Decentralized Crypto Exchange

Abhilash John
20MCA401 - S4 MCA

Guide by: NATHEERA BEEVI M

Introduction

- Centralized crypto exchanges provides users with the convenience of managing funds and conducting transactions using cryptocurrency, it also brings about some security risks.
- The best way to solve these problem is to adopt a distributed cryptocurrency exchange scheme, which is also in line with the idea of decentralization of cryptocurrency.
- A decentralized cryptocurrency exchange can be implemented using smart contracts based on Ethereum, which can verify different types of cryptocurrency transactions sent by different users.

Related Work

Sl.No	Title of the paper, Journal name, Publisher & Year	Pros	Cons
1.	M. Herlihy, “Atomic cross-chain swaps,” in Proc. ACM Symp. Princ. Distrib. Comput. (PODC), 2018, pp. 245–254	Based on hashed timelocks or signature locks enables secure cross-chain switching	There is limitation in practicality(long waiting time is often incurred during transmission)
2.	Metronome project, Metronome. Accessed: Apr. 2021. [Online]. https://www.metronome.io	Proposed a cryptocurrency called MTN that can be traded across different blockchains	Metronome can only be implemented in blockchains that support smart contracts, and cryptocurrencies that do not support smart contracts thus cannot be exchanged.
3.	A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, and W. Knottenbelt, “XCLAIM: Trustless, interoperable, cryptocurrency backend assets,” in Proc. IEEE Symp. Secur. Privacy (S&P), May 2019, pp. 193–210.	Generic framework for cryptocurrency to achieve untrusted and efficient cross-chain switching.	High gas fees

Related Work

Sl.No	Title of the paper, Journal name, Publisher & Year	Pros	Cons
4.	J. Kwon and E. Buchman. (2016). Cosmos: A Network of Distributed Ledgers. Accessed: Apr. 2021. [Online]. Available: https://cosmos.network/whitepaper	Working to solve the interoperability of blockchains, using the consensus algorithm of Tendermint.	Support the blockchain network that is compatible with Cosmos.
5.	G. Wood. (2016). Polkadot: Vision for a Heterogeneous MultiChain Framework. Accessed: Apr. 2021. [Online]. Available: https://github.com/w3f/polkadot-white-paper/raw/master/PolkaDotPaper.pdf	Working to solve the interoperability of blockchains, using the consensus algorithm of Tendermint.	Support the blockchain network that is compatible with Polkadot.

Gap Identified

- Single point of failure
- Identity Breach Risks
- High exchange fees
- Chances of being hacked
- Mostly supports few cryptocurrency only

Problem Statement

- Centralized crypto exchanges provides users with the convenience of managing funds and conducting transactions using cryptocurrency, it also brings about some security risks.
- Once users keep their properties in a centralized exchange platform, it means that the exchange platform is the “Archilles Heel” of the system which could result in malicious use of users’ properties and transaction information.
- As a central institution, there will always be a single point of failure.

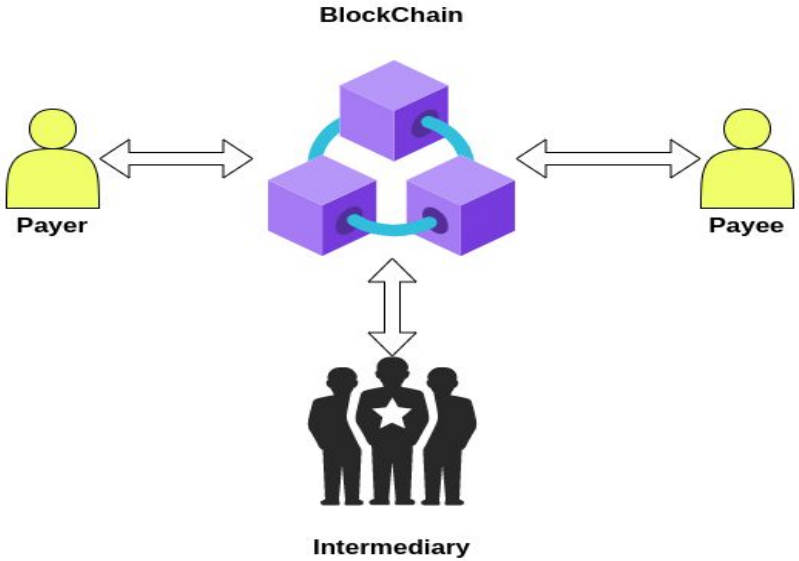
Objective

- Decentralized cross-cryptocurrency exchange scheme based on smart contracts, in which, by using randomly selected users as intermediaries, transactions between any two types of cryptocurrencies can be realized in single-user and multi-User scenarios.
- The exchange will be implemented and deploy on an Ethereum test network.
- Scheme uses smart contracts based on Ethereum to implement a decentralized cross cryptocurrency exchange scheme which can verify different types of cryptocurrency transactions sent by different user

Methodology

System Model

There are four main components in the system model:



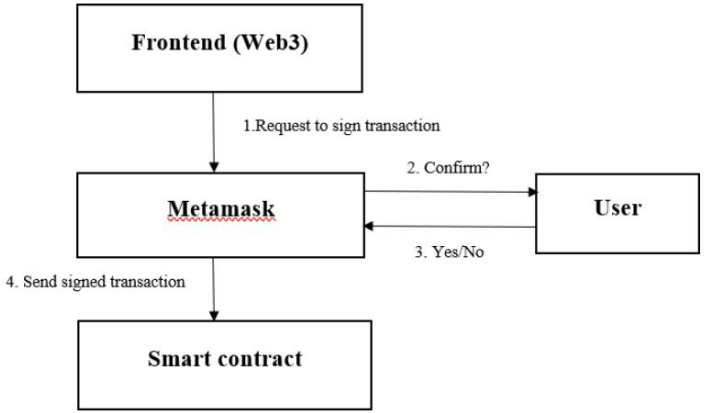
SYMBOL DEFINITION

Symbol	Description
$\mathcal{A}$	The payer of a transaction
$\mathcal{B}$	The payee of a transaction
$\mathcal{C}_1$	The first intermediary of a transaction
$\mathcal{C}_2$	The second intermediary of a transaction
$coin_1$	Cryptocurrency owned by the payer
$coin_2$	Cryptocurrency required by the payee

Methodology

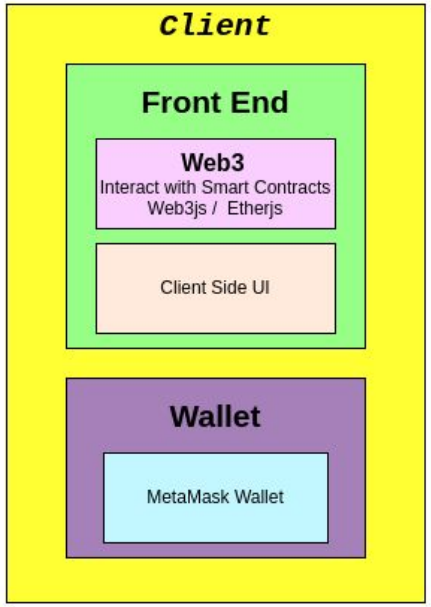
Smart Contracts

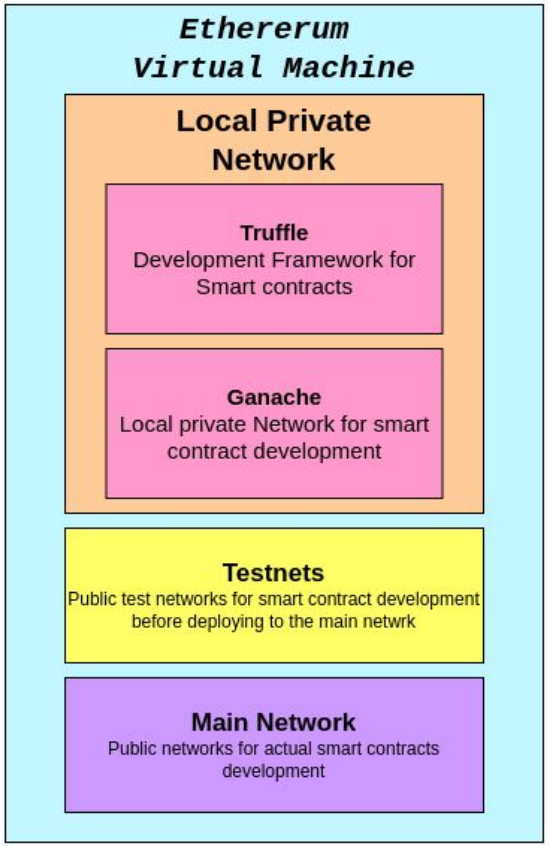
- Smart contracts are codes that can be deployed and executed on a blockchain.
- Developers can send their smart contract codes to the Ethereum network through transactions, which can then be verified by miners and added to the blockchain.
- Any smart contract code saved in the blockchain can be invoked by the users who meet certain conditions.
- In this project, we use Smart contracts based on Ethereum to implement a decentralized cross cryptocurrency exchange scheme which can verify different types of cryptocurrency transactions sent by different users.



Methodology

Modules





Current Features

1. Exchange cryptocurrency between payer and payee
2. Deposit crypto funds to exchange from any wallet

Upcoming Works

1. Swap cryptocurrency
2. Track the price of various crypto currency in real time using candle stick graph

References

[1] H. Tian et al., "Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3928-3941, 2021, doi: 10.1109/TIFS.2021.3096124.

[2] P. Shamili and B. Muruganantham, "Blockchain based Application: Decentralized Financial Technologies for Exchanging Crypto Currency," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-9, doi: 10.1109/ACCAI53970.2022.9752485.

[3] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais and W. Knottenbelt, "XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets," 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 193-210, doi: 10.1109/SP.2019.00085.