

A Blockchain-Based Peer-to-Peer Trading Scheme Coupling Energy and Carbon Markets

WeiQi Hua
Department of Engineering
Durham University
Durham, U.K.
weiqi.hua@durham.ac.uk

Hongjian Sun
Department of Engineering
Durham University
Durham, U.K.
hongjian.sun@durham.ac.uk

Abstract—Climate change enforces the integration of distributed renewable energy sources and development of carbon price scheme. Whilst the energy is traded among distributed prosumers, the carbon responsibilities and corresponding allowances trading need to be transferred from large-scale energy suppliers to prosumers. During this transformation, the issues of energy imbalance, carbon reduction imbalance, and residential privacy leakage in centralised trading market present serious challenges. In this paper, we propose a fully decentralised blockchain-based peer-to-peer trading scheme coupling energy and carbon markets. We implement pay-to-public-key-hash with multiple signatures as a transaction standard to realise a more secure transaction and reduced storage burden of senders. A script is hashed during the wallet address generation for each new transaction to protect residential privacy. A novel carbon accounting method and corresponding incentive mechanism for carbon reduction are designed to evaluate emission behaviours of distributed prosumers. Case studies demonstrate that the proposed scheme leads a reduced costs and carbon emissions compared to centralised trading systems and existing blockchain-based trading schemes.

Index Terms—blockchain, decentralized energy trading, low carbon, distributed energy sources, smart grids.

NOMENCLATURE

α_n	Monetary compensation rate.
δ_k	Random number for generating I_2 .
π_g, π_u	Offer of energy seller g (or carbon seller u).
π_k, π_v	Bid of energy buyer k (or carbon buyer v).
A	Address of prosumers.
C_n	Carbon allowances of prosumer n .
e_i	CEF intensity of branch i .
e_k	CEF intensity of prosumer k 's consumption.
E_k, E_g	Intended energy demand (or supply) of energy buyer k (or seller g).
e_l	CEF intensity of loss in branch l .
$e_{n,s}$	CEF intensity from generation source s of prosumer n .
I_1, I_2	Encrypted key pairs.
M_n	Monetary compensation of prosumer n for selling carbon allowances.
$P_{i,j}$	Share of power flow in branch j from branch i .
P_k	Consumption of prosumer k .
P_l	Transmission loss of branch l .

$P_{n,s}$	Active power output from generation source s of prosumer n .
P_n	power generation of prosumer n .
R_j	CEF rate of branch j .
R_n	Net CEF rate of prosumer n .
$Rscript$	Redemption script.

I. INTRODUCTION

A. Motivation and Background

In the conventional energy sector, around 80% of power demand is supplied by centralized fossil fuel-based power plants including coal, gas, and oil [1]. Enormous carbon emissions are produced by high carbon intensity of combusting fossil fuels and additional energy losses during long-distance transmission, which leads to air pollution and irreversible effects of climate change. Facing these environmental issues, policy makers, on one hand, facilitate distributed renewable energy sources (DRESSs) to be integrated into distribution systems for carbon mitigation and transmission efficiency. On the other hand, they formulate carbon pricing scheme as a market-based climate policy to charge carbon producers for allowances, so as to phase out the power plants with extreme high carbon intensities [2].

To help the integration of DRESSs, 200 million smart meters will be invested in E.U. by 2020 [3], which facilitates increasing number of consumers to produce or store electricity at home through solar panels [4], electric vehicles [5], and batteries [6]. The role of prosumers is formed when consumers actively manage their own electricity generation and consumption [7] relying on smart meters and these technologies. Involving prosumers to the distribution networks contributes to sustainability and efficiency of electricity system as well as benefits of consumers. Nonetheless, in existing centralized wholesale markets, energy and carbon allowances are traded among large scale power plants with precisely estimated demand and centralised wholesale price. This unique wholesale price is not suitable for small and independent prosumers, because it would result in either energy imbalance caused by localized generation uncertainties or emissions reduction imbalance caused by various consumption patterns. Besides, central authorities require to access the trading and consumption information for management, which may draw concerns

for residential privacy leakage. Hence, decentralised market structures and tariffs need to be reformulated to securely support the involvement of prosumers.

B. Relevant Literature

With respect to carbon price scheme, emission trading scheme or cap-and-trade scheme are typical approaches to establish carbon markets in a majority of countries [8], which forces emission producers to buy emission allowances they estimate to emit. Although this policy successfully realises a coal-to-gas transition, several issues have been brought by an inappropriate centralised carbon price due to surplus or scarcity of carbon allowances, notably for the involvement of prosumers. If the centralised carbon price lies below the estimates of social cost of carbon in a specific region, it fails to involve more DRESs to replace fossil fuel-based generators; If the centralised carbon price is set too high, the business competitiveness of large scale prosumers will be harmed. To tackle the inappropriate centralised carbon price issue, previous centralised auction method was extended to consumer-centric adjustment through revaluating consumers' actual carbon intensity in [9], but the auction of carbon markets was still based on a central authority such as market operator. Therefore, there are still opportunities for reforming carbon emission trading to accommodate decentralised energy trading. A decentralised carbon market is therefore desired, under which the localized carbon price is more suitable for incentivizing carbon mitigation considering specific prosumption pattern.

Blockchain technology, as a peer-to-peer distributed ledger, has the potential to establish a decentralised emission trading scheme for coupling prosumers' energy trading and protect residential privacy. For energy trading, Di Silvestre *et al.* [10] proposed a permissioned blockchain applying in the microgrids, by which functions of validation and organisation were performed by distribution system operators. Analogously, Kang *et al.* [11] designed a blockchain based peer-to-peer energy trading among electric vehicles performed by local aggregators. Although the relatively decentralised agents were included, the leakage of residential privacy and tampering by these agents were still unavoidable. For carbon allowance trading, Khaqqi *et al.* [12] customised it to industries using reputation system based blockchain technologies for encouraging low carbon behaviours. Although it contributed to carbon reduction and low-carbon investment, the market competitive might be harmed due to the domination by participants with high reputation. Instead of focusing on a blockchain-based energy market or carbon market separately in existing studies, coupling both markets is a novel option to provide an efficient and reliable trading scheme since the carbon market is directly related to the operating cost of prosumers and has the same settlement period with energy market.

With the involvement of DRESs, the responsibility of carbon mitigation is transferred accordingly from previous fossil fuel-based power plants to distributed prosumers. Carbon accounting in prosumer level becomes necessary. The carbon emis-

sion flow (CEF) was introduced for consumers' side carbon accounting in [13], [14]. However, the new system structure affected by local peer-to-peer energy exchange amplifies carbon tracing complexity. Existing carbon accounting methods may degrade when distinguishing which portion of emissions is caused by prosumers' own power consumption and which portion of emissions is caused by selling surplus power.

C. Contributions and Organization

This paper approaches a novel peer-to-peer energy and carbon trading in energy sector and has contributions as:

- We propose a decentralised peer-to-peer energy and carbon trading scheme to accommodate the integration of DRESs. Compared with existing centralized wholesale market and relatively decentralised blockchain-based approaches, our proposed fully decentralised blockchain scheme can reflect the localized power imbalance and carbon emission caused by consumption patterns.
- We design a monetary incentive mechanism for carbon reduction to realise tax neutralizing without market interventions in bidding process.
- Current carbon accounting methods are extended to involve the role of prosumers in distribution network. A more fair allocation of responsibilities and incentives for carbon mitigation is proposed.
- Case studies demonstrate that a trading scheme with more secure transaction and residential privacy is established. The halved cost and CEF can be realised compared to conventional centralised trading system.

II. SYSTEM MODEL

This section describes the overall framework of peer-to-peer energy and carbon trading. The blockchain technique selection and carbon emission trading mechanism are discussed.

A. Peer-to-Peer Energy and Carbon Trading Framework

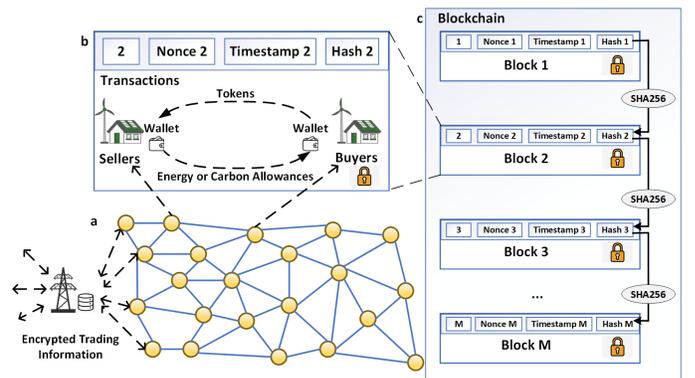


Fig. 1. Framework of blockchain-based peer-to-peer trading.

Fig. 1 presents framework of blockchain-based peer-to-peer energy and carbon trading. Prosumers directly interconnect with each other under peer-to-peer model to buy and sell services of energy and carbon allowances as shown in part a. Encrypted trading information including transactional data

of energy and carbon allowances, incentive information for carbon reduction, pseudonyms of prosumers' ID, consumption data, digital asset records, and timestamps of transactions are stored, shared, and audited by all nodes in blockchain to validate authenticity and accuracy. During each transaction as shown in part **b**, the ownership of tokens is changed after signing and broadcasting the encrypted trading information to the network. Transactions are structured in publicly available blocks and chronologically chained to each other through involving the hash of previous block into the current block, forming a blockchain as shown in part **c**. All blocks are protected by solving a proof-of-work via secure hash algorithm SHA256 [15]. The inputs of proof-of-work are block ID, nonce (number once), timestamp, and hash output of previous block, and the output of proof-of-work is fixed-length digest as unique identity. This unique identity is guaranteed by specially mined nonce, which means that if one block is changed, a different nonce results in an unverified block, and if all following blocks are changed, it will be extremely computationally difficult. Therefore, the chaining feature and difficulty of solving a proof-of-work enable transactions to be traceable, verifiable and tempering resistance. Additionally, token senders' private key is used to sign a transfer to an address generated by receivers' public key. The validation of this transaction is collectively voted by all nodes. This not only protects prosumers' residential privacy, but avoids the double spending attacks.

B. Blockchain Model Selection

1) *Transaction Standard*: In order to guarantee that all the nodes recognise the transactions, it is necessary to use specified script for standardizing the transaction information over blockchain. This specified script includes pay-to-public-key-hash (P2PKH), pay-to-public-key (P2PK), multiple signatures (MS), pay-to-script-hash (P2SH) [16]. During the process of transaction, token sender creates a script to specify the amount of transferred token (i.e. UTXO) and receiver's address. Meanwhile, receiver creates a script to specify its own signature. Subsequently, this transaction is broadcast to the overall network and the scripts of sender and receiver are matched by other nodes to verify the authenticity.

Under the transaction standard of P2PKH, the token sender's script is created by token receiver's public key as address (i.e. scriptPubKey) and the token receiver's script is created by its private key as identified signature (i.e. scriptSig). Unlike P2PKH, under the P2SH, the sender's scriptPubKey is substituted by receiver's redeem script which defines conditions under which a transaction is redeemed [16]. When receiver's hash matches the hash created by its redeem script and the signature belongs to receiver itself, the identity of receiver is verified. This enables the transaction to be more securely performed because token receiver cares more about where the token goes than sender. Without creating script, the storage burden of token sender also decreases. In addition, to protect the decentralised trading system from theft, other nodes within blockchain are involved as an arbitrator to sign a transaction

before it is validated. This process is defined as MS, in which minimum p signatures must match q provided public keys, before the token is spent. Compared with original MS using the whole script, P2SH uses Base58 to encode the script such that the complexity of original script is reduced. Therefore, in our proposed energy and carbon trading scheme, the P2SH is used as a transaction standard due to aforementioned advantages compared with other standards.

2) *Address Generation*: During the process of energy and carbon trading, a key-pair including private key and public key is important for authenticity of transaction. Private key is used to generate public key, before public key is used to generate public key hash (i.e. address) through SHA256. This generation process is irreversible, which means that with a given public key or address, the private key cannot be inferred. The process of generating address from private key can be expressed as following steps:

Step 1: A private key is randomly generated, before creating public key through secp256k1 of elliptic curve digital signature algorithm asymmetric cryptography [17].

Step 2: Under P2SH, instead of hashing the public key, a script hash is generated through hashing the redemption script using SHA256 and then RIPEMD160 [18].

Step 3: To guarantee the address is valid without any typographical error, a checksum is generated through truncating the result of double SHA256 to the first four bytes. Both version number and checksum are concatenated to the script hash through encoded by Base58. Therefore, an encrypted wallet address is generated.

C. Carbon Emission Trading Mechanism

1) *Carbon Emission Tracing for Prosumers*: In distribution systems, prosumers play as the role of both generators and consumers. An initiative carbon tracing method should be therefore designed to distinguish emissions caused by meeting prosumers' own demand, supplying other prosumers' demand, and demand being supplied by other prosumers. A virtual concept of CEF proposed by [14] is used to trace the carbon footprint. Compared to the original CEF which focuses on the overall power systems from generators to consumers, we extend this method to investigate the CEF caused by prosumers' behaviours. The CEF represents a concurrent virtual network flow with power flow, which is ejected from power outflow buses, and transmitted to power inflow buses through transmission networks. By abstracting network features of power systems, the carbon emission shares caused by transmission and consumption are evaluated.

Consider a peer-to-peer power networks with N prosumers, indexed by integer n . Each prosumer possesses a single or various generation sources, such as solar, and wind. For a prosumer with a single generation source, its CEF intensity is determined by emission factor of this source which is evaluated by life-cycle carbon assessment [19]. For a multi-source prosumer with S sources, indexed by integer s , the CEF intensity is determined by all the sources as

$$e_n = \frac{\sum_{s=1}^S (P_{n,s} \cdot e_{n,s})}{\sum_{s=1}^S P_{n,s}}, \quad (1)$$

where $P_{n,s}$ is active power output from s th generation source of n th prosumer, and $e_{n,s}$ is CEF intensity in a unit of tCO₂/MWh. When a prosumer generates power, it ejects power and corresponding CEF into branches. Analogously with power flow, the CEF is mixed in branches according to proportional sharing principle [20]. The branch receives CEF from outflow buses in a given proportion, and distributes this CEF to inflow buses in the same proportion, so that the share of outflow CEF in a branch, and the share of branch CEF in a inflow bus can be evaluated. Denote i and j as inflow and outflow branches of bus z , respectively. The CEF rate in j th branch can be expressed as the sum of CEF rates in inflow set of branches and bus-connected generation

$$R_j = \sum_{i \in z} (P_{i,j} e_i) + \sum_{n \in z} (P_n e_n), \quad (2)$$

where R_j is the CEF rate of j th branch in a unit of tCO₂/h, e_i is CEF intensity of i th branch, and $P_{i,j}$ is the share of power flow in j th branch from i th branch. According to proportional sharing principle, $\frac{P_{i,j}}{P_j} = \frac{P_i}{(\sum_{i \in z} P_i + \sum_{n \in z} P_n)}$. Hence

$$e_j = \frac{R_j}{P_j} = \frac{\sum_{i \in z} (P_i \cdot e_i) + \sum_{n \in z} (P_n \cdot e_n)}{\sum_{i \in z} P_i + \sum_{n \in z} P_n}. \quad (3)$$

Since the CEF of a branch loss is equivalent to a load on this branch, it has the same expression of inflow CEF of consumption. (3) can be also applied to the CEF intensity of branch loss e_l and consumption e_k for l th branch loss and k th prosumer's consumption, respectively. Therefore, the net CEF of prosumers is the difference between CEF caused by generation, consumption and transmission loss

$$R_n = P_n \cdot e_n - P_l \cdot e_l - P_k \cdot e_k, \quad (4)$$

where R_n is net CEF of prosumer n , and P_n , P_l and P_k are power generation, transmission loss, and consumption.

2) *Emission Reduction Incentive Mechanism*: In the reputation-based blockchain trading system [12], the emission reduction behaviour is quantified as priority value to categorize sellers' offers into different groups as buyers' access condition. Although this strategy can stimulate the carbon reduction, the priority value may harm the market discipline due to market intervention. Unlike this reputation-based trading system, our proposed incentive mechanism designs a monetary compensation strategy for carbon reduction to simplify the priority selection procedure during emission trading and guarantee the market discipline. This monetary compensation for each peer is generated by the decentralised trading system to distribute the received revenue from carbon allowances trading. If the CEF rate of prosumers is equal to the carbon allowances in a time slot, prosumers will not receive any compensation. By contrast, if the CEF rate of prosumers is less than the carbon allowances, prosumers will receive monetary compensation

from systems. Additionally, the monetary compensation at high CEF rate level is higher than that at lower CEF rate level. This relationship can be described as

$$M_n = \begin{cases} \alpha_n [(C_n)^2 - (R_n)^2], & C_n > R_n; \\ 0, & C_n = R_n, \end{cases} \quad (5)$$

where M_n is the received monetary compensation of prosumer, α_n is the monetary compensation rate, C_n is carbon allowances of prosumer, and R_n is the CEF rate of prosumer.

III. ENERGY AND CARBON MARKETS COUPLING THEORY

This section describes trading procedure for peer-to-peer energy and carbon markets. Different from trading mechanism in conventional markets which requires a central authority to match bids and offers and publish unique market clearing prices, the decentralized feature of blockchain is involved in the peer-to-peer trading. A prosumer is able to flexibly choose an offer. Moreover, compared to single energy trading, the coupled emission trading enables the incentive mechanism to be applied in the trading process for carbon mitigation in consumption side. Assume a peer-to-peer trading system for current transactions and let G, K, U, V to denote the size of energy sellers, energy buyers, carbon allowances sellers, and carbon allowances buyers, indexed by g, k, u, v , respectively, $g, k, u, v \in N$.

Step 1: Generate addresses of energy seller A_g , energy buyer A_k , carbon allowances seller A_u , and carbon allowances buyer A_v for each new transaction to provide an entry of trading.

Step 2: Energy buyer k announces intended energy demand E_k and its bid π_k as well as address A_k to blockchain network for verification of enough tokens. The overall demand of network is correspondingly increased by $\sum_{k=1}^K E_k$. The encrypted information key pairs for broadcasting are $I_{k,1} = \text{hash}\{Rscript_k \| E_k \| \pi_k \| \text{timestamp}\}$ and $I_{k,2} = \text{hash}\{I_{k,1} \| \delta_k\}$, where $I_{k,1}$ is a static key to verify the ownership of π_k tokens, $Rscript_k$ is a redemption script of buyer k , and δ_k is a random number for generating $I_{k,2}$.

Step 3: System servers perform power flow tracing, CEF tracing, and reduction incentive calculation. The required carbon allowances C_n and amount of monetary compensation M_n are quantified and transmitted to specific prosumer n .

Step 4: Carbon allowances buyer v announces required allowances C_v and their bids π_v to blockchain network. Encrypted information key pairs are $I_{v,1} = \text{hash}\{Rscript_k \| C_v \| \pi_v \| \text{timestamp}\}$ and $I_{v,2} = \text{hash}\{I_{v,1} \| \delta_v\}$.

Step 5: Energy and carbon allowances sellers announce intended supplies E_g and C_u , respectively, and corresponding offers π_g and π_u as well as addresses to blockchain network for verification through encrypted information key pairs: $I_{g,1} = \text{hash}\{Rscript_g \| E_g \| \pi_g \| \text{timestamp}\}$ (or $I_{u,1} = \text{hash}\{Rscript_u \| C_u \| \pi_u \| \text{timestamp}\}$) and $I_{g,2} = \text{hash}\{I_{g,1} \| \delta_g\}$ (or $I_{u,2} = \text{hash}\{I_{u,1} \| \delta_u\}$). $I_{k,2}$, $I_{v,2}$, $I_{g,2}$, and $I_{g,2}$ can be taken as locks and only be unlocked by senders and receivers' identities. Hence, either double spending of token or double spending of energy and carbon allowances is prevented.

Step 6: System servers update database of the offers π'_u and bids π'_v of carbon allowances by adding the monetary compensation to sellers' original offers and buyers' original bids as $\pi'_u = \pi_u + M_u$ and $\pi'_v = \pi_v - M_v$, before sorting them in sequence and publishing to the auction board.

Step 7: Buyers receive a list of filtered offers and corresponding addresses relevant to their queries by conditions: $E_g \geq E_k$ (or $C_u \geq C_v$), and select potential suppliers.

Step 8: Each of potential suppliers opens a transmission channel and feeds energy into peer-to-peer network, before generating multi-signature redemption scripts to note the amount and receivers. Receiving the redemption scripts, buyers hash them and specify purchasing tokens. These multi-signature transactions are broadcast to all nodes of networks for signing. If the signature script matches P2SH address, the transaction are validated by networks to transfer the ownership.

IV. CASE STUDIES

Case studies have been conducted to demonstrate the performance of the proposed trading scheme. Proposed scheme is applied in adjusted IEEE 14-bus test system which consists of 7 prosumers with DRESs including 4 solar, 2 wind, 1 biomass, and 4 vehicle-to-grid. The power generation and consumption of these DRESs is simulated from our previous research [21].

A. Evaluation of Decentralised Trading Scheme

TABLE I
MULTI-CRITERIA EVALUATION

	Cost [£]	Net CEF [kg]	Transmission Loss [kW]
Centralised	331.63	104.84	302.78
Decentralised	142.98	42.23	298.13

To compare the proposed fully decentralised peer-to-peer energy and carbon trading scheme with conventional centralised trading, a performance evaluation is performed to assess environmental, economic, and security benefits. The performance evaluation between centralised and decentralised trading is presented in TABLE I. The generating costs of each of sources are evaluated by multiplying the cost coefficients as [21] with power generation. The net CEF is evaluated according to (4). The transmission loss is obtained by performing power flow analysis. It can be seen that the decentralised trading system realises an improvement in all dimensions, notably for cost and carbon emissions reduction. Although in peer-to-peer trading system, the power flow is not optimized as conventional power systems, the transmission loss is still reduced because peers prefer to trade with neighbourhood considering transmission costs. Regarding the CEF tracing, according to (4), the negative net CEF means the CEF caused by generation is less than CEF caused by consumption and transmission. The initial carbon allowances are distributed according to carbon intensities of prosumers. When their prosumption behaviours cause positive net CEF, they will purchase for carbon allowances for next half hour.

The distributions of generation CEF (a), transmission CEF (b), consumption CEF (c), net CEF (d), carbon allowances (e), and compensation (f) for 11 prosumers in half-hour interval are presented in Fig. 2. Each column denotes the distribution of CEF and monetary compensation in peer-to-peer networks. The dark blue colour represents a lower value whereas the bright yellow colour represents a higher value. As shown in Fig. 2, the localized CEF caused by prosumption behaviours in blockchain network is reflected, such that a fair allocation of monetary compensation can be formulated.

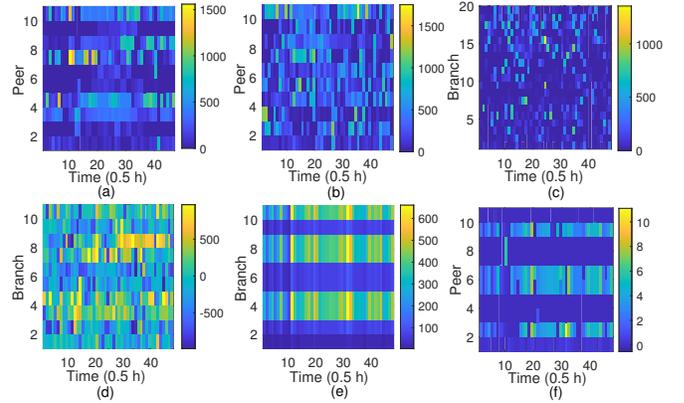


Fig. 2. The distributions of generation CEF (a), transmission CEF (b), consumption CEF (c), net CEF (d), carbon allowances (e), and compensation (f) for 11 prosumers. The x -axis denotes each half-hour settlement period and y -axis denotes the number of peers or branches.

With respect to security and residential privacy, the encrypted residential addresses guarantee that only the trading type and amount can be traced and reviewed by networks. The P2SH transaction standard with multi-signature can effectively prevent double spending of tokens, carbon allowances, and energy. Thus, a more secure trading platform compared to centralised trading system is established.

B. Peer-to-Peer Trading

The information of encrypted trading addresses, trading type, and trading amount is stored in data cell of each transaction. Available bids and offers involving proposed monetary incentive mechanism for the second settlement period are presented in TABLE II as an example. These bids and offers of each transaction are published in trading platform for participants' selection. Only those who produce positive net CEF are able to participant the carbon allowances trading because their prosumption behaviours are the direct source of carbon emissions. It can be seen that although carbon allowances seller 10 provides larger amount of allowance surplus than seller 7, it still has a lower offer price due to a higher monetary compensation. The trading and block generation procedures are shown in TABLE III. The first 2 blocks are selected as an example, in which the first block is a genesis block without trading information. The buyers match sellers based on the lowest price principle. For instance, carbon allowances buyer 10's options include 0.0302 £/kg

TABLE II
EXAMPLE OF AVAILABLE BIDS AND OFFERS FOR ONE SETTLEMENT PERIOD

Carbon Allowances Buyers			Carbon Allowances Sellers			Energy Buyers			Energy Sellers		
#	Amount [g]	Bid [£/kg]	#	Amount [g]	Offer [£/kg]	#	Amount [Wh]	Bid [£/kWh]	#	Amount [Wh]	Offer [£/kWh]
4	216	0.0308	7	173	0.0311	1	356	0.122	4	3617	0.108
11	16	0.0322	10	239	0.0302	2	16461	0.125	7	4432	0.133
						3	13272	0.123	8	48071	0.121
						5	14164	0.109	10	9449	0.126
						6	6687	0.123			
						9	4615	0.131			
						11	17508	0.110			

(purchase all 216 g from seller 10), 0.0309 £/kg (purchase 173 g from seller 7 and other 43 kg from seller 10). Hence, buyer 10 will choose the first option. Therefore, unlike the reputation based trading system, all the offers and bids are available for participants and the incentive is included without market intervention.

TABLE III
BLOCKCHAIN STRUCTURE FOR PEER-TO-PEER TRADING

Timestamp: t_1 ; Block index: 0; nonce: []
Data: Genesis Block
SelfHash: '075c27741a3506846368fa6e5b3477f85b31ceee71a5716e2'
Timestamp: t_2 ; Block index: 1; nonce: 224
Data: {Sender: '7b2891454769d57605dfceaa9967121'
Receiver: 'c9c940aec3ad22d7527863ecfc4cfc7c'
Type: 'Carbon Allowances'; Amount: 216 }
PreviousHash: '075c27741a3506846368fa6e5b3477f85b31ceee71a5716e2'
SelfHash: '00c8091e1a5055e933f8498c6095ad44'

V. CONCLUSION

To solve the inappropriate market cleaning price and carbon reduction imbalance caused by integration of DRESs, and guarantee trading platform security and residential privacy, a blockchain-based peer-to-peer trading scheme coupling energy and carbon markets is proposed. The underlying idea is using a proposed carbon accounting method to evaluate emission behaviours of prosumers and formulate an monetary compensation mechanism to incentivise carbon reduction, such that the localised energy and carbon emissions of DRESs can be involved through decentralised feature of blockchain networks. The decentralised trading scheme promotes more reductions of costs and carbon emissions than centralised systems. The P2SH with multi-signature prevents the double-spending attacks and guarantees residential privacy. In future work, the effects of proposed trading scheme on long-term investment of low carbon technologies should be investigated.

REFERENCES

- [1] B. M. Kefford, B. Ballinger, D. R. Schmeda-Lopez, C. Greig, and S. Smart, "The early retirement challenge for fossil fuel power plants in deep decarbonisation scenarios," *Energy Policy*, vol. 119, 2018.
- [2] Y. Sun, C. Kang, Q. Xia, Q. Chen, Z. Ning, and Y. Cheng, "Analysis of transmission expansion planning considering consumption-based carbon emission accounting," *Appl. Energy*, vol. 193, pp. 232–242, 2017.
- [3] B. P. Bhattarai, S. Paudyal, Y. Luo, M. Mohanpurkar, K. Cheung, R. Tonkoski, R. Hovsopian, K. S. Myers, R. Zhang, P. Zhao, M. Manic, S. Zhang, and X. Zhang, "Big data analytics in smart grids: state-of-the-art, challenges, opportunities, and future directions," *IET Smart Grid*, vol. 2, pp. 141–154(13), June 2019.
- [4] P. Shrivastava, M. S. Alam, and M. S. J. Asghar, "Design and techno-economic analysis of plug-in electric vehicle-integrated solar pv charging system for india," *IET Smart Grid*, vol. 2, June 2019.
- [5] H. Humfrey, H. Sun, and J. Jiang, "Dynamic charging of electric vehicles integrating renewable energy: a multi-objective optimisation problem," *IET Smart Grid*, vol. 2, pp. 250–259(9), June 2019.
- [6] C. K. Sundarabalan, Y. Puttagunta, and V. Vignesh, "Fuel cell integrated unified power quality conditioner for voltage and current reparation in four-wire distribution grid," *IET Smart Grid*, vol. 2, March 2019.
- [7] Y. Parag and B. K. Sovacool, "Electricity market design for the prosumer era," *Nature Energy*, vol. 1, p. 16032, 2016.
- [8] G. Perino, "New eu ets phase 4 rules temporarily puncture waterbed," *Nat. Clim. Change*, vol. 8, no. 4, p. 262, 2018.
- [9] Ying, Kong, and Dong-shan, "A carbon-intensity based carbon allowance allocation scheme among enterprises in shenzhen," *Ecolo. Econ.*, 2016.
- [10] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, and G. Zizzo, "A technical approach to the energy blockchain in microgrids," *IEEE Trans. Ind. Inform.*, vol. 14, no. 11, pp. 4792–4803, Nov 2018.
- [11] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Inform.*, vol. 13, no. 6, pp. 3154–3164, Dec 2017.
- [12] 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*, vol. 209, pp. 8–19, 2018.
- [13] W. Hua, D. Li, H. Sun, and P. Matthews, "Stackelberg game-theoretic model for low carbon energy market scheduling," *IET Smart Grid*, 2019.
- [14] C. Kang, T. Zhou, Q. Chen, J. Wang, Y. Sun, Q. Xia, and H. Yan, "Carbon emission flow from generation to demand: A network-based model," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2386–2394, 2017.
- [15] N. Saxena and S. Grijalva, "Efficient signature scheme for delivering authentic control commands in the smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4323–4334, Sep. 2018.
- [16] C. Prybila, S. Schulte, C. Hochreiner, and I. Weber, "Runtime verification for business processes utilizing the bitcoin blockchain," *Future Generation Computer Systems*, 2017.
- [17] W. Pan, F. Zheng, Y. Zhao, W. Zhu, and J. Jing, "An efficient elliptic curve cryptography signature server with gpu acceleration," *IEEE Trans. Inf. Foren. Sec.*, vol. 12, no. 1, pp. 111–122, Jan 2017.
- [18] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 46–56, 2018.
- [19] N. Arena, J. Lee, and R. Clift, "Life cycle assessment of activated carbon production from coconut shells," *J. clean. prod.*, vol. 125, 2016.
- [20] T. Ding, R. Bo, Z. Bie, and X. Wang, "Optimal selection of phase shifting transformer adjustment in optimal power flow," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2464–2465, May 2017.
- [21] W. Hua, H. Sun, H. Xiao, and W. Pei, "Stackelberg game-theoretic strategies for virtual power plant and associated market scheduling under smart grid communication environment," in *2018 IEEE Smart-GridComm*, Oct 2018, pp. 1–6.