Faculty of Science
SRINAKHARINWIROT UNIVERSITY

VDegree: Verifiable Credential-Based Digital Transcript Verification System Using Blockchain Technology

Thanagrit Banjongsilp, Parintorn Panditiyangkun, Pranitan Wittayaronnayutt, Asst Prof. Chantri Polprasert

Bechelor of Science Program in Computer Science

ABSTRACT

At present, fake transcripts are considered one of the most damaging problems globally due to lack of appropriate inspection processes and easy-to-access tools to generate counterfeit certificates. In addition, the conventional process to request transcripts from several academic institutions is slow and inefficient. In this work, we investigate a proof-of-concept (PoC) of the online digital transcript service called VDegree. With VDegree, the system provides a tamper-proof transcript in digital format using blockchain technology. By storing student's encrypted academic transcript in the user's devices, this system helps students easily access, share, manage and verify their transcript. The process of issuing, requesting or verifying the transcript is proposed in the PoC and a Hyperledger Fabric blockchain is developed and tested in the AWS-managed blockchain. We test the performance of our proposed system in the AWS-managed blockchain using bc.t3.medium instance type 2 vCPU 4 GB of RAM and CouchDB as State Database. Simulation results show that our proposed system can process approximately 2.5 transactions per second over a range of number of transactions. The results show promising potential both in the reduction of process and the performance of blockchain for the proposed use case.

BODY OF KNOWLEDGE

Asymmetric Keys

Asymmetric keys is a cryptographic scheme requiring two different keys[1], one to lock or encrypt the plaintext, and one to unlock or decrypt the ciphertext. Neither key will do both functions. One key is published (public key) and the other is kept private (private key).

Blockchain

Blockchain is a specific type of decentralized database that stores data in blocks and chained onto previously filled block[2].

Cryptography

Cryptography refers to secure information and communicationtechniques derived from mathematical concepts and a set of ule-based calculations called algorithms[3], to transform messages in ways that are hard to decipher.

Cloud Computing

Cloud computing is the delivery of different services through the Internet[4]. These resources include tools and applications like data storage, servers, databases, networking, and software. It is a popular option for people and businesses for a number of reasons including cost savings,increased productivity, speed and efficiency, performance,and security.

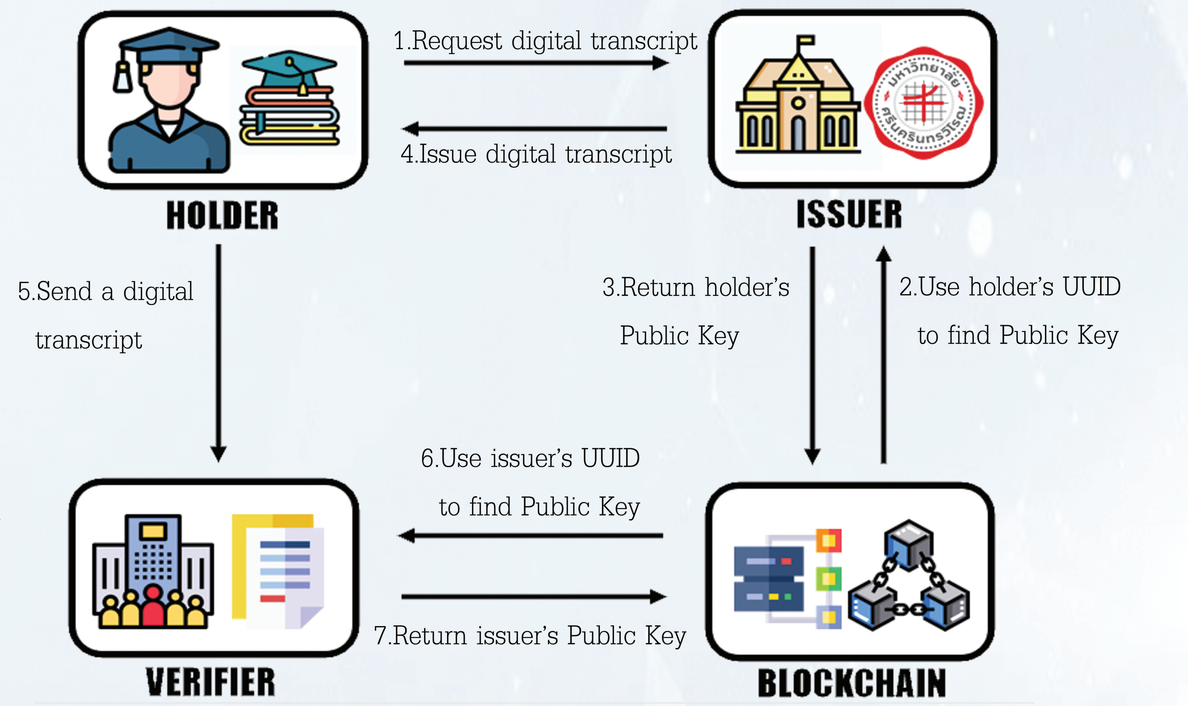
Hyperledger Fabric

Hyperledger Fabric is a modular blockchain framework[5] that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components that are aimed for use within private enterprises.

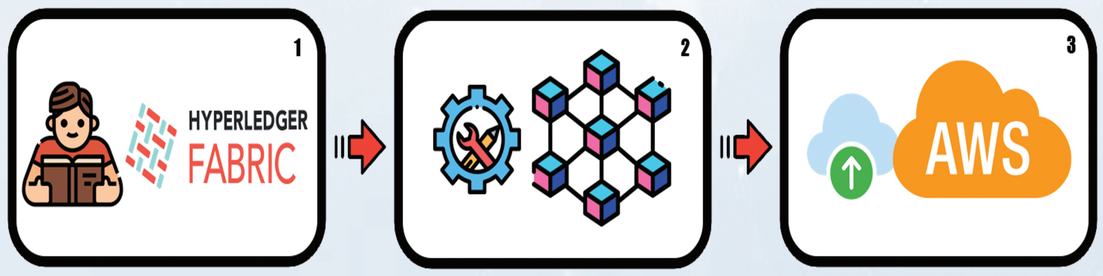
HYPERLEDGER FABRIC

WORKFLOW

*Store UUID and Public Key on Blockchain

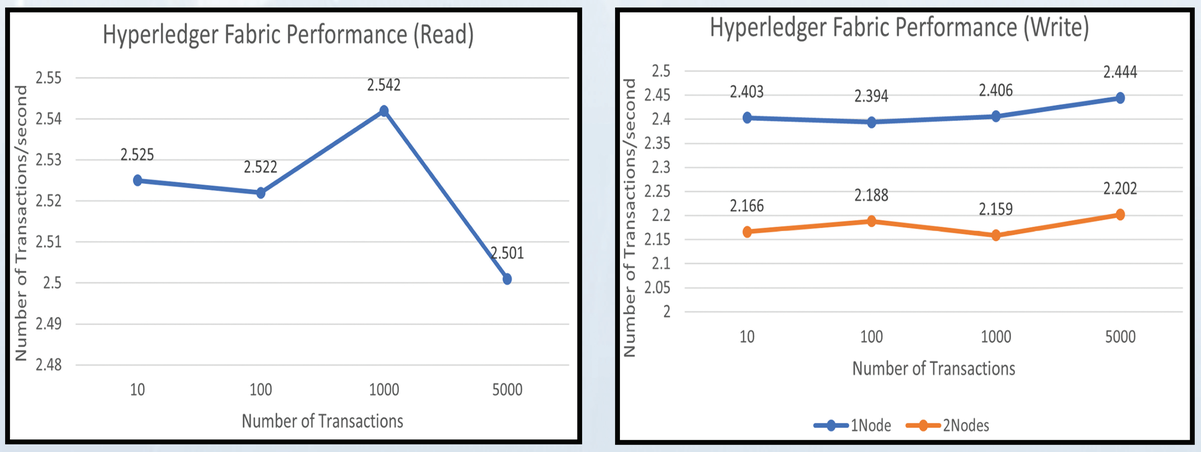


METHODOLOGY



1. Learn about Hyperledger Fabric Blockchain
2. Set up and develop prototype blockchain system for proof of concept
3. Deploy blockchain system on AWS Cloud
4. Develop application for connect to blockchain system
5. Testing performance of blockchain system

RESULTS AND DISCUSSION



Performance of reading and writing data from Blockchain.

CONCLUSION

In this work, we study the application of blockchain in online digital transcript service. We conduct performance analysis focusing on the throughput in terms of a number of completed transactions per second over the AWS-managed blockchain network. Results show that our proposed system can handle at least 2.5 transactions per second over a range of a number of transactions of interest. Hyperledger Fabric was chosen for this system due to its high performance and popularity. Other blockchain such as Ethereum might be more suitable for this application.

REFERENCES

[1] Thales, "What is an Asymmetric Key or Asymmetric Key Cryptography? ," cpl.thalesgroup.com. https://cpl.thalesgroup.com/faq/key-secrets-management/what-asymmetric-key-or-asymmetric-key-cryptography (accessed Mar. 23, 2021).psum

[2] Tanya Sattaya-aphitan, "ทบทวนความรู้เรื่อง Blockchain," Medium, Aug. 28, 2018. https://medium.com/@drtan/ทบทวนความรู้เรื่อง-blockchain-3691dded54a3 (accessed Aug.23, 2020).

[3] K. Richards, "What is cryptography? ," searchsecurity.techtarget.com, Apr. 2020. https://searchsecurity.techtarget.com/definition/cryptography (accessed Mar. 23, 2021).

[4] J. Frankenfield, "Cloud Computing Definition," Investopedia.com, Jul. 28, 2020. https://www.investopedia.com/terms/c/cloud-computing.asp (accessed Mar. 25, 2021).

[5] W. Kenton, "Hyperledger Fabric Definition," Investpedia.com, Feb. 03, 2020. https://www.investopedia.com/terms/h/hyperledger-fabric.asp (accessed Mar. 25, 2021).