COS 720 Documentation

May 25, 2023

1 Introduction

In this project a cryptocurrency was developed that makes use of a private blockchain. The goal of this system is to be used to incentivize specific behaviors or achievements in a company or small organization. This way employees who find traditional rewards not motivating enough can have a new motivating factor to excel in their work. Additionally such a reward system can be immune to fraud, for example an employee trying to claim a reward for work they did not do.

2 Overview of latest developments

A new field of post quantum cryptography is emerging to create cryptographic algorithms that are resistant to attacks from quantum computers. Zero knowledge proofs are being used in blockchain to provide anonymous transactions and identity verification without revealing sensitive data. Schnorr signatures are being proposed as a replacement for ECDSA in Bitcoin as they are more scalable and have better privacy features. To enable secure and private smart contract execution, homomorphic encryption is being considered as a possible solution. Multi-party computation is a cryptographic technique proving useful in cryptocurrencies to enable secure and private voting in consensus mechanisms.

3 What cryptography in blockchain entails

Cryptography in blockchain entails the use of digital signatures, one way hashes and public-key cryptography to enable integrity and trust in the blockchain.

4 Review of related work

Lin et al[1] provide an overview of the applications of blockchain in the agricultural sector. One of the applications proposed of interest is that of improving the efficiency of trade finance in the supply chain. Such a system could provide proof of payments, automated payments and dispute handling. Additionally

there are greater profits for the parties involved because of the reduction in expensive third party fees.

Yang et al[2] explore the application of private and public blockchains in the construction industry. Some areas of interest include automated conditional construction payment and blockchain enabled contract management. Smart contracts can be used with cryptocurrencies to provide protection against withheld payments and individuals not paying on time as the smart contracts are self-executed without any intermediaries.

Ramachandran et al[3] explore the use of blockchain in human resource management. One useful application is that of reducing costs in the recruitment process. This is done by providing faster and cheaper verification of a candidate's requirements through the use of the blockchain.

5 Research Overview

System feature + reference	Feature Description
Structure of blockchain(Zhai et al[4],Raikwar et al[5]	Each block consists of the following: 1. Merkle Tree root hash 2. Timestamp 3. Previous block hash 4. nonce 5. Block hash 6. mining difficulty level
Merkle Tree(Wang et al[6])	Verifies the integrity of lots of transactions quickly(See Figure 1).
Hashing algorithm(Pittalia[7],Gilbert et al[8])	• SHA256 is used which is collision resistant and resistant to collision search attacks.
Digital Signatures(Saho et al[9], Fang et al[10])	• RSA is used over ECC because of faster encryption times • Private keys used for generating transaction signatures • A certificate authority is used for secure public key distribution
Threat Models to secure against(Rawal et al[11],Zhang et al[12])	• Dictionary attack by using double hashing • Sybil and impersonation attack by using Certificate Authority(CA) • DDoS attack by only allowing users registered with CA to participate in blockchain • Hijacking attack by using digital signatures • Double spending through the use of an account nonce
Proof of work(Nakamoto[13])	• Integer representing a 'difficulty" level used to determine how many 0's a hash of a block should start with before being mined. • The difficulty level increases up to a maximum threshold

Table 1: Table showing system overview

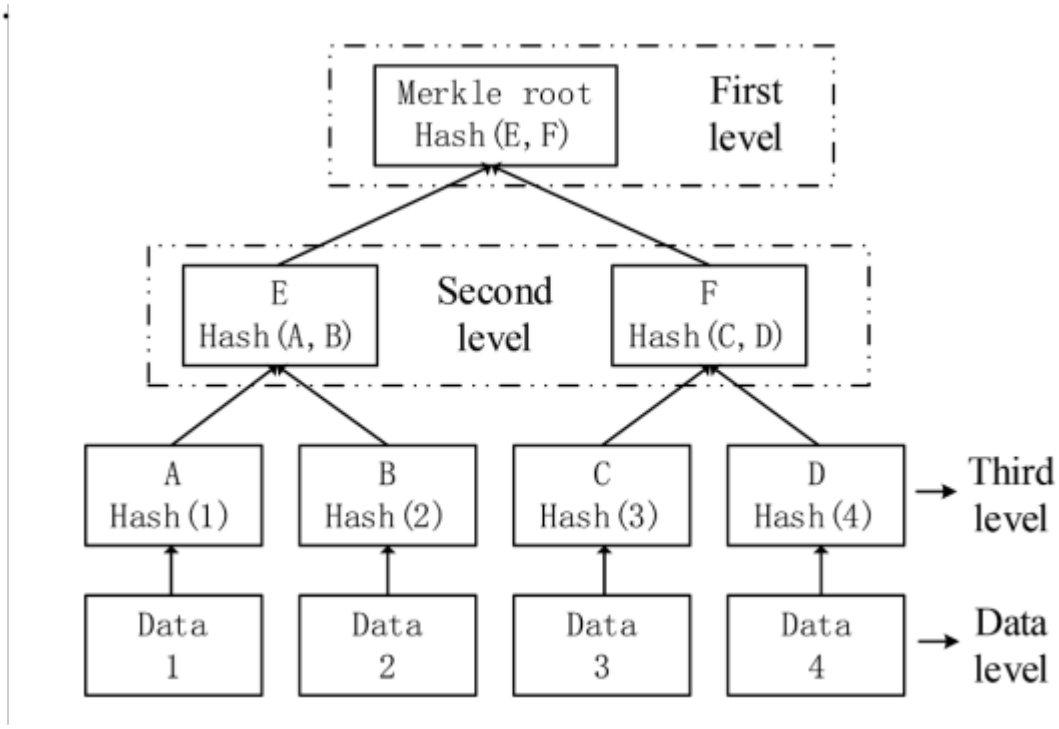

Figure 1: Merkle Tree

6 Requirements Specification

1. The system must allow a user to be able to verify the public key of another user to ensure that person is who they claim they are through the use of a Certificate Authority.
2. The system must maintain the integrity of the transaction data using hashes.
3. The system must allow for non repudiation when it comes to transactions through the use of digital signatures.
4. The system must be able to quickly verify the integrity of all the transactions in a block by making use of a merkle tree.
5. The system must prevent the possibility of double spending occurring through the use of an account nonce.
6. The system must be relatively quick to respond through the use of efficient algorithms and data structures.
7. The system must allow users to mine blocks and progressively make it more difficult to mine blocks as the number of blocks in the blockchain increases. The difficulty will be limited to a maximum threshold.
8. The system must allow for two factor authentication when individuals are authenticating themselves to the Certificate Authority.
9. The system must maintain the integrity of the blockchain by verifying that the previous blocks have not been tampered with when a new block is added to the blockchain.
10. The system must reject transactions from any users that are not part of the company/organization who might have illegally gained access. This is done by only allowing users who have been authenticated by the Certificate Authority to participate.

7 System UML Diagrams

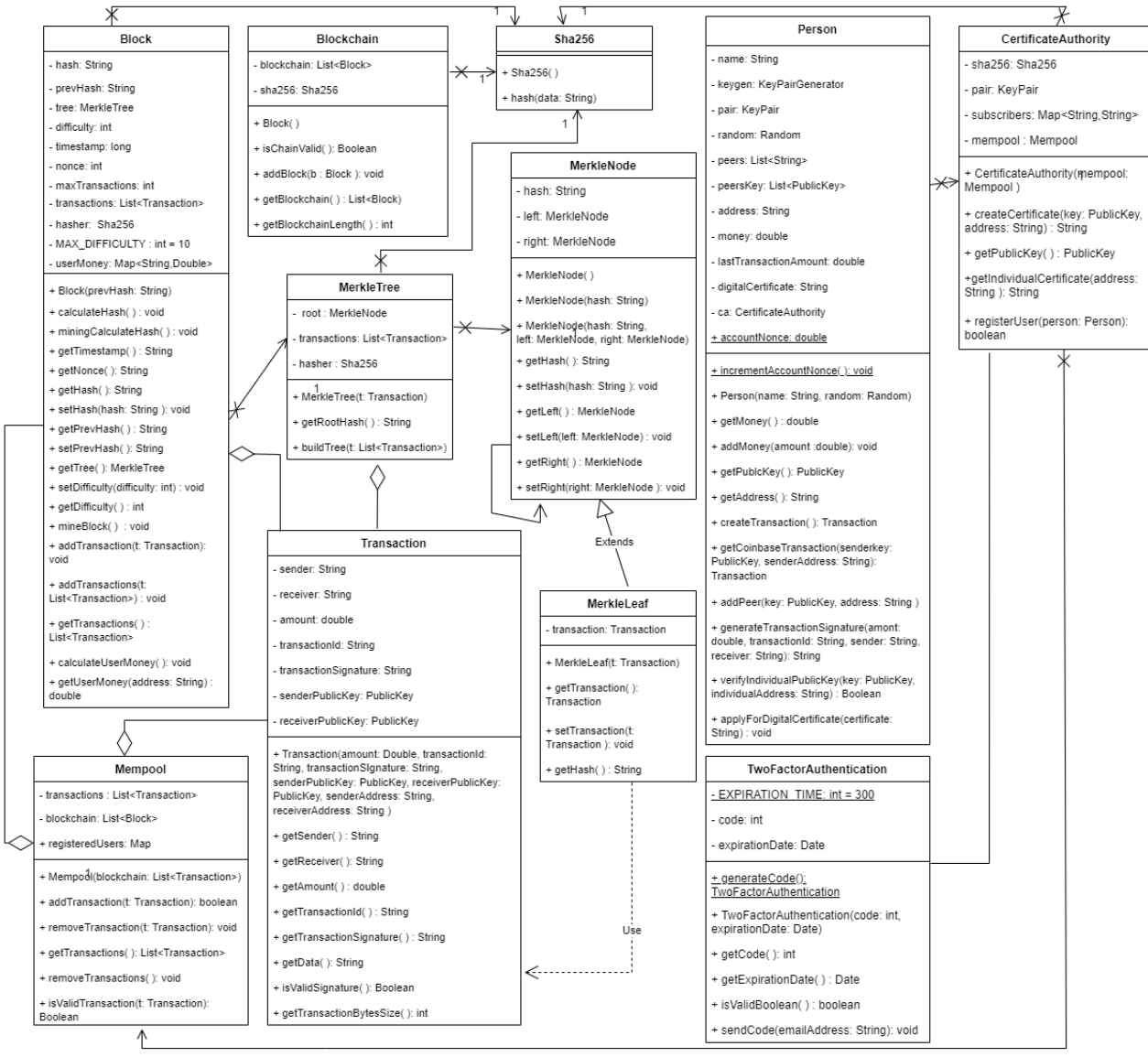

Figure 2: System UML Class Diagram

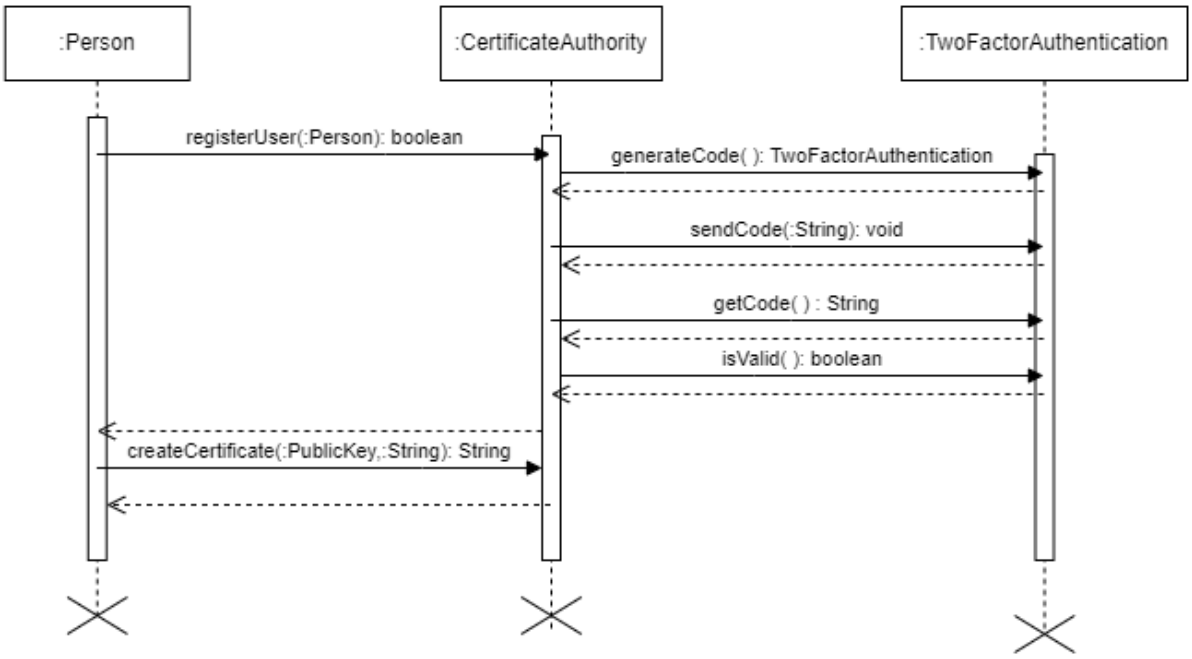

Figure 3: Sequence diagram showing user registration

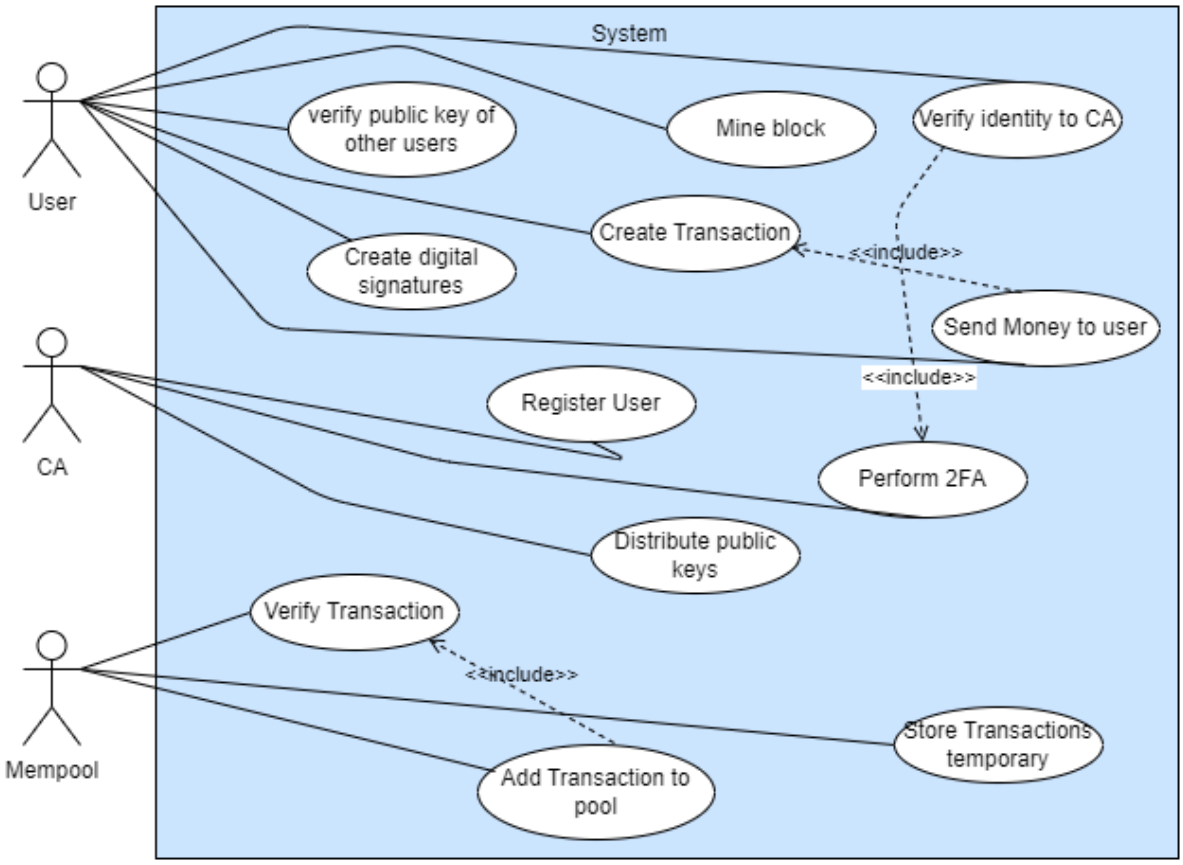

Figure 4: Use case diagram of system

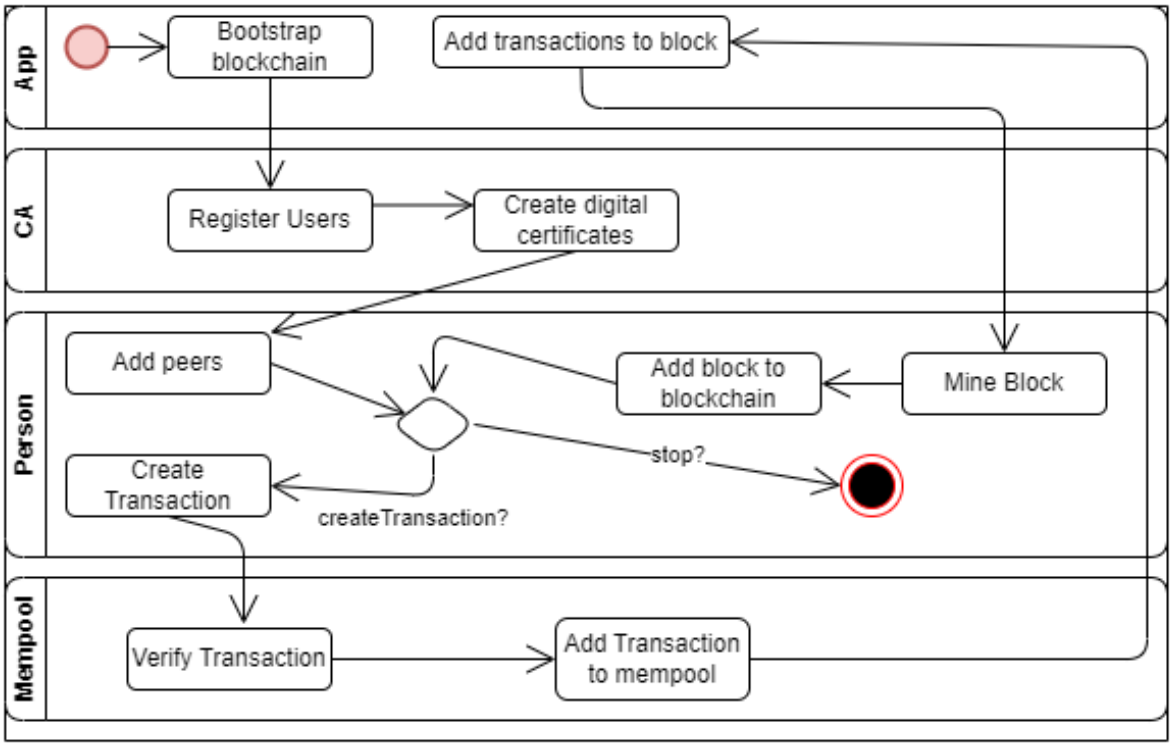

Figure 5: Activity Diagram of system

8 External Packages used in project

1. Java package for implementations of cryptographic algorithms: `https://mvnrepository.com/artifact/org.bouncycastle/bcprov-jdk15on/1.70`

2. For sending emails the following 2 packages where used:

- `https://jar-download.com/?search_box=javax.activation`

- `https://javaee.github.io/javamail/`

References

[1] W. Lin, X. Huang, H. Fang, V. Wang, Y. Hua, J. Wang, H. Yin, D. Yi, and L. Yau, "Blockchain Technology in Current Agricultural Systems: From Techniques to Applications," *IEEE Access*, vol. 8, pp. 143920–143937, 2020.

[2] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe, and S. Chen, "Public and private blockchain in construc-

tion business process and information integration," *Automation in Construction*, vol. 118, p. 103276, Oct. 2020.

[3] R. Ramachandran, V. Babu, and V. P. Murugesan, "The role of blockchain technology in the process of decision-making in human resource management: a review and future research agenda," *Business Process Management Journal*, vol. 29, pp. 116–139, Jan. 2022. Publisher: Emerald Publishing Limited.

[4] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the Application of Cryptography on the Blockchain," *J. Phys.: Conf. Ser.*, vol. 1168, p. 032077, Feb. 2019.

[5] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of Used Cryptography in Blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019.

[6] J. Wang, B. Wei, J. Zhang, X. Yu, and P. K. Sharma, "An optimized transaction verification method for trustworthy blockchain-enabled IIoT," *Ad Hoc Networks*, vol. 119, p. 102526, Aug. 2021.

[7] P. Pittalia, "A Comparative Study of Hash Algorithms in Cryptography," *IJCSMC*, vol. IJCSMC, 8, June 2019.

[8] H. Gilbert and H. Handschuh, "Security Analysis of SHA-256 and Sisters," in *Selected Areas in Cryptography* (T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, O. Nierstrasz, C. Pandu Rangan, B. Steffen, D. Terzopoulos, D. Tygar, M. Y. Vardi, M. Matsui, and R. J. Zuccherato, eds.), vol. 3006, pp. 175–193, Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. Series Title: Lecture Notes in Computer Science.

[9] N. J. G. Saho and E. C. Ezin, "Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm," 2020.

[10] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," *J Wireless Com Network*, vol. 2020, p. 56, Dec. 2020.

[11] B. S. Rawal, P. M., G. Manogaran, and M. Hamdi, "Multi-Tier Stack of Block Chain with Proxy Re-Encryption Method Scheme on the Internet of Things Platform," *ACM Trans. Internet Technol.*, vol. 22, pp. 1–20, May 2022.

[12] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *ACM Comput. Surv.*, vol. 52, pp. 1–34, May 2020.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System,"