TRADERCHAIN PROTOCOL

Decentralized Marketplace for Trading Systems

Hai Minh Nguyen
traderchain.eth
traderchain.org

Abstract. Traderchain is a protocol that allows the creation of a Decentralized Fund (DeFu) whose assets are always secure and available for users to withdraw at any time. Participants of the protocol include fund managers, professional traders, as well as investors will interact with the protocol in a decentralized and trustless manner. All transactions via the protocol are transparent and auditable. Investors' assets are stored in Non-Custodial Vaults in which investors can deposit and withdraw their investment anytime without worrying about fund insolvency. In other words, unlike centralized institutions, a decentralized fund is not in need of proof of reserves as fund assets are always available for audits. Besides, the protocol's liquidity layer is built on top of Decentralized Exchanges (DEX) which provide a safe way for fund managers to exchange their fund assets. Moreover, a particular fund is created as a Non-Fungible Token (NFT) in accordance with EIP-1155 multi token standard, with the purpose of enabling exchange for the shares issued by that fund, which is similar to the mechanism of the Exchange Traded Fund (ETF).

1. Introduction

Stores of Wealth (SoW) in our modern society have come to rely almost exclusively on big centralized financial (CeFi) institutions such as banks, mutual funds, index ETFs and pension funds. While the system works well in a normal economic condition with appropriate liquidity shown on the balance sheets, an economic catastrophe still happens from time to time at the end of an economic cycle or in a black swan event. For example, The 1929 Great Depression with a series of bank runs and the 2008 Financial Crisis [6] with the collapse of many financial institutions were two biggest and well known catastrophic events in the past, and there has not been any reliable solution to prevent them from happening again in the future. One cause of such economic disaster lies in the flaw of a trust based model, in which everyone has no choice but to access a centralized entity to freely control and decide the use of their hard-earned money. Furthermore, almost every country today follows the Fractional Reserve Banking [3], a system of banking operation, in which only a fraction of bank deposits are backed by actual cash on hand and available for withdrawal. This system cannot guarantee the safety and availability of investors' funds all the time, as most of them are lent out or locked in illiquid assets. To make it worse, on March 15, 2020, the Federal Reserve Board even eliminated reserve requirements for all depository institutions by reducing the reserve requirement ratio to zero percent [4]. This action would make the counterparty risk become the highest risk for people's money deposited in any reserve of a centralized financial institution. In the United

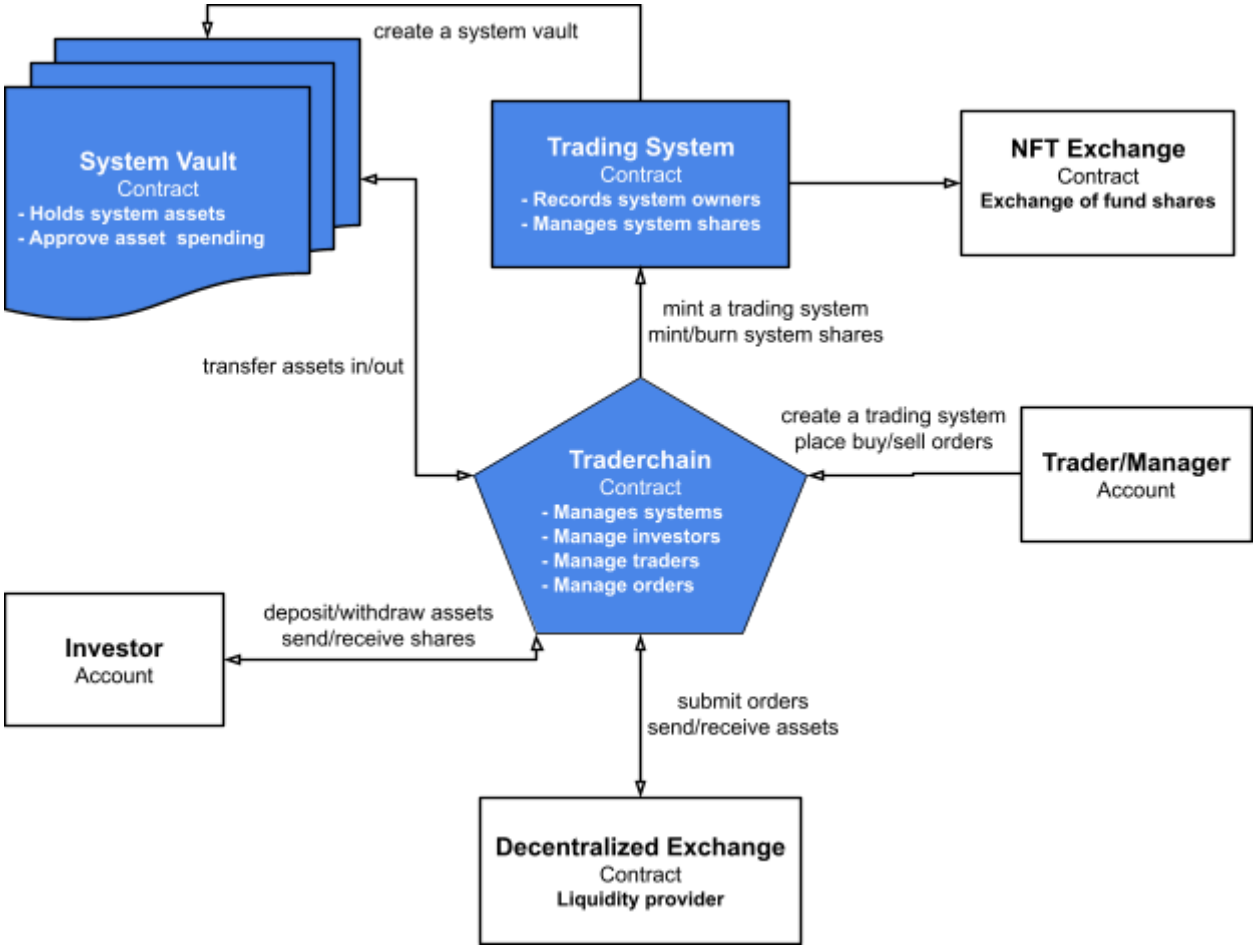
States, the Federal Deposit Insurance Corporation (FDIC) was created to help boost confidence in the American banking system by providing deposit insurance for bank accounts and other assets if financial institutions fail. Their designated reserve ratio is 2% [5] that is supposed to be enough for a normal economic downturn. However, that ratio may not eliminate all the risks, especially in severe crises.

Bitcoin, a decentralized digital currency initially released in 2009, has started a Decentralization movement in the global money and currency market in which a payment transaction can be sent directly from one party to another without going through a centralized financial institution for verification [1]. Later on, Ethereum, a successful decentralized blockchain released in 2015 with the smart contract functionality [2], has proved that the entire financial market including payment transactions, wealth reserves or financial contracts can be governed by codes that are fully decentralized, trustless with significantly less or zero counterparty risk. Followingly, many decentralized financial (DeFi) applications [8] have been built on top of smart contract blockchains, such as Decentralized Stablecoin DAI, Decentralized Exchange Uniswap or Decentralized Lending Protocol Aave and Compound. We believe that DeFi applications will become foundational pillars of the financial infrastructure in the future. A fully decentralized and trustless application has to make sure the funds deposited by customers are noncustodial in which only the owners can make decisions on the use of their assets. In accordance, the rules of how and by whom the funds will be used have to be fixed in smart contracts conforming to a general agreement between all participants. These smart contracts will keep governing all activities regardless of the size of assets or who are the participants. All transactions should be transparent, immutable and auditable. As a result, a user can store his assets in a DeFi application without worrying about its insolvency as no one other than the owner can use the assets for different purposes, unlike the way a traditional financial institution does.

Despite the innovative core value of blockchain technology with its decentralization feature, many crypto projects, while raising the flag of decentralization, ironically operate in the same manner as traditional financial (TradFi) systems do (i.e. customer funds are stored in a centralized financial institution like a bank or trust). Thus, we have witnessed the bankruptcy of Mt. Gox crypto exchange in 2014 and recently the devastating collapse of FTX exchange, followed by its catastrophic contagion to the whole crypto industry. A long list of CeFi companies, Celsius, Voyager, 3AC and others failed and went bankrupt in 2022. The insolvency of FTX fund reserve, similar to a bank run in the traditional financial world, has proved that a crypto project that utilizes blockchain without fundamentally building its system in a decentralized way from the bottom up could not handle the capital management on a large scale in the long run. Among the current projects, DEXs has been serving the community well through the bear market of 2022. Therefore, we build the Traderchain protocol on top of DEXs and make sure our system will be decentralized, trustless, transparent and scalable from the bottom up.

2. Smart Contract Design

Traderchain protocol includes three smart contracts in its core: Traderchain controller contract, Trading System contract and System Vault contract. Firstly, Traderchain controller contract provides external interfaces for investors and fund managers/pro traders to interact with the protocol. Accordingly, investors will deposit and withdraw their investment to a fund via this interface. At the same time, fund managers interact with it to manage their portfolios or configure properties of a fund. Secondly, the Trading System contract defines the structure of a fund and management of its share issuance and redemption. This contract enables a fund and its shares to be traded in any NFT decentralized exchange, reduces the costs of liquidating assets in a redemption process, and gives more flexibility to investors. Thirdly, fund assets are stored in a System Vault contract which declines any direct request from external accounts to transfer assets out. Assets can only be allocated in compliance with a set of rules defined by the protocol contracts.



3. Traderchain Controller Contract

This is the starting point for all state-changing transactions in the protocol. Fund managers/pro traders will interact with the controller contract to create a new trading system, submit orders and request commission payout. On the other hand, investors will interact with this contract to buy and sell shares of a fund. In order to implement these features, the controller contract includes a set of rules to govern how the assets are used or who can send the request. It also records information of owners and investors of the fund and their permissions, as well as provides computation for tracking the fund value and its share price. Furthermore, only internal requests from this contract are permitted to interact with the System Vault contract with the aim of securing assets in the vault, which will be further discussed in Section 5 below.

4. Trading System Contract

Each trading system/fund is a Non-Fungible Token (NFT) conforming to the EIP-1155 smart contract standard [7]. EIP-1155 allows the protocol to issue an amount associated with a token ID that serves as a number of shares for an investment. This will empower the Traderchain protocol to provide two significant features. 1) Allow investors to buy and sell shares of a trading system in the similar way they do to the shares of a mutual fund. 2) Allow investors to trade the shares on a NFT exchange in the similar manner as how an ETF does. We would like to call this the share conversion mechanism and explain the concept as follows:

Once an investor sends his investment to a fund, he will receive a number of shares that are presented as a proof of his deposit. The number of shares can be calculated by the following formula, $New\ Issued\ Shares\ =\ Investment\ Value\ /\ Share\ Price$. The unit of value and price can be set to a base cryptocurrency such as a stablecoin DAI, USDC or any designated cryptocurrency depending on the fund setting. Besides, a new investment will be allocated immediately or at a cutoff time following the fund's current portfolio allocation. Later on, investors can send their shares to the protocol and withdraw their investments. During this redemption process, the protocol will liquidate a portion of the fund assets via a DEX into the base cryptocurrency and send it back to the investor. At the same time, it will burn those disposable shares to make sure that the share price of that system is unchanged.

5. System Vault Contract

A new instance of the System Vault contract will be created for each fund separately to store the assets of that fund for the purpose of better security and easier auditability. Investors can only deposit their assets into or withdraw their investments from the vault via the share conversion mechanism that has been explained in the previous section. There is no external interface exposed in the vault contract so that a user cannot interact with the vault directly. Fund managers/pro traders can only request to use vault assets for trading operations in compliance with their trading systems. In other words, they can never withdraw or use the assets for any other purposes. This is totally different from the traditional asset management in which a bank can lend out investors' money and keep a fractional reserve on their balance sheets. In contrast,

in the Traderchain system, the assets in a vault are always fully reserved and available for the share owner to withdraw anytime. Therefore, investors and fund managers will have no concern for the fund insolvency. In accordance, the performance of a fund will depend on the manager's skills and the effectiveness of his trading system without suffering an unexpected total loss because of a counterparty risk.

6. Fund Value Calculations

Each fund can choose a base cryptocurrency as the unit of account which will be used for accounting and tracking value of the fund and its share price. By default, a high liquidity stablecoin like DAI or USDC will be set as a fund's base cryptocurrency. Followingly, we would like to present the basic formulas for calculating an investment value, a fund's net asset value and its share price for a mutual fund model. (Different fund models will require a slightly different calculation method).

$$Net\ Asset\ Value\ = \sum_{1}^{n} (Value\ of\ Asset_i)$$

$$Share\ Price\ = Net\ Asset\ Value\ /\ Total\ Shares\ in\ Circulation$$

$$New\ Issued\ Shares\ = Investment\ Value\ /\ Share\ Price$$

$$Investor\ Equity\ Value\ = Investor's\ Shares\ \times\ Share\ Price$$

7. Asset Allocation of an Investment

Fund managers can choose a method to allocate a new investment and redeem shares that will replicate a fund's current portfolio allocation in real time or at a cutoff time.

Realtime Asset Allocation: A new investment will be allocated immediately into the assets portionally in line with the current portfolio allocation and these new shares will be issued right away to the investor. When an investor sells shares, a portion of each asset will be liquidated immediately into a base cryptocurrency to be returned to the investor.

Pros:

- This method is simple to implement.
- The value of an investment can correspond to the portfolio performance in realtime.
- Fund managers don't need to manage asset allocation for each new investment.
- It works for small funds that have a few investments and a small number of assets.
- The protocol does not need to hold fees for deferred allocating transactions.

Cons:

- Investors pay higher frontend-load/backend-load fees. However, cheaper transaction fees will help.
- It may require minimum investment if a portfolio has too many assets. We could use a Sampling Replication method to mitigate this problem, such as buying only the top assets which cover 80% of portfolio value.

Cutoff Time Asset Allocation: Any new investment with estimated fees will not be allocated into the fund assets until a cutoff time, e.g. the end of day. In other words, all aggregated investments will be allocated at the cutoff time with only a few transactions for all investors. Investors will receive shares after the allocation process completes. The same mechanism will be applied to the asset liquidation procedures.

Pros:

- Investors may pay less frontend-load/backend-load fees.
- Lower minimum investment for a complex trading system.

Cons:

- This method is more complicated to implement.
- Investors need to wait until cutoff time to receive shares.
- Managers need to manage asset allocation for new investments at cutoff time.
- Small funds that only have a few investments per day do not have much benefit.
- The protocol needs to hold fees for deferred allocating transactions.
- It is hard to estimate the fees accurately in advance as transaction fees fluctuate.

8. Use Cases of Traderchain Protocol

Decentralized Platform for Copy Trading: Investors can follow a successful trading system accurately without actually tracking and managing their portfolio allocation manually.

Decentralized Platform for Mutual Funds: Mutual fund managers can utilize Traderchain Protocol to store funds, replicate portfolios following an index with much lower fees, and manage share issuance and redemption all automatically. On the other hand, investors can receive the benefit of diversification by buying a total index of the cryptocurrency market with just a little of capital.

Decentralized Exchange for ETFs: Shares of a fund can be traded on our specialized DeFu exchange or any other NFT DEX such as OpenSea and Uniswap NFT. It helps increase the fund’s management efficiency and liquidity for the fund's shares. Thus, investors do not need to liquidate their assets reserved in a vault to receive the capital which costs them less transaction fees, especially if the fund is well diversified.

Decentralized Platform for Hedge Funds: Hedge fund managers can utilize Traderchain Protocol to raise funds, set fundraising schedule or set locking period, commissions and so on. In addition, investors that seek high returns can have more opportunities to join a successful trading strategy under a team of professional traders. For example, two simple but effective trading strategies, namely Dollar Cost Averaging (DCA) and Trend Following System, can be fully implemented in a decentralized way via Traderchain protocol.

Decentralized Governance for DAO Funds: A fund manager can be a Decentralized Autonomous Organization (DAO) that governs the investment decisions and execution for a group of investors or a community. Examples of DAO Funds (Squads) [9]:

Friend groups of 2-20 people

Today, a group of friends that want to invest together often pool their money into a single Externally-Owned Account (EOA) wallet (e.g. MetaMask), trusting that the holder of the private keys will keep the group's money safe. This single point of failure is a significant security risk and has caused many friend groups to lose their funds. A DAO fund helps such groups eliminate the trust in one holder and their funds will be secure in a vault with greater transparency.

Investing Communities

Large communities like Web3 communities that desire to invest into NFTs together have a great power of investment given the cumulative capital that could be pooled together. However, they have to deal with slower decision-making, challenges of ownership tracking, legal considerations and membership management over time. In order to resolve these problems, Traderchain Manager DAO will streamline group decision-making quickly on chain before transactions. Moreover, ownership tracking and new contributions are always recorded by default in the protocol.

9. Conclusion

We have designed a protocol to manage a decentralized fund securely and effectively without relying on trust of how the fund assets are reserved. Accordingly, a vault that stores assets for each fund is protected via a controller contract layer which ensures that the fund is secure and is only used for the transactions under the preset consensus among all participants. In addition, as the funds are implemented in compliance with the EIP-1155 standard, any fund manager or investor will have a very flexible and automatic solution to exchange an investment for the fund value and vice versa. In particular, not only can an investor contribute and withdraw his investment anytime, but also trade the fund shares in any NFT exchange for many benefits such as saving loading fees or seeking income from an arbitrage. Furthermore, our system is decentralized from the bottom up with its liquidity provider layer built on top of decentralized exchanges, in order to make sure that all transactions are transparent and auditable. All participants will be confident in their investment and trading decisions when interacting with the Traderchain protocol, for the reason that they do not need to trust on any intermediaries as all outcomes are governed by immutable smart contracts on a blockchain.

References

[1] Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf

[2] Ethereum Whitepaper: https://ethereum.org/en/whitepaper/

[3] Fractional Reserve Banking: https://en.wikipedia.org/wiki/Fractional-reserve_banking

[4] Reserve Requirements: https://www.federalreserve.gov/monetarypolicy/reservereq.htm

[5] FDIC Designated Reserve Ratio:
https://www.fdic.gov/resources/deposit-insurance/deposit-insurance-fund/dif-fund.html

[6] Financial Crisis of 2007: https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%932008

[7] EIP-1155: Multi Token Standard: https://eips.ethereum.org/EIPS/eip-1155

[8] Decentralized Finance: https://en.wikipedia.org/wiki/Decentralized_finance

[9] Squads, example of DAO funds: https://docs.prysm.xyz/getting-started/who-is-using-squads