Private Blockchain Interoperability: a Case Study of Interoperable Verification for Professional Assessment Certification

1st Thada Jaipradite
School of Information Technology
King Mongkut's University of Technology Thonburi
Bangkok, Thailand
thada.ja@mail.kmutt.ac.th

2nd Narongrit Waraporn
School of Information Technology
King Mongkut's University of Technology Thonburi
Bangkok, Thailand
narongrit@sit.kmutt.ac.th

3rd Pichet Limvachiranan
School of Information Technology
King Mongkut's University of Technology Thonburi
Bangkok, Thailand
pichet@sit.kmutt.ac.th

***Abstract*— Many researches have aimed to create a model of interoperability between blockchains that can exchange data or assets with each other. However, the current interoperability between blockchains need to improve on the consistency across blockchains. The optimization on blockchain verification should be considered. Also, the exchange of data should maintain a decentralized principle. Interoperability blockchain should avoid the third-party agent on verification. This research presents a private blockchain interoperability model allowing nodes within the blockchain to participate in verifying and signing data for maintain its integrity. It eliminates the need of the third-party agent for the verification. Key commitments are used to validate the keys exchanged between blockchains. Finally, we applied the model to a case study of interoperable verification for a professional assessment certification between two organizations by using our separate private blockchains. The experimental results can verify the exam taker scores correctly. The result of assessment was interoperable recorded at the blockchain of both organizations when the verification is correct.**

Keywords—Blockchain Interoperability, Threshold Signature, Commitment, Certificate System

I. INTRODUCTION

Blockchain technology has evolved and found applications in various fields, which can be categorized into different eras as follows: Blockchain 1.0: This era marked the advent of digital currencies like Bitcoin, primarily used for the exchange and transfer of assets. Blockchain 2.0: In this era, blockchain technology expanded beyond basic digital currency transactions. It began serving as the foundational framework for broader economic and financial systems, extending beyond simple money exchange. One of the pivotal developments in Blockchain 2.0 is the introduction of smart contracts. These programmable contracts allow for the definition of more complex transaction conditions. Blockchain 3.0 is an era of blockchain is used in many fields such as marketing, finance, health, science, education, culture government, and also realizing the interconnection of various chains or interoperability blockchain. [1,2]

There are various solutions to achieve interoperable blockchains, such as the Notary Mechanism and Relay/Side Chain. However, a problem with these solutions is the presence of intermediaries in data exchange. Another problem with blockchain interoperability lies in the complexity of the exchange process and the structures of blockchains, which may vary and serve different purposes across various organizations. For example, two organizations want to create something that requires collaboration between them. However, they operate on separate blockchains, have different roles in the collaboration, and intend to record the data on either blockchain. Due to these cases, data exchange between blockchains becomes difficult and complicated. [3] Furthermore, for blockchains to collaborate and exchange information, a reliable and secure process must be established for data exchange.

Therefore, this research proposes a model of interoperability between private blockchains that can work together automatically without third parties to verification in order to be completely decentralized. Additional implement a model as a case study of interoperable verification for a professional assessment certification to demonstrate the data exchange process between blockchains. Simulate two organizations that wish to issue interoperable certificates. They have distinct roles and utilize separate blockchains. One organization provides exam taking services, while the other handles exam evaluation by receiving exam taking-data from the first organization. Afterward, they record the evaluation result for use as certificates on either blockchain. Furthermore, users can search for certifications using a certification ID.

In this paper, we explain the methodology that can be used to confirm the fact among blockchains in section 2. In sections 3 we explain the methodology of blockchain interoperability with a case study of interoperable verification for a professional assessment certification. We implement a certificate verification application and show it in section 4. We conclude the process of blockchain interoperability in section 5.

II. COMPONENTS OF INTEROPERABLE BLOCKCHAIN

In this section, explain the background and basics of blockchain interoperability and the technologies that can enhance security when exchange data, such as threshold signatures and Pedersen Commitments, which are intended for use in the proposed model. Additionally, summarize previous research on blockchain interoperability, including concepts and technologies that have been utilized.

A. Interoperable Blockchain

Private blockchains that are used to maintain the privacy or confidentiality of data, and each organization develops its own blockchain for its own work. But interoperability is necessary in collaboration between blockchains with seamless integration [4] and communication should be of secure and transparent manner without affecting security [5]. Therefore, the methods for data exchange are still difficult and complicated, and there is no stable method. The exchange should not have any third party verification in order to be completely decentralized [6].

979-8-3503-3094-6/24/$31.00 ©2024 IEEE

[7] categorized interoperability approaches in blockchain into five categories; sidechains, notary schemes, hashed time lock contracts, relays, and blockchain-agnostic protocols. They evaluated each category by using popular cross-chain protocols within each category. Experiments indicated that the latency depends on the block time of the blockchain and the security requirements of the cross-chain protocol. Their performance of the cross-chain protocol was limited by the performance of the underlying blockchain. Additionally, the cost of the cross-chain protocol depends on the interaction with the smart contract. Notably, Hashed Timelock Contracts (HTLC) [8] incurred higher costs for both deployment and invocation of smart contracts. Protocols that only require blockchain settlements tend to have lower costs.

There are many studies that researches blockchain interoperability models, for example: [3] proposed interoperability architecture of blockchains with trusted services called InterTrust. They proposed a model of trustworthy blockchain interoperability by using threshold signature. The threshold signature relies on the verification of both interoperative blockchains during data exchange. If the exchange process is not completed, the transaction will not be recorded on the blockchain as the atomic swap. [9] uses the atomic swap principle and the threshold signature for data exchanging over the Ethereum private sidechains with atomic cross-chain. Moreover, [10] also proposed a method for the interoperability of public and private blockchains. One of the limitations of private blockchains is the ability to communicate with external blockchains. This authors of [10] demonstrated the interoperability between public and private blockchain by letting public blockchains function as a gateway for connecting with cloud consumers. Requests were sent from the public blockchain to the private blockchain where transactions were verified during the exchange by using multiple signatures to guarantee trustworthiness. [11] proposed exchanging assets across blockchains in case of different assets are used on different blockchains. Relay Chain was used as an intermediary blockchain to convert assets in the consistency with the destination blockchain. It confirmed the authenticity of the person along with records of the user's information. Moreover, interoperability does not solely depend on blockchain-to-blockchain connections, but it can also extend to interactions between blockchain and traditional systems. For instance, ZeroTrustBlock, [12], proposed blockchain that aimed to integrate with existing systems like Electronic Health Records (EHRs). The confidentiality of sensitive data, such as patients' medical records, is paramount over the traditional systems of the centralized databases. It raises the risk of a single point of failure and susceptibility to cyberattacks. ZeroTrustBlock addressed this concern by leveraging blockchain technology and seamlessly integrating the EHRs without causing disruptions. Integration gateways that utilize the HL7 FHIR standard interfaces, establish connections between blockchain storage and EHRs. Furthermore, the implementation involved smart contracts and a hybrid on/off-chain storage approach to manage permissions for accessing confidential data. To enhance storage capabilities, ZeroTrustBlock employed IPFS decentralized storage off-chain to expand storage capacity and accommodate files such as image reports. Their consensus protocol relied on a RAFT-based consensus. It is optimized for high throughput when compares to the Proof of Work, and ensured the efficiency and the security of data processing.

B. Atomic Swap

Atomicity principles in database systems are the management of events that occur when changes are made that must be completed or not performed at all. For example, if a data processing error occurs that causes the transaction to be incomplete, some processes must be canceled or restarted. We can apply the atomicity principles as solution in blockchain interoperability [13], which is called atomic swap, in order to maintain the integrity and consistency of data, The most commonly used method for the atomic swap is Hashed Timelock Contract (HTLC) [8]. By locking assets and specifying the time and conditions for releasing the lock.

C. Threshold Signature

Data exchanging between blockchains requires authenticity, non-repudiation, and integrity [3]. The threshold signature can meet these requirements. Participants in the blockchain must participate in signing transactions for, at least, the specified criteria. Participants in the blockchain must actively engage in signing transactions that meet specified criteria. The private key is divided into secret keys for each participant. Each participant will generate a partial digital signature using their secret key. If a participant is absent during the data signing, and the total number of participants is less than specified criteria, the final signature created from the partial signatures will be incomplete. This incomplete signature won't be able to decrypt the original data. Collaboration among participants on data signing and verification by threshold signature can prevent any node for being an intermediary [14]. Therefore, there is no need to rely on third parties on blockchain interoperability. Moreover, digital signature can increase security and reliability during data exchange.

Threshold signature has three fundamental functions similar to a digital signature:

1) Key Generation: Initially, a public key is generated for verification purposes. Subsequently, the private key is divided into multiple secret keys, which are distributed to nodes. Each node's secret keys is kept confidential, preventing the recovery of the original private key

2) Signing: Each node generates a partial signature using their received secret key to sign the data. These partial signatures are then collected and combined into one.

3) Verification: The public key generated in the key generation process is used to verify the validity of the collected signature.

D. Pedersen Commitment

When distributing sensitive information such as secret keys to individual nodes, the recipient cannot guarantee the validity of the provided secret. In order to verify the confidentiality, interoperability blockchain should apply the commitment, instead of sending the secret directly. Commitment is generated by the secret holder or sender. It is then sent over a private network channel to the recipient so that the recipient can use the commitment to, later, validate the received secret. According to Pedersen Commitment [15], the recipient cannot decrypt the commitment to view the secret before later receiving the secret from the sender for validation. The commitment process details start with the sender creating commitment and a random number from secret. Subsequently, the sender sends commitment to the receiver for later validation. Afterward, the sender reveals the random number and the secret. The receiver then validates the secret by utilizing the secret and the random number through a commitment algorithm. The results must match the commitments received. [16] used Pedersen Commitment to validate secret keys of the threshold signature that were sent between nodes for the voting-based blockchain interoperability.

III. SYSTEM DESIGN

Professional certificates have been adopted in various industry in order to confirm the professionalship of workforce in industry. However, confirmation of professionalship over the paper or electronic file can be falsified. Verification over the reliable system using blockchain would be trusted in professional industry.

Professional certificates issued by a single organization could be simply relied on the blockchain infrastructure for the trusted certificates. However, the online learning platforms mostly collaborate with other professional vendors or expert in order to teach and assess the learners. Their certificates issued to the learners should be trusted by both online learning platform and the professional vendor. Therefore, we proposed the interoperability between cooperative blockchains in order to verify the certificate by both agents.

Our proposed interoperative blockchain applied the trust services of InterTrust [3] in interoperability architecture with the secret key of threshold signature to secure the secrecy of messages. Our secret key utilizes Pedersen Commitment [8] to verify its validity. Two blockchain infrastructure will interoperate seamlessly with trustworthy to all participants. The components of our proposed method are in the autonomous system running on our verification procedure. The proposed model supports atomic swaps by utilizing signal sending to indicate operations between autonomous systems. Furthermore, it employs threshold signatures to sign data for verification purposes.

A. Autonomous System

The autonomous system composed of nodes built-in with the interoperable blockchain. It was implemented with various APIs in order to proceed our collaborative verification procedure between nodes.

- Blockchain is the bottom line infrastructure of each node. It stores its own records regarding to its role such as assessment results or exam questions. Each blockchain works independently from another blockchain.
- Node in autonomous system of collaborative blockchains are responsible to verify the transaction and communicate among nodes within its blockchain. Each node also has private and public keys for the digital signature.
- Gateway node is a chosen node among nodes within each blockchain. This node is a gateway of the blockchain to request the verification of the transaction which is not under its role. The transaction will be sent to verify with the gateway node of another blockchain who is under the responsible role of the transaction. For example, one blockchain has responsibility for certificate verification while another blockchain has responsibility for assessment. Both blockchains will request the not-own-role verification via its gateway node to the gateway of another blockchain as shown in Fig. 1.

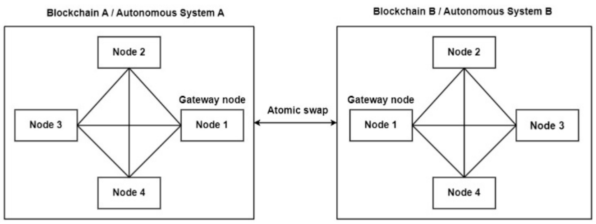


Fig. 1. Overall autonomous system

B. Interoperability blockchain with a case study of interoperable verification for a professional assessment certification

For the interoperability blockchain model, major components needed for interoperable verification are autonomous system, gateway, secret key, and commitment.

- Autonomous System, AS, contains nodes in each interoperable blockchain.
- Gateway, G, is a trusted node working as gateway that transfers data between autonomous system.
- Secret Key, SK, is the key created from the threshold signature process is used to sign data and generate a partial signature.
- C (Commitment) is an operation to verify the received secret key.

In case study, we setup two organizations having a separated blockchain on different roles. Organization A is for the exam taking while organization B is to evaluate the answer of questions. When exam taker finishes the examination at organization A, blockchain in organization A will send exam-taking data to the blockchain of organization B for exam evaluation. When the exam evaluation is finished, the result will be recorded at both organizations A, and B. We will call the organization A that provides exam testing services as Initial and the organization B that provides exam evaluation services as Settle.

1) Setup initial data: Upon exam submission, the exam-taking data is forwarded to $G_{Initial}$ to begin the initial data setup operation. This step involves preparing essential data necessary for participating in data signing. Initially, $G_{Initial}$ requests commitments (C_{Settle}) from G_{Settle} to subsequently validate SK_{Settle}. Afterwards, $G_{Initial}$ will send $C_{Initial}$ along with the request for SK_{Settle} to G_{Settle}. The $C_{Initial}$ will be used by Blockchain $_{Settle}$ to validate the later received $SK_{Initial}$. Upon receiving enough distinct SK_{Settle} for the member in $AS_{Initial}$ and successfully validating it, $G_{Initial}$ proceeds to send SK_{Settle}, C_{Settle}, and raw data (exam-taking data) to members in $AS_{Initial}$ for the subsequent data signing operation.

2) Locking exam data: Upon receiving data from $G_{Initial}$, each node in $AS_{Initial}$ will proceed to lock the raw data by signing it using the received SK_{Settle} and its own private key. This process of locking the data involves securely holding the raw data until a signal is received from Blockchain $_{Settle}$, indicating the subsequent operation for the raw data. Once the data signing is completed, each node will send the raw data signature back to $G_{Initial}$. Subsequently, $G_{Initial}$ will verify these raw data signatures and collect the valid ones. The collected raw data signatures (Signed$_{\text{raw data}}$) and SK$_{\text{Initial}}$ will be sent to G$_{\text{Settle}}$ for further verification.

3) Exam taking verification: In this operation, Blockchain$_{\text{Settle}}$ is responsible for evaluating the results of exam and subsequently sending them back to Blockchain$_{\text{Initial}}$. The process begins with G$_{\text{Settle}}$ receiving data from G$_{\text{Initial}}$, after which it validates SK$_{\text{Initial}}$ and evaluates the exam results. Subsequently, G$_{\text{Settle}}$ forwards the data to AS$_{\text{Settle}}$ for a secondary evaluation. If AS$_{\text{Settle}}$ successfully evaluates the results of the examination, they will transmit an unlock signal (Signal$_{\text{final}}$) back to G$_{\text{Settle}}$. Once G$_{\text{Settle}}$ receives the unlock signals from AS$_{\text{Settle}}$ that meets the specified criteria, it proceeds to record the evaluation results in the internal blockchain. Then, G$_{\text{Settle}}$ sends both the collected signal and evaluation results (Settle$_{\text{final}}$) back to G$_{\text{Initial}}$ for the next operation. If AS$_{\text{Settle}}$ fails to evaluate the examination result, they will transmit an abort signal to G$_{\text{Settle}}$ instead.

4) Signal verification: Upon Blockchain$_{\text{Initial}}$ receiving Settle$_{\text{final}}$ from Blockchain$_{\text{Settle}}$, G$_{\text{Initial}}$ will initiate signal verification. This operation involves verifying the received signal and subsequently choosing an action to either record or not record the result of evaluation, depending on the received signal. The process begins with G$_{\text{Initial}}$ verifying the received signal and then transmitting it to AS$_{\text{Initial}}$ for verification by each node. Upon G$_{\text{Initial}}$ receiving verified unlock signals from AS$_{\text{Initial}}$ that meet the specified criteria, it will proceed to record the evaluation results on the internal blockchain. Subsequently, it will move to the final operation to complete the data exchange. If the verified signals from AS$_{\text{Initial}}$ are abort signals, G$_{\text{Initial}}$ will proceed to the final operation without recording the evaluation results.

5) Finish exchange data: The operational process involves the deletion of unused commitments to clear storage and complete the data exchange. G$_{\text{Initial}}$ will send the request to delete the commitments to G$_{\text{Settle}}$. At that point, G$_{\text{Settle}}$ will delete the commitments and respond to G$_{\text{Initial}}$. Subsequently, G$_{\text{Initial}}$ will also delete the commitments as shown in Fig. 2.

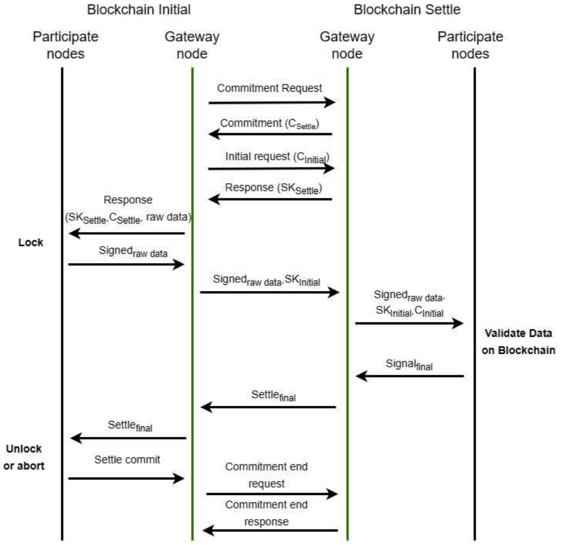


Fig. 2. Interoperability model process

IV. Result

A. Trusted data exchange

This model architecture focuses on achieving interoperability among blockchains through the use of threshold signatures, Pedersen Commitments, and our designed processes. This model can enhance the reliability of data exchanged between blockchains. Initially, the verification of the source blockchain involves sending the data to a gateway node before it is forwarded to the destination blockchain. This gateway node is considered a trusted node, as defined by each blockchain. If the gateway node receives an invalid secret key from the destination blockchain (where the secret key does not match the commitment) or receives signature data that does not meet the specified criteria, the gateway node will cancel sending the data to the destination blockchain. However, if all verification results are valid, the gateway node will proceed to send the data to the destination blockchain and continue the process. This verification process ensures the validity of the data being sent. Additionally, on the destination blockchain's side, the verification process involves validating the signature data from the source blockchain using the public key of the signer and the public key of the secret key. Through this process, it ensures that the data originates from the genuine source blockchain.

The process dictates that data must pass through the gateway before it reaches the destination blockchain, which might make the gateway node act as an intermediary. However, the use of threshold signatures can address this issue by preventing any single node from centralizing control. It achieves this by enabling nodes to participate in data signing before data exchange. This active participation ensures that data exchange remains fully decentralized, aligning with the decentralization principles of blockchain technology.

Moreover, in data exchange between blockchain, it can successfully perform atomic swaps by using signal sending and threshold signatures to indicate operations and data signing between blockchain. When the source blockchain sends a signal indicating failed verification (an abort signal), the destination blockchain will also cancel the process accordingly. Instead, the blockchain will send a signal indicating an allowed operation (an unlock signal) if verification passes. This means that this data exchange maintains atomicity in recording data operations among blockchain.

B. Example application system based on case study

In order to test our model, we implemented a professional certification application over the interoperable blockchains. The exam questions were stored and ready to be taken at the examination proctor on one side of the blockchain interoperability. However, the exam questions and their solutions were created earlier by the professional vendor on another side of blockchain interoperability.

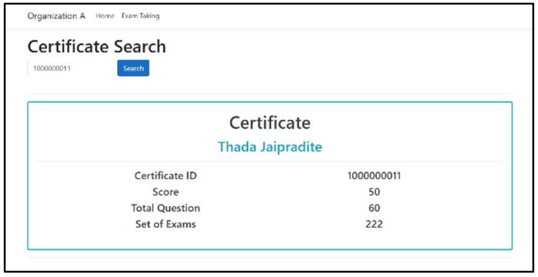
When the exam taker wants to be professional certified, he/she has to take the exam at the exam proctor site. However, the exam proctor does not have solutions of the exam. The exam proctor must collaborate with professional vendor by sending the answers of exam taker to the professional vendor to evaluate the answer.

The result of the evaluation will be stored at blockchain of the professional vendor. In order to maintain the reliability of certification, the result of the evaluation was also sent back to exam proctor and stored into the blockchain of the exam proctor. Exam takers can reveal the result of the evaluation to any chosen person. The chosen person can request the result from any blockchain. For further implementation, we aim to enhance the interoperable blockchain to verify results with another blockchain, ensuring the maintenance of reliable data.

The professional certification application was developed in order to test of our interoperability model regarding to business of professional certification verification. It can be divided into two functions; exam taking function and certificate confirmation function.

1) Exam taking function: The exam taker or examiner must specify the exam-taking ID, name of test taker and exam series ID. The exam taker then selects the correct answer and presses to submit or save the information. The answer of each question will be evaluated for the correctness at the professional vendor's blockchain. The exam-taking ID are unique to any existing ID. If checking exam series ID or exam-taking ID is incorrect, all processes will be canceled. Before data is sent between sites, the sending site will first sign the data using the secret keys of the receiving site. Before using the secret key to sign the data, the sending site will validate the secret key through a commitment process. If the professional site successfully evaluates the answers, it will send an unlock signal along with the evaluation results to the proctor site for recording. However, if the evaluation fails, it will send an abort signal to instruct the proctor site to cancel the operation.

2) Certificate confirmation function: This function allows users to browse for professional certificates by entering the certificate ID. Then, the application will send the request to the blockchain. The consensus among nodes on the blockchain will return the certificate ID, exam taker's name, score obtained, and the exam series ID, as shown in Fig. 3.



Certificate Search

1000000011

Certificate

Thada Jaipradite

Certificate ID	1000000011
Score	50
Total Question	60
Set of Exams	222

Fig. 3. Certificate or exam result searching function

V. CONCLUSION

The blockchain interoperability model consists of the process of sending data to be verified, recording on the destination blockchain, acknowledging back to the source blockchain, and, at last, recording on the source blockchain. Our data exchanging process used threshold signature, where nodes signed the data and verified the data together to ensure data consistency. It could prevent any nodes from being an intermediary. It, also, eliminated the need to rely on the third-party agency. Pedersen Commitment was used to verify the correctness of the secret keys sent between blockchains.

Moreover, signal sending and threshold signatures can achieve atomic swaps during data exchange by using signals. These signals will indicate the operation of the destination blockchain according to the source blockchain. It will ensure that the final result is identical between blockchains.

In addition, our model was applied to the case study of interoperable verification for a professional assessment certification. The exam-taking data such as answers of exam taker was sent to professional vendor's blockchain in order to evaluate the result and recording on this blockchain. Then, the evaluation results were sent back and recorded on the proctor's blockchain. The result of the experimental model worked correctly according to the entire process through case studies. As a result, interoperable blockchains can exchange the verified data confidentially, reliably, and correctly without third-party agency involving in the interoperable process among different nodes participating the data verification.

Our model effectively addresses issues related to verification dependency on the third-party entities and the centralization of the notary mechanism. There's no necessity to establish a new chain for data verification between exchanges through side-chain mechanism. Furthermore, through the InterTrust Service [3], our model significantly enhances the reliability of key exchange operations. We achieved it by employing Pedersen Commitment to validate secret keys before generating a signature. This approach ensures that confidential data, such as keys, attains a higher level of reliability and security in the overall process.

In future work, our goal is to implement our model for web service certification verification between universities and professional organizations. Universities often require the verification of certificates to students through a certification authority. To enhance the value of these certificates, universities can collaborate over API requests to the certification authorities to facilitate the certification verification process that leverages blockchain for secure certificate storage. Ensuring trust and data consistency in the exchange of information between the blockchain is crucial. This model is designed to provide the necessary trust and data consistency for seamless data exchange between blockchains. It establishes a reliable framework for universities and certification authorities to collaborate effectively, enhances the overall integrity and secures the certification verification process.

To enhance the verification process, we can create an interface or abstract class to define the necessary methods for verification. This entity would act as a parent for all objects that need the verification. Subsequently, to implement this approach, one can create an object requiring verification and ensure it adheres to the methods specified by the parent class. For instance, a certificate application of a learning institute such as school or university can create a certificate object under the verification of the guidelines set by the parent class of the department of higher education of the country. This systematic approach allows for the effective verification of various object types by following the structure provided by the verifiable parent class as shown in Fig. 4.

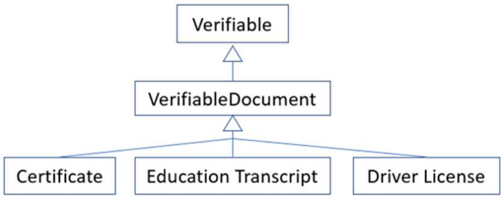


Fig. 4. Verifiable class for the verfication among academic institures

REFERENCE

[1] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," in 8th Annual International Conference on Biologically Inspired Cognitive Architectures BICA 2017. ScienceDirect, 2017, pp. 116–121.

[2] S. Lin, Y. Kong, S. Nie, W. Xie and J. Du, "Research on cross-chain technology of blockchain," in 2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA). IEEE, 2021, pp. 405-408.

[3] G. Wang and M. Nixon, "InterTrust: towards an efficient blockchain interoperability architecture with trusted services," in 2021 IEEE International Conference on Blockchain (Blockchain), 2021, pp. 150–159.

[4] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," IEEE Access, vol. 7, pp. 45201-45218, 2022.

[5] W. Yang, S. Garg, A. Raza, D. Herbert and B. Kang, "Blockchain: trends and future," in Pacific Rim Knowledge Acquisition Workshop. Springer, 2018, pp. 201-210.

[6] S. Choudhari, S. K. Das and S. Parasher, "Interoperable blockchain solution for digital identity management," in 2021 6th International Conference for Convergence in Technology (I2CT). IEEE, 2021, pp. 1–6.

[7] K. Ren, N. Ho, D. Loghin, T. Nguyen, B. C. Ooi, Q. Ta and F. Zhu, "Interoperability in blockchain: a survey," IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 12, pp. 12750-12769, 2023.

[8] J. Poon and T. Dryja, "The bitcoin lightning network: scalable off-chain instant payments," URL: https://lightning.network/lightning-networkpaper.pdf, pp. 30-31, 2016.

[9] P. Robinson, R. Ramesh and S. Johnson, "Atomic crosschain transactions for Ethereum private sidechains," Blockchain: Research and Applications, vol. 3, no. 1, pp. 1-17, 2022.

[10] B. C. Ghosh, T. Bhartia, S. K. Addya and S. Chakraborty, "Leveraging public-private blockchain interoperability for closed consortium interfacing," in IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, 2021, pp. 1-10.

[11] X. Wang, W. Qiu, L. Zeng, H. Wang, Y. Yao and D. He, "A credible transfer method of cross-chain assets based on DID and VC", in 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE), 2021, pp. 238-242.

[12] P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned blockchain," Big Data Cogn. Comput., vol. 7, no. 4, 2023.

[13] S. Zhu, C. Chi and Y. Liu, "A study on the challenges and solutions of blockchain interoperability," China Communications, vol. 20, no. 6, pp. 148–165, 2023.

[14] A. Afshar and C. Heart, "Threshold digital signatures: how to keep your crypto secure," Built In, Jan. 11, 2022. [Online]. Available : https://builtin.com/blockchain/threshold-digital-signatures-crypto. [Accessed: Apr. 5, 2022].

[15] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in Annual international cryptology conference. Springer, 1991, pp. 129–140.

[16] M. Sober, G. Scaffino, C. Spanring and S. Schulte, "A voting-based blockchain interoperability oracle," in 2021 IEEE International Conference on Blockchain (Blockchain), 2021, pp. 160-169.