehicles and smart buildings) that trade energy in a P2P manner. An EN has three energy options in energy trading: purchasing energy, selling energy, and being idle. Each EN can choose one option based on its current energy state and future energy demands. In the realm of Industry 4.0 where entities are equipped with advanced computation and communication devices, each energy node is able to perform the abovementioned operations.

Smart Meters (SMs): are built-in devices in energy nodes that computes and records the amount of transacted energy. It also records the identity of each trading object. The records within each SM are tamper-proof.

Energy Brokers (EBs): are energy transaction managers that verifies and records energy transactions among energy nodes. EBs can be advanced metering infrastructures, energy substations, and local aggregators. During an energy trading process, an EB verifies the seller's deposits, and it returns them to ES if no complaint is made by EP before T expires. An EB verifies the attributes of energy sellers within its area to check whether they are qualified to sell energy.

Certificate Authority (CA): is a government department that initializes the FeneChain system. All energy nodes and energy brokers register to CA to become a legitimate entity by receiving a unique energy identity and cryptographic keys.

B. Security Model

During energy trading, diverse security threats originate from internal and external adversaries. A majority of energy nodes strictly follow the protocols and dutifully trade energy, however they can be honest-but-curious, i.e., they may attempt to obtain the identities of trading partners. Some energy sellers are malicious, and they can launch: (i) cheating attack, i.e., refuse to transfer energy to energy purchasers after they are paid; and, (ii) unauthorized trading attack, i.e., try to sell energy even if they are not qualified to do so. Since we assume the existence of malicious energy sellers, it is reasonable to assign different attributes to pertinent energy sellers, imposing restrictions on their energy trading activities. Smart meters are secure devices and the data inside are infeasible to be obtained or falsified by adversaries. Energy brokers are also honest-but-curious. External adversaries can eavesdrop on communication channels, and initiate replay and impersonation attacks.

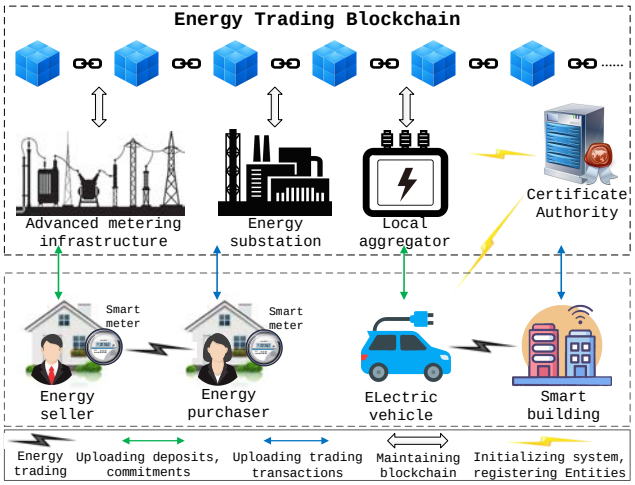


Fig. 1. System model of FeneChain

TABLE I
Key Notations

Notation	Definition
CA, EB	Certificate authority, energy broker
ES, EP	Energy seller, energy purchaser
$\mathbb{G}; g; H_1, H_2, H_3$	Group; group generator; hash function
$\mathbb{G}_1, \mathbb{G}_2; \tilde{g}; e$	Group; group generator; bilinear pairing
$mak = (\beta_1, \beta_2, \beta_3, \beta_4)$	Master key
$a; \mathcal{AU} = \{a_i\}$	Attribute; attribute universe
$avk = v_a$	Attribute version key
$pak_a = (pak_a^1, pak_a^2)$	Public attribute key
$ts; CBC$	Time slot, consortium blockchain
$prik; pubk$	Private key; public key
$x; y, h_1, h_2$	private key; public key
$usk = (S, L, \forall x \in A : S_x)$	User attribute key
de, pr	Demanded energy, bit price
$ct; \sigma; ER$	Ciphertext, signature, energy request
tq	Trading qualification string
$I; ik; \overrightarrow{v}; \mathcal{T}$	Item; item key; vector; access structure
$\delta; \mathcal{F}; tk$	Correlating function; set; token
$tk; \tau; Comm; T$	Signature; commitment; expiry time

C. Design Goals

Authentication: the real identity of an energy node which uploads data to the blockchain should be authenticated to rule out illegal entities.

Access control: the attributes of an energy node that interacts with the blockchain should be validated whether they are qualified to sell energy. Unauthorized trading attack from unqualified energy sellers is catastrophic for Industry 4.0 since it will sabotage the operation order of the whole system.

Privacy: FeneChain preserves the following privacy in the energy trading system: (i) Identity: when an energy node engages in energy trading, the other entities cannot disclose the energy node's real identity or link one energy nodes' trading identities at different times, and (ii) Transaction: Energy nodes' trading activities, i.e., purchasing energy and selling energy, should not be linked by anyone but the energy nodes

themselves. Privacy preservation is vital for energy nodes in Industry 4.0 which have sensitive information to protect. Especially when the energy transactions are not guarded, their private activities could be leaked [7].

Verifiable fairness: the energy trading transactions between EPs and ESs should be conducted in a fair manner such that the EPs will receive the right amount of energy after paying corresponding energy fees. The fairness should be verifiable in the sense that anyone can check the fairness of energy transactions. For transactions in Industry 4.0, this is important since trading entities may not know each other and, the verifiable fairness provides a certain degree of system assurance.

Integrity and auditability: the energy trading system should provide integrity and auditability of energy trading transactions such that they are difficult to be tampered with and easy to be audited.

Efficiency: FeneChain offers the following efficiency: (i) Low computational cost, i.e., use of a lightweight process for energy trading, and (ii) Low communication overhead, i.e., the size of transmitted data should be as low as possible.

IV. Preliminaries

A. Anonymous Authentication

The anonymous authentication technique [26] achieves anonymous verification of an entity's identity. It is based on decisional Diffie-Hellman (DDH) problem, and it includes following three algorithms: $\mathsf{KeyGen}(1^k, \mathbb{G}, q, g)$: given a security parameter 1^k, a group $\mathbb{G}$ with k-bit prime order q, and a group generator g; outputs private key $x \in_R \mathbb{Z}_q^*$ and public key $(y \in_R \mathbb{G}, h_1 = g^x, h_2 = y^x)$. $\mathsf{Sign}(g, x, y, h_1, h_2, m, H_1, H_2)$: given group generator g, private key x, public key (y, h_1, h_2), message $m \in \{0,1\}^*$, and two hash functions H_1, H_2, calculates $z = H_1(h_1, h_2)$ and $s = g^z y$; chooses $r \in_R \mathbb{Z}_q^*$ and calculates commitment $t = s^r = (g^z y)^r$; outputs signature $(\sigma_1, \sigma_2) = (H_2(m, h_1, h_2, t), r - x\sigma_1 \bmod q)$. $\mathsf{Verify}(y, h_1, h_2, \sigma_1, \sigma_2, m)$: given public key (y, h_1, h_2), a signature (σ_1, σ_2), and message m; calculates $z = H_1(h_1, h_2)$ and $t' = (g^z y)^{\sigma_2}(h_1^z h_2)^{\sigma_1}$; outputs 1 if $\sigma_1 = H_2(m, h_1, h_2, t')$, and 0 otherwise.

B. Timed Commitments

A timed-commitment scheme [25], [31], [32] has a committer C and a verifier V. The committer opens her/his secret before a timestamp or pays a penalty. This property will help us achieve fairness of energy trading for Industry 4.0. The timed-commitment scheme has two following steps. Commit: The commit step is denoted as $\mathsf{Commit}(C, d, T, M)$. C puts some deposits d and a commitment $Comm$ on a ledger. The deposits can be redeemed with a key possessed only by C. T is the expiry time. M contains some randomness and the message to which C commits. Open: The open step is denoted as $\mathsf{Open}(C, d, T, M)$. An honest C opens $Comm$ by T and retrieves his money which means V verifies a transaction redeemed with a key possessed only by C. If a malicious C is reported cheating, he cannot open $Comm$ by T, thus it causes him to lose his deposited money to the ledger.

C. Access Control

The attribute-based access control technique [27] ensures that data accessing requests are qualified and the accessing qualification of unauthorized entities are revoked timely. It includes the following seven functions: $\mathsf{Setup}(1^k)$: given a security parameter 1^k, returns a master key msk, public parameters pp and a set of public attribute keys $\{pak_x\}$. $\mathsf{USKeyGen}(msk, AT, \{vk_x\}_{x \in A})$: given master key msk, a set of attributes AT, and a set of attribute version keys $\{avk_x\}_{x \in AT}$, returns a user secret key usk. $\mathsf{Encrypt}(pp, \{pak_x\}, m, \mathcal{ST})$: given public parameters pp, a set of public attribute key $\{pak_x\}$, a message m and an access structure $\mathcal{ST}$, encrypts m to output a ciphertext C. $\mathsf{Decrypt}(C, usk)$ given a ciphertext C including an access structure $\mathcal{ST}$ and a user secret key usk for a set of attributes AT, decrypts C to return a message m if AT satisfies $\mathcal{ST}$. $\mathsf{UKeyGen}(msk, vk_{\widetilde{x}})$: given master key msk and current version key $vk_{\widetilde{x}}$ of the revoked attribute $\widetilde{x}$, returns a new version key $\widetilde{vk_{\widetilde{x}}}$ of $\widetilde{x}$ and an update key $uk_{\widetilde{x}}$. $\mathsf{USKUpdate}(usk, uk_{\widetilde{x}})$: given current user secret key usk and an update key $uk_{\widetilde{x}}$ of the revoked attribute $\widetilde{x}$, returns a new user secret key $\widetilde{usk}$. $\mathsf{CUpdate}(C, uk_{\widetilde{x}})$: given a ciphertext C and an update key $uk_{\widetilde{x}}$, returns a new ciphertext $\widetilde{C}$.

V. The Proposed Scheme FeneChain

A. System Initialization

First, CA chooses security parameter 1^k, generates a group $\mathbb{G}$ with k-bit prime order q, a group generator g, and two hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$. Then, CA generates multiplicative groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with the same order p, a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, a generator $\widetilde{g}$ of $\mathbb{G}_1$, and a hash function $H_3 : \{0,1\}^* \to \mathbb{G}_1$. CA selects random numbers $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{Z}_p$ as the master key msk and generates $(\widetilde{g}^{\beta_1}, \widetilde{g}^{1/\beta_2}, \widetilde{g}^{\beta_2}, e(\widetilde{g}, \widetilde{g})^{\beta_4})$. After discussing with energy brokers, CA obtains an attribute universe $\mathcal{AU} = \{a_i\}$. For each attribute a, CA selects a random number $v_a \in \mathbb{Z}_p$ as the initial attribute version key $avk_a = v_a$, and computes a public attribute key $pak_a = (pak_a^1, pak_a^2) = (H_3(a)^{v_a}, H_3(a)^{v_a \beta_3}))$. Last, CA initializes a consortium blockchain CBC with energy brokers. They partition time into a string of time slots $\{ts_1, ts_2, ...\}$. Each energy broker EB_i creates a self-maintained ledger $CBC_i = B_0$, i.e., genesis block, consisting of an empty block header, energy brokers' identities and public keys, a timestamp, and each energy broker's signature on previous items in B_0.

B. Entity Registration

Each energy broker EB registers to CA: obtains a private key $prik^{EB} \in_R \mathbb{Z}_q^*$ and a public key $pubk^{EB} = g^{prik^{EB}}$, and generates a qualification key qk and an empty blacklist $\mathcal{BL}^{eb}$. Each energy purchaser EP registers to CA: applies some tokens tks based on her current reputation value rv^{ep} and energy demand, and obtains a private key $x^{ep} \in_R \mathbb{Z}_q^*$ and a public key $pubk^{ep} = (y^{ep} \in_R \mathbb{G}, h_1^{ep} = g^{x^{ep}}, h_2^{ep} = y^{x^{ep}})$ as her wallet address. It is worth noting that each energy purchaser registers a set of private keys and public keys for privacy protection. Each energy seller ES registers to CA: obtains a private key $x^{es} \in_R \mathbb{Z}_q^*$ and a public key $(y^{es} \in_R \mathbb{G}, h_1^{es} = g^{x^{es}}, h_2^{es} = y^{x^{es}})$ as his wallet address,

and a user secret key $usk^{es} = (S = \widetilde{g}^{\frac{\beta_1+\beta_4 l}{\beta_2}}, L = \widetilde{g}^{l}, \forall x \in A : S_x = \widetilde{g}^{l\beta_2^2 \cdot H_3(x)^{v_x l \beta_2}})$ where $l \in \mathbb{Z}_p$ is a random number chosen by CA. The usk^{es} indicates a valid energy trading membership of ES.

C. Energy Requesting

Each EB broadcast its public keys $pubk^{EB}$ in its coverage area. When an energy purchaser EP is ready to purchase some energy, she forms an energy request ER^{eb} as follows: Decide an amount of demanded energy de^{ep} and a bid price pr^{ep}. Encrypt de^{ep} and pr^{ep} with $pubk^{EB}$ to obtain a ciphertext:

$$ct^{ep} = (g^{r_0}, (de^{ep}||pr^{ep}) \cdot (pubk^{EB})^{r_0}), \tag{1}$$

where $r_0 \in \mathbb{Z}_q^*$ is a random number. Calculate $z^{ep} = H_1(h_1^{ep}, h_2^{ep})$ and $s^{ep} = g^{z^{ep}} y^{ep}$, choose $r_1 \in_R \mathbb{Z}_q^*$, and calculate $t^{ep} = (s^{ep})_1^r = (g^{z^{ep}} y^{ep})^r$ and a signature $\sigma^{ep} = (\sigma_1^{ep}, \sigma_2^{ep})$: $\sigma_1 = H_2(ct^{ep}, h_1^{ep}, h_2^{ep}, t^{ep})$, $\sigma_2 = r_1 - x^{ep}\sigma_1 \bmod q$. Send the energy request to EB:

$$ER^{ep} = (pubk^{ep}, ct^{ep}, \sigma^{ep}). \tag{2}$$

D. Energy Responding

Upon receiving an energy request ER^{ep} from an energy purchaser EP, the local energy broker EB verifies the request and broadcast valid requests as follows: Calculate $z = H_1(h_1^{ep}, h_2^{ep})$ and $t' = (g^z y^{ep})^{\sigma_2^{ep}} (h_1^{ep z}\ h_2^{ep})^{\sigma_1^{ep}}$, drop ER^{ep} if $\sigma_1 \neq H_2(ct^{ep}, h_1^{ep}, h_2^{ep}, t')$, or execute the following operations. Decrypt ct^{ep} with its private key $prik^{EB}$ to obtain EP's amount of demanded energy de^{ep} and bid price pr^{ep}. Prepare a *trading qualification* string tq^{eb} varying with time, and partition tq^{eb} as $tq^{eb} = (I_1, ..., I_4)$ with each item representing data, time, area, and amount. Encrypt each I_i with different item keys ik_i $(1 \leq i \leq 4)$ via AES encryption. Decide an access structure $\mathcal{T}$ over the universe of attributes $\mathcal{AU}$ for each item key ik_i $(1 \leq i \leq 4)$. Encrypt ik_i under $\mathcal{T}$ via Encrypt: assume $\mathcal{T}$ is a $f \times 4$ matrix where f is the total number of possessed attributes; choose a random encryption exponent $c \in \mathbb{Z}_p$ and a vector $\overrightarrow{v} = (c, l_2, l_3, l_4)$ where l_2, l_3, l_4 share c; for $i = 1$ to f, compute $\eta_i = \overrightarrow{v} \times \mathcal{T}_i$, where $\mathcal{T}_i$ is a vector of the i-th row of $\mathcal{T}$; randomly choose $b_1, ..., b_f \in \mathbb{Z}_p$ and compute a ciphertext of tq^{eb}: $ct^{eb} = (ct_1^{eb}, ct_2^{eb}, ct_3^{eb}, ct_4^{eb}, ct_5^{eb})$, where $ct_1^{eb} = ike(\widetilde{g}, \widetilde{g})^{\beta_1 c}$, $ct_{21}^{eb} = \widetilde{g}^{\beta_2 c}$, $ct_3^{eb} = \widetilde{g}^{\beta_4 \eta_i} (\widetilde{g}^{\beta_2})^{-b_i} H_3(\delta(i))^{-b_i v_{\delta(i)}}$, $ct_4^{eb} = H_3(\delta(i))^{v_{\delta(i)} b_i \beta_3}$, $ct_5^{eb} = \widetilde{g}^{b_i/\beta_2} (1 \leq i \leq f)$, and function δ correlates rows of $\mathcal{T}$ to attributes. Broadcast ct^{eb}, de^{ep}, pr^{ep}, and a period of time T, with other verified energy requests to energy sellers within its coverage area.

After receiving the energy requests from EB, an energy seller ES responds as follows: Define $\mathcal{F} \subset \{1, 2, ..., f\}$ as $\mathcal{F} = \{i : \delta(i) \in A\}$, select a set of constants $\{a_i \in \mathbb{Z}_p\}_{i \in \mathcal{F}}$, rebuild $c' = \sum_{i \in \mathcal{F}} a_i \eta_i$ if $\{\eta_i\}$ are valid shares of c based on $\mathcal{T}$, and calculate:

$$\frac{e(ct_2^{eb}, S)}{\Pi_{i \in \mathcal{F}} (e(ct_3, L) e(ct_5, S_{\delta(i)}))^{a_i}} = e(\widetilde{g}, \widetilde{g})^{\beta_1 c} \tag{3}$$

Recover the item key $ik = ct_1 / e(\widetilde{g}, \widetilde{g})^{\beta_1 c}$, and then obtain tq^{eb} by using AES decryption. Here, only the qualified energy seller is able to recover the tq^{eb}, which prevents other unqualified energy sellers in Industry 4.0. This has served as a guard to improve energy quality. Encrypt tq^{eb} with $pubk^{eb}$ to obtain ct^{es}, generate a similar signature σ^{es}, and deposit some tokens tk^{es} on the blockchain by sending a deposit transaction to EB (as depicted in Fig. 2):

$$Tx_{dep}^{es} = (\text{“Deposit”}, pubk^{es}, ct^{es}, tk^{es}, \sigma^{es}). \tag{4}$$

The deposit here has played as another guard to defend the qualified-but-malicious energy seller from not transferring the energy after being paid. EB verifies ES's identity and attributes as it does for EP, and checks if the decrypted tq^{eb} is equal to the original one. If the verification passes, EB acknowledges its membership regarding energy trading and broadcast $pubk^{es}$ as an available energy source.

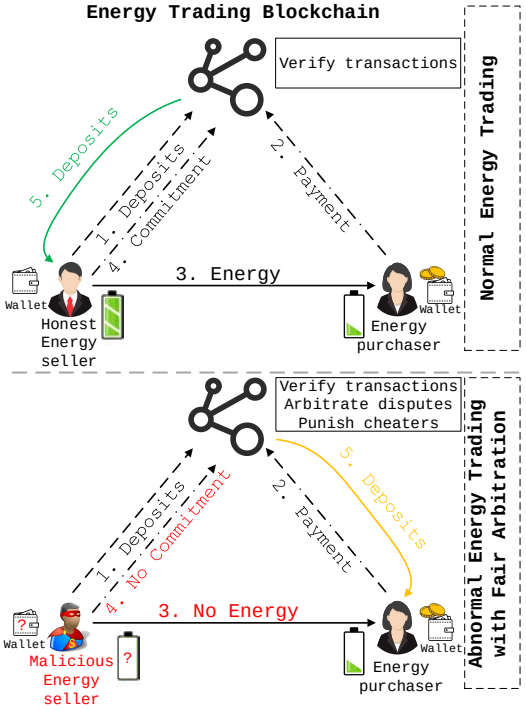


Fig. 2. The illustration of energy trading from two aspects

E. Fair Energy Trading

Upon seeing $pubk^{es}$, EP pays some tokens tk^{ep} of bid price to ES by sending a payment transaction to EB:

$$Tx^{ep} = (\text{“Payment”}, pubk^{es}, tq_{pay}^{ep}, tk^{ep}, pubk^{ep}, h_1^{ep}, \tau^{ep}), \tag{5}$$

where tq_{pay}^{ep} is a timestamp, and τ^{ep} is a digital signature generated with x^{ep}. Then, an honest ES transfers the corresponding energy to EP via $pubk^{ep}$ (communication with EP) and obtains a energy trading bill $\mathcal{B}$. The $\mathcal{B}$ is produced by the smart meter possessed by ES and it contains the energy account of EP, the energy account of ES, an amount of transferred energy, and transfer time. Next, ES creates a commitment $Comm^{es} = H_1(\mathcal{B})$ and puts $Comm^{es}$ on the blockchain by sending a commitment transaction to EB:

$$Tx_{com}^{es} = (\text{“Commitment”}, pubk^{es}, tq_{com}^{es}, Comm^{es}, \tau^{es}), \tag{6}$$

where tq_{com}^{es} is a timestamp and τ^{es} is a digital signature generated with x^{es}. For all the transactions, energy brokers

are the blockchain miners which co-maintain CBC by running practical byzantine fault tolerance (PBFT) [33] as their consensus mechanism. If no complaint is filed against ES after T expires, the energy trading between EP and ES is acknowledged by the system.

F. Dispute Arbitration

When a complaint is submitted by EP against ES before T expires, ES is required to open the commitment $Comm^{es}$ by showing the energy trading bill $\mathcal{B}$ to EB. If ES cannot present $\mathcal{B}$, it means that ES has cheated in previous energy trading. Then, he will be added to a blacklist $\mathcal{BL}^{eb}$ and his reputation value rv^{ep} is decreased as well. The blacklist is a local list maintained by EB and it is also broadcasted with an EB's signature. The duration of an ES on the $\mathcal{BL}^{eb}$ depends on specific applications. It could be one hour, one week, or one month. Next, certain attributes of ES will be revoked as explained in the following subsection. As depicted in Fig. 2, we present the energy trading in two aspects: normal energy trading and abnormal energy trading with fair arbitration. In the upper part of Fig. 2, there is an honest energy seller and an energy purchaser. After an energy trading process, the honest energy seller will obtain payments and the energy purchaser will have energy. In the bottom part of Fig.2, there is a malicious energy seller and an energy purchaser. When the malicious cheats in an energy trading process, his misbehavior will be exposed.

G. Membership Updating

When an energy seller ES is found cheating in the trading system, then one or more of his attributes ought to be removed. For example, assume Bob has cheated in selling energy, and the corresponding attribute x has to be revoked to make sure that he cannot sell energy to other energy buyers during a period of punishment time. CA chooses a random number $v'_x \in \mathbb{Z}_p$ ($v'_x \neq v_x$) as a new attribute version key, calculates an update key $uk_x = (uk_x^1 = v'_x/v_x, uk_x^2 = (v_x - v'_x)/(v_x\beta_3))$, sends uk_x to all the non-revoked energy brokers via secure channels, renews the public attribute key of x as $pak'_x = (pak_x^1 = \mathcal{H}(x)^{v'_x}, pak_x^2 = \mathcal{H}(x)^{v'_x\beta_3})$, and broadcasts a message including pak'_x that the public attribute key of the revoked attribute x is updated. Next, each non-revoked energy seller sends $L = \widetilde{g}^o$ and S_x to CA which computes a new S'_x as $S'_x = (S_x/L^{\beta_2^2})^{uk_x^1} \cdot L^{\beta_2^2} = \widetilde{g}^{o\beta_2^2} \cdot \mathcal{H}(x)^{v'_x o\beta_2}$ and returns it to the non-revoked energy seller. The energy seller's user secret key is updated as $usk' = (S, L, S'_x, \forall x \in A\backslash\{x\} : S_x)$. This is essentially a trivial replacing of S_x with S'_x. Finally, EB updates the ciphertext related to x and generates a new ciphertext ct_{pd}^x.

VI. Security and Privacy Analysis

Authentication. Our energy node authentication is similar to the Chow's signature [26]. In FeneChain, the energy node authenticates to an energy broker using a signature. If the signature is successfully verified, the energy broker confirms that the energy request is generated from a legal energy node and broadcasts her energy request. Meanwhile, an adversary cannot pass the authentication by forging a valid signature. Specifically, the security of the signature scheme is modeled by the existential unforgeability under adaptive chosen message attack (EUF-CMA) in the random oracle model under the DDH problem. If there is a probabilistic polynomial time (PPT) adversary $\mathcal{A}$, which owns a non-negligible advantage ϵ against the EUF-CMA security of the signature scheme, being allowed at most q_0, q_1, q_2 queries on signing oracle, H_1 and $H2$, respectively. Then there exists an algorithm $\mathcal{A}'$ which can solve the DDH problem with a non-negligible advantage not less than $\epsilon - \mu - (\mu + q_2 + q_0)/2^q$, where μ is the probability of successfully breaking the interactive commitment protocol [26].

Access control. An energy seller, who does not hold the attributes corresponding to the access structure $\mathcal{T}$, cannot sell energy in the FeneChain. This is because he cannot rebuild the encryption exponent c, or decrypt the ciphertext ct^{eb} of trading qualification string tq^{eb} with his user secret key. If some attributes of an energy seller are revoked, and if the energy seller entity tries to decrypt ct^{eb} with his old user secret key, then it will not be able to do so. For example, assume an attribute x is revoked from an entity, CA selects a new attribute version key to produce a new update key and sends it to the energy broker to update all the ciphertexts related to x. Due to the different values of the attribute version key in the ciphertext, the revoked energy seller cannot decrypt the ciphertext with his old user secret key. In this way, the unqualified trading attack is defended and the unqualified energy sellers are ruled out from the trading system which stands as a frontline of defense for Industry 4.0.

Privacy. First, energy nodes utilize a signature [26] to prove their qualification of requesting energy in the energy trading system to prevent energy brokers and other entities from knowing their real identities. If an energy node requests/sells energy more than once, she/he will randomize the signature such that any of their signatures cannot be linked. Hence, identity privacy is guaranteed due to the anonymity and unlinkability above. Second, each energy purchaser registers a set of private keys and public keys. It uses each public key only once to break the linkability of energy purchasing activity. Each energy seller also performs in the same way. Thus, transaction privacy is guaranteed. By doing so, the sensitive information of energy nodes are preserved and their private activities in Industry 4.0 are protected with respect to energy trading.

Verifiable fairness. Before the energy is transferred, the energy seller has to put some deposits on the blockchain in advance. After the energy purchaser pays the negotiated money, the energy seller is supposed to transfer the negotiated energy to the energy purchaser, produce a commitment of the transfer bill, and then upload the commitment. If the energy seller behaves honestly, then his deposits will be returned to him after the preset time period runs out. Otherwise, the energy purchaser will accuse him of cheating, and the energy seller is required to open the commitment. Since the energy seller had not actually transferred the energy, he did not produce a proper commitment for him to open. Therefore, the fairness of the energy trading process is verifiable. Also, anyone can check that the EPs and the ESs have faithfully executed their transactions via checking the blockchain transactions. Therefore, the cheating attack is defended and the malicious

TABLE II
COMPARISON OF SECURITY AND PRIVACY PROPERTIES

Property	NRG-X-Change [28]	DET [29]	MILP [30]	BSeIn [10]	EneBloc [3]	PriWatt [7]	BETS [11]	FeneChain
Authentication	√	×	×	√	√	√	×	√
Access Control	×	×	×	√	×	×	×	√
Identity Privacy	×	×	×	√	√	√	×	√
Transaction Privacy	×	×	×	√	√	√	×	√
Verifiable fairness	×	×	×	×	×	×	×	√
Integrity	√	×	×	√	√	√	√	√
Auditability	×	×	×	√	√	√	√	√

energy sellers are ruled out from the trading system. This acts as a final check for energy trading in Industry 4.0.

Integrity and auditability. There are three types of data that are stored on the blockchain, namely deposit, payment, and commitment. Before data are uploaded to the blockchain, it has to be signed by a data provider, i.e., energy seller, energy purchaser and energy seller, respectively. After the data has been stored on the blockchain, the unforgeability of the blockchain has ensured the data integrity. Any data provider can later audit their data on the blockchain by comparing with their own data. Therefore, the integrity and auditability are guaranteed. We compare FeneChain with existing works regarding S&P privacy properties in Table. II. From Table II, it can be seen that the first scheme NRG-X-Change [28] only provide basic security protection (authentication and integrity), while DET [29] and MILP [30] do not adopt security mechanisms at all. The next four schemes BSeIn [10], EneBloc [3], PriWatt [7], and BETS [11] aim to protect S&P in blockchain-assisted energy trading. But they fail to include access control (except BSeIn [10]), and they cannot provide a fair environment for energy trading.

We now discuss the importance of having the aforementioned S&P features in FeneChain for Industry 4.0 concerning the following three major aspects: **Benefits.** The FeneChain can provide several significant security and privacy properties, i.e., authentication, access control, identity privacy, transaction privacy, verifiable fairness, integrity, and auditability. Towards a secure, privacy-preserving, and fair energy trading environment, we believe such properties are indispensable. **Performance.** There is always a balance between performance and security. If we aim for a highly secure energy trading system, we have to resort to various yet different protection measures, which leads to inevitable performance degradation. If we only pursue a highly efficient energy trading system, then some of the security features will be sacrificed. However, FeneChain provides all the required security features while maintaining an acceptable level of performance concerning computational costs and communication overhead (refer to Section VII). **Economy.** In a secure, privacy-preserving, and fare energy trading system, more users will be willing to participate and transact energy with others, even if, they are never acquainted with each other, especially in an open and distributed environment. For such an environment, verifiable fairness is fundamental. If the users are not assured that our energy trading activities are fare or verifiable, they will drop out of the system with a high probability. Therefore, FeneChain helps the energy trading system to operate uninterrupted that allows energy sellers to make profits by selling their surplus energy.

VII. PERFORMANCE ANALYSIS

A. Experiment Settings

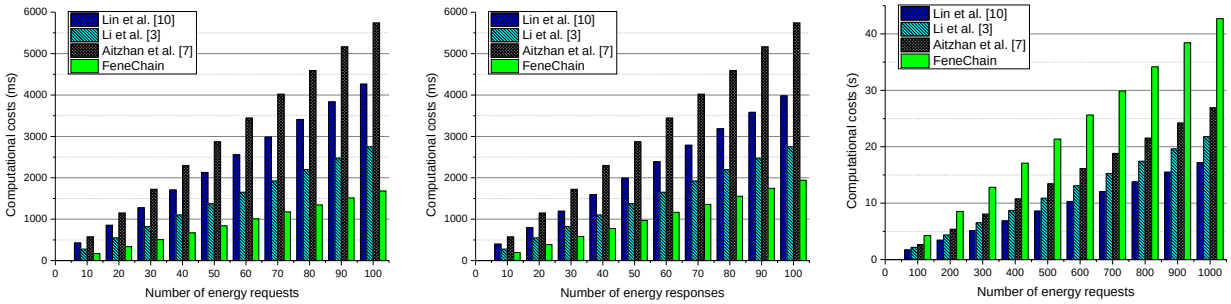
We instantiate the FeneChain on a laptop with 8.00GB of RAM, an Intel Core i7-7500 CPU @2.70GHz, running Windows 10 Home and Visual Studio 2010. We chose Ethereum as our blockchain platform and Miracl[4] as our cryptographic toolset. The elliptic curve is defined as $y^2 = x^3 + 1$ over $\mathbb{F}_{\hat{q}}$. The length of $q, p, \hat{q}$ is 256, 256, and 160, respectively. The hash function is $SHA256$. We installed the Ethereum-Wallet[5] and Geth[6], and set the block creation time as 2 seconds.

B. Computational Costs

In energy requesting phase, an energy purchaser encrypts de^{ep} and pr^{ep}, calculates z^{ep}, s^{ep}, t^{ep}, and a signature σ^{ep} with total cryptographic operations of two multiplications in $\mathbb{G}$, four exponentiations in $\mathbb{G}$, one hash, one division, one exponentiation, and one multiplication in $\mathbb{Z}_q^*$. The computational time is approximately 11.2 milliseconds. In energy responding phase, an energy broker calculates $z, t', H_2(ct^{ep}, h_1^{ep}, h_2^{ep}, t')$, decrypts ct^{ep}, encrypts four items and tq^{eb} with total operations of eight exponentiations in $\mathbb{G}$, three multiplications in $\mathbb{G}$, four AES encryptions, two hashes, seven exponentiations in $\mathbb{G}_1$, one exponentiation in $\mathbb{G}_2$, two subtractions, six multiplications, and one division in $\mathbb{Z}_p$. The costed time is approximately 42.7 milliseconds. An energy seller calculates $e(\widetilde{g}, \widetilde{g})^{\beta}$, recovers ik and tq^{eb}, encrypts tq^{eb}, and generates a signature σ^{es}. The total operations are seven bilinear pairings, one exponentiation in $\mathbb{G}_2$, one division in $\mathbb{G}_2$, four AES decryptions, two exponentiations in $\mathbb{G}$, one multiplication in $\mathbb{G}$, two hashes, four exponentiations in $\mathbb{G}$, one division, one exponentiation, and one multiplication in $\mathbb{Z}_q^*$. The costed time is approximately 13.7 milliseconds. In energy trading phase, the energy purchaser generates a signature τ^{ep} and the energy seller generates a commitment and a signature. The computational time is 5.6 milliseconds and 5.7 milliseconds, respectively. The results are recorded in Table III.

The comparison experimental results in Fig. 3 show that the time costs of all the entities increases linearly with the number of energy requests (and the number of revoked

[4]http://www.certivox.com/miracl
[5]https://github.com/ethereum/mist/releases
[6]https://ethereum.github.io/go-ethereum/downloads



(a) Time cost of an energy purchaser (b) Time cost of an energy seller (c) Time cost of an energy broker

Fig. 3. Computational Costs in Energy Trading

TABLE III
IMPLEMENTED RUNNING TIME (UNIT: MILLISECOND)

Entity	Requesting	Responding	Trading
EP	11.2	0	5.6
ES	0	13.7	5.7
EB	0	42.7	0
Operation	*CA*	*ES*	*EB*
Attribute Revoking	3.7	<1	5.3

attributes). FeneChain performs better than the other three schemes regarding computational costs of energy purchaser and energy seller. The reasons are as follows. [10] used complicated attribute-based signatures and multi-receivers encryption. [3] used time-consuming short group signatures [34] to anonymously authenticate entities, and the generation and verification of signatures incur many cryptographic primitives, e.g., bilinear pairings. [7] used multi-signatures to validate an energy trading transaction which requires at least several specified public keys to produce a signature on such a transaction. Not only it causes extra computational costs, but also communication overhead. [11] is not included here because they do not protect identity or transaction privacy via cryptographic techniques, and their focus is defending block data against linking attacks and malicious data mining algorithms. From Fig. 3(c), we can see that the FeneChain has a higher cost for an energy broker than other schemes. It is because the energy broker has to conduct a series of operations regarding fine-grained access control, including decryptions and encryptions, exponentiations and multiplications in $\mathbb{G}$, and hashes. Nonetheless, the FeneChain provides all the security and privacy guarantees.

Attribute Revoking. The CA calculates an update key uk_x, renews the public attribute key of x, and computes a new S'_x with total cryptographic operations of two divisions, subtraction, and six multiplications, and five exponentiations in $\mathbb{Z}_p$, and one exponentiation, one addition, and one division in $\mathbb{G}$. The time cost is approximately 3.7 milliseconds. Each honest energy seller updates the user secret key usk' (simply replacing the component S_x with the new S'_x) in less than 1 millisecond. The energy broker updates the ciphertext ct^x_{pd} in 5.3 milliseconds as shown in Table III.

Scalability. Fig. 3 and Fig. 4 show the scalability of FeneChain. As shown in Fig. 3(c), if 1000 energy purchasers send 1000 energy requests to an energy broker and 1000 energy sellers send 1000 energy responses to the same energy broker at the same time, the energy broker needs to consume approximately 40 seconds to respond to these energy requests. Fig. 4 illustrates that the *CA* only need 0.37 seconds to revoke 1000 attributes and the energy broker only spends 0.53 seconds to update 1000 ciphertexts. Even if the number of received energy requests, energy responses, and attributes to be revoked is large, the energy broker and the CA can respond rapidly.

C. Communication Overhead

An energy purchaser sends an energy request ER^{ep} that has a length of $|pubk^{ep}| + |ct^{ep}| + |\sigma^{ep}| = 0.219$ KB. Then she sends a payment transaction Tx^{ep} with a length of $|\text{“Payment”}| + |pubk^{es}| + |tq^{ep}_{pay}| + |tk^{ep}| + |pubk^{ep}| + |h^{ep}_1| + |\tau^{ep})| = 0.128$ KBytes. The total communication overhead of an energy purchaser is 0.347 KB. An energy seller first submits a deposit transaction Tx^{es}_{dep} that has a length of $|\text{“Deposit}''| + |pubk^{es}| + |ct^{es}| + |tk^{es}| + |\sigma^{es}| = 0.128$ KB. Then he submits a commitment Tx^{es}_{com} with a length of $|\text{“Commitment}''| + |pubk^{es}| + |tq^{es}_{com}| + |Comm^{es}| + |\tau^{es}| = 0.095$ KB. The total communication overhead of an energy purchaser is 0.223 KB. In one energy trading process, an energy broker broadcasts a ciphertext of trading qualification string, an energy request, a period of time, and the public key of an available energy seller, with a total length of $|ct^{eb}| + |de^{ep}| + |pr^{ep}| + |T| + |pubk^{es}| = 0.066$ KB.

D. Experiments on Raspberry Pi 3

We use a Raspberry Pi 3 Model B+ with Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @ 1.4GHz, and 1GB LPDDR2 SDRAM, which is connected to a desktop with four threads Intel(R) Core(TM) i3 7100 CPU @ 3.90GHz and 8GB memory. We connect the Raspberry Pi to the desktop, distribute an IP address for the Raspberry Pi using the network connection settings, and install Samba service[7] to set a shared folder to make file transfer more convenient. We export the JAVA codes on Eclipse to a Runnable Jar file and choose the “Package required libraries into generated JAR” option. Fourth, for the AES256 operations, we download the Unlimited Strength Jurisdiction Policy Files from the Oracle official

[7]https://www.samba.org/samba/download

website[8], transfer them to the Raspberry Pi using file sharing protocol, and move them to $JAVA_HOME/jre/lib/security in case of Illegal KeySize Exception. We transfer the exported Runnable Jar file to the Raspberry Pi and use the java -jar command to run the experiments. The computational costs for energy purchaser, energy seller, and energy broker are 1632 ms, 1872 ms, and 4740 ms. The experiment on Raspberry Pi is important for demonstrating the practicability of the FeneChain, since more suppliers and engineers view Raspberry Pi as being suitable for real-world industrial application[9]

VIII. Discussion

A. Malicious Energy Purchasers

If a malicious purchaser denies a transaction, we could utilize the "open" function of signature schemes such as BBS [34] and BBS+ [35] to arbitrate disputes. The CA can arbitrate a dispute as follows. It reveals the private key of the malicious purchaser using his one-time signature, searches the private key in its registration list, and then reveals the real identity of the malicious purchaser according to the matched identity record of the search result. However, in this work, we focus on defending attacks from malicious energy seller, while not considering malicious energy purchasers in our security model. Meanwhile, the deny attack from malicious purchasers are not difficult to resist, since we can use group signature to reserve the capability of revealing all real identities at the *CA*.

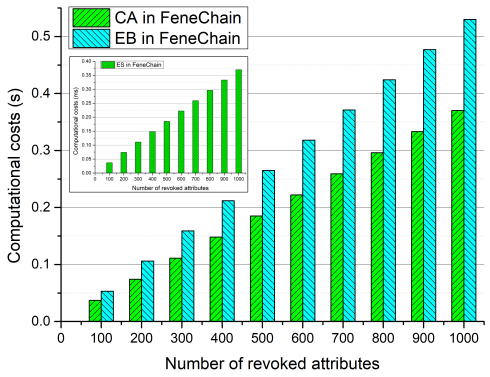


Fig. 4. Computational Costs in Attribute Revoking

B. Improvement of Energy Trading for Industry 4.0

First, for residential users who wish to sell extra energy and purchase energy, the FeneChain will create a secure, privacy-preserving, and fare environment. The energy sellers can make a profit and the energy purchasers can buy energy at an acceptable price. FeneChain exhibits its power especially when some energy purchaser cannot connect to the utility company, but can communicate with nearby energy sellers. This improves energy utilization for residential users greatly.

Second, for the utility company which mainly monitors energy consumption and distribute energy upon multiple energy requests, the FeneChain further assists in handling energy exchanges with many energy sellers and energy purchasers, an increased trading volume, and trustworthy trading.

Next, for the new requirements of Industry 4.0, we discuss what the FeneChain could offer from three aspects. (1) Benefits. The FeneChain enhances self-awareness, self-reconfiguration, and self-maintenance [36] of Industry 4.0. An efficient and secure energy trading system enables energy nodes in Industry 4.0 to readily transact energy and be more aware of their energy status. Based on the status, they are capable of making rational decisions via dynamically reconfiguring energy-related activities. In the end, the whole system can enter a (partially) self-maintained state, which operates upon the energy nodes' transactions. (2) Competitive advantages. The FeneChain enhances the flexibility [37], reliability, and cost-effectiveness for Industry 4.0. The energy trading system allows different energy nodes to easily trade energy in a secure manner, making energy ecosystem more flexible and reliable. Consequently, it can save a centralized energy manager from strenuously monitoring the energy consumption in order to distribute energy to each region, thus making the energy management more cost-effective. All these features promote competitiveness against other business practitioners. (3) Advantages for other domains such as manufacturing and factories. Industry 4.0 is an ecosystem that is constructed on highly automated smart factories and it produces various opportunities for sustainable manufacturing. For factories that need a great deal of energy to keep their machines running, the FeneChain provides a convenient way for them to collect energy from other users and factories. Meanwhile, some factory has an urgent plan for mass production and their energy demand cannot be met timely solely by the utility company. In this situation, with the proposed scheme, the factory can trustingly execute its production plan. Furthermore, the FeneChain assists the manufacturing in building towards a valuable smart manufacturing ecosystem with a complete energy chain.

C. Relationship between Industry 4.0 and Application Context

We focus our work in smart grid environments and we now discuss the relationship between Industry 4.0 and the application context (smart grid) with respect to its related services and features. The services and features reflect the basic requirements of the smart grid, and how the proposed work relates to them further emphasize its effects and influence. (1) Services. The smart grid is the next generation power grid combining the current power system and communication technology. It enables peer-to-peer energy trading services for grid customers and management for the utility company. As a key element of Industry 4.0, energy penetrates every link in industrial manufacturing and householding. Flexible, reliable, and effective energy trading manages to keep the energy flow among grid customers in a healthy manner. In this way, more functionalities and objectives in the higher level are supported. (2) Features. The smart grid requires a reliable operating environment to maintain the whole system. This is addressed from two aspects. First, the fairness of energy trading should be guaranteed in order to encourage customers to buy energy from other customers. Second, the energy trading transactions

[8]https://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

[9]https://www.automationworld.com/products/control/blog/13319680/is-raspberry-pi-ready-for-industry.

should be verifiable in the sense that the trading activities are recorded and verified. These two properties are crucial to building a smart environment in Industry 4.0 where all grid entities collaborate tightly and depend on each other. In summary, the energy trading system in the smart grid has played a fundamental role in Industry 4.0 by significantly changing our industrial production and daily life.

IX. Conclusion

In this paper, we have presented a blockchain-based energy trading scheme FeneChain to supervise and manage the energy trading process towards building a secure energy trading system and improving energy quality for Industry 4.0. FeneChain achieves efficient management, i.e., transparency, unforgeability, and verifiability, of energy trading data with the assistance of a consortium blockchain. It provides anonymous authentication for energy nodes and fine-grained access control for energy trading services. Moreover, it preserves identity privacy and transaction privacy during energy trading and guarantees energy trading fairness against malicious energy sellers. With FeneChain, energy nodes upload and verify energy trading data via the blockchain. Energy nodes readily engage in the system without security or privacy concerns.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (NSFC) under the grant No. U1836102. It is also partially supported by EU LOCARD Project under Grant H2020-SU-SEC-2018-832735.

References

[1] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," Applied Energy, 2017, 195:234-246.

[2] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Trans. Industrial Informatics (TII)*, 2014, 10 (4): 2233-2243.

[3] 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 Trans. Industrial Informatics (TII)*, 2018, 14 (8): 3690-3700.

[4] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchain-based software-defined Industrial Internet of Things: A dueling deep q-learning approach," *Internet of Things Journal*, 2018, PP (99): 1-14.

[5] Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," *IEEE Commun. Mag.*, 2016, 54 (11): 158-164.

[6] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Trans. Smart Grid (TSG)*, 2016, 8 (2): 619-626.

[7] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable and Secure Computing (TDSC)*, 2018, 5 (15): 840-852.

[8] "Crash Override: The Malware That Took Down a Power Grid, 2016. https://www.wired.com/story/crash-override-malware/?verso=true.

[9] "UK power cut: We were stuck on a train with no food or toilets, 2019. Available: https://www.bbc.com/news/uk-49304977.

[10] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications (JNCA)*, 2018, 116: 42-52.

[11] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Industrial Informatics (TII)*, 2019, 15 (6): 3548-3558.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. Avaliable: https://bitcoin.org/bitcoin.pdf.

[13] A. Kosba, A.Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," *Proc. 37th IEEE S&P*, May 2016: 839-858, San Jose, USA.

[14] E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," *Proc. 13th European Conference on Computer Systems (EuroSys)*, April 2018: 1-15, Porto, Portugal.

[15] M. Li, L. Zhu, and X. Lin, "CoRide: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing," *Proc. ACM SecureComm*, June 2019: 408-422.

[16] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," *37th IEEE INFOCOM*, April 2018: 1-9, Honolulu, USA.

[17] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys and Tutorials*, 2018, 20 (4): 3416-3452.

[18] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Trans. Industrial Informatics (TII)*, 2019, online.

[19] Y. Zhang and C. Xu and X. Lin and X. Shen, "Blockchain-based pPublic integrity verification for cloud storage against procrastinating auditors," *IEEE Trans. Cloud Computing (TCC)*, 2019, PP (99): 1-15.

[20] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Industrial Informatics (TII)*, 2018, 14 (11): 4724-4734.

[21] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Comm. Mag.*, 2018, 56 (7): 82-88.

[22] L. Zhu, M. Li, Z. Zhang, C. Xu, R. Zhang, X. Du, and N. Guizani, "Privacy-preserving authentication and data aggregation for fog-based smart grid," *IEEE Communications Magazine*, 2019, 57 (6): 80-85.

[23] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Trans. Dependable and Secure Computing (TDSC)*, 2018, PP (99): 1-12.

[24] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: Review and outlook," *IEEE Transactions on Consumer Electronics (TCE)*, 2011, 57 (1): 76-84.

[25] M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek, "Secure multiparty computations on bitcoin," *Proc. the 35th IEEE Symposium on Security and Privacy (S&P)*, May 2014: 443-458.

[26] S. S. M. Chow , C. Ma, and J. Weng, "Zero-knowledge argument for simultaneous discrete logarithms," *Proc. International Conference on Computing & Combinatorics*, July 2010: 520-529, Nha Trang, Vietnam.

[27] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," *Proc. 8th ACM ASIACCS*, 2013: 523-528.

[28] M. Mihaylov, S. Jurado, K. V. Moffaert, N. Avellana1 and A. Nowé, "NRG-X-Change: a novel mechanism for trading of renewable energy in smart grids," *Proc. 11th International Conference on the European Energy Market (EEMs)*, 2014: 101-106.

[29] Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," *IEEE Comm. Mag.*, 2016, 54 (11): 58-164.

[30] C.-C. Lin, D.-J. Deng, C.-C. Kuo, and Y.-L. Liang, "Optimal charging control of energy storage and electric vehicle of an individual in the Internet of energy with energy trading," *IEEE Trans. Industrial Informatics (TII)*, 2018, 14 (6): 2570-2578.

[31] Dan Boneh and Moni Naor, "Timed commitments," *Proc. 20th Annual International Cryptology Conference (CRYPTO)*, August 2000: 236-254.

[32] J. A. Garay and M. Jakobsson, "Timed release of standard digital signatures," *Proc. 6th International Conference on Financial Cryptography*, March 2002: 168-182, Southampton, Bermuda.

[33] M. Castro and B. Liskov, "Practical byzantine fault tolerance," *Proc. 3rd Symposium on Operating Systems Design & Implementation (OSDI)*, August 1999: 173-186, New Orleans, USA.

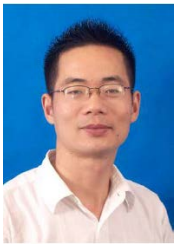
[34] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Proc. 24th Annual International Cryptology Conference (CRYPTO)*, 2004: 41-55, Santa Barbara, USA.

[35] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," Proc. of Conference on Security and Cryptography for Networks (SCN), 2006, 4116: 111-125.

[36] Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," *Robotics and Computer-Integrated Manufacturing*, 2018, 54: 133-144.

[37] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Applied Energy*, 2018, 209: 8-19.

Meng Li (mengli@hfut.edu.cn) received the Ph.D. degree in Computer Science and Technology from Beijing Institute of Technology, Beijing, China in 2019, received the B.E. degree in the Information Security from Hefei University of Technology, Hefei, China, in 2010, and received the M.S. degree from Computer Science and Technology from Beijing Institute of Technology in 2013. He is now an Associate Researcher in the School of Computer Science and Information Engineering, Hefei University of Technology. He was sponsored by the China Scholarship Council to study as a visiting Ph.D. student in Wilfrid Laurier University and University of Waterloo from 2017 to 2018. His research interests include applied cryptography, security and privacy, vehicular networks, fog computing and blockchain.



DonghuiHu (hudh@hfut.edu.cn) received the B.S. degree from Anhui Normal University, Wuhu, China, in 1995, the M.S. degree in computer science and technology from University of Science and Technology of China, Hefei, China, in 2004, and Ph.D. degree in information security from Wuhan University, Wuhan, China, 2010. He was a Visiting Researcher with UNCC IN 2013-2014. Currently, he is a Professor and Director of Institute of Network and Information Security in the School of Computer Science and Information Engineering at the Hefei University of Technology. His research interests include information trustworthiness evaluation, privacy protection, steganography and steganalysis, and he has published extensively in these areas in various journals and conferences. His research has been supported by many government foundations and industrial companies.

Chhagan Lal is currently working as a postdoctoral research fellow at Simula Research Laboratory, Norway. Previously, he was a postdoctoral fellow at Department of Mathematics, University of Padua, Italy, where he was part of the SPRITZ research group. He received his PhD in Computer Science and Engineering from the Malaviya National Institute of Technology, Jaipur, India, in 2014. During his PhD, he has been awarded with the Canadian Commonwealth Scholarship under the Canadian Commonwealth Scholarship Program to work in University of Saskatchewan, Saskatoon, SK, Canada. His current research areas include applications of blockchain technologies, security in software-defined networking, and Internet of Things networks.

Mauro Conti is Full Professor at the University of Padua, Italy, and Affiliate Professor at the University of Washington, Seattle, USA. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of Security and Privacy. In this area, he published more than 300 papers in topmost international peer-reviewed journals and conference.

ZijianZhang (zhangzijian@bit.edu.cn) received his Ph.D. degree in Beijing Institute of Technology. He is an Associate Professor with the School of Computer Science and Technology, Beijing Institute of Technology. He was a visiting scholar in the Department of Computer Science and Engineering, State University of New York at Buffalo in 2014. His research interests include authentication and key agreement in communication security, user behavior recognition and preference inference in AI security. He has published more than 60 papers on journals and conferences including TSG, TDSC, TII, INS, NeurIPS, IWQoS, ICC, etc, and transactions and journals including TDSC, TVT, TCC, IoT J, etc.