IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 5, 2020, accepted May 21, 2020, date of publication May 26, 2020, date of current version June 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2997650

BEMPAS: A Decentralized Employee Performance Assessment System Based on Blockchain for Smart City Governance

EMMANUEL BOATENG SIFAH[1,2], HU XIA[1], CHRISTIAN NII AFLAH COBBLAH[1], QI XIA[2,5], (Member, IEEE), JIANBIN GAO[3], (Member, IEEE), AND XIAOJIANG DU[4], (Fellow, IEEE)

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]CETC Big Data Research Institute Company Ltd., Guiyang 550008, China
[3]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu 611731, China
[4]Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA
[5]Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Jianbin Gao (gaojb@uestc.edu.cn)

This work was partially supported by the Program of International Science and Technology Cooperation and Exchange of Sichuan Province (2017HH0028, 2018HH0102, 2019YFH0014, 2020YFH0030), and by the Science and Technology Program of Sichuan Province (2020YFSY0061). This work was also sponsored by CCF-Tencent Open Research Fund WeBank Special Funding.

ABSTRACT In recent years, the use of blockchain has gained attention in industrial interventions and research. Blockchain technologies can be particularly utilized in the domain of Smart Governance, which is a critical component of Smart Cities. Smart Governance aims to ensure smarter decision making, openness and collaborative participation of all entities involved as well as help minimize resource usage, reduce consumption and save cost. Smart Governance involves putting in place systems for monitoring and evaluating the performance of government workers. However, government workers lack trust in these systems because they are mostly centralized systems which are prone to single-point of failure problems and also data fed into these systems can be tampered with by the higher-ups or employers to favour individual workers. With these problems, there is a need for a decentralized system that can ensure trust, tamper-resistance, accountability, reliability, transparency and security. In this paper, we propose a decentralized employee evaluation system based on blockchain. We utilized a 3-chain model, namely; ID-Chain, Behavior Chain and Credit Chain fused to make a single unified chain. Our system also makes use of an automated game-based employee evaluation approach. Our system is based on Hyperledger Fabric as the blockchain platform and operating mechanism. Our Proof of Concept (PoC) results shows that in utilizing the Blockchain system, security concerns such as trust, privacy, accountability, among others, that are present in current employee performance evaluation systems are tackled and also in the adoption of the game-based automated system, our system can make an effective decision regarding employee performance. Our system achieves trust, transparency, security and accountability among government workers under a Smart City governing environment.

INDEX TERMS Smart city, blockchain, employee performance evaluation systems, digital identification, game theory.

I. INTRODUCTION

Since the digital age, governments have been looking for ways to enhance the quality of lives of their citizens by improving the technological infrastructures and seize the benefits that come with these technologies. The motive for technology modernization is to be able to simplify complex processes while allowing innovation. Governments now seek to comprehend how these new concepts and technologies like Smart City and Distributed Ledger Technologies (DLT) can play a part. The Fourth Industrial Revolution (Industry 4.0) has arrived, and governments recognize the necessity to

The associate editor coordinating the review of this manuscript and approving it for publication was Xiping Hu.

innovate to avoid disruptions. Governments now invest in an aggressive and different innovation strategy that focuses on change, revolution and results [1].

The concept of Smart City has been gaining attention recently due to its potential of creating a city whose system is sophisticated and able to sense and act independently [2]–[4]. A smart city should be able to embrace all the parties involved in political participation, functioning of local administration and services for its members (citizens). Authors in [2] define Smart City as a city that functions well in a six-dimensional domain: *smart people, smart economy, smart living, smart mobility, smart environment and smart governance*. The ultimate purpose of constructing a smart city is to enhance the quality of living of the general citizens by seizing the benefits from the existing modern technologies. Smart City research is a strand of a local electronic government research area. As a component of Smart City, smart governance aims at applying adequate fair and transparent policies, geared towards improving the lives of its citizens [3]. Its prime focus is to ensure a creative, innovative, economic growth, excellent quality of life and must be environmentally and socially secure and safe [3].

Moreover, the performance of government officers working in the Smart City environment needs to be evaluated in order to reward excellent performance or improve on poor performance. In a general view, the implementation of smart city projects is a transformation process that requires policies, accompanied by objectives, managed by active leadership management which uses advanced technologies for improving its efficiency. With the same idea, we narrow it down to an organizational scenario where the processes, as mentioned earlier, is implemented. As employees are the primary backbone of every organization, and a proper performance assessment can provide an accurate image of an employee status at any given time. The purpose of employee evaluation is not only to evaluate the lousy performance and enhance it but also to promote staff to work better. An adequately designed employee assessment system can contribute to organizational goals and improve the efficiency of employees. It serves as a measure for current and future improvements of an organization in other to meet their goals and objectives. It has been proved by many research works that an effective appraisal system is directly related to employee motivation and productivity [5], [6].

Despite the enormous technological developments, employee performance evaluation in most organizations remains manual. The manual employee assessment systems are incredibly prone to human prejudice since managers can assess employee performance [7]. Biases can occur because of human nature or if managers receive insufficient training to produce impartial feedback. The managers generally concentrate exclusively on the latest worker results, while lousy performance ignored in the early portion of the assessment period. Besides, it is hard for the promoted managers to rate those who were his workers once. Moreover, the performance

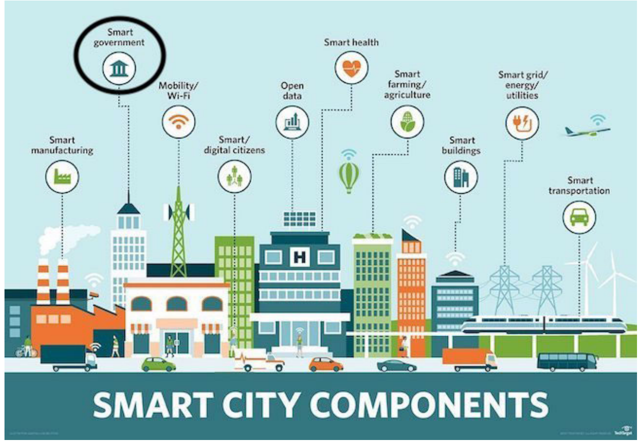


FIGURE 1. Smart city components (Source: Web).

evaluations have very little priority from the managers, as they are a time-consuming task [8].

All these variables lead to a biased performance assessment which results in discontent among those employees who receive biased feedback. Consequently, the integrity of the performance assessment scheme is wiped off intentionally or unintended. According to a study in [9], the present performance assessment scheme discovered that only 36 percent of staff were satisfied. Therefore, human biases must be eliminated during performance assessments, and one of the options is to move towards an automated performance assessment scheme. However, automated employee assessment schemes are still facing similar challenges of trust and accountability. Therefore, a technology that ensures confidence, transparency while at the end of performance assessments, offering the staff with a rewarding experience is needed. This is where blockchain comes in.

Blockchain, which originated from the cryptocurrency Bitcoin [10], is one of the most ground-breaking technologies of this era. It can store and share transparent, safe, controllable and unalterable information through distributed ledger technology (DLT). It is capable of making organizations decentralized, secure, accountable and transparent.

Thus, we propose a fully decentralized employee assessment system that is base on blockchain in order to ensure trust, transparency and accountability in a Smart City environment. Our investigations show that this is the first of its kind. In this paper, we denote ***Government Officers*** working in a Smart City as ***Employees*** and the ***Government Institution*** tasked with evaluating their performance as ***Organization***.

The contributions of this paper are enumerated below;

- Our proposed system makes use of a 3-chain model namely; ID-Chain, Behavior Chain and Credit Chain fused to make a single unified chain. ID-Chain is tasked with the creation, storing and authentication of digital IDs created for employees in the blockchain system. The ID-chain is directly linked to the Behavior Chain and the Credit chain which are responsible for assessment information and rewards or punishment informatio respectively

- We present a security analysis of the digital ID generation on the ID-chain.
- We utilized a game-based automated employee evaluation approach using assessment or evaluation data from employees to maximize organization profit.

This paper is structured into five sections. Section II will present the background on blockchain and the need of blockchain in employee assessment systems. In Section III, we present our proposed system with its core protocols and algorithms. In Section IV, we present the analysis and evaluation of our proposed system. Finally, the conclusion and future works will come under section V.

II. LITERATURE REVIEW

Bitcoin [10] was previously the only dominant blockchain technology application. However, this can now be applied in other areas with further technical growth. Major sectors include finance, insurance, health and medicine, the Internet of Things (IoT), education, copyright, smart grid, automobile and supply chain management [11]–[14]. Blockchain is a new and mostly open distributed block database ledger. It records all transaction data known as blocks. Each record or block has a timestamp and connected with the preceding block. It does not allow data alteration of any kind and is therefore trusted, verifiable and secure for transactions between any two entities.

Blockchain is a distributed ledger technology (DLT) that enables transactions to work in a decentralized manner, i.e. enables transactions to be checked without the need of any central organisation [15]. It makes use of cryptographic proofs of work, digital signatures, and peer-to-peer (P2P) networking to provide a distributed ledger containing transactions [15]. Once a block is added into the blockchain, it cannot be modified or removed for two reasons: first, a block change would cause the hash chain values to result in wrong verification, and secondly, a block change would require intense efforts to change each blockchain replicate that is supposed to be hosted at a wide variety of independent nodes. The nodes in blockchain are organized in a P2P network [16]. There are two keys in each node in a network; a public key to encrypt messages sent to a node, and a private key to decrypt and to read messages by a node. The public key encoding mechanism is therefore used to make a blockchain consistent and irreversible and non-reputable [17].

The process of verifying and adding new blocks in the blockchain depends on the mining process, which is based on the proof of work method. A difficult cryptographic puzzle has to be solved by miners and winners awarded. The key concept behind the difficulty of the cryptographic puzzle is to regulate the creation of fresh block procedure [16]. The transactions that are not recognized in case of a failure or invalidation are dropped. Eventually, every node verifies and adds a copy of confirmed transactions to their ledger. Conceptually blockchain operates by linking, chaining and saving data blocks of transactions in a chronological sequence.

Consequently, employee performance evaluation system is a popular tool used by many organizations to measure employee job performance, duties, employees and personnel development which eventually influences the growth of any organisation [18]. Every organization relies on the employee assessment method. This method consists of self-evaluation, employer evaluation and colleague evaluation. The precise and unbiased assessment will lead to corporate policies that evolve and fulfil the organization's strategic objectives.

Authors in [5] suggested the use of a Decision Support Systems with profile matching mechanisms to help identify the most prospective employees. Their system defines the weight value of individual attributes and proceeds with a classification process which selects the best alternative for the most potential employee. The outcome of an assessment of employee performance using 200 staff assessment information gained 93 percent precision levels whereby 193 information corresponded to the value gained from an assessment method.

Moreover, authors in [8] also proposed a game-theoretical strategy for an industry IoT based assessment of employee performance. The scheme provides helpful outcomes on employee performance through the mining of sensory node information from the MapReduce model. The data is then used to make automated choices for staff by making use of game theory. Their findings show that the suggested scheme effectively evaluates employee performance and demonstrates enhancement in employee efficiency compared to other methods. It also demonstrates that the right employee assessment system efficiently motivates staff to benefit the entire organization. However, it fails to solve the trust and transparency problems associated with employee assessment systems.

Similarly, authors in [18] developed a free form online evaluation system for organizations with a vast employee base and intricate processes for controlling the quality of tasks. Their scheme is versatile for the assessment of each workforce. Their results can be correctly evaluated according to the systematic database. Managers can improve productivity in the organization with the overall evaluation results combined with standard organizational criteria. However, their system does not solve the problem of managerial bias or the case of tampering of the recorded data.

Authors in [19] also proposed an employee performance assessment system based on a fuzzy logic approach which considers different performance assessment requirements. The principal objective of the suggested strategy is to determine the quality indicators in different qualitative and quantitative assessment requirements of staff taking into account their efficiency and then choosing the most outstanding employee with the lowest efficiency coefficient comparing all other indicators. Fuzzy control is used to ascertain the general index of performance by combining performance outcomes with chosen criteria and supplied with numerical

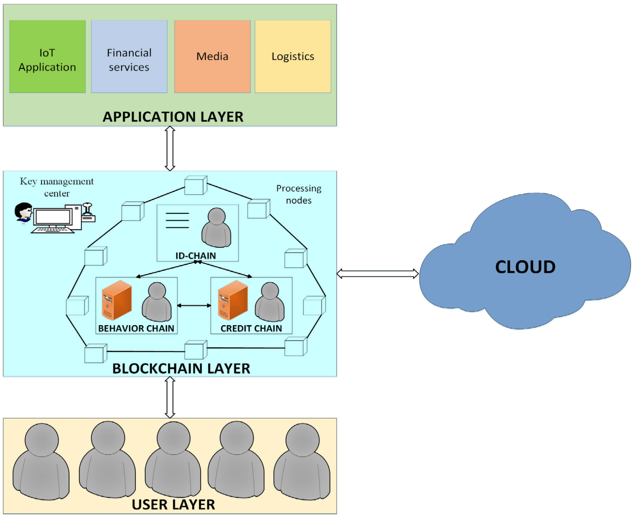


FIGURE 2. **Overview of proposed architecture.**

values that will certainly provide a comfortable performance rating calculation for the staff involved. The results of their proposed method show that it effectively measures employee performance. However, it fails to solve the trust and transparency issues that most employees have about the entire employee evaluation process.

III. PROPOSED SYSTEM

In this section of the paper, we give a detailed description of the components and algorithms used in our proposed blockchain-based employee assessment system, BEMPAS in the smart city environment. Our system is made up of three tiers, namely: the user tier, the blockchain tier, and the application tier.

The *figure 2* describes the architectural overview of our proposed system. The various components are described briefly below.

- **User Layer**: In this section of the paper, we give a detailed description of the This layer is made up of potential employees and existing employees who access the services provided by BEMPAS system. This layer links straight with the blockchain network and allows potential employees to enrol in the system. A potential employee registers with the necessary attributes of identification, and the data will be forwarded to blockchain nodes (i.e. ID Controllers) for verification and identification by ID providers. If the checking process is successful, then the employee is registered on the system.
- **The Blockchain Layer**: The blockchain network consists of various participants and specialized nodes that help to process, verify, create and manage employee digital identities, store employee assessment information and computes individual employee credit scores. This layer calculates the information sent to the network by identifying the characters with functionalities which help to monitor all activities carried out on the network. Blockchain technology is also known as distributed accounting. One of its core ideas is how to keep the data synchronized on each node, that is, to ensure that each node can reach a consensus on the data on the chain, which is the biggest difference between blockchain technology and other conventional database technologies. We used two specialized nodes, namely; ID controller nodes and Evaluation Processing nodes.
  1) ID controller Nodes: These specialized group of nodes are responsible for the creation and management of digital IDs on the blockchain. Major digital identity management operations include creating and storing a new digital identity and deactivating an existing identity.
  2) Evaluation Processing Nodes: These specialized set of nodes are also responsible for storing the digital formats of employee assessment information and computing the credit scores of employees using a predefined Game theoretical approach.

  We implemented a 3-Chain model; namely ID-chain, Behavior chain and Credit chain (these are later discussed in the next section). Hyperledger Fabric, which is a permissioned blockchain, is employed to provide secure access to employee and organizational data. However, permissionless blockchains can be utilized dependent on the application environment. Due to the inherent features of the blockchain, decentralization, transparency and security can be achieved.
- **Key Management Center**: It is a fully trusted entity on the blockchain network, and It realizes the essential functions of key generation, hash operation, signature verification, encryption and decryption. The key of user data encryption and decryption is stored on the key management centre, and this entity also configures the data encryption mode. Moreover, key management centres use a Hardware Security Module (HSM) to generate, store and handle key pairs. HSM is a dedicated encryption processor explicitly designed to protect the encryption key (i.e. manages, processes, and saves encryption keys safely in reliable and tamper-resistant devices). Each module has one or more secure cryptoprocessor chips to prevent tampering and bus probing. In order to ensure the security of data encryption and decryption, the key configuration is fully automated; no one has access to the key and the key provider. At the same time, the key management centre is entirely transparent for all entities on the blockchain. Also, a limit is set to the number of transactions the key management centre can handle in a given period. Moreover, mechanisms are put in place to choose another key management centre to serve as a backup on failure or malicious instances.
- **Cloud Platform**: Actual data are forwarded to the cloud for storage while all transactional logs are stored on the blockchain system. When the data is stored on the cloud platform, the corresponding tag attributes and corresponding pointers will be recorded on the blockchain.

In order to support the storage of massive and heterogeneous data, it is necessary to store the index, hash value and secret key of data on the data link, while the original data is stored on the cloud platform. By using blockchain technology to store data solidified, the data can be traceable, non-modifiable, and to ensure non-repudiation.

In uploading data to the cloud, employees first upload the original data to the system, then the system computes the hashes of the data to get a hash value, and through the secret key generation algorithm, get a unique data secret key, then encrypt the original file, and finally calculate an index. After completing these steps, the system stores the corresponding information on the chain and uploads the encrypted file embedded with the hash value to the cloud platform. Once the cloud service provider receives the transaction from the blockchain system, It checks its validity and also confirms that cloud space is available. If so, it computes the hash of data received and compares it to the hash value received. If both hashes match, data is stored in the cloud. This ensures that any data alterations are noticeable by everyone in the network.

Moreover, when requesting for actual data from our system, assuming that the requester has been authenticated, our system first obtains the encrypted data from the cloud platform through the index value stored on the chain. The secret key on the chain decrypts the encrypted data, verifies the hash value of the data, and finally returns it to the requester.

- **Application Layer**: This tier consists of the various applications that can be built on top of our proposed system. Applications such as the Internet of Things (IoT), financial services, healthcare, media, logistics, manufacturing, among others.

A. 3-CHAIN MODEL

The 3-Chain model is the core foundation of our proposed system. The data content and the development process of the 3-chain model is explained below. The *figure 3* describes the layered architecture of the 3-Chain model.

As stated earlier in this paper, we denote ***Government Officers*** working in a Smart City as ***Employees*** and the ***Government Institution*** tasked with evaluating their performance as ***Organization***.

1) ID-CHAIN

With the current issues regarding digital identity still unsolved, blockchain has been chosen as one of the solutions to solve this problem because of its decentralized nature [28]–[30]. ID-chain primarily involves the collection of government-issued IDs such as passport, national IDs, driving license, degree certificate, work card, driving license, real estate card information, as well as employee biometric information.

To create a digital ID that is used in the BEMPAS system, the users (i.e. employee) of the system needs to submit his/her details, government-issued ID or valid document as well as his/her biometric information to the blockchain system. Upon hiring, every employee's biometric data are collected, and a hashed copy is stored on the blockchain system using SHA-256. This guarantees that nobody can calculate a pre-image of the hash. We define that every employee after an appointment belongs to a particular department based on his skills and profession. The blockchain system verifies the information (government ID plus biometric data) submitted by the employees, and after successful verification, a digital ID is then created. Users are not granted access to organizational transactions and opportunities until their identities are activated after successful verification.

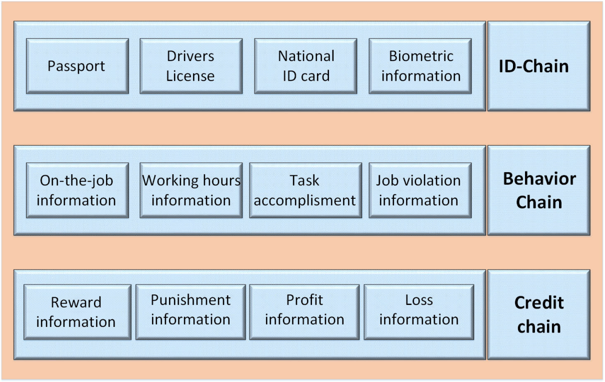


FIGURE 3. Simplified 3-Chain model.

We suggest the use of key-value pairs encrypted with a cryptographic key owned by the employee [31]. Encrypted hashes of employee private data attributes are aggregated and stored on the blockchain system. Digital identities can be described as key-value binding-entries. For instance, two entries such as ***key = passport number + hashed biometric data*** and the ***value = D123246 + sqw3123814***. Moreover, JSON-LD[3] is used to convey workings of the "keys" of digital identity. As a result, each employee will have a unique identifier in the blockchain system. Our scheme for digital ID creation is mostly based on the work done in [20]. In this work, we consider a process which incorporates four key participants denoted as:

- ***Employee***: An employee is the one whom a digital ID is created to uniquely identify him/herself and to interact with the blockchain system.
- ***Identity Provider***: Identity provider is a centralized entity which enables the user to build the blockchain system's digital identity. We suppose that the creator of the identity is trusted, i.e. it does not cooperate in the production of false digital IDs. As a government agency generally acts as an identity-maker, this is a reasonable hypothesis.
- ***Aggregated Biometrics***: These are the biometric information such as fingerprint, face and voice of employees that are stored on the blockchain system. This sensitive biometric information is encrypted and only applied when the ID Controllers has to check if the fingerprint of an employee matches the recorded one.

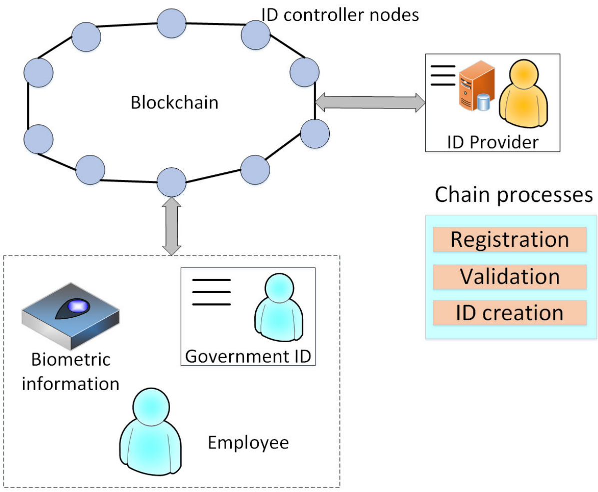


FIGURE 4. **Proposed ID-Chain component.**

- ***Identity Controllers***: Identity Controllers are a set of specialized nodes that operate together to share identity-related transactions on the blockchain scheme in connection with identification operations. These specialized group of nodes are responsible for the creation and management of digital IDs on the blockchain. Major digital identity management operations include adding a new digital identity and deactivating an existing identity. Both can also be combined to update an existing identity.
    1) Storing New Digital ID: The digital identity D_{id} will only take effect once it is incorporated into the blockchain system. However, after the D_{id} has been created, a consensus protocol will be initiated, and Id_{con} nodes will establish whether the D_{id} should be accepted or not.
    2) Deactivating an Existing ID: If an employee loses his/her private key, a transaction can be sent to the blockchain requesting that the corresponding (D_{id}) be revoked. One or more (Id_{con}) nodes have to endorse the deactivation transaction and decide whether to include it in the blockchain. Unless endorsed, an employee cannot send a deactivation transaction; otherwise, a denial-of-service (DOS) attack can be launched. Participants will not accept the signatures generated using sk after the cancellation transaction is included in the blockchain.

If Algorithm 1 succeeds, $D_{id} = h(k, v)$ is the employee's digital identity which is recognizable for other users in the blockchain system.

- ***Security Analysis of Digital ID Generation***: Our system guarantees that only one unique digital ID belonging to a real owner can be created for a user enrolled on our system [20], [31]. It does this by ensuring these features;
    1) Binding: Binding means that the digital identity used in this blockchain is linked with the user, identity issued by his/her government and biometric information. If the binding characteristic is not maintained, the digitally identified person who uses it may not reflect the correct information. Only legitimate users may authenticate themselves on the blockchain system using their biometric information (e.g. fingerprint, voice or face) to permit them to interact with the system
    2) Integrity: Since blockchain uses one-way hash functions to regulate data manipulation of any kind on the system, it protects the integrity of all data stored on; thus, a hashed identity cannot be altered in any way.
    3) Privacy: A pre-image of hashed digital identity cannot be revealed without the employee's consent.
    4) Non-repudiation: An employee cannot alter his/her digital identity or repudiate its ownership.
    5) Timestamp: it is easy to prove the specific time an identity was generated, modified or revoked (and thus, invalid), using the blockchain system.

Algorithm 1 Digital ID Generation

Require: Initialization of parameters:
Participants: An employee Emp with valid ID Id_v, Identity provider Id_{prov}, Aggregated Employee biometrics Emp_{bio}, ID Controllers Id_{con}, Digital ID D_{id}, Key Management Center K_c
System Processes:

```
Emp submits Id_v to Id_con
Id_con verifies with the Id_prov A: the authenticity of the Id_v
  B: the connection between Id_v and Emp
if A = B = true then
    Id_con checks Emp_bio
    if Emp_bio is successfully verified then
        K_c generate (pk, sk) for Emp ← KEYGEN
        sk is stored securely by Emp
        Id_con gathers information i on Emp ← Id_prov
        Id_con construct the list of Emp job requirements
        Id_con generates D_id & authenticate D_id → sk;
        D_id set as an indicator pointing to all Emp tasks
        return D_id
    else
    end if
end if
return fail
```

Algorithm 2 Digital ID Verification

Input: Requested (D_{id})
Output: *Succeed* or *Fail*

```
if (D_id) = K_c then
    return Succeed
else
    return Fail
end
```

2) BEHAVIOR CHAIN

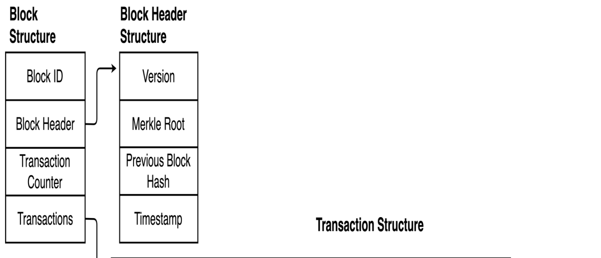
Behaviour in this system refers explicitly to the work behaviour and activities of employees in an organization. Our system captures employee behaviour data by getting output data from Management Information Systems (MIS) from the various departments of the government organization such as their Office Automation (OA) systems, Financial systems, Workflow Systems, among others. The system will link up the data of performance assessment information, on-the-job information and job change information of employees and update their behaviour information according to these data.

The organization's automatic data acquisition goal is accomplished by utilizing IoT systems installed in the organizational infrastructure [32]. The quantity and type of information that the IoT devices receive are dependent on the organization. The organization embed GPS and IoT devices in their infrastructure to collect data on employees, such as their identification, location, among others [8]. The data gathered by sensor nodes and other IoT systems are used to show the behaviours of employees in the organization, i.e. IoT sensors can be used to monitor employee activities depending on the organization's requirements.

IoT devices such as RFID sensors are used to track the movement of employees. For instance, employee movement will be recorded at the main-gate or at any sub-gates, which will be considered as checking points, and these data inputs are sent to the blockchain network to be analyzed and stored on the chain. All sensor inputs are, therefore translated into different types of activity sets and then used to assess employee performance by measuring their engagement in different activities. Other types of data inputs, such as employee log-ins and employee use of organizations resources, are also recorded. Consequently, all data recorded from the monitoring of employee behaviours in the organization are recorded on the behaviour chain. Evaluation processing nodes are responsible for determining the overall participation of employees towards organizational objectives.

Behavior data acquired from the various departments are analyzed using colocation mining [8], [25], where an employee's participation in positive or negative behaviours is determined. An employee E_x is said to be engaged in a behaviour B_y when E_x and B_y are colocated, where B_y can be any event of daily behaviour set B.

Employee's organizational behaviours are divided into two types: positive and negative behaviours. Positive behaviours are beneficial to the organization, while negative behaviours lead to a loss to the organization. Some behaviours such as high achievements of organizational goals constitute positive behaviours whiles behaviours such as lateness, absenteeism, insubordination are negative behaviours. The set of all positive behaviours is described as the positive behaviour set B_P, and the set of all negative behaviours is referred to as the negative behaviour set B_N. In addition, a set "B" comprising all employee behaviours recorded during the day by an immediate supervisor is called a daily behaviour set such that $B = B_P \cup B_N$.



Transaction ID	Employee DID	Transaction Type	Chain	Transaction Hash Value	Transaction Time	Transaction Details
121	wb124561	ID Generation	ID-Chain	fb324657978	2019-09-28 03:45:32	'ID Generation' ID-Chain, 134397625
122	wftqrw67q	Storing Sensors Data	Behavior Chain	ws13536851	2019-09-25 11:17:59	'Storing Sensor Data' B- Chain, 123432
123	agt3836f12	Update Biometrics	ID-Chian	af24345784	2019-09-22 13:05:12	'Update Biometrics' ID-Chain,13422354
124	fvhja6q3q8	Deactivate ID	ID-Chain	bv23467535	2019-09-21 15:25:45	'Deactivate ID' ID-Chain, 1324399

FIGURE 5. **A simplified block and transaction structure.**

Our proposed system assesses employee performance using a participation index (PI) [25] to calculate an employee's involvement in the positive and negative behaviours. The participation of an employee E_x in behaviour sets B_P and B_N is done by computing the PI for each behaviour set type using

$$PI\left(E_x, B_y\right) = \frac{\alpha}{\beta} \tag{1}$$

$$PI\left(E_x, B\right) = PI\left(E_x, B_P\right) - PI\left(E_x, B_N\right) \tag{2}$$

where α is the number of participating behaviours in a behaviour set, and β is the total number of behaviours in the behaviour set, B_y denotes the behaviour sets B_P and B_N. Higher PI (E_x, B_P) value suggests higher employee participation in positive behaviours. The same thing applies to PI (E_x, B_N). After computing the values of PI (E_x, B_P) and PI (E_x, B_N), the system calculates the overall employee participation in all the behaviours [represented as PI (E_x, B)], following equation 2.

Behavior chain is far more than simply recording data. It can provide a time-axis-based record of the employee's behaviour. In addition to supporting auditor's review more effectively and quickly, it also provides a basis for the construction of a credit chain.

Moreover, the figure 5 above is a simplified structure we utilized in our blockchain set-up. The *block structure* includes the block ID which specifies the block height (it uniquely identifies the block); *the block header* (i.e. metadata about the block) which includes several fields such as *version* which is used to keep track of software upgrades; *previous block hash* which is a reference to the hash of the previous (parent) block; *merkle root*, which is a hash of the root of the merkle tree of this block's transactions; *timestamp*, which specifies the creation time of the block. The *transaction counter* keeps track of the number of transactions in the chain and the *transaction* field specifies the transactions recorded in the chain.

Similarly, the transaction structure consists of several fields such as; *transaction ID* which uniquely identifies a specific transactions in the chain; *employee ID*, the entity initiating the transaction; *transaction type* which determines the kind of transaction being initiated; *chain* which specifies which chain this transaction is to be stored on; *transaction hash* is the hash value created for that particular transaction, *transaction time* determines the time the transaction was made and finally *transaction details* provides a brief description of the transaction.

3) CREDIT CHAIN

The Credit Chain incorporates rewards and punishment information. We utilized a game-based automated employee evaluation approach [21]–[24]. Employees who participate more positively must be compensated, while employees who participate in behaviours that violate organizational policies should be punished. The game theory automates the decision-making method. The choice is to reward or punish an employee for beneficial or bad work. The game theory is centred on matters involving the organization and the employee.

- ***Game Parameters***:
  1) R denotes Reward
  2) P denotes Punishment
  3) L denotes Loss to the organization
  4) F denotes Profit to the organization
  5) S_M denotes management strategy
  6) S_N denotes non-management strategy
- ***Game Players and Their Strategies***: Two viable players in the game are identified, organization and employee. The aim of player 1 (organization) is not just to maximize its profit, but also to construct an intelligent, secure and reliable organization. This objective is achieved by motivating competent and honest staff to receive rewards or by using punitive action against misbehaving staff. The system thus determines the strategy set $S_g = (S_R, S_P)$ for player 1, where S_R and S_P are respectively the reward and punishment policies.

  Player 2 (employee) can contribute to the development of the organization or his/her benefits. The workers involved in organizational development tasks are said to pursue a management strategy S_M, and the employees who work against the organization or who participate in operations that violate company policies are said to pursue a non-management strategy S_N. This system, therefore, defines a strategy set for player 2 as $S_y = (S_M, S_N)$.
- ***Game Payoff***: In computing the payoff for each strategy, the model calculates the cost-benefit matrix for the game. If the organization decides to use strategy S_i and employee uses strategy S_j, then let G_o (S_i, S_j) and G_e (S_i, S_j) indicate organization and employee payoff, respectively. Moreover, when the organization utilizes a reward strategy, and the employee uses a management strategy, the employee receives the reward "R". The organization, on the other hand, obtains profit "F" as a result of management strategy played by employees but must bear reward "R" costs. Therefore, G_o (S_R, $S_M = F$ - R) and G_e (S_R, S_M) = R.

  If the organization employs rewards strategy without management of staff, then the organization spends on reward "R" costs, but the workers don't gain (i.e are not rewarded) nor lose. Therefore, G_o (S_R, S_N = 0) and G_e (S_R, S_N) = 0. However, the employees are denied a reward if the organization selects S_P while the worker performs S_M, and the organization does not bear any costs. Thus, G_o (S_P, S_M = 0) G_e (S_P, S_M) = 0.

  When the organization plays the punishment strategy and employees select the non-management strategy, employees get punished "P". Moreover, the organization is subject to loss "L". Hence, G_o (S_P, S_N = L) and G_e (S_P, S_N) = P.
- ***Nash Equilibrium***: It is clear from the cost-benefit matrix that the employee is given the greatest benefit when it plays the management strategy and the organization rewards. Therefore, (S_R, S_M) provides employees with the best gain. The organization's ultimate gain is the same. Thus, the best strategy profile to adopt is (S_R, S_M), which then forms the pure Nash equilibrium of the game.

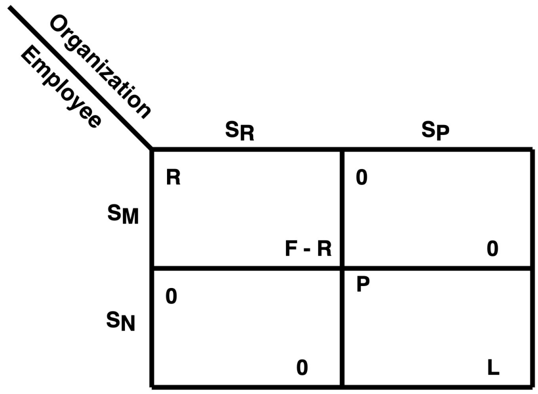


FIGURE 6. Cost-benefit matrix.

Therefore, to select a particular employee or groups of employees to award credits to, we total the number of rewards against the total number of punishments taking it to account their overall Participation Index (PI). If the total number of rewards outweighs the total number of punishments for a particular employee, he/she can be selected to obtain incentives which can be in the form of job promotions, monetary benefits, weekends vacations, among others. Also, this information is stored in the credit chain.

IV. IMPLEMENTATION AND PERFORMANCE EVALUATION

In this section, we demonstrate our system execution and also assess our system efficiency. We tested and evaluated some

Algorithm 3 Game-Based Algorithmic Process

Input: Employee E_x, Set of employee behaviors B_y

Output: Employee Rewards and Punishment

System Processes:

1: Classify set B into two sets B_P and B_N such that $B = (B_P \cup B_N)$ where B_P and B_N are the sets consisting of positive and negative behaviors.

2: Calculate the participation index (PI) of all employee to ascertain overall employees participation in all behaviors.

3: Calculate profit "F" and loss "L" based on the game-based playoff.

4: Calculate parameters reward "R" and punishment "P" in accordance with the organizational policies.

5: Apply Game theory for automated decision making for each employee.

system parameters. Employees wanting to be part of our system will need to submit their government IDs together with their biometric information to the blockchain system. After successful verification of the government IDs and biometric data, the ID controller nodes generate digital IDs for them, and the transactions pertaining to that particular identity is processed into a block.

We made use of the Hyperledger Fabric (v1.0.2) [26]. On a desktop computer with 3.0 GHz, Intel i-7, 16 GB 1600 MHz DDR3 simulating the global blockchain; we used a Ubuntu 16.04.1 operating system. The peer nodes were operated with a virtualization technique based on Ubuntu containers. We created two groups of specialized nodes, namely; ID Controller nodes and Evaluation processing peer nodes for the Global blockchain network. Moreover, we also indicate the location of the Membership Service Provider (MSP) path for each member. Orderer specifies the configuration or transaction structure such as the number of transactions per block, maximum block size, and maximum transactions processing time. In our set-up, we chose to fine-tune these values according to experimental requirements. The underlying platform on which our blockchain system relies adopts a mechanism of pluggable consensus algorithm based on PBFT [27]. Through this mechanism, the whole system can easily switch the consensus algorithm, thus realizing the flexibility and scalability of the system. Three distinct experiments are used to assess the performance of our proposed system. The first test was concerned with ID-chain, and it involves the time it takes for the ID controller nodes to generate the digital IDs for employees. The generation of IDs for an employee involves the verification of the submitted government IDs with ID providers and also verifying that the biometric information submitted matches the one recorded on the system. The second test was focused on the block generation time in our system, and lastly, we made a comparison between a Game-theoretical approach and Fuzzy logic approach to justify the reason we chose to use the Game-theory.

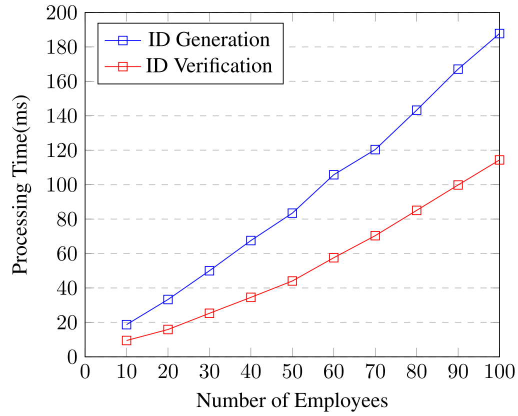


FIGURE 7. ID-Chain processing time.

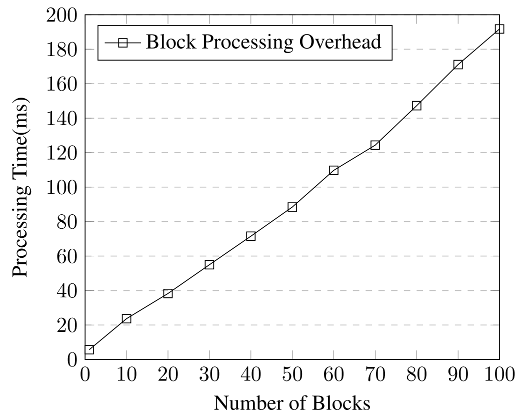


FIGURE 8. Block processing time.

Figure 7 shows the time it takes for several digital IDs to be created on the system. It can, therefore, be seen that there is a steady increase in the time it takes for the generation of digital IDs as the number of employees increases. Similarly, it is the same for ID verification; as the number of digital IDs that need verification increase, so does the processing time.

Figure 8 shows the block processing time. The time it takes for the blockchain nodes to validate and process the transactions emanating from the chain into blocks and add them to the chain. It can be seen that there is a linear rise as the number of blocks increases, so does the time it takes to process them and add them to the chain. Unlike execution time, the space required for execution increases only linearly with the increasing blocks since the data for each employee are stored separately.

Consequently, to ascertain the benefits of using the game theory for decision making, we experimented on using a fuzzy logic system to automate the decision-making process of employee performance evaluation and compared it to that of the game theory. The following settings are created for comparison purposes.

- Setting 1: The Game Theoretical Decision Making
- Setting 2: The Fuzzy Logic system is used rather than the game theory

Figure 9 shows the comparison between the decision making computation using game theory and that of using fuzzy logic.

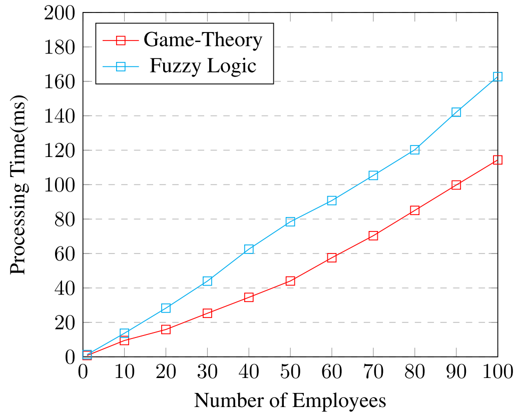


FIGURE 9. Justification for choosing Game-Theory.

TABLE 1. Comparison between proposed system and other related systems.

Metric	[5]	[8]	[18]	[19]	Our System
Decentralized Storage	N	N	N	N	Y
Immutability	M	L	M	M	H
Returns	M	M	M	M	H
Security	M	M	L	M	H
Privacy	L	M	L	M	H
Accountability	Y	N	Y	N	Y
Overall Quality	L	M	M	L	H

H-High, L-Low, M-Moderate, Y-Yes and N-No

The processing time was recorded for the game-theory-based system and the Fuzzy Logic system in a 60 minutes experiment where data was sent to the system. It should be noted that in the above experiment, only the decision-making model is changed whiles the rest of the system remains unchanged. It can be observed from figure 9, that with the increase in the number of employees, the game-theory based decision making time is lower than that of the fuzzy logic. This is as a result of the less complicated nature of the game theory process. The fuzzy logic process involves the creation of complex structures which sometimes prolongs the processing time for decision making.

H-High, L-Low, M-Moderate, Y-Yes and N-No

A. SYSTEM COMPARISON

To validate our proposed system, we compared them with current employee evaluation systems in multiple aspects. The table above shows the comparison between our proposed system and other related systems. Our approach which utilized the blockchain system was able to ensure decentralized storage, data immutability, quality, high returns, privacy and accountability which makes our system trustworthy, transparent and robust as compared with other related systems.

- **Decentralized Storage:** Our proposed system benefits from the strengths of using a decentralized database, while most current systems use the centralized database. Any participant (employee and employer) has complete control of their information (assets) due to the differentiation of private and public key(s). Any particular company or employee can refuse no unique authentication and contract information. Our framework reduces the risk of a single point failure (SPF) because it takes advantage of reliable validation from multiple entry points. However, most existing employee evaluation systems are centralized, thus face a single point of failure problems.
- **Immutability:** With the use of hashing (i.e. SHA 256), data within our system is virtually impossible to alter or tamper. Contrary, current evaluation systems face many problems when it comes to data tampering.
- **Returns:** Our system requires a large amount of storage space, a higher rate of power usage, and this requires more effort during the initial set-up phase relative to the current systems. However, in the long run, the return is projected to be even higher than the cost. It shall also save any extra costs incurred as a result of losing employees due to biased evaluations and taking ineffective decisions as compared to existing systems, as stated in the introduction of this article. Moreover, consulting intermediate or third parties shall incur unreasonable fees for handling training, testing, dispute resolution, among others. However, blockchain removes the need for intermediaries and thereby reduces the company's spending. Furthermore, businesses appreciate an open and impartial employee evaluation system.
- **Security:** Our system guarantees high security. Blockchain technology is implemented via the use of cryptographic techniques for data encryption and decryption. This technique requires strong data security and the use of both private and public keys to read transactions in each blockchain, as well as to perform some transaction. The principle that all nodes in the network must first validate the transaction before each node executes the transaction increases the security of this smart technology.
- **Privacy:** Data within our system is completely private. Without the proper authorization keys or credentials, access to particular employees, information is strictly prohibited. Contrary, this is not always the case in existing systems.
- **Accountability:** History and logs of network transactions are kept, and thus it guarantees accountability of system operations.
- **Overall Quality:** The use of blockchain technology guarantees the quality of the system. Our system can process, record, verify and order employee information with full transparency and safety. Because our system does not allow any wrong and biased assessments, there is no room for system quality reduction as compared to current systems.

V. CONCLUSION AND FUTURE WORKS

In this paper, we proposed BEMPAS, an employee performance evaluation system based on blockchain for

Smart city governance. The blockchain system is composed of 3-chains referred to as ID-Chain, Behavior Chain and Credit chain that works together to evaluate employee performance. We utilized a game-theoretical approach where a game is played between the ***Government Institution*** denoted as ***Organization*** and ***Government Officers*** denoted as ***Employees***. The organization tries to get more benefits by incentivizing its employees to work harder towards the good of the company. Our Proof of Concept (PoC) result shows that our system is effectively able to motivate the employees in addition to effectively evaluating their performance. The employees feel encouraged by the incentives they receive for achieving organizational objectives. Also, our system achieves trust, transparency, security and accountability among government workers under a Smart City governing environment. Future works might include the use of blockchain in other Smart City areas.

REFERENCES

[1] B. Carson, G. Romanelli, P. Walsh, and A. Zhumaev. (2018). *Blockchain Beyond the Hype: What is the Strategic Business Value? | McKinsey & Company*. [Online]. Available: https://www.mckinsey.com/businessfunctions/digital-mckinsey/our-insights/blockchain-beyond-the-hypewhat-is-the-strategic-business-value

[2] D. M. Ni and R. H. Liu, "Study on the enlightenment from EU smart city evaluation system," in *Applied Mechanics and Materials*, vol. 641. Stafa, Switzerland: Trans Tech, 2014, pp. 624–628.

[3] H. J. Scholl and M. C. Scholl, "Smart governance: A roadmap for research and practice," in *Proc. IConference*, 2014, pp. 163–176.

[4] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. A. Pardo, and H. J. Scholl, "Understanding smart cities: An integrative framework," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 2289–2297.

[5] L. Tanti, R. Puspasari, and B. Triandi, "Employee performance assessment with profile matching method," in *Proc. 6th Int. Conf. Cyber IT Service Manage. (CITSM)*, Aug. 2018, pp. 1–6.

[6] G. E. Roberts, "Employee performance appraisal system participation: A technique that works," *Public Personnel Manage.*, vol. 32, no. 1, pp. 89–98, Mar. 2003.

[7] A. M. Awadh and M. S. Alyahya, "Impact of organizational culture on employee performance," *Int. Rev. Manage. Bus. Res.*, vol. 2, no. 1, p. 168, 2013.

[8] N. Kaur and S. K. Sood, "A game theoretic approach for an IoT-based automated employee performance evaluation," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1385–1394, Sep. 2017.

[9] R. Intartaglio, "Evaluation of the need for a performance appraisal system for the South Trial Fire Department," Nat. Fire Acad., Fort Myers, FL, USA, Appl. Res. Rep., 2000. [Online]. Available: http://www.usfa.fema.gov/pdf/efop/efo14655.pdf

[10] S. Nakamoto. (Oct. 2018). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[11] M. H. Onik, M. H. Miraz, and C. S. Kim, "A recruitment and human resource management technique using blockchain technology for industry 4.0," in *Proc. Smart Cities Symp. (SCS)*, Manama, Bahrain, 2018, pp. 11–16.

[12] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, Apr. 2017.

[13] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeD-Share: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[14] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[15] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in *Proc. 22nd Int. Conf. Digit. Signal Process. (DSP)*, Aug. 2017, pp. 1–5.

[16] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Proc. IFIP Int. Conf. Distrib. Appl. Interoperable Syst.* Cham, Switzerland: Springer, Jun. 2017, pp. 206–220.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.

[18] K. Kuppusamy, N. Shanmugasundaram, E. N. Ganesh, and S. Kumar, "Implementation of performance evaluation of employees through online system," *Int. J. Manage., Technol. Eng., Delhi, India*, vol. 8, no. 12, p. 5482, 2019.

[19] I. Ahmed, I. Sultana, S. K. Paul, and A. Azeem, "Employee performance evaluation: A fuzzy approach," *Int. J. Productiv. Perform. Manage.*, vol. 62, no. 7, pp. 718–734, Sep. 2013.

[20] Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen, and W. Shi, "Blockchain-based identity management with mobile device," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock)*, 2018, pp. 66–70.

[21] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.

[22] W.-C. Chang, T.-H. Wang, F. H. Lin, and H.-C. Yang, "Game-based learning with ubiquitous technologies," *IEEE Internet Comput.*, vol. 13, no. 4, pp. 26–33, Jul. 2009.

[23] X. Luo, X. Wei, and J. Zhang, "Guided game-based learning using fuzzy cognitive maps," *IEEE Trans. Learn. Technol.*, vol. 3, no. 4, pp. 344–357, Oct. 2010.

[24] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 920–925.

[25] Y. Huang, S. Shekhar, and H. Xiong, "Discovering colocation patterns from spatial data sets: A general approach," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 12, pp. 1472–1485, Dec. 2004.

[26] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, p. 30.

[27] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, Feb. 1999, pp. 173–186.

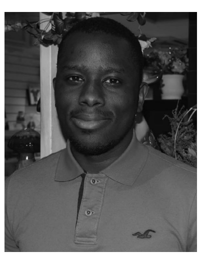
[28] S. E. Haddouti and M. D. E.-C. El Kettani, "Analysis of identity management systems using blockchain technology," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–7.

[29] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1336–1342.

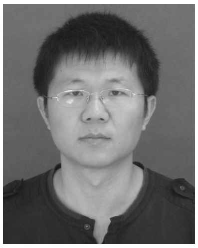
[30] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 8, nos. 2–4, pp. 1735–1745, 2018.

[31] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identity on the blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jul. 2018, pp. 582–587.

[32] S. Li, L. D. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2177–2186, Nov. 2013.



EMMANUEL BOATENG SIFAH received the B.Sc. degree in telecommunications engineering from Ghana Technology University College, Ghana, in 2014, and the M.Eng. degree in computer science and technology with the School of Computer Science and Engineering, UESTC, in 2017. He is currently pursuing the Ph.D. degree in computer science and technology with UESTC. His current research interests include blockchain technologies, big data security, and privacy.



HU XIA received the Ph.D. degree from the University of Electronic Science and Technology of China, China, in 2012. He was a Visiting Scholar with the University of Minnesota, Twin Cities, USA, from 2010 to 2011. He is currently an Associate Research Fellow with the University of Electronic Science and Technology of China.

CHRISTIAN NII AFLAH COBBLAH received the B.Sc. degree in information science from the University of Ghana, Legon, in 2014, and the M.Eng. degree in computer science and technology with University of Electronic Science and Technology of China (UESTC), in 2019, where he is currently pursuing the Ph.D. degree in computer. His current research includes blockchain technology and applications, named data networking (NDN), the IoT security, and privacy.

QI XIA (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science from the University Electronic Science and Technology of China (UESTC), in 2002, 2006, and 2010, respectively. She is currently a Professor at the University of Electronic Science and Technology of China (UESTC). She is also the Deputy Director of the Cyberspace Security Research Centre, the Executive Director of the Blockchain Research Institute, the Executive Director of the Big Data Sharing and Security Engineering Laboratory of Sichuan Province, a member of the CCF Blockchain Committee, and the Chief Scientist with YoueData Company Limited. She was a Visiting Scholar with the University of Pennsylvania (UPenn), USA, from 2013 to 2014. She serves as the PI of the National Key Research and Development Program of China in Cyber Security and has overseen the completion of more than 30 high profile projects. She has published over 40 academic articles and won second place at the National Scientific and Technological Progress Awards, in 2012. Her research interests include network security technology and its application, Big Data security, and blockchain technology and its application.

JIANBIN GAO (Member, IEEE) received the Ph.D. degree in computer science from the University Electronic Science and Technology of China (UESTC), in 2012. He was a Visiting Scholar with the University of Pennsylvania, USA, from 2009 to 2011. He is currently an Associate Professor at UESTC.

XIAOJIANG DU (Fellow, IEEE) received the B.S. and M.S. degrees in electrical engineering from the Automation Department, Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 2002 and 2003, respectively. He is currently a tenured Full Professor and the Director of the Security and Networking (SAN) Lab, Department of Computer and Information Sciences, Temple University, Philadelphia, USA. His research interests are security, wireless networks, and systems. He has authored over 400 journal and conference papers in these areas, as well as a book published by Springer. He is a Life Member of ACM. He has been awarded more than six million U.S. Dollars research grants from the U.S. National Science Foundation (NSF), Army Research Office, Air Force Research Lab, NASA, the State of Pennsylvania, and Amazon. He won the Best Paper Award at the IEEE GLOBECOM 2014 and the Best Poster Runner-Up Award at the ACM MobiHoc 2014. He serves on the editorial boards of three international journals.