Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 9922167, 7 pages
https://doi.org/10.1155/2022/9922167

Research Article

Increasing Cyber Defense in the Music Education Sector Using Blockchain Zero-Knowledge Proof Identification

Ying Zhang

Zhengzhou Preschool Education College, Zhengzhou, Henan 450000, China

Correspondence should be addressed to Ying Zhang; zhangying198002@126.com

Received 4 May 2022; Revised 23 May 2022; Accepted 26 May 2022; Published 28 June 2022

Academic Editor: Konstantinos Demertzis

Music creation and its promotion are encouraged both in music education and through activities organized in the context of artistic creation as part of the education in question. Although copyright registration is the primary way authors protect their rights, this is not feasible in most cases, as the processes take a long time to complete and incur high costs. We utilize modern innovative technologies and their developments in copyright protection matters to increase security and trust in music education. In particular, an advanced model of ensuring the methods and innovation produced in music education processes is proposed, using blockchain technology and smart contracts. But given that, even in an advanced system like the proposed one, authentication evidence can be easily intercepted, this work proposes a single and robust identification scheme based on an innovative zero-knowledge proof (ZNP) system, which allows one side of communication to convince the other of its validity.

1. Introduction

In recent years, cloud computing has been widely used in many areas of everyday life, mainly for data storage [1, 2]. This raises questions about the reliability and how to manage the data in question. The multitude of these services targets widespread attacks by third parties. These attacks find fertile ground as they exploit security vulnerabilities, resulting in data leaks [3]. The result is that both the security and the privacy of the data stored in cloud services are questioned [4, 5]. In addition, users' data is often used for exploitation purposes or given to third parties such as advertising companies. Another deterrent is that data providers usually store that information without encryption, making user data easily accessible [6].

An attractive solution that can give another approach to the issue is blockchain, which proposes a decentralized and highly secure solution for data storage [7]. Similarly, the blockchain can be used as an intermediary whose primary function is to maintain and validate actions within the chain. In general, blockchain implements a distributed global platform that runs smart contracts [8], utilizes proven technologies, and has an architecture that allows various additional functions to be implemented simply and transparently [9]. It enables the creation of different security levels and licenses only certified users to access specific services or resources. Due to the encryption [10, 11] of transactions and its operating environment, it is ideal for environments that require reliability without the mediation of third-party trusted entities, as it can achieve complete confidentiality of transactions and selective access between participants only to licensed information. This achieves the confidence of the participants in the sharing of information, combined with all the benefits of blockchain [12, 13].

This function is advanced further by using blockchain-provided smart contracts, which allow access to information under precise, strictly specified, and preagreed-upon conditions [8, 14]. When unavoidable circumstances are met, these contracts will close deals. It is simply a protocol designed to digitally facilitate, verify, or enforce the negotiation or execution. These contracts enable the performance of trustworthy transactions without the involvement of third parties, with the transactions being secure, monitored, and irreversible [15, 16]. They seek to protect the scope of contract law while also reducing the additional processing expenses involved with the award and implementation of

intermediary contracts [17]. Blockchain implementation is based on the Byzantine Fault Tolerance (BFT) consent algorithm [18, 19], which means that its command service must be jointly controlled by network members. Using the BFT algorithm, the standard guarantees coverage or the ability to reach consensus, even if there are rival nodes (malicious) or if the nodes are offline [20].

In this paper, we present an enhanced model that uses blockchain technology and smart contracts to guarantee the approaches and innovation achieved in music education. Given that, even in a progressive system like the one that is being proposed, the proposed approach is that the authentication items can be easily copied, guessed, or revealed by automated methods and technical means, the main contribution of this work is to offer a single and robust identification scheme, which is based on an innovative ZNP system [12], which enables one side of communication to convince the other side of its validity.

The following is the structure of the paper. In the following section, an overview of the several appropriate methods that have been identified in the relevant literature is presented. In Section 3, we will discuss the ZNP protocol that has been delivered. In Section 4, the scenarios and results prove that ZNP and complexity exist. In the final part of the report, Section 5, a summary of the findings and a list of possible following study directions are presented.

2. Related Literature

The literature on blockchain technologies, smart contracts, and zero-proof knowledge is becoming more and more frequent since these innovative technologies are gaining confidence in the community [21].

Hu et al. [14] gave a detailed study of smart contracts, emphasizing current applications and the problems they confront. They introduced the idea of a blockchain-based smart contract, a digital software meant to enable the settlement or contract terms immediately among users when specific circumstances are satisfied. With the improvement in blockchain technology, smart contracts are being utilized to fulfill a wide variety of objectives, from self-maintained accounts on public blockchains to automating corporate collaboration on blockchain systems.

On the other hand, Wang et al. [8] provided a systematic and extensive assessment of blockchain-enabled intelligent contracts to motivate more study in this developing research field. Following the introduction of the operational mechanism and mainstream platforms for blockchain-enabled smart contracts, they proposed a scientific framework for smart contracts based on a groundbreaking six-layer design, which was accepted by the scientific community. Second, the technological and legal difficulties, as well as current research advances, were detailed. Thirdly, they discussed some representative application cases. They concluded by debating the future development patterns for smart contracts.

Yang and Li [12], employing smart contracts and zero-knowledge proof methods to create identity unlikability, have successfully avoided the disclosure of attribute ownership in the present claim identification model on the blockchain. Aside from that, they created a system prototype known as BZDIMS, which features a challenge-response protocol that allows users to reveal their ownership of characteristics to service providers, thereby maintaining the privacy of their activities. Performance and security analyses demonstrated that their system provided good attribute privacy security and a broader application breadth than the previous paradigm.

Sankar et al. [17] examined and compared the viability and efficiency of blockchain consensus algorithms. The consensus protocol is at the heart of blockchain technology. Academics are eager to design a well-optimized Byzantine fault-tolerant consensus system in light of the advent of new possibilities in blockchain technology. Exciting options include developing a worldwide consensus protocol or creating a cross-platform plug-and-play software application to support a variety of consensus mechanisms. Incorporating the principles of quorum slices and federated Byzantine Fault Tolerance, the Stellar Consensus System is a global consensus protocol designed to be fault-tolerant and claims to be Byzantine Fault Tolerance. Additionally, the hyperledger is an open-source project led by the Linux Foundation that focuses on realizing the notion of realistic Byzantine Fault Tolerance and providing a framework for the plug-and-play deployment of many different consensus protocols and chain applications.

Finally, Buchman [18] developed Tendermint, a novel protocol for organizing events in a dispersed network under adversarial circumstances, as part of his examination of Byzantine Fault Tolerance. Known more frequently as unanimous agreement or atomic broadcast, the problem has gained significant attention in recent years because of the widespread growth of digital currencies such as Bitcoin and Ethereum, which effectively remedy the issue in public settings without the intervention of a central authority. Their concept modernized previous academic work in the field by providing a safe consensus mechanism with accountability requirements and functionality for creating arbitrary applications atop the consensus. Their idea is a high-performance blockchain, capable of processing several events per second over dozens of nodes scattered across the world, with a latency of less than one second and performance deteriorating very slightly in the face of hostile assaults.

3. Proposed ZNP Protocol

Entering a service electronically involves different authentication methods. It often requires repetition of the same information or distinct numbers and codes, which can be easily intercepted or revealed [22]. The service provider usually keeps a summary of each user's password. Each time the user wants to connect to the service, the password is given in the summary function, and the result is compared to the saved one [23]. This protocol may not allow the password to be saved in its original form, but the server temporarily learns it [24, 25]. This process could be replaced with a ZNP indicating that each customer owns the password [12].

Although it has offered us many benefits, including openness, immutability, and decentralization, blockchain

technology may not provide the necessary level of anonymity for certain types of transactions. However, integrating blockchain technology with ZNP has the potential to deliver to customers a potent combination of immutability and security. A ZNP is a sort of cryptography that allows one person (the prover) to demonstrate to another party (the verifier) that certain information is accurate without giving any extra information. When it comes to messaging applications, end-to-end encryption has been a significant factor in developing private message transmission. On the other hand, traditional messaging applications demand that users verify their identities on a central server. Individuals can demonstrate their identity using ZNPs without divulging any more personal information.

In the proposed ZNP, each calculation is performed by exchanging messages between an entity called prover (P) and an entity called verifier (V). Typically, P wants to convince V that a proposition is true (witness). P and V are probabilistic Turing machines, where P has unlimited computing power while V is limited to probabilistic calculations of polynomial complexity [26].

Zero knowledge is realized, given that V learns nothing more than the fact that P's claim is valid [27]. A key role in proving that an interactive system has the property of zero knowledge is played by the simulator (S), which simulates P but does not have access to the witness. His contribution is as follows [28]: V interacts with S. At some point, V will put S in the "difficult position" of not being able to answer a question as he does not have access to the witness. In this case, we return the V tape to a state before rewinding and running the protocol from that point on. If V (with continuous rewinds) finally accepts S's proof, the protocol holds the status of zero knowledge, as V cannot distinguish a P who knows the witness and an S who pretends. V cannot export any additional information from the protocol (since, in the second case, there is no information to ship) [29, 30].

Let an NP language L and M be a polynomial Turing machine such that [31, 32]

$$x \in L \Leftrightarrow \exists w \in \{0,1\}^{p(|x|)}: M(x,w) = 1, \tag{1}$$

where p is a polynomial. One proof of zero knowledge for L is two possible Turing Polynomial Time (TPT) machines P and V for which the following three properties apply [33]:

(1) Completeness: if $x \in L$ and w are a witness to this, that is,

$$M(x,w) = 1, \tag{2}$$

then

$$\Pr\left[\text{out}_{\mathcal{V}} < P(x,w), V(x) > (x)\right] = 1 \geq \frac{2}{3}, \tag{3}$$

where

(a) $P(x,w), V(x)$ is the interaction between P and V with standard (public input) x and private input of P at w.
(b) $\text{out}_{\mathcal{V}}$ is the output V at the end of the protocol.

(2) Correctness: if $x \notin L$, then

$$\forall (P^*, w) \Pr\left[\text{out}_{\mathcal{V}} < P^*(x,w), V(x) > (x)\right] = 1 \leq \frac{2}{3}.OP^*, \tag{4}$$

where P^* does not need to be TPT.

(3) Validity: V does not accept false statements (even if P tries to trick him).

The proposed model appears to be related to the NP complexity class in the above definition [34–37].

4. Evidence of ZNP and Complexity

To prove the proposed ZNP methodology, we will use three different examples which show its power as a computational and cryptographic model which can respond to the proposed implementation [15, 38].

4.1. Graph Isomorphism. The first example concerns the isomorphism of graphs. Specifically, two isomorphic graphs where the mapping from ABCD to CDAB corresponds to the first graph to the second, as shown in Figure 1.

Two graphs, $G1$ and $G2$, are said to be isomorphic if they have the same number of vertices. There is a shift, that is, function 1–1 and on, between their nodes such that two nodes of one are connected by acne if and only if the corresponding nodes of the other are connected by acne. Equivalently, there is a renaming of the nodes of a graph such that the charts are identical. The problem of graph isomorphism belongs to the NP class, but it is not known whether it is NP-complete or not [39]. Assume that both P and V know the graphs $G1$ and $G2$; that is, the latter is a common input of the protocol. In addition, P knows the isomorphism between them ϕ: $G1 \longrightarrow G2$ (private input of V or the witness mentioned above). Using a zero-knowledge protocol, he can prove that he knows the isomorphism without revealing it [40]:

(1) P randomly selects one of $G1$, $G2$, and Gi. By some permutation ψ of the vertices of Gi, P produces the graph $H = \psi(Gi)$, which is isomorphic with Gi. Because P knows the isomorphism ψ between H and Gi, he also knows the isomorphism $\psi\phi$ between H and $G3 - i$. Anyone else has as much difficulty finding an isomorphism between H and $G1$ or between H and $G2$ as finding an isomorphism between the initials $G1$ and $G2$.

(2) P binds to ψ, sending H to V.

(3) V randomly selects a graph from $G1$, $G2$, and Gj and sends his selection as a challenge to P, asking him to prove that H and Gj are isomorphic. That is, he asks for a permutation of Gj to produce H.

(4) P responds by doing the following:

$(\widehat{I} \pm I')$if $G_i = G_j$, send to V the permutation ψ.
$(\widehat{I}^2 I')$if $G_i \neq G_j$, then we have the following:

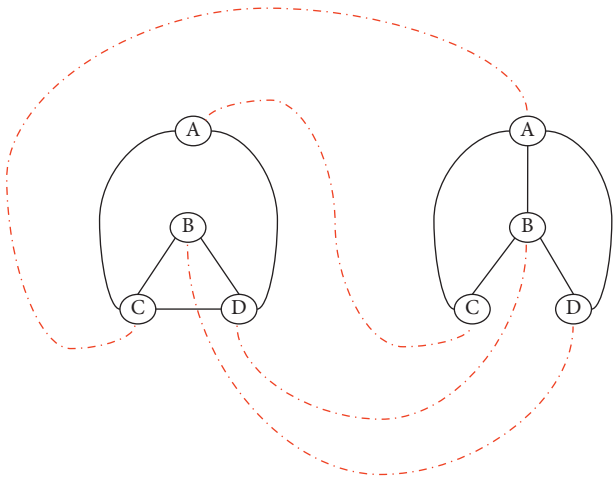

Figure 1: Two isomorphic graphs where the mapping from ABCD to CDAB corresponds to the first graph to the second.

(i) If $G1$ and $G2$ are isomorphic (then $\exists\rho$: $G_i = \rho(G_j)$), send to V the permutation $\psi\rho$
(ii) If $G1$ and $G2$ are not isomorphic (i.e., P is not honest), then it cannot find a suitable permutation and sends any random permutation

(5) If V receives a correct permutation, he continues (repeat steps 1–5); otherwise, he stops rejecting (i.e., he considers that the graphs are not isomorphic).

If V has not rejected after k repetitions of steps 1–5, he accepts (considers the graphs isomorphic). The above protocol fulfills the properties of the zero knowledge mentioned above. First, it is complete because if there is an isomorphism between $G1$ and $G2$, then P will convince V with a probability of 1 (V never rejects) [27, 41].

Regarding correctness, if there is no isomorphism, then P has a 1/2 chance at each step to deceive V (this will only happen if $Gi = Gj$). After k repetitions, this probability becomes $1/(2^k)$.

V does not get any additional information regarding the isomorphism between $G1$ and $G2$ regarding the zero knowledge. When interacting with S, his first step will be the same as P; that is, he will make a new random graph isomorphic to one of $G1$ and $G2$ each time. The probability of choosing either $G1$ or $G2$ is precisely 1/2. So, at this stage, V cannot separate them. Thus, the likelihood of cheating in k repetitions remains $1/(2^k)$. So, the expected execution time is polynomial as it results from the relation [15, 39, 42]:

$$T_{\mathscr{V}} \frac{\sum_{k=1}^{\infty} 1}{\left(2^k\right)} = T_{\mathscr{V}}, \tag{5}$$

where $T_{\mathscr{V}}$ is the execution time of V, which is polynomial.

4.2. 3-Coloring. A zero-knowledge protocol for an NP-complete problem would mean that all NP problems have zero-knowledge protocols [12, 26, 32, 39]. In the NP-complete problem of 3-Coloring, P knows a coloring c for a graph $G = (V, E)$ such that [43]

$$c\colon V \longrightarrow \{1,2,3\} \text{and } c(v_1) \neq c(v_2) \Leftrightarrow (v_1, v_2) \in E. \tag{6}$$

He wants to prove this knowledge to V without revealing c:

(1) P selects a random permutation π of {1, 2, 3}. From this, an alternative 3-$\pi \cdot c$ of G then uses a commitment scheme for $\pi.c$, that is, calculates values commit$((\pi.c)(v_i), r_i), \forall v_i \in V$ and sends them to V.
(2) V selects a random edge $(v_i, v_j) \in E$ and sends it to P.
(3) P releases the values $\pi \cdot c(v_i), \pi \cdot c(v_j)$ and sends them to V.
(4) V checks if $\pi \cdot c(v_i) \neq \pi \cdot c(v_j)$.

It is evident that the above protocol is complete. Regarding the correctness, we observe that if P does not have a valid 3-color, then V will choose an edge with the same peak colors with probability $1/|E|$. By repeating the protocol, we can make the probability that prover $1 - 1/|E|$ cheats him extremely small. About zero knowledge, even S does not have a valid coloring. If V chooses an edge with the same peak colors, then it rewinds to a previous state, and S selects a new random permutation that it uses in the new execution. It can be shown that the protocol with S does not have an expected execution time of a different order of magnitude than with P and V does not understand the difference. So, the protocol has the property of zero knowledge [15, 42].

4.3. Noninteractive Proof of Zero Knowledge. To make a noninteractive proof, we use a hash function [26, 39]:

$$H\colon \{0,1\}^* \longrightarrow Z_q, \tag{7}$$

such that the discussion

$$(y, c, s) = g^t, H\left(g^t\right), t + H\left(g^t\right) w \bmod q. \tag{8}$$

Assume that H is a random oracle controlled by the simulator to demonstrate that ZNP holds. In the random oracle model, a nonhonest verifier V can ask questions of the random oracle and receive answers. In this case, c is forced to be selected after y, which is directly dependent on the characteristics of the hash function [12, 13]. Figure 2 shows how V^* interacts with H.

When the verifier asks for the proof of $h = g^w$, the simulator randomly selects c and s to compute $y = g^s h^{-c}$. Set (y, c) in History and return $\langle y, c, s\rangle$. The nonhonest verifier cannot separate an honest prover from an emulator unless $(y, c') \in$ History with $c \neq c'$. Then, V^* achieves with probability $(1/m)q_H$, where q_H is the number of questions in the random oracle. Then, we want to produce two discussions that end in acceptance with the same y but with different challenge values. Using these two discussions, we can extract a witness. Note that $c = H(y)$. If a dishonest prover P^* asks a unique question in the random oracle before producing $\langle y, c, s\rangle$, the resolution is the same as the interactive protocol. Problems arise when P^* asks more than one question [31, 38, 39].

Assume that, in the first round, P^* asks q_H questions before ending the discussion. The knowledge exporter then

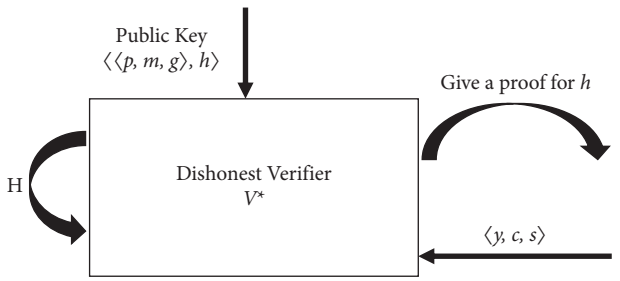

Figure 2: In the random oracle model, the simulation of dishonest verifier V^* is performed.

returns P^* to a previous step, with no guarantee that P^* will request q_H questions again. When P^* finishes, it will return y', c', s' with $c' = H(y')$ and possibly $y \neq y'$. This limits our capacity to compel a witness to testify, so we should modify the probability of having two acceptance discussions with the same y.

Assume that, after asking q_H questions, P^* selects a question he asked and uses the corresponding answer he got for it from the random oracle at his exit. Let $\text{Prob}[A] = \alpha$ be the probability that the discussion will end in acceptance. Let $\text{Prob}[Q_i] = \beta_i$ be the probability that the dishonest prover uses the i-th answer c_i, in which $1 \leq i \leq q_H$. We define $\text{Prob}[A \cap Q_i] = \alpha_i$. Respectively, for the repetition of the experiment, we write A', Q_j', c_i'. Then, it is valid [15, 29, 30, 42]:

$$\sum_{i=1}^{q_H} \alpha_i = \alpha \text{ and } \sum_{i=1}^{q_H} \beta_i = 1. \tag{9}$$

We define $\text{Prob}[E]$ as the probability of extracting a witness from P^*, and we have

$$\text{Prob}[E] = \text{Prob}\left[A \cap A' \cap (i = j) \cap \left(c_i \neq c_j'\right)\right]. \tag{10}$$

Similarly, we have

$$\text{Prob}[E] \geq \text{Prob}\left[A \cap A' \cap (i = j)\right] - \text{Prob}\left[\left(c_i = c_j'\right)\right]. \tag{11}$$

So,

$$\begin{aligned}\text{Prob}[E] \geq \text{Prob}\left[A \cap A^{'}\right] - \frac{1}{q} &= \sum_{i=1}^{q_H} \text{Prob}\left[A \cap Q_i \cap A^{'} \cap Q_i^{'}\right] - \frac{1}{q} \\ &= \sum_{i=1}^{q_H} \text{Prob}\left[A_i \cap A_i^{'}\right] - \frac{1}{q}.\end{aligned} \tag{12}$$

From the definition of exporter in our calculations, we know that

$$\text{Prob}\left[A_i \cap A_i'\right] \geq \frac{\text{Prob}\left[A_i\right]^2}{4} = \frac{\alpha_i^2}{4}. \tag{13}$$

The total probability is calculated as follows:

$$\text{Prob}[E] \geq \sum_{i=1}^{q_H} \text{Prob}\left[A_i \cap A_i^{'}\right] - \frac{1}{q} = \frac{1}{4}\sum_{i=1}^{q_H} \alpha_i^2 - \frac{1}{q}. \tag{14}$$

From the statistics, we know that

$$\frac{\sum\left(\alpha_i^2\right)}{q_H} \geq \left(\frac{\alpha}{q_H}\right)^2. \tag{15}$$

And so,

$$\sum\left(\alpha_i^2\right) \geq \frac{\alpha}{q_H}. \tag{16}$$

And for any real α_i, they have an average:

$$\frac{\alpha}{q_H}. \tag{17}$$

As a result, we infer that we have a good chance of extracting a witness, given a persuasive prover:

$$\frac{\alpha^2}{4q_H} - \frac{1}{q}. \tag{18}$$

If it is necessary for the person who is proving a statement to possess certain confidential knowledge, then the person who is verifying the statement will not be able to prove the statement to anyone else unless they also possess the confidential information. The assertion that the prover possesses such information must be included in the statement that is being proven, but the knowledge itself cannot be included in the assertion, nor can it be transmitted with it. If this were not the case, the statement could not be proven using the zero-knowledge proof method since it would present the verifier with more information about the statement by the time the protocol was completed. A proof of knowledge is considered to be in the particular situation of zero knowledge when the assertion consists of nothing more than the fact that the prover is in possession of the confidential information.

As proved, concerning zero knowledge, even a node that does not hold a piece of valid information will rewind to a previous state and choose a new random permutation employed in the new execution. This is because zero knowledge prevents a node from storing any information at all. It is possible to demonstrate that the protocol with random nodes does not have an expected execution time of a different order of magnitude. Still, this protocol does not comprehend the distinction. Therefore, the protocol possesses the quality of not revealing any information.

5. Conclusions

This work proposed an innovative ZNP system [12] to ensure the methods and innovation produced in music education processes, using blockchain [9, 42] technology and smart contracts [14, 44]. The motivation for the development of this protocol is that, in the "conventional" authentication protocols [39, 45], at the end of their execution, the member who verifies the identity of his peer has messages and secrets that he can use for impersonation [37, 46]. Contrary to the proposed standard, the secret used to prove a member's identity depends on a specific time, so that, at another time, it is useless. In other words, the musical educational processes and the participants may know a secret, but without revealing any information about this secret. Three different examples were used to demonstrate

the capability of the template as both a computing and a cryptographic model, capable of responding to the suggested implementation and ensuring the authentication processes of blockchain technology.

Even though it may be possible to achieve a level of protection in musical educational processes that are practically acceptable, it is evident that a significant amount of research work is still required because the requirements are high and are continually increasing [47]. The sheer number of potential solutions and the associated expenses illustrate how challenging it is to ensure the safety of a comparable system in a safe setting. It is acceptable to conclude that, to secure it, specialized methods of issuing identities to the blockchain nodes, scattering the nodes, instant data copying, and an access mechanism that gives high possibilities of maintaining security and privacy are required [48].

A main future extension is a study of how the proposed methodology is improved when additional information is added to it, both from the network and from the music education content. This would apply to both of these sources of data. In addition to this, we intend to study the impact that the amount of the data has on the algorithm's scalability and evaluate how well our method performs in additional private databases. It would be interesting also to investigate new ways of encoding the available information with crypto-tensioners to integrate this further information into the technique that has been proposed on a methodological level.

Data Availability

The data used in this study are available from the author upon request.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] H. N. Chua, J. S. Teh, and A. Herbland, "Identifying the effect of data breach publicity on information security awareness using hierarchical regression," *IEEE Access*, vol. 9, pp. 121759–121770, 2021.

[2] A. Bates and W. U. Hassan, "Can data provenance put an end to the data breach?" *IEEE Security & Privacy*, vol. 17, no. 4, pp. 88–93, 2019.

[3] N. Li, "Combination of blockchain and AI for music intellectual property protection," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–8, Article ID 4482217, 2022.

[4] A. S. Al-Ahmad and H. Kahtan, "Cloud computing review: features and issues," in *Proceedings of the 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pp. 1–5, Singpore, Juy 2018.

[5] F. Wang, H. Wang, and L. Xue, "Research on data security in big data cloud computing environment," in *Proceedings of the 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 1446–1450, China, Octomber 2021.

[6] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: when, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019.

[7] R. Amelin, V. Arkhipov, S. Channov, M. Dobrobaba, and V. Naumov, "Prospects of blockchain-based information systems for the protection of intellectual property," *Communications in Computer and Information Science*, vol. 1038, pp. 327–337, 2019.

[8] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[9] C. G. Akcora, M. Kantarcioglu, and Y. R. Gel, "Blockchain data analytics," in *Proceedings of the 2018 IEEE International Conference on Data Mining (ICDM)*, p. 6, Coimbatore, Chennai, November 2018.

[10] M. R. Ogiela and M. Oczko, "Comparison of selected homomorphic encryption techniques," in *Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pp. 1110–1114, Zhengzhou, February 2018.

[11] R. Sendhil and A. Amuthan, "A descriptive study on homomorphic encryption schemes for enhancing security in fog computing," in *Proceedings of the 2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 738–743, September 2020.

[12] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Computers & Security*, vol. 99, Article ID 102050, 2020.

[13] S. Sahai, N. Singh, and P. Dayama, "Enabling privacy and traceability in supply chains using blockchain and zero knowledge proofs," in *Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain)*, pp. 134–143, Augest 2020.

[14] Y. Hu, M. Liyanage, A. Mansoor, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "Blockchain-based Smart Contracts-Applications and Challenges," 2018, https://arxiv.org/abs/1810.04699.

[15] L. Cao and Z. Wan, "Anonymous scheme for blockchain atomic swap based on zero-knowledge proof," in *Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, pp. 371–374, June 2020.

[16] G. Hua, L. Zhu, J. Wu, C. Shen, L. Zhou, and Q. Lin, "Blockchain-based federated learning for intelligent control in heavy haul railway," *IEEE Access*, vol. 8, pp. 176830–176839, 2020.

[17] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pp. 1–5, Coimbatore, India, January 2017.

[18] E. Buchman, *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*, 109 pages, The University of Guelph, Guelph, Ontario, Canada, 2020.

[19] K. Lei, Q. Zhang, L. Xu, and Z. Qi, "Reputation-based byzantine fault-tolerance for consortium blockchain," in *Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 604–611, Singapore, December 2018.

[20] G. Ra, T. Kim, and I. Lee, "VAIM: verifiable anonymous identity management for human-centric security and privacy in the internet of things," *IEEE Access*, vol. 9, pp. 75945–75960, 2021.

[21] K. Gao, F. Han, P. Dong, N. Xiong, and R. Du, "Connected vehicle as a mobile sensor for real time queue length at

signalized intersections," *Sensors*, vol. 19, no. 9, Article ID 2059, 2019.

[22] X. Wang, Q. Li, N. Xiong, and Y. Pan, "Ant colony optimization-based location-aware routing for wireless sensor networks," in *Wireless Algorithms, Systems, and Applications*pp. 109–120, Berlin, Heidelberg, 2008.

[23] L. Avigad and O. Goldreich, "Testing graph blow-up," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, D. Zuckerman and O. Goldreich, Eds., Springer, Berlin, Heidelberg, pp. 156–172, 2011.

[24] Y. Jiang, G. Tong, H. Yin, and N. Xiong, "A pedestrian detection method based on genetic algorithm for optimize XGBoost training parameters," *IEEE Access*, vol. 7, pp. 118310–118321, 2019.

[25] R. Wan, N. Xiong, and N. T. Loc, "An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, p. 18, 2018.

[26] P. Mateus, F. Moura, and J. Rasga, "Transferring proofs of zero-knowledge systems with quantum correlations," in *Proceedings of the 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, p. 9p. 9, January 2007.

[27] A. Broadbent, Z. Ji, F. Song, and J. Watrous, "Zero-knowledge proof systems for QMA," in *Proceedings of the 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 31–40, NY, Heidelberg, October 2016.

[28] *EUROCRYPT'92 Advances in Cryptology-*, 2020, https://www.bookdepository.com/Advances-Cryptology-EUROCRYPT-92-Rainer-Rueppel/9783540564133.

[29] M. Bellare and O. Goldreich, "On probabilistic versus deterministic provers in the definition of proofs of knowledge," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, D. Zuckerman and O. Goldreich, Eds., Springer, Berlin, Heidelberg, pp. 114–123, 2011.

[30] L. E. B. Salasar, J. G. Leite, and F. Louzada, "Likelihood-based inference for population size in a capture-recapture experiment with varying probabilities from occasion to occasion," *Brazilian Journal of Probability and Statistics*, vol. 30, no. 1, pp. 47–69, 2016.

[31] Z. Wan, Y. Zhou, and K. Ren, "Zk-AuthFeed: protecting data feed to smart contracts with authenticated zero knowledge proof," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. –1, p. 1, 2022.

[32] H. Ryu, D. Kang, and D. Won, "On a partially verifiable multiparty multi-argument zero-knowledge proof," in *Proceedings of the 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, pp. 1–8, Heidelberg, China, January 2021.

[33] Y.-H. Chen, C.-Q. Ye, and P. Zhang, "Efficient group signature scheme based on RSA cryptosystem," in *Proceedings of the 2006 International Conference on Computing & Informatics*, pp. 1–3, NY, USA, June 2006.

[34] Y. Lu, S. Wu, Z. Fang, N. Xiong, S. Yoon, and D. S. Park, "Exploring finger vein based personal authentication for secure IoT," *Future Generation Computer Systems*, vol. 77, pp. 149–160, 2017.

[35] O. Baudron, P.-A. Fouque, D. Pointcheval, J. Stern, and G. Poupard, "Practical multi-candidate election system," in *Proceedings of the twentieth annual ACM symposium on Principles of distributed computing-PODC'01*, pp. 274–283, New York, NY, USA, December 2001.

[36] Z. Fei, K. Liu, B. Huang, Y. Zheng, and X. Xiang, "Dirichlet process mixture model based nonparametric Bayesian modeling and variational inference," in *Proceedings of the 2019 Chinese Automation Congress (CAC)*, pp. 3048–3051, Henan, China, Augest 2019.

[37] T. Shen, F. Wang, K. Chen, K. Wang, and B. Li, "Efficient leveled (multi) identity-based fully homomorphic encryption schemes," *IEEE Access*, vol. 7, pp. 79299–79310, 2019.

[38] T. Miyamae, F. Kozakura, M. Nakamura et al., "ZGridBC: zero-knowledge proof based scalable and private blockchain platform for smart grid," in *Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–3, China, February 2021.

[39] A. Pathak, T. Patil, S. Pawar, P. Raut, and S. Khairnar, "Secure authentication using zero knowledge proof," in *Proceedings of the 2021 Asian Conference on Innovation in Technology (ASIANCON)*, pp. 1–8, Heidelberg, China, December 2021.

[40] O. Goldreich, M. Sudan, and L. Trevisan, "From logarithmic advice to single-bit advice," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, L. Avigad, M. Bellare, Z. Brakerski et al., Eds., Springer, Berlin, Heidelberg, pp. 109–113, 2011.

[41] A. Broadbent and A. B. Grilo, "QMA-hardness of consistency of local density matrices with applications to quantum zero-knowledge," in *Proceedings of the 2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 196–205, Berlin, Heidelberg, Augest 2020.

[42] W. Lin, X. Zhang, Q. Cui, and Z. Zhang, "Blockchain based unified authentication with zero-knowledge proof in heterogeneous MEC," in *Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Heidelberg, June 2021.

[43] O. Goldreich and D. Zuckerman, "Another Proof that $\mathcal{BPP}\subseteq \mathcal{PH}$ (and More)," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, L. Avigad, M. Bellare, Z. Brakerski et al., Eds., Springer, Berlin, Heidelberg, pp. 40–53, 2011.

[44] V. Aleksieva, H. Valchanov, and A. Huliyan, "Implementation of smart-contract, based on hyperledger fabric blockchain," in *Proceedings of the 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA)*, pp. 1–4, Berlin, Heidelberg, June 2020.

[45] J. Kim and A. Yun, "Secure fully homomorphic authenticated encryption," *IEEE Access*, vol. 9, pp. 107279–107297, 2021.

[46] M. Mohan, M. K. K. Devi, and V. J. Prakash, "Homomorphic encryption-state of the art," in *Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2)*, pp. 1–6, NY, USA, June 2017.

[47] C. Jiang and C. Ru, "Application of blockchain technology in supply chain finance," in *Proceedings of the 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, pp. 1342–1345, Zhengzhou, China, September 2020.

[48] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: an overview and recent trends," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 42–52, 2013.