Liu, Qi; Wan, Pengbo; Chen, Fen; Li, Weiting

Article

Cost efficient management of complex financial energy trading systems: Knowledge-based blockchain technique

Journal of Innovation & Knowledge (JIK)

Provided in Cooperation with:
Elsevier

Suggested Citation: Liu, Qi; Wan, Pengbo; Chen, Fen; Li, Weiting (2023) : Cost efficient management of complex financial energy trading systems: Knowledge-based blockchain technique, Journal of Innovation & Knowledge (JIK), ISSN 2444-569X, Elsevier, Amsterdam, Vol. 8, Iss. 1, pp. 1-7, https://doi.org/10.1016/j.jik.2023.100323

This Version is available at:
https://hdl.handle.net/10419/327235

Journal of Innovation & Knowledge 8 (2023) 100323

Journal of Innovation & Knowledge

https://www.journals.elsevier.com/journal-of-innovation-and-knowledge

Cost efficient management of complex financial energy trading systems: Knowledge-based blockchain technique

Qi Liu[a], Pengbo Wan[b,*], Fen Chen[b], Weiting Li[c]

[a] School of Employment and Entrepreneurship, Hubei University of Technology, Wuhan, Hubei, P. R. China,
[b] School of Finance, Hubei University of Economics, Wuhan, Hubei, P. R. China
[c] School of Public Administration, Zhongnan University of Economics and Law, Wuhan, Hubei, P. R. China

ARTICLE INFO

Article History:
Received 28 August 2022
Accepted 1 January 2023
Available online 11 January 2023

Keywords:
Encryption
Blockchain
Energy market trading
Privacy and efficiency enhancement
Smart power system

JEL Code:
A10
C89
P48

ABSTRACT

Industry 4.0 has led to the growth of smart cities utilizing the Internet of Things (IoT). Wireless sensor network (WSN) has drawn considerable interest as an important element of the IoT. The Energy Internet (EI) is growing in importance as a significant component of constructing the intelligent city, especially in terms of its reliability and security. EI is moving in a new direction of energy trading advancement where distributed energy transaction models are replacing the conventional centralized layout. Blockchain technology, which is the underlying support, has gained interest as a result of its benefits, namely integrity, and nonrepudiation. Privacy disclosure, despite the benefits, is a concern for many blockchain-enabled trading layouts. The paper presents encryption according to the cryptographic text properties as the main scheme for reconstructing the dealing layout in order to resolve the issue in the electricity market. In particular, the blockchain energy trade plan with privacy (BETPWP) has been developed to manage the distributed transaction. Transaction arbitration in ciphertext form is employed for achieving precise access control. As a result of this method, the transaction layout could be made considerably more secure and reliable, as well as maximizing the security of private data. BETPWP also proposes a credibility-enabled equity proof consensus method that would significantly improve operational performance. A study of security and the test assessment of the suggested method are performed in order to demonstrate its effectiveness.

Introduction

In the recent years, smart cities (SCs) including integration of the Internet of Things (IoT) has been attracted more attention due to higher reliability, resiliency, and sustainability. New generations of mobile information technologies, such as the IoT and cloud computing, allow the intelligent city to carry out complete perception, distributed connectivity, and pervasive computation. One of the focuses of studies in this layout would be to ensure the security of sensor networks utilized as a part of IoT. Researchers and industry have both been paying great emphasis to make clean energy networks more secure, which is a critical component of the SCs. The energy Internet (EI) network uses IoT devices for the data measuring modules, as well as wireless sensor networks (WSN), which are also contributing significantly to the creation of the SC.

The conventional power generation and distribution systems face to many challenges including poor performance, vulnerabilities, and insufficient reliability to alone-step attacks, all of that are becoming more prevalent in the energy system. Thus, the EI idea is gaining in popularity and has taken over the energy revolution. In the EI, a massive energy network has been constructed using developed power electronics, the newest information technologies, and intelligent management technologies, which include distributed energy harvesting equipment, distributed energy storage equipment, and a variety of user equipment. EI reliability and security are essential in terms of the SC.

As a result of the benefits of blockchain (BC) technology over centralized transactions, including openness, independence, nonmanipulation, and resilience to alone-step attacks, the EI has incorporated BC technology instead of the conventional centralized transaction layout. In contrast, BC-enabled trading layouts usually have no privacy protections for users. Traceability and transparency of transactions are enabled by BC, but it makes both parties' private data public as well, which clearly isn't sufficient to protect privacy. Various studies attempt to address the problem indirectly by obscuring the BC data and the links among consumers.

* Corresponding author.
E-mail address: wanpengbo@hbue.edu.cn (P. Wan).

https://doi.org/10.1016/j.jik.2023.100323

The proposed layout integrates BC and cryptographic technologies, including pseudonyms, differential privacy, and active multilateral computational integration, to provide secure energy trading data.

The architecture of conventional cities is being challenged by SCs. The conceptual advancement as well as practical applications of SCs are the focus of numerous scholars. A detailed study and summary of the concept, framework, and applications of SCs is presented in refs (Appio, Lima & Paroutis, 2019) and (Skare & Soriano, 2021). A number of studies have been conducted on the applications of IoT in SCs (Kavousi-Fard, Nikkhah, Pourbehzadi, Dabbaghjamanesh & Farughian, 2021) and (Giaretta & Chesini, 2021). EI advancement is receiving a lot of interest and advancement in SCs as well. Effectual energy management for the IoT in SCs is presented in refs (Khattak, Tehreem, Almogren, Ameer, Din & Adnan, 2020) and (Saura, 2021). An essential industrial network that is emerging quickly in the Industrial 4.0 era is the EI (Mahapatra & Nayyar, 2019) and (Kim & Upneja, 2021). Numerous approaches have been developed by studies on the EI recently to solve its inherent shortcomings. Ref (Popli, Jha & Jain, 2018) presented a comprehensive analysis of the framework, processes, and EI technologies. During the emergence of the EI, distributed energy trading became a point of controversy. Because of its benefits, BC has been extensively utilized as a distributed ledger in the EI. A comprehensive analysis and the categorization of current BC-enabled energy trading layouts in the electrical power network are presented in ref (Guan, Lu, Wang, Wu, Du & Guizani, 2020). Ref (Li, Chen & Zhou, 2020) presented the localized P2P electric vehicle energy trade layout according to the consortium chain that utilizes the duplicate dual bid procedure for maximizing the public well-being in the transactions. Ref (Aitzhan & Svetinovic, 2016) used anonymous encrypted, multisignature message process, and BC scheme in order to provide dealing safety in distributed intelligent electrical network energy dealing by eliminating the need for third parties. A convertible, delayed process for controlling information availability to smart grids powered by renewable energy resources is presented in ref (Yang, Guan, Wu, Du & Guizani, 2020).

It is usually a transaction initiator (TI) intention not to allow users without appropriate access to view transaction information, which results in their private data being disclosed (Bagheri, Madani, Sahba & Sahba, 2011), (Sabha, Sahba & Lin, 2014), and (Dabbaghjamanesh, Kavousi-Fard & Mehraeen, 2018). Access control algorithms enable participants to specify who has access to their personal data. Using access control strategies, private data can be protected from leakage to irrelevant participants by filtering access participant accounts. Currently available studies, on the other hand, ignore the same access control issues. As a cryptography algorithm, Encryption according to cryptographic text properties (Eat-CTP) (Liu & Fan, 2019) is ideal for solving this issue as the small available control encryption layout. By combining Eat-CTP and BC technologies (Liu, Yuen, Zhang & Liang, 2018), this paper provides a generalized transaction layout that has the capability of available control and umpire in order to support the requirements of Industry 4.0 and preserve the privacy of participants. This paper makes the following contributions:

1. The BETPWP layout preserves privacy while executing distributed energy transactions in BCs. Eat-CTP represents the main scheme for developing a fine-grained ciphertext-enabled access control model. Numerous umpire nodes could support transaction arbitration and lightweight ciphertext updates, enhancing the user's security.
2. The suggested credibility-enabled equity proof consensus procedure in BETPWP, capable of significantly improving system performance, will address the weaknesses of BC's lower performance and high delay. The mechanism is designed as a basic layout and an improved layout customizable for handling various application case studies.
3. Lastly, a comprehensive security survey and efficiency assessment of BETPWP is conducted. The suggested BETPWP system has been proven to be highly secure following evaluation and derivation from multiple angles. The suggested system has been tested experimentally and compared to the previous works as well. Based on the findings, the suggested system appears to be effective.

Following is an overview of the remainder of the present study. The preliminary findings are presented in Part 2. Part 3 discusses layouts and objectives. Part 4 presents the fundamental and improved model of BETPWP. Part 5 presents the security study. Part 6 evaluates the efficiency of BETPWP. Part 7 provides the conclusion of the study.

Preliminary findings

This part explains the preliminary findings found in BETPWP. Following are 3 descriptions that are utilized in part 5 to describe the decryption process.

Bilinear maps

Description 1. (Bilinear Maps): G_0 and G_1 are 2 first-order multiplication cycle groups p, and g is the producer of G_0. The bilinear map e is, e: $G_0 \times G_0 \to G_1$, for whole $a, b \in Z_p$: 1) Bilinearity: $\forall u, v \in G_1, e(u^a, v^b) = e(u,v)^{ab}$; 2) Computability: $\forall f, h \in G_1, e(f, h)$ could be computed; 3) Non-degeneracy: $e(g, g) \neq 1$

Access framework

Description 2. (Access Framework): $\{P_1, P_2, \ldots, P_n\}$ is a set of parties. The set $A \subseteq 2^{(P_1, P_2, \ldots, P_n)}$ shows monotone when $\forall B, C$: *if* $B \in A$ and $B \subseteq C$ so $C \in A$. An access framework represents a set A of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}$, $A \in 2^{(P_1, P_2, \ldots, P_n)} \backslash \{\emptyset\}$. It is called the authorized sets, that do not belong in A are called the unauthorised sets.

Linear secret-sharing layouts

Description 3. (linear secret-sharing layout.): The secret sharing layout Π among a group of parties has been described as linear when:

(1) The divides of entire parts form a vector on Z_p.

(2) The matrix M with l tiers and n columns exists, known as the divide-producing matrix for Π. For whole $i = 1, \ldots, l$, in the i' *th* tier of M, the function $P(i)$ is applied as the tier tag. The column vector $v = (s, r_2, \ldots, r_n)$ has been created, in which $s \in Z_p$ shows the secret to be shared and $r_2, \ldots, r_n \in Z_p$ have been selected by random, afterward, Mv shows the vector of l divides of the secret s based on Π. The share $(Mv)_i$ is part of party $P(i)$.

Layouts and objectives

Fig. 1 shows the system framework for the BC energy trade plan with privacy (BETPWP). Besides being large in number, distributed production agents have a variety of applications. A micro-production unit, like a household or power station, can generate electricity. Solar, wind, and water energy are used to produce electricity, which is then dealt in BETPWP. Transaction nodes transmit dealing datum streams via mobile smart terminal, like smartphones, computers, and embedded equipment. Each trading node establishes a distributed system of energy exchange according to BC technology and communicates via wireless systems. A final step entails packaging the transaction into

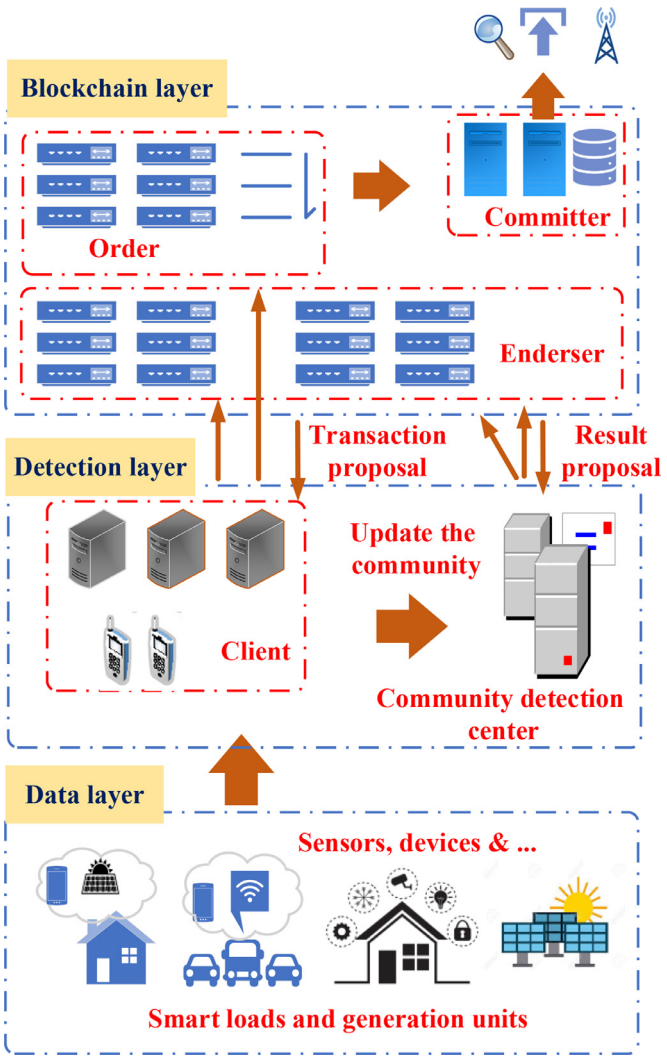

Fig. 1. BC-enabled energy trading system layout.

blocks and recording it in the chain. The microgrid transmits power to users by means of a physical network.

Design objectives

The conventional distributed transaction layout provided via the BC requires whole transaction records to be publicly recorded in clear text for realizing fairness, transparency, and auditability, and each node maintains a full backup of the whole chain. It is assumed that participants have a curiosity for one another despite the fact that they cannot alter or disrupt the BC framework. Furthermore, while the BC ensures data integrity, a few sensitive data can reveal private data about others.

Furthermore, conventional Proof of Work (PoW) consensus mechanisms in the BC system involve heavy computation power and require significant latency. In order to be secure, PoW assumes that the single point computational power of the network does not exceed 50%. Yet even with fewer than half of the system's mining power, an attack is feasible. If a single node possesses significant computational power or if several nodes collude with one another, it might pose main security threats to the network, and their computational power might be more than 50% of the whole network. The PoW mechanism will then have broken its security assumption that directly threatens the fairness and security of the dealing network, and entails serious security concerns for the whole EI system.

The design objectives of BETPWP contain the next 3 features for overcoming these issues and facilitating electric energy trading.

i) **Protection of privacy:** During a transaction, both parties' private information has been protected. As long as the system is functioning normally, BETPWP controls access and hides the transaction data.
ii) **Performance:** By replacing the conventional PoW consensus with a weightless validation-enabled justice-proof consensus system, the BETPWP system could be more operationally efficient. In comparison to the conventional proof of stake consensus, the scheme for ordering priority with similarity to an ideal solution (SOPSIS) complete assessment process is combined for developing a more fair, reliable, and customized consensus process.
iii) **Anti-attack:** Due to its BC-enabled base, BETPWP is very stable and robust. Thus, alone-step attacks in conventional centralized energy trading layouts could be eliminated, and long-range, safe and abiding operations could be achieved.

Description of the system layout

i) **Transaction entity:** Each trading entity in the system uses its own pseudonym for transactions. Electricity could also be sold by them as generators, including home photovoltaic, distributed wind turbine, little hydropower units, and so on. Additionally, electricity could be purchased by them as end-users, including electric devices, households, industries, and so on.
ii) **Certification authority (CA):** Those entities engaged in distributed transactions rely on the CA, a third-party fundamental production center, for the generation, distribution, and management of identity authentication digital certificates.
iii) **Accounting node:** At the end of each trading round, the node that has high credibility has been chosen as the accounting node. BC transactions are packaged into blocks by the accounting node and added them to the BC. Upon reaching a consensus, the node receives the relevant incentive.
iv) **Arbitration node:** In contrast to other physical commodities, due to the continuous nature of the delivery of electrical energy, it may be difficult for the parties to the trading contract to agree whether the real volume of electrical energy transmitted will meet the contract conditions. In the meantime, parties that believe their own interests are damaged might seek arbitration. A judgment could be made by the arbitration node according to proof such as meter readings.

Fig. 2 illustrates the suggested trading layout in detail. In the event that an electric energy generation unit needs to sell the remainder of its power, it sends transactions as an initiator. Initially, the TI can draft the transaction data in accordance with the needs and develop the access method. Once the encrypted transaction request has been broadcasted in the BC network, participants that match the access policy will be able to view it. Moreover, energy users wouldn't have to depend on one single supplier of electricity and can select generators that fit their particular requirements and deal with them directly. Electrical users could select to buy the amount of electricity they need and transmit transaction applications. Selecting a dealing section from the demandants and negotiating to achieve a dealing contract are the 2 actions that the initiator performs. Now, the dealing sections are drafted by 2 parties for forming an agreement and sent to the accountancy tie for confirming consensus. Therefore, accounting nodes have begun to pack and record dealing datum during the time threshold. When the 2 parties have a dispute following the completion of the transaction, they could use the adjudication tie for umpire. Following the adjudication outcome, the main ciphertext updates so that a new dealing record can be created which can't be decrypted by the arbitration node. Finally, the accounting

nodes would determine the subsequent round by using the gathered node data for calculating a confidence score.

BCs as distributed and immutable ledgers seem ideally suited to this recently distributed system. PPBCETS developed a BC-based platform for direct transactions among energy producers and consumers. Since energy commodities have some unique characteristics, smart contracts are used for conducting transactions. Part 7 provides information about the contract features and the data on BC transactions. Transaction participants are aware of the circulation of finance via their wallets.

BETPWP: improved layout

Considering the real application case, it is not just the arbitration success rate that determines whether a node is credible. The suggested improved layout of BETPWP provides a customized and personalized feature choosing process during the election step of accounting nodes. BETPWP utilizes the SOPSIS complete assessment scheme for calculating the validity point. It is possible to set assessment targets based on real application case studies, like arbitration success rates, participations, computational power, etc. Suppose that m assessment targets exist, every assessment target includes n monitoring indexes, and the j^{th} index amount of the i^{th} assessment goal equals x_{ij}. The algorithm is detailed below. (1) The Entropy Weight Method (EWM) is used for weighing every feature amount that influences credibility and ranking the outcomes. It can be expressed in the following way. In which, $X_iY_i \ldots$ shows the system-described reference items in order to determine the credibility score, like the adjudication prosperity rates, offline rates, number of dealings, and default rates.

$$score = \sum X_iY_i \ldots \tag{1}$$

Due to the various measurement units of the indicators, they can be classified in two categories: a cost-enabled indicator and a profitability indicator. Prior to the complete assessment, the indicator must be normalized.

a) In the cost-enabled indicator:

$$X_{ij}^{*} = \frac{max_j x_{ij} - x_{ij}}{max_j x_{ij} - min_j x_{ij}} \tag{2}$$

b) In the profitability indicator:

$$X_{ij}^{*} = \frac{x_{ij} - min_j x_{ij}}{max_j x_{ij} - min_j x_{ij}} \tag{3}$$

c) The proportion of the j^{th} indicator of the i^{th} assessment target is calculated:

$$p_{ij} = \frac{X_{ij}^{*}}{\sum_{i=1}^{m} X_{ij}^{*}} \tag{4}$$

d) The entropy of the jth index is calculated:

$$e_j = -\frac{1}{\ln m} \sum_{i=1}^{m} p_{ij} \ \ln p_{ij} \tag{5}$$

e) The entropy weight of the jth index is calculated:

$$w_j = \frac{1 - e_j}{\sum_{j=1}^{n} (1 - e_j)} \tag{6}$$

The previous algorithm allows for customizing the index in order to measure credibility. The chosen credibility assessment target items in the system initialization step are determined by BETPWP, and every target item is quantified into various assessment indices. Furthermore, various weight amounts are assigned to every target item based on the level of impact on the credibility by the SOPSIS assessment process, and the last credibility score is a complete validity amount.

Security evaluation

The following part provides a complete study of the security of BETPWP from 5 perspectives: information, consensus, umpire, algorithm securities, and privacy protection.

Information security

As a result of the distributed nature of the EI, data security needs to be enhanced, however, it is very hard to ensure data security. BETPWP relies on the distributed BC in its transaction structure, making it resistant to single-point attacks. Moreover, the BC makes use of cryptographic techniques like universal key systems, hash computations, and digital signature to perform unidentified dealings, which ensures the security and integrity of transaction information. As well as ensuring data security, the BC allows for data traceability. In the event that the information isn't correct, it could be identified and corrected promptly. Thus, the BC guarantees the security of dealing information.

Algorithm security

Algorithm security constitutes system security. An attack on the algorithm puts the whole trading system at risk. For algorithm security, Eat-CTP enabled available control layout is used as the main scheme. The suggested Eat-CTP layout was found to be selected-plaintext attack security (CPAS). The suggested layout is proved secure by using the CPAS game described below:

Theorem 1. *If the structure of ref (Liu & Fan, 2019) proves to be CPAS, therefore, the BETPWP presented here will be CPAS.*

Proof. The main layout is Eat-CTP presented in ref (Liu & Fan, 2019). In the case of BETPWP attacks, let's assume adversary A has the non-negligible benefit. Afterward, a simulator B is built and the challenger C, B could attack the main layout using the non-negligible benefit.

Setup: The challenger C firstly selects a set G_0 with primary order p and generator g. Afterward, it can randomly select α, $a \in Z_p$, $h_1, \ldots, h_u \in G_0$ and give the public key $PK' = \{g, e(g, g)^{\alpha}, g^{a}, h_1, \ldots, h_1\}$ to B. B can select an exponent $b \in Z_p$ and give PK to A.

$$PK = \left\{g, e(g,g)^{\alpha}, e(g,g)^{b}, g^{a}, h_1 \cdots \mathrm{h_U}\right\}$$

The parameter c in the layout is omitted since it does not contribute to transaction security, as it isn't applied to generate key or decrypt, just in order to update the ciphertext.

Phase 1. A can submit a group of features S^{*} to B, B can send it to C. C can randomly choose $t \in Z_p$ and generate the related secret key

$$SK' = \left\{K' = g^{a} g^{at}, L' = g^{t}, \quad x \quad S^{*}, K_x' = h_x^{t}\right\}$$

Afterward, C can send SK' to B, B can compute $K = K'.g^{b} = g^{\alpha} g^{a+tb}$ and can return the secret key SK to A.

$$SK = \left\{K, L = L, \ \forall x \in S^{*}, K_x = K_x'\right\}$$

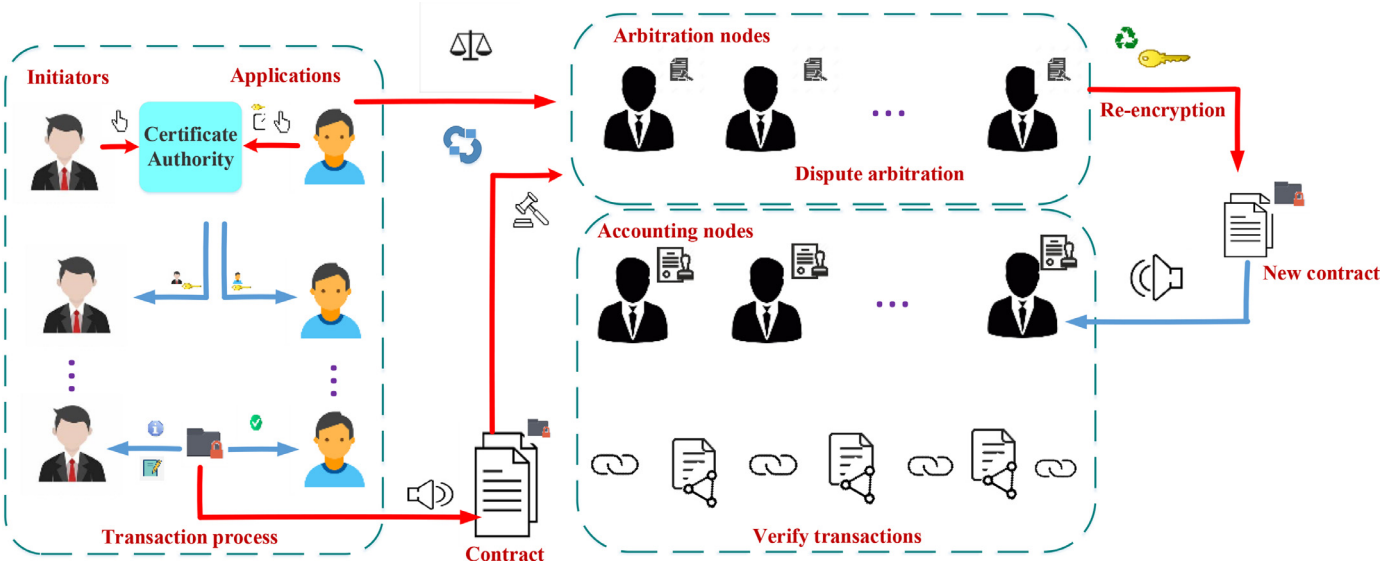

Fig. 2. The BC energy trade plan with privacy.

Challenge: A can select 2 messages M_0, M_1 with same length and the available framework (M, ρ) and submit them to B. For S^* queried via A, (M, ρ) could not be met via each S^*. B can forward M_0, M_1 to C and C can choose a fortuitous bit $b \in \{0, 1\}$ and encryption M_b within the available framework (M, ρ). Afterward, C can return CT' to B.

$$CT' = \left\{ C = M_b e(g,g)^{\alpha s}, C' = g^s \ \forall 1 \le i \le l, C_i = g^{a\lambda_i} h_{\rho(i)}^{-r_i}, D_i = g^{r_i} \right\} \quad (7)$$

B can set $d_0 = a - b$ and compute:

$$\tilde{C}_2 = C / e\left(g^{d_0}, c'\right) = M_b . e(g,g)^{(\alpha - d_0)s} \quad (8)$$

$$\hat{D}_i = e(C_i, g) \cdot e\left(h_{\rho(i)}, D_i\right) = e(g,g)^{\alpha\lambda_i} \cdot e\left(h_{\rho(i)}, g\right)^{-r_i} \cdot e\left(h_{\rho(i)}, g\right)^{r_i} = e(g,g)^{(d_0+b)\lambda_i} \quad (9)$$

Lastly, B can send the challenge ciphertext CT to A.

$$CT = \left\{ \tilde{C}_1 = C, \tilde{C}_2, C', \forall 1 \le i \le l, C_i, D_i, \hat{D}_i \right\} \quad (10)$$

Phase 2. : A can frequently issue the secret key queries as Step. It should be noted that (M, ρ) can't be met via each new input S^*.

Guess: A can output a surmise b', and win the game when $b' = b$. B can give C the similar guess. Clearly, when A displays a non-negligible advantage $Adv_A^{\text{PP-BCETS}} = \delta$ if attacking the BETPWP, B uses A to attack the main layout with an advantage $Adv_B^{\text{basic}} = \delta$. Thus, when the main layout is CPAS, afterward, the BETPWP will be CPAS, the proving of Theorem-1 has been done.

Privacy retention

BETPWP protects the privacy of participants throughout the transaction method. The paper has aimed at efficiently protecting the privacy data throughout the transaction method by designing and implementing a fine-grained access control layout. Just users that meet the access policy will be able to access precise transaction data due to the two-level ciphertext design. During the initiation of a transaction, information on the first level has been encrypted based on the established access framework, and just the participants that satisfy the needed conditions could access it. Just the participant that participated in the transaction will have access to detailed data once the transaction is complete. When the transaction is disputed, the key would be updated following the arbitration, so that the arbitration node cannot gain new data by utilizing the same key.

Consensus security

The new validity-enabled impartiality proof consensus procedure has been used in the suggested layout. By utilizing this mechanism, the conventional equity affirmation procedure is improved. In proof-of-stake consensus mechanisms, the major security concern is how to choose reliable accounting nodes with fairness. When a malicious node has been selected, it deliberately skips the packing of transactions into blocks, resulting in the transaction failing. The security of the consensus mechanism is severely threatened by malicious nodes. To solve the problem, the obscure view of validity as the numerical point is quantified. The amount has been computed by a set of reference terms that reflect the validity of the tie's default rates and umpire success rates.

These validity points have been generally calculated and stored on the blocks, therefore evil participants can't alter them. The suggested mechanism selects the accounting nodes fairly and safely, and just the most trustworthy nodes are chosen.

Arbitration security

During the arbitration procedure, the majority of nodes are assumed to be reliable and honest. Arbitration results are determined by numerous arbitration nodes voting. The last outcome won't be affected by malicious nodes, even if they judge incorrectly. Additionally, the node's credibility would be reduced by this malicious judgment behavior. Nodes with higher credit scores are less likely to be selected as accounting nodes. This further constrains how arbitration nodes behave. As a result, the suggested arbitration procedure has credibility and reliability.

Experimental assessment

The following part presents the trial assessment outcomes on the efficiency of BETPWP.

The major overheads of the suggested layout can be divided into two categories. The first is computation costs resulting from encryption and decryption, and the second is the upper involved with communication among participants of energy dealing and other tasks

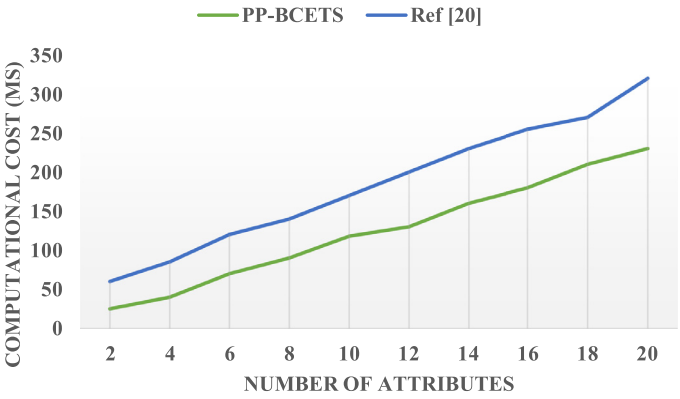

Fig. 3. Relation among the number of features and the computation costs in dealing requisition step.

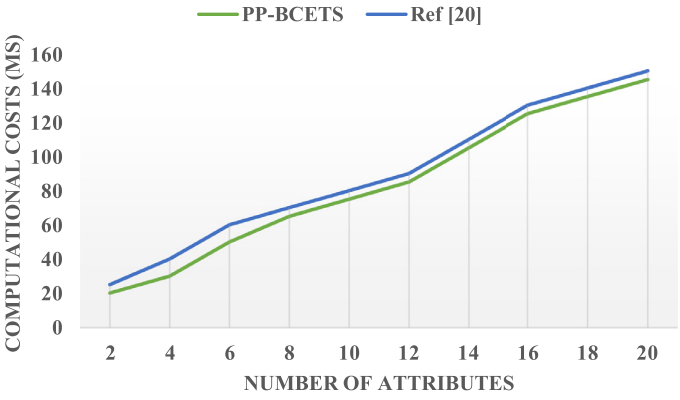

Fig. 4. Relation among the number of properties and the computation costs in dealing reply step.

within the network. According to the previous study, the next experiments are conducted to evaluate efficiency.

This paper provides a comparison of the computation costs in the dealing appeal and dealing response steps of BETPWP and ref (Li, Hu, Lal, Conti & Zhang, 2020), that incorporates BC technology and the Eat-CTP layout into the energy trading case study. Figs. 3 and 4 show the computation costs of dealing appeal and dealing response steps in BETPWP and ref (Li, Hu, Lal, Conti & Zhang, 2020) rise as the number of features increases. BETPWP has a lower overhead compared to ref (Li, Hu, Lal, Conti & Zhang, 2020) for the same number of features in the dealing appeal step. This is due to the fact that in BETPWP, just the TI executes the trade request step. In ref (Li, Hu, Lal, Conti & Zhang, 2020), both the initiator and the energy dealer (ED) execute it. As part of BETPWP, the TI executes available control encryption activities containing the variables needed for umpire and ciphertext update. In ref (Li, Hu, Lal, Conti & Zhang, 2020) the TI encrypts the dealing appeal data initially and transfers it to ED; afterward, ED executes the available control encryption activities. There is no clear benefit of the BETPWP in the trade response step, the computation costs remain less than in ref (Li, Hu, Lal, Conti & Zhang, 2020). The numerical study is presented here to support the results of the experiment.

G_E and G_H are used for representing the exponentiation's time cost, and hash processes in set G and G_{TE} for representing the exponentiation's time cost processes in set G_T. Z_H, P, C_{AES} show the time cost of hash processes in Z_p, pairing processes, decryption/encryption, respectively and n shows the number of features T_{EP}, T_{DP}, T_{EL} shows the overhead dealing appeal, the dealing reply in BETPWP, and T_{DL}shows the overhead dealing appeal, the dealing reply in ref (Li, Hu, Lal, Conti & Zhang, 2020); Thus:

$$T_{EP} = (1 + 4n)G_E + (2 + 2n)G_{TE} \quad (11)$$

$$T_{DP} = G_E + nG_{TE} + (2 + 2n)P \quad (12)$$

$$T_{EL} = (10 + 5n)G_E + G_{TE} + 4Z_H + G_H + 4C_{AES} \quad (13)$$

$$T_{DL} = 4G_E + (1 + n)G_{TE} + (1 + 2n)P + Z_H + 4C_{AES} \quad (14)$$

The average time cost of G_E, G_{TE}, G_H, Z_H, P, C_{AES} are [2.68, 0.21, 3.89, 0.018, 3.35, 0.04] *ms*.

This paper compares the communication overhead of BETPWP with ref (Li, Hu, Lal, Conti & Zhang, 2020) and ref (Aitzhan & Svetinovic, 2016). BC technology was presented in ref (Li, Hu, Lal, Conti & Zhang, 2020) as well as ref (Aitzhan & Svetinovic, 2016) to address privacy and security concerns involved in energy trading. According to the layout of ref (Aitzhan & Svetinovic, 2016), several technologies like elliptic curve signatures and multi-signatures were employed, but access control was not implemented, making comparisons between BETPWP and ref (Aitzhan & Svetinovic, 2016) difficult. Thus, the paper just compares the communication overhead of the 3 layouts.

As a result of the instability, the system transition velocity is adjusted to a constant amount. The communication overhead of BETPWP contains: the TI has broadcasted and the dealing demandant has interacted with the TI for obtaining the keyg^{d_0}. The communication overhead of ref (Li, Hu, Lal, Conti & Zhang, 2020) contains: EDs have broadcasted the generic keys, the energy bought has sent requisition to ED and ED broadcasts the encrypted requisition. The communication overhead of ref (Aitzhan & Svetinovic, 2016) contains: the energy marketer has interacted with distribution network

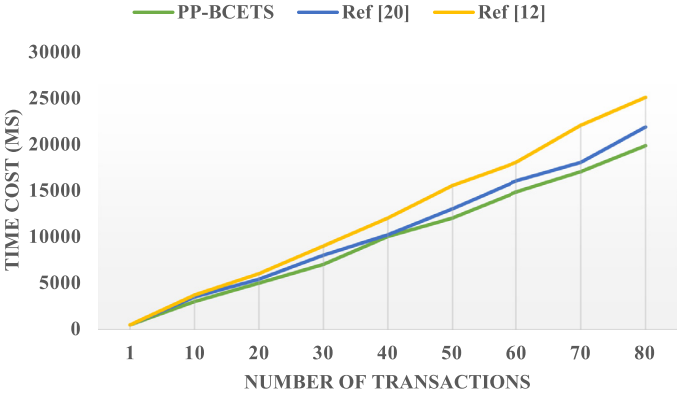

Fig. 5. Comparing communication overhead.

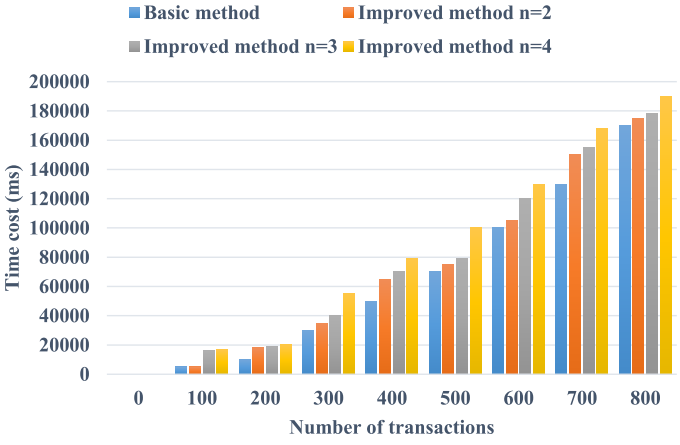

Fig. 6. Relation among the number of dealings and the total time cost of various layout.

Table 1
Test related data.

Notation	Average gas cost	Total transactions	Datapoint	Gas applied	Monthly capacity
Values	9.65921659 Gwei	434	46,044	1129,171,462	1483 MW

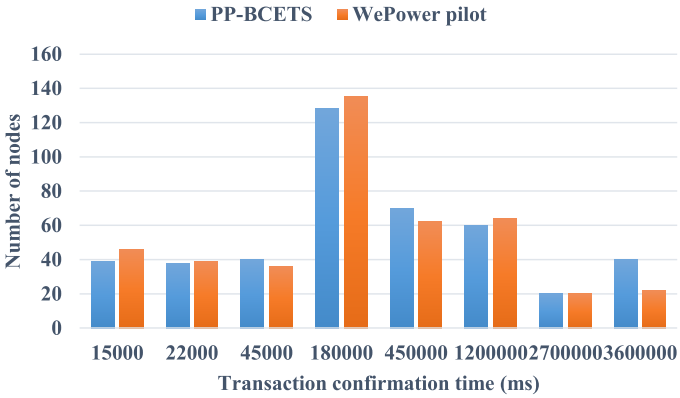

Fig. 7. Relation among the number of dealings and the dealing validation time.

operator (DNO), DNO has interacted with the energy buyer. Energy buyer has interacted with energy seller. Afterward, Energy buyer, seller and DNO have interacted for achieving multi-signature transaction. Fig. 5 shows that even though the layout of ref (Aitzhan & Svetinovic, 2016) does not use cycle teams and bilinear maps with somewhat longer terms, repetitious interplays, and multiple-signature procedures result in significant amounts of communication overhead.

b. Improved layout

Fig. 6 shows *n* as the number of validity reference inputs. Increasing transaction numbers, both the base layout and improved layout have similar time overheads. As n increases, the performance of the improved layout reduces a little, but the growth is not significant if transactions remain within a specific range. Therefore, the overhead of the complete assessment process of SOPSIS is little in the improved layout.

c. Simulation

In BETPWP, distributed energy dealings are implemented according to the BC, and enhanced Eat-CTP as the main scheme is used for privacy keeping and available control. According to the pilot trial of ref (Li, Hu, Lal, Conti & Zhang, 2020), a BC-enabled renewable energy trade scheme, the efficiency of the suggested BETPWP is evaluated. BC is used to save transaction data securely and immutably. The initial phase of the test uses Estonia's nationwide power generation and usage information. The main focus was on testing how to write the actual information into Ethereum's BC. There is too much electricity consumed by 700,000 Estonian households yearly, and Ethereum's major network's block time is too short. A few details regarding the trial are shown in Table 1.

Fig. 7 compares BETPWP and We Power pilots. According to the suggested process, the number of dealings with small verification times rises, whereas the number of dealings with wide verification times declines, indicating that BETPWP performs better compared to the algorithm in ref (Aitzhan & Svetinovic, 2016). The suggested tests show that PPBCETS can solve the privacy leak issue and maintain system performance while maintaining privacy.

Conclusion

In this paper, a newly approach based on the distributed BC has been developed for dealing scheme BETPWP using privacy conservation and available control is proposed in the present study. Eat-CTP was applied as the main algorithm for small available control using dealing umpire in ciphertext type, ensuring maximum privacy for users. A validity-enabled equity affirmation consensus procedure has been suggested for improving the performance of operations and implementing a lightweight distributed transaction layout. BETPWP was evaluated in detail for security and efficiency. It was found to be effective based on the findings of the experiments.

Declaration of Competing Interest

There is no conflict of interest to report for this submission.

References

Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840–852.

Appio, F. P., Lima, M., & Paroutis, S. (2019). Understanding smart cities: Innovation ecosystems, technological advancements, and societal challenges. *Technological Forecasting and Social Change*, *142*, 1–14.

Bagheri, M., Madani, M., Sahba, R., & Sahba, A. (2011). Real time object detection using a novel adaptive color thresholding method. In *Proceedings of the 2011 international ACM workshop on Ubiquitous meta user interfaces* (pp. 13–16).

Dabbaghjamanesh, M., Kavousi-Fard, A., & Mehraeen, S. (2018). Effective scheduling of reconfigurable microgrids with dynamic thermal line rating. *IEEE Transactions on Industrial Electronics*, *66*(2), 1552–1564.

Giaretta, E., & Chesini, G. (2021). The determinants of debt financing: The case of Fintech start-ups. *Journal of Innovation & Knowledge*, *6*(4), 268–279.

Guan, Z., Lu, X., Wang, N., Wu, J., Du, X., & Guizani, M. (2020). Towards secure and efficient energy trading in IIoT-enabled energy internet: A blockchain approach. *Future Generation Computer Systems*, *110*, 686–695.

Li, M., Hu, D., Lal, C., Conti, M., & Zhang, Z. (2020). Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *16*(10), 6564–6574.

Li, Z., Chen, S., & Zhou, B. (2020). Electric vehicle p2p electricity transaction model based on superconducting energy storage and consortium blockchain. *2020 IEEE international conference on Applied Superconductivity and Electromagnetic Devices (ASEMD) (pp. 1–2). IEEE.*

Liu, J. K., Yuen, T. H., Zhang, P., & Liang, K. (2018). Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list. International conference on applied cryptography and network security (pp. 516–534). Springer.

Liu, Z., & Fan, Y. (2019). Provably Secure Searchable Attribute-Based Authenticated Encryption Scheme. *International Journal of Network Security*, *21*(2), 177–190.

Kavousi-Fard, A., Nikkhah, S., Pourbehzadi, M., Dabbaghjamanesh, M., & Farughian, A. (2021). IoT-based data-driven fault allocation in microgrids using advanced μPMUs. *Ad Hoc Networks*, *119*, 102520.

Khattak, H. A., Tehreem, K., Almogren, A., Ameer, Z., Din, I. U., & Adnan, M. (2020). Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. *Journal of Information Security and Applications*, *55*, 102615.

Kim, S. Y., & Upneja, A. (2021). Majority voting ensemble with a decision trees for business failure prediction during economic downturns. *Journal of Innovation & Knowledge*, *6*(2), 112–123.

Mahapatra, B., & Nayyar, A. (2019). Home energy management system (HEMS): Concept, architecture, infrastructure, challenges and energy management schemes. *Energy Systems*, 1–27.

Popli, S., Jha, R. K., & Jain, S. (2018). A survey on energy efficient narrowband internet of things (NBIoT): Architecture, application and challenges. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 16739–16776.

Sahba, A., Sahba, R., & Lin, W. M. (2014). Improving IPC in simultaneous multi-threading (SMT) processors by capping IQ utilization according to dispatched memory instructions. *2014 World Automation Congress (WAC) (pp. 893–899). IEEE.*

Saura, J. R. (2021). Using data sciences in digital marketing: Framework, methods, and performance metrics. *Journal of Innovation & Knowledge*, *6*(2), 92–102.

Skare, M., & Soriano, D. R. (2021). How globalization is changing digital technology adoption: An international perspective. *Journal of Innovation & Knowledge*, *6*(4), 222–233.

Yang, W., Guan, Z., Wu, L., Du, X., & Guizani, M. (2020). Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach. *IEEE Internet of Things Journal*, *8*(10), 8632–8643.