E^{2}C-Chain: A Two-stage Incentive Education Employment and Skill Certification Blockchain

Liyuan Liu†, Meng Han*,†, Yiyun Zhou†, Reza M. Parizi‡
†Data-driven Intelligence Research (DIR) Laboratory, Kennesaw State University
‡College of Computing and Software Engineering, Kennesaw State University
*Corresponding. menghan@kennesaw.edu, †{lliyuan,yzhou20}@students.kennesaw.edu, ‡rparizi1@kennesaw.edu

***Abstract*—Employment and workforce industry become more important because the human capital value is linked to the company's profitability. Company becomes employee-centric in the 21st century. To hire an appropriate employee, and reduce hiring liability workplace violence, background screening marketing growth quickly. However, in the human resource industry, background check still is a pain point, especially for employment, education, and skill verification. The traditional background check is prolonged and inaccurate. For overseas recruitment, background check will be more troublesome. This paper comprehensively addresses the above issues by proposing an innovation E^{2}C-Chain, a two-stage blockchain-based education, employment and skill certification system. In the first stage, the new blocks are created when a trust organization verifies the education and employment information of the employee. In the second stage, to encourage the verifiers to participate in the skill verification process, we employ a Vickrey-Clarke-Groves (VCG) game based incentive mechanism to find the Nash Equilibrium and ensure social cost minimization. We also present the theoretical proofs and extensive simulations to demonstrate beneficial properties and efficiency of our proposed system.**

***Index Terms*—Blockchain, education certification, employment certification, skill certification, Vickrey-Clarke-Groves (VCG) mechanism.**

I. Introduction

Businesses meet a significant hurdle in recruitment when they need to verify candidates' credentials, such as employment, education, and skills. They keep spending a lot of money on the employee's background check to the third parties. Regarding the ResearchAndMarkets's report, the employment screening services market is supposed to increase from \$3.74 billion to \$5.46 billion by 2025 [1]. Even though the employment screening market boosting recently, there still exist fraud and opacity in employee credentials. According to the survey of HireRight, 88% employers misrepresentation their credentials on the resume [2]. The duplicity resume will result in altered recruitment. With the report from CareerBuilder [3], there is 75% of employers affirmed that they had recruited inappropriate employees, the average cost of one unseemly hiring is around \$17,000. The mistake of hiring is a cost not only the monetary loss of employers but also lost the time and human resource to re-hire and re-training a new candidate, and neutralizing the employees' morale.

Education, employment, criminal, and credit score *et al.* information of candidates are the primary aspects that employers are considered. Figure 1 shows the percentage of

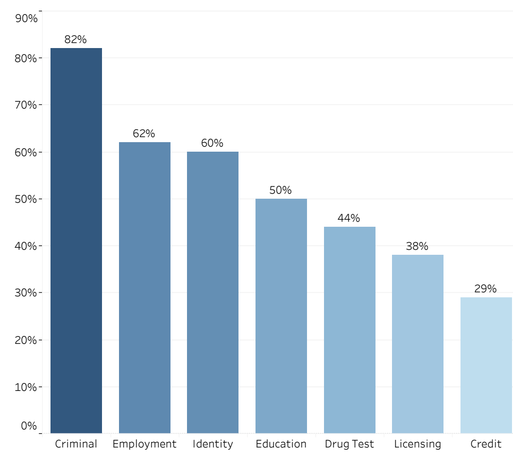

Figure 1. Percentage of Different Background Check Credentials

these features in background screening, the data collected from CareerBuilder's report released in 2016 [3]. The top 5 check credentials are criminal, employment, identity, education, and drug usage. Among these, criminal and identity have the national databases that employers can retrieve the truthful information. Drug usage report usually issued by clinical organizations which also ensure authenticity. Moreover, with the credit bureaus reports, the credit information also is easy to reach out. However, how to guarantee the authenticity of education and employment information is the most significant challenge to employers. Also, because the third party background screening is time-consuming, the waiting period is another potential reason that results in employers lost great talents. Besides, skill verification is another unproven part of resume. Employers are hard to confirm the skills which employees claimed they have. Blockchain, as a distributed, digitized, secure, open record of all cryptographic data exchange technology start to change the world in many fields [4]. Since use blockchain, participates can verify the transactions without a central certifying authorization. It has implied for many industries which rely on the record, store and track transactions secure, accurate, and unmodifiable. It can changed supply chain [5], healthcare [6], Internet of Things [7], agriculture [8] *et al.* Similar, in the business recruitment, the truthful of candidates' education, employment, and skills information are

978-1-7281-4693-5/19/\$31.00 ©2019 IEEE
DOI 10.1109/Blockchain.2019.00027

very important, the information asymmetry between employee and employer will cause not only a financial problem but also time cost, social trust, and other problems. Therefore, this motivated us to propose the blockchain based education employment and skill certification framework: E^{2}C-Chain.

The general idea of E^{2}C-Chain is to use blockchain technology to record features of professional accomplishment, expert skills or education and employment certification on the distributed ledger.

However, we confront several challenges.

- To our best knowledge, the blockchain based education employment and skill verification still be an open question from now.
- In the second stage, how to encourage the participants to verify others' skill is another question. The cost of each participant for completing a skill verify is private. It is challenging to encourage all verifier to describe their real costs.
- It is hard to choose the optimal set of participants that minimize the cost of requesters. The incentive mechanism needs to be established in the peer-to-peer verify process

Therefore, to overcome the challenges, we proposed a two-stage blockchain system. In the first stage, we focus on introducing a framework that can store employees' education and employment experience permanently. When the universities, enterprises issue the proof to employees' employment and education record, a new transaction is created. In the second stage, the Vickrey-Clarke-Groves (VCG) is implemented to encourage the participants to verify the requesters' proposed expert skills. With the mechanism, we prove that our proposed mechanism is individually rational and truthfulness and computation efficiency. The details of the two-stage E^{2}C-Chain are displayed in Figure 2. Our contributions are concluded below:

- E^{2}C-Chain provides a trusted source of employees' information that is not modifiable and permanently. It offers more immutable, fair, trust, and direct pathway between employers and employees.
- We implement a Vickrey-Clarke-Groves (VCG) game to find the equilibrium that verifiers in the second stage can bid their reward price and reach the social cost minimization.
- Our E^{2}C-Chain is a secure and incentive chain that protects all nodes' private information. With zero knowledge proof(ZK-SNARK), the task can be complete without disclosing any information beyond the validity of the statement itself.

The rest of this paper is organized as follows. Section II introduces the related works of different technologies. The architecture and overview of the E^{2}C-Chain are presented in Section III. Section IV formulates the incentive mechanism and provides theoretical investigation. Section V displays experimental results of the two-stage E^{2}C-Chain. Lastly, Section VIconcludes the study.

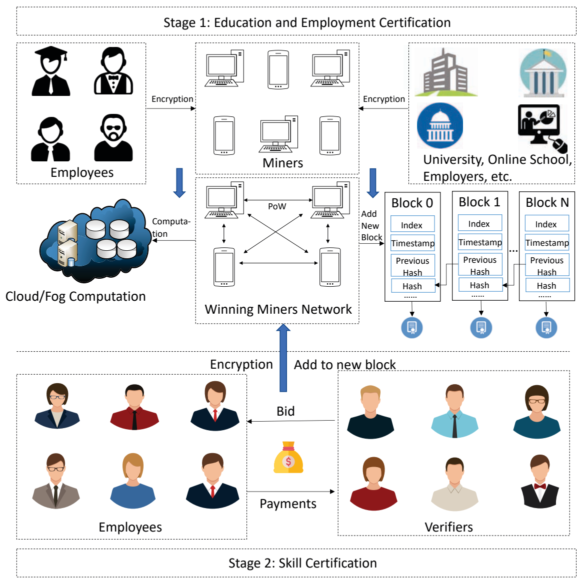

Figure 2. Architecture of E^{2}C-Chain

II. Related Work

A. Education Employment and Skill Blockchain

There are three main contents in each blockchain: the previous block hash, the transaction data, and the timestamp. Blockchain is an append-only transaction ledger. The function of every ledger is to store and write new information in it.

Recently, there are many researchers focus on blockchain. There are several different domains, such as Internet of Things(IoT) [9], [10], cyber-physical systems [11], education [4], supply chain management [12], and crowdsourcing and crowdsensing [13], *etc*. It is evident that the characteristics of blockchain, such as non-modifiable, anonymity, security, can revolute employment market fairer, more efficiency, and universal. However, there are not abundant research focus on human research industry.

The most famous application of blockchain is Bitcoin. Nakamoto [14] proposed a peer to peer electronic cash system-Bitcoin on 2008. In their system, the network timestamps transaction will be hashed by SHA-256 based on PoW, and then the miners will solve the mathematically hash to get a reward.

Regarding recent research, most education, employment, and skill certification based blockchain research are in the initial step. This problem still is an open question from now. Turkanovic *et al.* [15] proposed a framework called "EduCTX" which is a novel blockchain-based higher education credit platform. They also performed the implementation of the model using the Ark Blockchain Platform. Grather *et al.* [16] also presented a blockchain-based education platform to issue the education certificates for students. They defined their system overview in their paper, and illustrate the implementation details includes certification authorities management and smart contract. Chen [17] introduced his blockchain based system and named “Echo”. He illustrated that using Echo, the employment information such as skill, and career can be verified. Pinna *et al.* [18] proposed a system using blockchain to protect temporary employment’ right. In their system, the employees will get fair and legal payout regarding their work performance. And this system also can help employers automatically manage the contracts through smart contract. However, most of them are not illustrate how to encourage peer-to-peer verification in their system.

B. VCG and Blockchain

Vickrey-Clarke-Groves (VCG) mechanism is a mechanism that is truthful and enables to assist in accomplishing a social welfare maximization solution. Several studies employ VCG in a blockchain environment. Most of them are focus on the computation resource allocation between miners and edge service providers. Jiao *et al.* [19] deployed an auction game between edge computing service provider and the miner who need the computation resources. With their auction mechanism, it can optimize the social welfare; at the same time, it can guarantee the individual rational, truthfulness, and computation efficiency of authors proposed method. Gu *et al.* [20] implemented a VCG auction mechanism to solve the storage transactions problem. They perform their model using the Ethereum platform, and the experimental results showed their method could construct a safe, efficient, and economic resource trading.

At the time we write this paper, to our best knowledge, there are a few blockchain incentive mechanisms use VCG to reward the verifiers. VCG is frequently used in edge computing, wireless networks, crowdsourcing, and crowdsensing domains *etc*. Li *et al.* [21] formulate the offloading games for the mobile edge computing environment. With the optimal incentive scheme, when the users’ experience, the process of decision making will reach the equilibrium that social welfare will be maximization incorporate with VCG. Li *et al.* [22] employed VCG in their research in the mobile crowdsensing field. They proposed the algorithms theoretically to help the platform more efficient and beneficial to seek the participates. Zhou *et al.* [23] proposed a new framework in the crowdsensing area. They used VCG to reward the participators, implemented the edge computing to reduce the high computation traffic and burden, suggested incorporate with deep learning algorithms, such as Convolutional Neural Networks(CNN) to filter the fake and unrelative information which selfish participates offered. With the case study, their framework can reach high robustness.

C. Privacy-Preserving in Blockchain

Since most blockchains are stored sensitive, valuable records, how to make a secure blockchain system will be one crucial research area. There are many researchers focus on designed privacy-preserving algorithms to protect the transaction data. Kosba *et al.* [24] introduced a novel method called “Hawk”, which is a smart contract system that decentralized, the transactions data will not be stored in the appearance on the blockchain, it will create a private smart contract and use RSA to make sure the data is cryptography and security. Lu *et al.* [25] presented a novel privacy-preserving network named “CreditCoin” in the IoT environment. With their blockchain-based incentive mechanism, the announcement network will be efficient anonymous the vehicular’s announcement protocol. Yue *et al.* [26] developed a novel APP named Healthcare Data Gateway that enables to store, control and share the patient data since the patients’ data are sensitive, they provided a new method to protect the data private. Recently, the zero-knowledge proof is modern cryptography in blockchain. For example, Lu *et al.* [27] proposed a private and anonymous decentralized crowdsourcing system named ZebraLancer. This system is atop an open blockchain that can prevent data breach.

III. Architecture of E^2C-Chain

There are six main components in E^2C-Chain.

- Nodes: Users in the E^2C-Chain.
- Transaction: A certification request is broadcast to the network and collected into the blocks.
- Block: Blocks are files where the employment, education and skill certification recorded permanently in the E^2C-Chain network.
- Chain: A list of certification blocks in a particular order.
- Miners: The particular nodes which solve the hashed puzzles, and help to affirm a new block and add to blockchain.
- Consensus: A set of mechanisms and systems to make sure blockchain works. We implement Proof of Work (PoW) in this study.

In the first stage, as Figure 2 shows, employees input their education and employment information, the system rewards several E^2C-coins to the employees regarding their completion of the information. Also, the system will give each user an effective weight score to represent his or her weight when they participate in the skill verification in the second stage. Some trust organizations, such as universities, online schools, employers issue proofs of employees about their employment and education information can also get the E^2C-coins reward. The system enables to require the trust organizations make the official email and documents confirmation when they sign up to make sure the trust organizations are guaranteed. Then a new transaction is created. The transaction will generate a hash with SHA-256 algorithm. The creator of the new block will be the first miner that solved the hash function. In the verification process, ZK-SNARK is employed to protect sensitive data. The trust record will be stored to the new block without revealing that information, and without any interaction between the prover and verifier.

After the education and employment certification stored in the blockchain, it will be unmodifiable, permanently and trustful.

In the second stage, an auction is employed using VCG algorithm. The description of the incentive mechanism process can be implemented as follow:

Algorithm 1 First Stage Transaction Verification

Input: Transactions

Output: New Certification Block ID

```
Verify Transaction: R_Employment, R_Education
Verify PK_p
if PK_P is match then
    Reject Transaction
else
    Transaction Verified
    New cBlock ID ← f(ID_u, ID_b)
end if
```

- When the users upload their personal information to the system, the system assigns an amount of E^2C-coins regarding their profile completeness.
- The employees decide several skills need to be verified and then publish the price of each skill they willing to pay to the verifiers. As same as the first stage, ZK-SNARK will be implemented to protect data privacy.
- Every skill s has its price p decide by the requester. Based on the VCG model, a set of winners will be selected and the payment will be decided. Each verifier has a sufficient weight represents their weight. When the sum of all winners' weight reach a qualifying score, the skill verification process complete, and the record can be stored to a new block. After each success verification, the weight of verifiers will be increase regarding their past performance.

In this study, ZK-SNARK is a technique to protect sensitive data. ZK-SNARK is a non-interactive zero-knowledge proof. With ZK-SNARK, the duplicated interaction is not required between requester and verifier; it enables to present sound-proof. Each user has a public key Pu_k, and a private key denotes to Pr_k. The Pu_k as a user's encrypted information, and no other party knows the user's identifications. The user could send a concatenation of the encrypted information Ω; the concatenation can be denoted as $\mathrm{CPr}_k(\Omega)$ and is sent to the miners. The miners can confirm if the user's input information is authentic by decrypting $\mathrm{CPr}_k(\Omega)$ with the user's public key. However, the users' are anonymous, and the miners cannot know any identity information of users [28]. Figure 3 shows the process of ZK-SNARK. The verifiers and the provers can easily verify and complete the verification process, protect the completeness of computation, and keep the sensitive employment and education records secure. More details of the auction formulation will be introduced in Section IV.

IV. Incentive Mechanism of Peer-to-peer Skill Verification

An incentive blockchain mechanism can attract participants to verify the skills of requesters, and to help requester achieve skill certification as soon as possible. Therefore, how to design the reward system to encourage participants will be an interesting problem. In this study, we employed a game theory algorithm VCG to encourage verifiers bid truthfully, rationally and computation efficiency. Table I illustrates the frequently used notations in this paper.

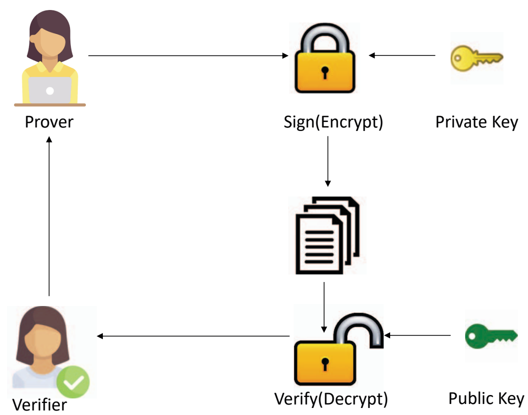

Figure 3. ZK-SNARK Process

Notations	Description
ξ	Employee who request skill verification
V_s, ν_i	Set of each skill verifiers and verifier
S, s_i	Set of skills and skill
D_s	Description for skill s_i
ω_i	Effective weight for verifier ν_i
β	The score allow create block of skills
U_i	Utility of verifier ν_i
W, W_s	Set of winners and winners of skill s_i
N_V, N_w	Number of verifiers and winners of s_i
b_i, b_{-i}	Bid of verifier ν_i Bids if ν_i is not attend
ζ_i	Cost of verifier ν_i
ρ_i	Payment of verifier ν_i for s_i
B_s	Budget of employee for each skill s_i
γ_s	The price verifier claimed to verify s_i

Table I
Notations and Description

We consider employee ξ has a set of S=$\{s_1, s_2, s_3, ..., s_i\}$ proposed skills, each skill need to be verified by a set of verifiers V=$\{\nu_1, \nu_2, \nu_3, ..., \nu_i\}$ while i=N_V. For each skill s_i, there exist a description of s_i such as "Programming C++", "Data Analytics" defined as s_i=$\{D_s\}$. When the employee or certification requester posts skills, the system will send the notifications for each verifier. The verifier has his effective weight score of ω_i, which represent the verify weight in the verification process. The effective weight score will decide by many factors such as the verifier's age, education level, job title, relationship with a requester, *etc.* A deep neural network can achieve a weighted score that when the users input their information, the platform enables to predict a reasonable weight score to each user. β is employed to decide if the skill verification is qualified to store in a new block. If s_i can be added in the blockchain will decide by:

$$\sum_{\nu_i \in W_s} \omega_i \geq \beta \tag{1}$$

When the verifiers received the tasks, the verifiers who willing to participate will prepare the bid price, $\forall\{\nu_i\} \in V_s$, the bid of ν_i denotes as b_i. Regarding VCG model, a set of winners W_s=$\{W_1, W_2, W_3, ..., W_j\}$ will be selected to finish the verification, the number of winners defined as $j = N_w$. The total payment cannot exceed the budget of requesters planned for each skill verification task; it can be defined as equation 2.

$$\sum_{\nu_i \in W_s} \rho_i \leq B_s, \tag{2}$$

The utility of verifier will be maximized in the auction process. The utility can be defined as:

$$U_i = \begin{cases} \rho_i - \zeta_i, & \text{if } \nu_i \in W_s \text{ for } s_i. \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

A. Desirable Properties

When we design the incentive mechanism to encourage verifiers to participate and finish the verification process, we describe three desirable properties as following:

- Truthfulness: It is truthful that in an auction mechanism every verifier ξ reports the true cost ζ_{true}. The verifier's utility U_i will not be improved when they report the cost is different from his true value, denotes as ζ_{false}.
- Individual Rationality: Each verifier will get a non-negative utility when he bid the true cost ζ_{true}, $U_i \geq 0$, $\forall i \in U$.
- Computational Efficiency: The incentive mechanism will be computationally efficient if the outcome can be computed in polynomial time.

According to the previous research [29]–[31], we get some definitions as following:

Definition 1: **Monotonicity** The verifier winner selection process is monotone. The winner selected with bid price γ_S^* and S^* will still win γ_s' and S' with any $\gamma_s^* \geq \gamma_s'$, $S^* \leq S'$.

Definition 2: **Critical payment** There has a critical payment ρ_{ci} for the winning verifier ν_i that claim his bid price γ_s individually. ν_i will win if $\gamma_s' \leq \rho_{ci}$, otherwise he will lose.

Theorem 1: An auction mechanism will be truthful if and only if it satisfies monotonicity and existing a critical payment.

B. Optimal Social Cost Solution

In our second stage, to encourage more and more verifiers to participate in the verification is crucial. In the meantime, it is essential that minimizing the social cost when the requester rewards the winning verifier. Our objective function that each skill s_i, the formulation can be defined as following:

$$\begin{aligned} &\min \sum_{\nu_i \in W_s} \zeta_i \\ &\text{s.t.} \sum_{\nu_i \in W_s} \omega_i \geq \beta \\ &\sum_{\nu_i \in W_s} \rho_i \leq B_s \\ &W_s \subseteq V_s \end{aligned} \tag{4}$$

It had been proven that VCG mechanisms are truthfulness and individual rationality [32]. According to the VCG algorithm, the each winner's payment ρ_i will be the difference between the total cost for the other when verifier i is not participating and the total cost for the others when verifier i joins. It can be defined as:

$$\rho_i = \sum_{\nu_j \neq \nu_i} \zeta_j(W_{-i}^*) - \sum_{\nu_j \neq \nu_i} \zeta_j(W_i^*) \tag{5}$$

The set of winning verifiers selection process and the price determination process of the skill verification also follow the VCG mechanism. Algorithm 2 shows the process of the winning verifiers' selection. For each skill, each verifier ν_i has similar cost ζ_i, sort ζ_i ascendingly, the set of the winner will be the verifiers with the smallest cost while the sum of all the costs less than requesters' total budget. The algorithm 3 shows the determination of verification price for each skill verification task. The price determination is following the VCG-based Mechanism. It will return a set of payment for each verifer of skill verificaton task s_i.

Algorithm 2 Set of Winning Verifiers Selection

Input: Verifier Set V_s, Cost ζ_i for verifiers, Budget B_s
Output: Winning Verifiers Set

```
1:  Initialization:
2:  k=argsort_{i∈V_s}(ζ_i)
3:  W=Ø, C=0
4:  for j in k do
5:      if C ≤ B_s then
6:          Append ν_{j+1} to W
7:          C=C+ζ_j
8:      end if
9:  end for
10: return W = [W_1, W_2, W_3, ..., W_n]
```

C. Proof of Designed properties

In this section, we present the proofs of designed properties which are truthfulness, individual rationality, and computation efficiency. We first present the proof of definition 1 and show that the winner selection process is monotonic.

Proof: Let ν_i denotes as one winner of the winning verifiers set when verifying the skill s_i; the cost is ζ_i. When the ν_i bidding as ζ_i^*, and $\zeta_i^* \leq \zeta_i$, regarding Algorithm 2 line 2-9, when sort all the verifier ν_i with their ζ_i, ν_i will be

Algorithm 3 Price Determination

Input: Winning Verifiers Set W, Cost ζ_i for verifiers, Verifier Set V_s
Output: Price Set P

1: m=$argsort_{\nu_i \in W}(\zeta_i)$
2: P=Ø
3: **for** j in m **do**
4: $\quad \rho_i = \zeta_{N_w+1}$
5: $\quad$ Append ρ_i to P
6: **end for**
7: **return** $P = [\rho_1, \rho_2, \rho_3, ..., \rho_n]$

selected in advance with bidding price ζ_i^*. ν_i will always win if his or her bidding with $\zeta_i^* \leq \zeta_i$ with skill task s_i. Therefore, the winner selection process is monotonic. ■

As we mentioned above, there existing a critical payment ρ_{ci} for the winning verifier ν_i that claim his bid price γ_s individually.

Proof: Suppose the critical payment ρ_{ci} for each verifier ν_i and skill task s_i is equal to the critical cost ζ_{ci}. If the verifier nu_i bidding with a cost $\zeta_i^* > zeta_{ci}$, regarding to Algorithm 3 line1 and line4, the payment $\zeta_i* > \zeta_j$ since all the cost will be sorted in the beginning. Therefore, in the sorted list, the index of verifier ν_i is behind ν_j. The verifier ν_i will not be the winner. ■

Theorem 2: Our proposed skill verification system is truthful.

Proof: Regarding theorem 1, our proposed mechanism will be truthful if and only if it satisfies monotonicity and existing a critical payment. We have proven for any s_i, the winner nu_i will always win if he or she bid with $\zeta_i^* \leq \zeta_i$. Also, we proven that there exist a critical payment ρ_{ci} for each verifier ν_i in definition 2. Therefore, theorem 2 can be proven. ■

Theorem 3: Our proposed skill verification system is individual rational.

Proof: For each verifier ν_i, there existing a critical cost ζ_{ci} which equal their payment ρ_i. A verifier's utility will be non-nagetive when ν_i is selected as a winner, there must have $\zeta_i \leq \zeta_{ci}$. Otherwise, the utility of verifier will be 0. Theorem 3 can be proven because the individual rationality is guaranteed. ■

Theorem 4: Our proposed skill verification system is computation efficiency.

Proof: The time complexity of Algorithm and algorithm are O(n) which indicates the implementation time complexity of our proposed skill verification mechanism is adequate. ■

V. Experiments Results

A. Incentive Mechanism

In order to evaluate the performance of the second stage incentive auction mechanism, we simulate random numbers of some variables and test it. The limited qualify score fixed as $\beta \in \{50, 60, 70\}$, The number of verifiers fixed as $N_V \in \{40, 60, 80, 100\}$. The cost of each verifier ζ_i is distributed over [1,50] uniformly and the effective weight ω_i is randomly chosen from [1,5].The verifiers' asking price γ_i is set from [1,30]. We first compare the social cost of different verifier numbers by β as Figure 4 shown. From

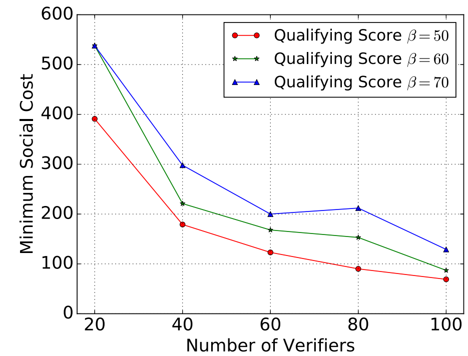

Figure 4. The Social Cost of Different Number of Verifiers

this figure, we observed that the social cost will decrease with the increase number of verifiers. The higher β value, higher social cost. Figure 5 shows the relationship between the number of winners and the β score by different numbers of the verifier. It shows when β value gets high and there doesn't have enough verifiers, all the verifiers can be the winner but the skill certification cannot be issued since the sum of winners' effective weight wouldn't reach the qualifying score β. We also test the utilities of winning verifiers using our

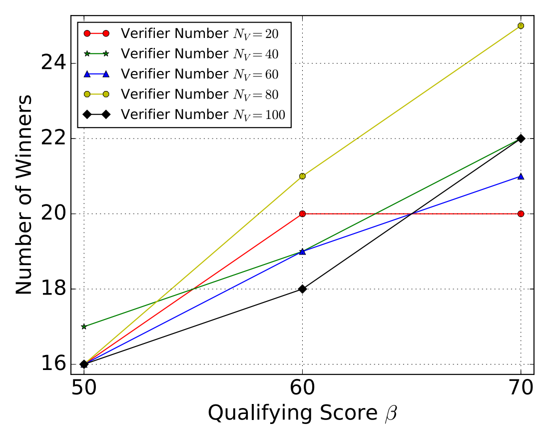

Figure 5. The Winners Number of Different Qualifying Score β

proposed VCG-based skill verification model. We randomly choose two winning verifiers defined as "Random Verifier 1" and "Random Verifier 2". The utility of random verifier 1 shows as Figure 6, the true cost of random verifier 1 is ζ_{rv_1}=5. If the verifier asks truthful price which is 5, he will get the optimal utility 5. However, if he overbids greater than 10, he will not be selected, and his utility is 0. The true cost of random verifier 2 ζ_{rv_2}=2. If the verifier asks price truthfully for 2, he will reach the optimal utility which is 7. If he overbids a value greater than 8, then he will not be selected, and his utility will drop to 0.

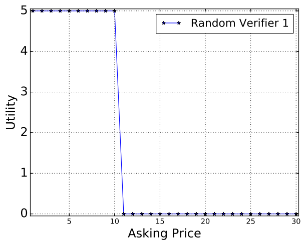

Figure 6. Utility of Random Verifier 1 with Different Asking Price

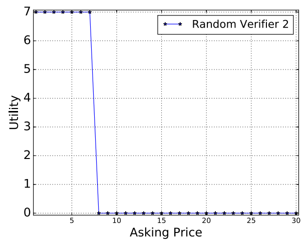

Figure 7. Utility of Random Verifier 2 with Different Asking Price

B. Implementation and Evaluation of E_2C-Chain

We initial implement the proof of concept our first stage verification E^2C-Chain. We simulate pairwise transactions with a local implementation of blockchain. The simulations are running on a MacOS of 1.6GHz Intel Core i5. We first initialized the wallets and then generated transactions. The transactions are included organization, employee, and information. We also use PoW in our blockchain. The difficulty of the SHA256 set as “2” which is easy. The miners allow to solve the function and earn the reward. We also create Flask API to maintain blockchain nodes. Figure 8 shows the API of E^2C-Chain with several example transactions.

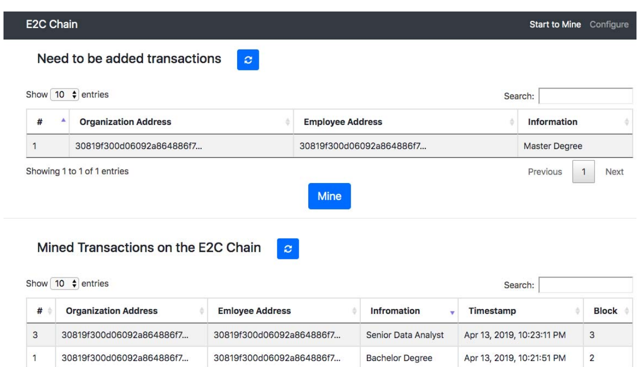

Figure 8. E^2C-Chain API Screen

Because the peer-to-peer architecture for our proposed E^2C-Chain, DoS attacks apt to less compared with traditional solutions. The system permission system if a node has inadequate behavior, he will be forbidden to access the network. This process also can handle Sybil attacks. Furthermore, data encryption will also protect sensitive individual information. We also show the simulate time assumption of from 1 to 500 transactions in Figure 9.

We also increase the difficulty of SHA256, the time of one transaction increase significantly as Figure 10 shown. Figure 11 shows the times of transaction encryption with 500 transactions. We test different hash function with 500 transactions and the running time are shown in Figure 12.

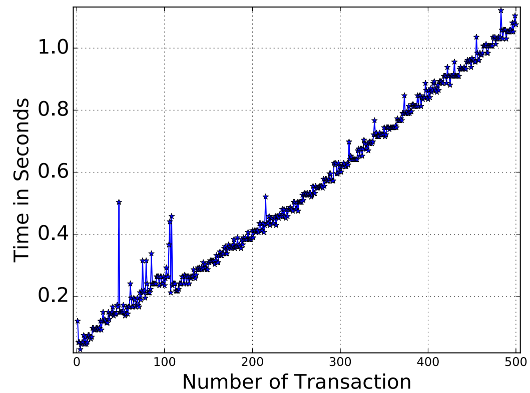

Figure 9. Time of Transaction with Easy Hash

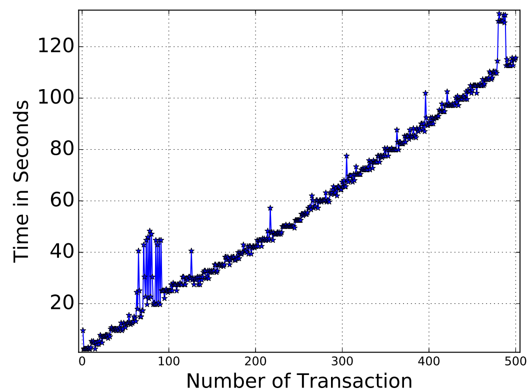

Figure 10. Time of Transaction with Hard Hash

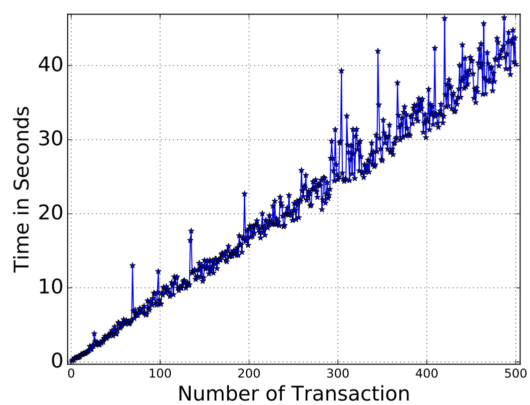

Figure 11. Time of Transaction Encryption

We compare SHA-256, SHA-384 and SHA-512 in this case. With the experiments results, SHA-512 costs least time and SHA-384 takes longer compare with others. The more details of implementation and evaluation will be discussed in future work.

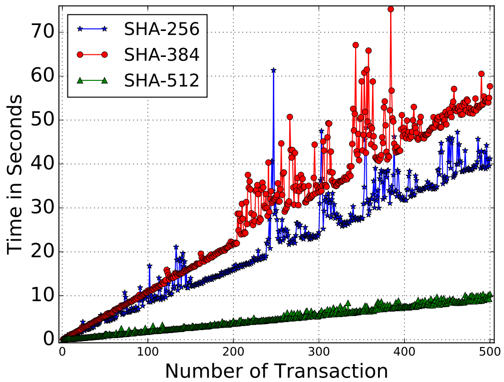

Figure 12. Time of Transaction with Different Hash Function

VI. Conclusion

In this study, we proposed a novel and incentive two-stage blockchain based employment, education, and skill certification framework; it provided a trusted source of employees' information that is not modifiable and permanently. It offers more immutable, fair, trust, and direct pathway between employers and employees. With the implementation of the Vickrey-Clarke-Groves (VCG) game, we found a Nash equilibrium that helps to select the set of winners and determine the price. With the incentive auction mechanism, it can reach the social cost minimization. It will help employer rapid and accurate to target the right candidate, and support employee moves forward to advanced career life.

References

[1] "Global analysis & forecasts by services & application - researchandmarkets.com," https://www.businesswire.com/news/home/20180202005232/en/5.46-Billion-Employment-Screening-Service-Market-2025.

[2] HireRight, "Hireright survey finds 88 percent of employers have found a misrepresentation on a resume," https://www.hireright.com/news/press-release, 2016.

[3] B. GOLDBERG, "75% of employers have hired the wrong person, here's how to prevent that," https://resources.careerbuilder.com/news-research/prevent-hiring-the-wrong-person, 2016.

[4] M. Han, Z. Li, J. S. He, D. Wu, Y. Xie, and A. Baba, "A novel blockchain-based education records verification solution," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*. International World Wide Web Conferences Steering Committee, 2018, pp. 178–183.

[5] E. Hofmann, U. M. Strewe, and N. Bosia, *Supply chain finance and blockchain technology: the case of reverse securitisation*. Springer, 2017.

[6] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2016, pp. 1–3.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[8] Y.-P. Lin, J. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, and Y.-F. Ho, "Blockchain: the evolutionary next step for ict e-agriculture," *Environments*, vol. 4, no. 3, p. 50, 2017.

[9] S. Zhu, W. Li, H. Li, L. Tian, G. Luo, and Z. Cai, "Coin hopping attack in blockchain-based iot," *IEEE Internet of Things Journal*, 2018.

[10] Y. Zhou, M. Han, L. Liu, Y. Wang, Y. Liang, and L. Tian, "Improving iot services in smart-home using blockchain smart contract," *IEEE Conference on Internet of Things*, 2018.

[11] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, 2018.

[12] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.

[13] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, and R. Deng, "Crowdbc: A blockchain-based decentralized framework for crowdsourcing," *IEEE Transactions on Parallel and Distributed Systems*, 2018.

[14] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[15] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "Eductx: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[16] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres, and F. Wendland, "Blockchain for education: lifelong learning passport," in *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.

[17] S. Chan, "Blockchain based professional networking and recruiting platform."

[18] A. Pinna and S. Ibba, "A blockchain-based decentralized system for proper handling of temporary employment contracts," in *Science and Information Conference*. Springer, 2018, pp. 1231–1243.

[19] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," in *2018 IEEE international conference on communications (ICC)*. IEEE, 2018, pp. 1–6.

[20] Y. Gu, D. Hou, and X. Wu, "A cloud storage resource transaction mechanism based on smart contract," in *Proceedings of the 8th International Conference on Communication and Network Security*. ACM, 2018, pp. 134–138.

[21] L. Li, T. Q. Quek, J. Ren, H. H. Yang, Z. Chen, and Y. Zhang, "An incentive-aware job offloading control framework for mobile edge computing," *arXiv preprint arXiv:1812.05743*, 2018.

[22] J. Li, Z. Cai, J. Wang, M. Han, and Y. Li, "Truthful incentive mechanisms for geographical position conflicting mobile crowdsensing systems," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 324–334, 2018.

[23] Z. Zhou, H. Liao, B. Gu, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, "Robust mobile crowd sensing: When deep learning meets edge computing," *IEEE Network*, vol. 32, no. 4, pp. 54–60, 2018.

[24] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[25] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[26] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[27] Y. Lu, Q. Tang, and G. Wang, "Zebralancer: Private and anonymous crowdsourcing system atop open blockchain," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018, pp. 853–865.

[28] 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 Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[29] J. Wang, J. Tang, D. Yang, E. Wang, and G. Xue, "Quality-aware and fine-grained incentive mechanisms for mobile crowdsensing," in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2016, pp. 354–363.

[30] J. Xu, Z. Rao, L. Xu, D. Yang, and T. Li, "Mobile crowd sensing via online communities: Incentive mechanisms for multiple cooperative tasks," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2017, pp. 171–179.

[31] Z. Duan, M. Yan, Z. Cai, X. Wang, M. Han, and Y. Li, "Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems," *Sensors*, vol. 16, no. 4, p. 481, 2016.

[32] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic game theory*. Cambridge university press, 2007.