Pay with Crypto

Emre Kaan Satış - Mehmet Berat Öztürk

Introduction

Existing payment systems use centralized authority for approving or reviewing transactions. In today's world, almost all businesses use POS systems to take their payments. The system which customers use when paying via credit or debit cards is called a point of sale (POS). These systems are making up the most commonly used infrastructure in the world today. They became purely digital, taking payment from all around the world and help shop owners to track all the transactions easily. But this system has some major drawbacks, such as costly software upgrades, less convenience than web-based systems, the problems caused by the hardware, not being secure enough, and don't have transparency. Unlike typical software updates that we use every day to applications in our mobile phones or computers, POS system's updates are not free. Also, centralized payment systems such as Visa and Mastercard cut fees between %1-2.5. This makes the payment processing services unnecessarily expensive and inconvenient. Beside all these problems, today's payment system is extremely harmful to the world. Numerous servers, high number of credit card production and receipt usage resulting in depleting the earth's resources day by day. Given that the world's resources are limited, it is urgent to transition into a healthier system for everyone. Using blockchain technology in payment systems can help solve most of these problems. [1]

Overview

In today's world, blockchain technologies are all around us. We are using them in our daily lives more and more every day. Right now, cryptocurrencies are one of the most used assets in trading. But their aim was to be a tool in the payment sector as it suggests in Bitcoin whitepaper. Pay with Crypto will offer a worldwide on-chain payment solution. This document provides high level information about Pay with Crypto POS and Pay with Crypto App. Pay with Crypto is the name of an infrastructure solution for the payment system which is designed to replace existing centralized payment methods for better security, low operational costs, faster transaction speeds, easier supervision for governments and reducing harm to ecosystem. The project aims to have fast transactions, secure connection, and ease of usage.

The whole system can be used on all EVM based blockchains for transactions and has a new encryption solution for privacy concerns occurring with usage of blockchain technology for payment systems. For the project, Avalanche Network will be used because of its high-speed transactions and low gas(transaction fee). During the tests, Fuji Test Network was used, as proposed.

Mathematical Background

Homomorphic Encryption

Homomorphic encryption enables us to carry out mathematical operations on encrypted data. The term "homomorphic" signifies the transformation of data while preserving the relationships between its elements. This unique property enables mathematical operations to yield the same results in this transformed domain. As a result, we can perform desired operations on ciphertexts while maintaining privacy. We aimed to modify the user's balance by adding or subtracting the transaction amount, without exposing this information to anyone. To accomplish this, we opted for the Paillier Encryption scheme due to its extensive support for operations. [2]

Key generation

1. Two random and independent large prime numbers p and q.
2. Confirm
$$\gcd(p*q,(p-1)*(q-1)=1$$
3. Define $L(x)=x-1n$
4. Compute λ $lcm(p-1,q-1)$
5. Random integer g in the set $Z*n^2$
6. Modular multiplicative inverse
$$\mu=\left(L(g^{\lambda}\ mod\ n^2)\right)^{-1}\ mod\ n$$
7. The public key which will be used in encryption is (n, g)
8. The private key which will be used in decryption is λ.

Encryption

Any m in the range 0 ≤ m < n. m is the message to be encrypted.
1. Random number r in the range 0 < r < n.
2. Ciphertext
$$c=g^m*r^n\ \ mod\ n^2$$

Addition

Multiplication of two ciphertext results in addition of plaintexts:

$$c_1*c_2=m_1+m_2$$

Multiplication

A ciphertext raised to the power of a plaintext results in multiplication of these two:

$$c_1{}^{m_2}=m_1*m_2$$

Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) provide a strategy for handling large numbers, which is especially useful in cryptographic scenarios or modular arithmetic.

In the project, very large numbers were used in additions during money transfers. Most of the homomorphic encryption methods has a value limitation and zero-knowledge proof algorithms cannot extend a specific size in their inputs. CRT was used to mitigate this problem by breaking the problem into more digestible pieces. Dealing with these little pieces first, then computing the total value in the other end. [3]

Two large coprime numbers p and q.

$$x=a\ (mod\ p)$$
$$x=b\ (mod\ q)$$

Has a unique solution for x modulo pq.

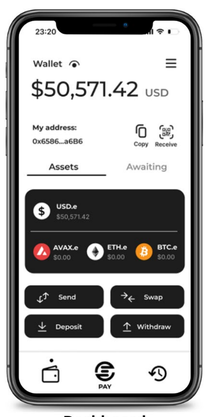
For example:

$$x=6\ (mod\ 9)$$
$$x=4\ (mod\ 11)$$

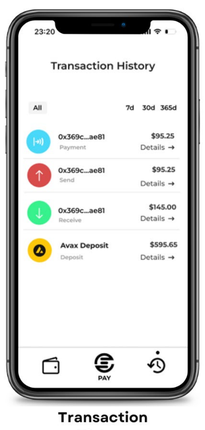
resulting in

$$x=15\ (mod\ 99)$$

Results



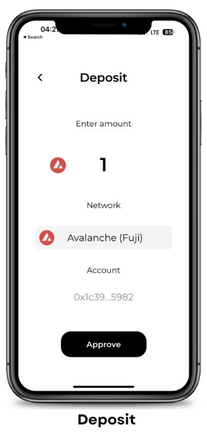
Dashboard



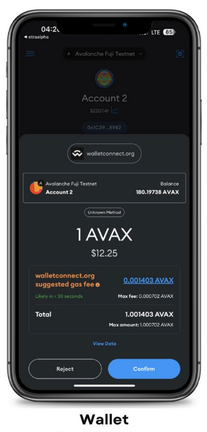
Transaction History

Dashboard gives detailed information about the user's wallet. User can send-receive money, make deposit and payment, withdraw coming transactions from this page. Using this page user can logout and reach his personal settings such as notifications.

Transaction History page shows a history about last payments. Users can see the incoming and outgoing transactions. With a simple click, the user can access all the necessary information about a payment such as detailed date or virtual receipt.

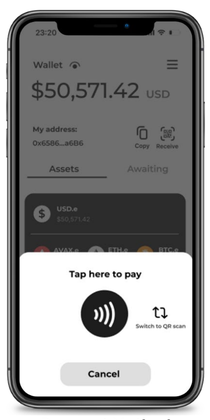


Deposit

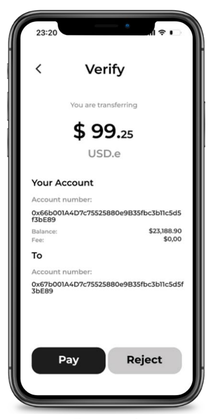


Wallet Confirmation

User can deposit money to his account using Deposit page, accessible from the main menu. Tokens can be deposited to the system from any crypto wallet. Transaction needs to be confirmed inside the used wallet app, giving users one last check. Deposited tokens are exchanged to stable coins before deposited inside the app. Therefore, user doesn't get effected by the changes in the value.



Payment Method Selection



Payment Confirmation

Two different payment methods can be used to pay. NFC scanning and QR code method implemented inside the app. With a simple tap with NFC to the POS machine, the user can start the payment process. In payment confirmation page, user can see the exact amount of money demanded from him. By pushing the Pay button, he allows the app to initiate the payment process. POS starts to listen the network and when it captures the payment event coming from the exact user, the process is complete.

POS Device App

A lightweight POS app that can be installed into all Android devices. It supports NFC and QR code scanning.

Conclusions

In the first semester, we finished designing our mobile app and did a lot of research on important topics. This helped us figure out what tools and resources we would need for the next steps of our project. In the second semester, we completed the app for our Point of Sale (POS) device and added Near Field Communication (NFC) functionality, as per our plan. We also got the payment system to work in a test environment using a tool called Hardhat. This was a big step for us and allowed us to find and fix issues before using the system for real. In recent months, we added blockchain technology to our mobile app and POS device. This technology makes our system secure and trustworthy. Next, we're going to connect all these parts to form a complete system. After that, we'll test everything to make sure it works properly. If we find any problems or areas that can be improved, we'll make those changes. So far, we've been able to do everything on time, as per our plans proposed earlier. We've also achieved all the goals we set for ourselves at the start of the project. Our project is about creating a payment system using blockchain technology. This system keeps the details of everyone involved in a transaction, as well as the amount of money transferred, private. Our system also respects government rules. When needed, we can decrypt information to follow legal requirements. This ensures our system is not just secure, but also responsible and law-abiding.

References

[1] "The Key Disadvantages Of POS Systems | National Processing." https://nationalprocessing.com/blog/the-key-disadvantages-of-pos-systems (accessed Oct. 13, 2022).

[2] "What is the Paillier cryptosystem?" https://blog.openmined.org/the-paillier-cryptosystem/ (accessed Jun. 22, 2023).

[3] "Number Theory - The Chinese Remainder Theorem." https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html (accessed Jun. 22, 2023).