

cos 720 pROJECT

Computer Information & Security



May 19, 2023

**Name: MHL Moloantoa**

**Student No.: u22809695**

Contents

[Cryptography in Block-chain: Implementation in Cryptocurrency systems 2](#_Toc135936359)

[Requirements Specification 3](#_Toc135936360)

[UML design diagrams 4](#_Toc135936361)

[Domain Model for user 4](#_Toc135936362)

[Domain Model for Blockchain 4](#_Toc135936363)

[Domain Model for verifyNTransact 5](#_Toc135936364)

[Domain Model for AdsNStories 5](#_Toc135936365)

[System UML Model 6](#_Toc135936366)

[Table of Technology 7](#_Toc135936367)

[References 8](#_Toc135936368)

# Cryptography in Block-chain: Implementation in Cryptocurrency systems

Blockchain is a distributed encrypted record or ledger that enables its vendors to securely distribute the original data; if a vendor tries to modify, change, alter, edit, copy, or duplicate any part of the data on it, all the vendors will be made aware of it, and the chain will become corrupted. That is made possible by the blockchain's use of cryptography and hashing (Nakamoto 2008).

Blockchain technology depends on cryptography as a core or key factor to assure the security of the users’ data and transactions. Security in the blockchain is based on two ideas: cryptography and hashing (Christidis & Devetsikiotis 2016). Cryptography is a method of protecting, safeguarding transactions and data from unauthorized users by utilizing code to secure the data, by altering it into an unreadable format that can only be translated by authorized parties, it is a two-way function that can be reversed (Swan 2015).

On the other hand, hashing utilizes a hash function to alters data into a fixed-length string, it is used to ensure that a file or piece of data is valid and unaltered (Yang et al. 2020). Hashing is irreversible, meaning that the plaintext is scrambled into a unique digest that cannot be decrypted (Guegan 2017).

In cryptocurrency systems, cryptography and hashing are implemented to provide secure transactions and authentication (Zheng et al. 2018). They are used to create digital signatures that verify the authenticity of that data (Berners-Lee 2012). Cryptography ensures that cryptocurrency systems are resistant to fraud, tampering, and unauthorized access, providing users with confidence in the security and privacy of their digital assets and transactions (Zhou et al.2011).

Cryptography in blockchain involves using code and mathematical algorithms to secure transactions, data, and protect user privacy within the decentralized network, making it a crucial element in maintaining the security and trustworthiness of the blockchain and Cryptocurrency systems (Lai & Chuen 2018).

Incorporating Cryptography and Cryptocurrency entails that data systems will have more validated information and transactions, in our case, we will create an online web application that uses Cryptography, Hashing and Cryptocurrency to assist Non-governmental organizations (NGOs), charities and crowdfunding’s get the funding and donations through a reliable, secure and trustworthy platform that’s efficient and takes out the middle man.

The web application will assist people and make their lives convenient by offering funding at a push of a button. No more waiting in queues and list at Non-governmental organizations (NGOs) and charities, the web application is available 24/7 and it saves time. The web app enables the users to posts about their needs or course then philanthropist can see and donate to their cause using the web application. The web app posts are stored on a blockchain in the web application to ensure that its temper proof and are also digitally signed for verification.

# Requirements Specification

* **FR 1.** The system should allow users to link their metamask to the system
* **FR 2.** Contribution and donation Mechanism
  + Users should be able to contribute funds to crowdfunding’s, Non-governmental organizations (NGOs) and charities using cryptocurrencies or fiat currencies.
  + The system will provide a secure payment gateway for transactions.
* **FR 3.** Security and Privacy:
  + The system will implement security measures to protect user data, transactions, and funds.
  + The system will maintain User privacy, and personal information will be handled securely.
  + The system will follow best practices for data encryption and secure communication.
* **FR 4.** Project/Posts Creation:
  + The system should allow Users to be able to create new crowdfunding projects.
  + Projects should include a detailed description.
  + The System should allow users to encrypt their posts on the system.
* **FR 5.** The system should Authenticate using blockchain and metamask technology to ensure the security of user data.
* **FR 6.** The system should provide digital signatures using metamask sign function/algorithm to ensure the integrity of user data.

# UML design diagrams

## Domain Model for user

The user subsystem is responsible for the users.

**Key points:**

* To be a user you must first have a metamask account to make transactions on the system.
* The user must log in to metamask to gain access to the web application’s transactions functionality.

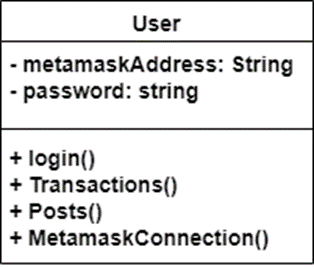


Figure 1: Subsystem Domain Model for user

## Domain Model for Blockchain

The Blockchain subsystem facilitates user interactions by enabling them to input post messages, apply digital signatures, generate QR codes for the information, and securely store them within an encrypted linked list.

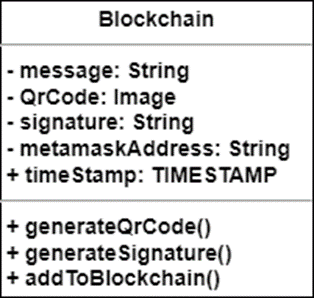
* For users to apply digital signatures they must have a MetaMask account.
* The user must Install the MetaMask browser extension on your preferred web browser.
* 

Figure 2: Subsystem Domain Model for blockchain

## Domain Model for verifyNTransact

The verifyNTransact subsystem plays a crucial role in the verification of QR codes and facilitating fund transactions. This subsystem is responsible for verifying the information encoded in the QR codes, ensuring its validity. Additionally, it establishes a connection with your MetaMask account to securely transfer the funds.

* For users to apply digital signatures they must have a MetaMask account.
* The user must Install the MetaMask browser extension on your preferred web browser.
* The user must ensure that their MetaMask wallet has sufficient cryptocurrency funds to perform transactions.
* When interacting with web application, carefully review the details presented by Qr – code verifier before approving any transactions.
* Verify the recipient address and amount to ensure accuracy and security.

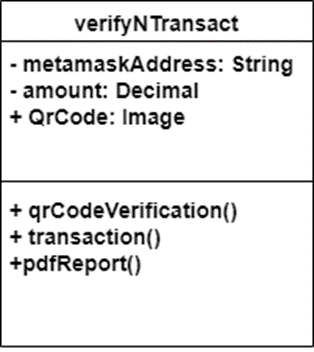


Figure 3: Subsystem Domain Model for verifyNTransact

## Domain Model for AdsNStories

The adsNStories Subsystem enables users to create and share stories and advertisements, ensuring privacy by encrypting them and restricting access only to authorized users possessing the secret passcode associated with each post. Furthermore, the system employs encryption for every post created, enhancing data security and confidentiality.

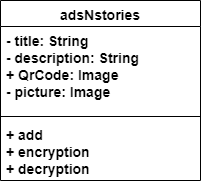


Figure 4: Subsystem Domain Model for Post

# System UML Model

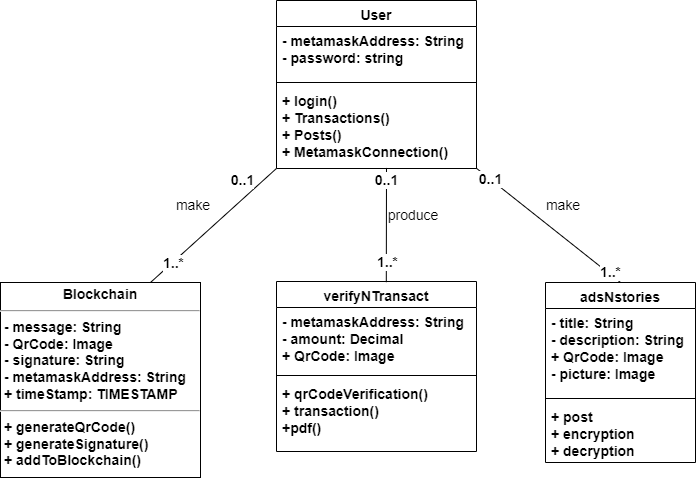


Figure 5: System Domain Model

# Table of Technology

|  |  |  |
| --- | --- | --- |
| **Name of used Technology:** | **Explanation (why did you use this specific Technology)** | **alternatives** |
| Development frameworks:   * **React.js** | * React.js uses a component-based architecture, allowing for a breakdown of the code into reusable, self-contained and structured components. * React.js has a large ecosystem with a wide variety of third-party libraries and packages. Many of these libraries, such as Web3.js, Ethers.js, or crypto-js which will be used in this project. | * Angular: * Vue.js: * Django: * ASP.NET * Express.js: * Spring Boot: |
| Hash Algorithm:   * **SHA-256** | * SHA-256 generates a hash value of 256 bits (32 bytes), striking a favourable equilibrium between security and computational efficiency. On the other hand, SHA-512 imposes greater computational demands, while SHA-224 yields a smaller hash space and possibly diminished security owing to its reduced output size | * SHA-512 * SHA-224 |
| Symmetric encryption algorithm:   * **AES (Advanced Encryption Standard)** | * the same key is used for both encryption and decryption. This simplifies the implementation and makes it efficient for encrypting and decrypting large amounts of data. | * Asymmetric Encryption |

# References

Berners-Lee, T. J. (2012), Information management: A proposal, Technicalreport.

Christidis, K. & Devetsikiotis, M. (2016), ‘Blockchains and smart contracts for the internet of things’, *Ieee Access* **4**, 2292–2303.

Guegan, D. (2017), ‘Public blockchain versus private blockhain’.

Lai, R. & Chuen, D. L. K. (2018), Blockchain–from public to private, *in* ‘Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2’, Elsevier, pp. 145–177.

Nakamoto, S. (2008), ‘Bitcoin: A peer-to-peer electronic cash system’, *Decentralized Business Review* p. 21260.

Swan, M. (2015), *Blockchain: Blueprint for a new economy*, ” O’Reilly Media,

Inc.”.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G. & Chen, S. (2020), ‘Public and private blockchain in construction business process and information integration’, *Automation in construction* **118**, 103276.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017), An overview of blockchain technology: Architecture, consensus, and future trends, *in* ‘2017 IEEE international congress on big data (BigData congress)’, Ieee, pp. 557– 564.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. & Wang, H. (2018), ‘Blockchain challenges and opportunities: A survey’, *International Journal of Web and Grid* *Services* **14**(4), 352–375.

Zhou, X. and Tang, X., 2011, August. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology (Vol. 2, pp. 1118-1121). IEEE.