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 moment. 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. Investor assets are stored in Non-Custodial Vaults in which investors can deposit and withdraw their investment anytime without worrying about fund insolvency. Fund assets are always available for audits, thus no need for proof of reserves like a centralized financial institution. The controller layer of the protocol also makes sure the assets in the vaults can only be used for investing and trading transactions that obey a managed trading system, not for any other purposes. 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. A fund is created as a Non-Fungible Token (NFT) following EIP-1155 multi token standard with the purpose of enabling exchange for the shares issued by a fund 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 and when there is enough liquidity 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. A series of bank runs in 1929 Great Depression or the collapse of many financial institutions in 2008 Financial Crisis were two biggest and well known catastrophic events in the past and there is still no reliable solution to prevent it happening again in the future. One of the causes is the flaw of the 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. Fractional Reserve Banking is a system of banking operation in almost all countries worldwide, in which only a fraction of bank deposits are backed by actual cash on hand and available for withdrawal. This system cannot guarantee the money of people is always safe and available, as most of them were lent out or locked in illiquid assets. To make matters worse, on March 15, 2020, the Federal Reserve Board reduced the reserve requirement ratios to zero percent that eliminated reserve requirements for all depository institutions. The counterparty risk as the outcome of this action would 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. However, their designated reserve ratio is still 2% assuming that would be enough for a normal economic downturn.

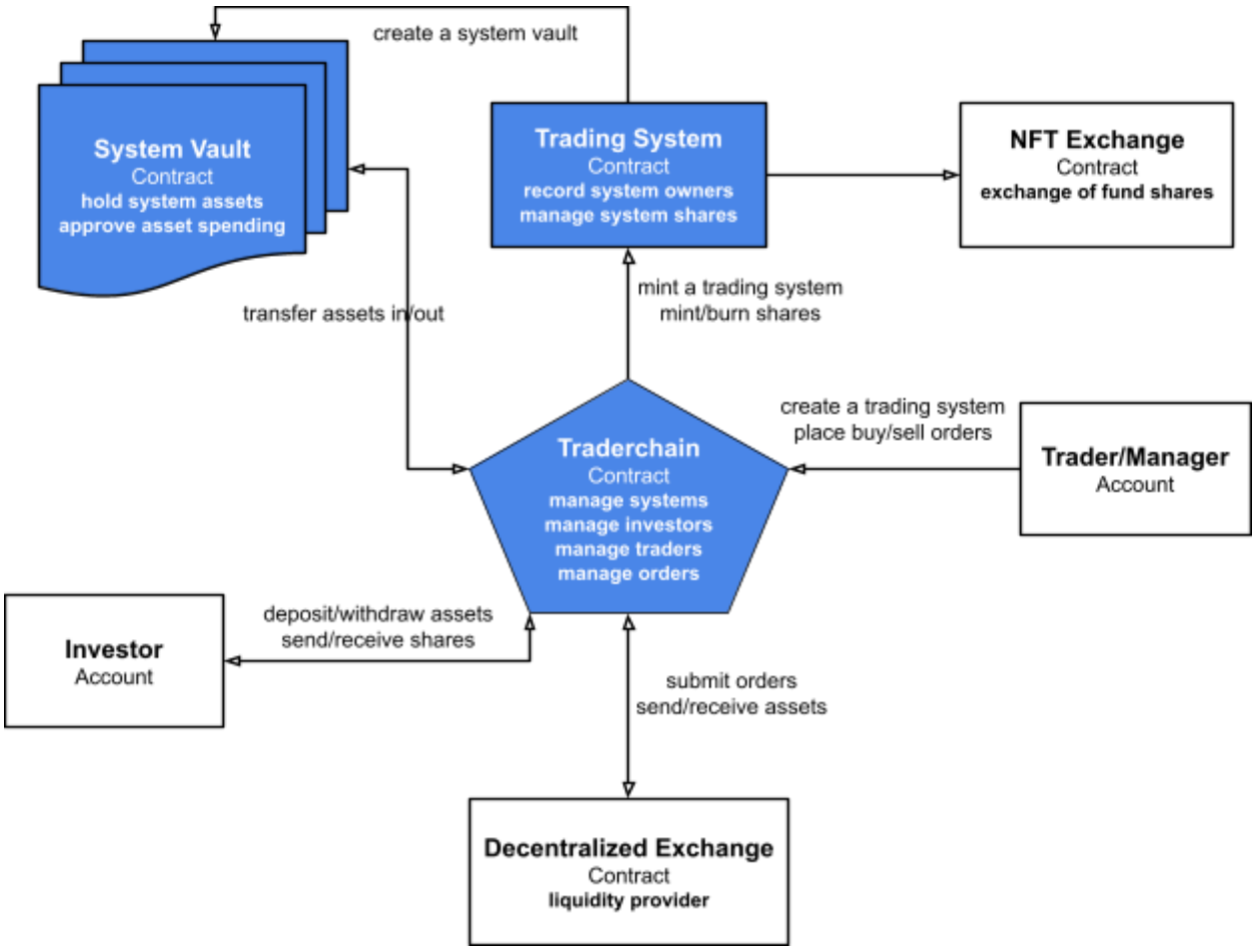
Bitcoin, a decentralized digital currency initially released in 2009, has started a Decentralization movement in the global money and currency market in which a payment transaction can be sent directly from one party to another without going through a centralized financial institution for verification. Later on in 2015, Ethereum, a successful decentralized blockchain with smart contract functionality, had proved that the entire financial market including payment transactions, wealth reserves or financial contracts can be governed by code that is fully decentralized, trustless and significantly less or zero counterparty risk. Many decentralized financial (DeFi) applications 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 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 Non-Custodial in which only the owners can make decisions on the use of their assets. The rules of how the funds will be used by whom have to be fixed in smart contracts following a general agreement between all participants. These smart contracts will keep governing all activities no matter what of the size of assets or who is the participant. All transactions should be transparent, immutable and auditable. Users can store their assets in a DeFi application without worrying about its insolvency as no one other than the owner can use the assets for different purposes like the fractional reserve banking system does.

Even though many crypto projects raised the flag of decentralization, fundamentally their operations were very similar to traditional financial (TradFi) systems in which customer funds are stored in a centralized financial institution like a bank or trust. The collapse of crypto exchange Mt. Gox in 2014 and recently the bankruptcy of FTX exchange with the contagion it brang to the crypto industry were catastrophic. A long list of CeFi companies, Celsius, Voyager, 3AC, BlockFi and more failed and went insolvent in 2022. The insolvency of FTX fund reserve was very similar to a bank run in the traditional financial world. It showed that a crypto project that uses 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. On the other hand, DEXs has been serving the community well through the beak market of 2022. Traderchain protocol which is built on top of DEXs will make sure its system 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. Traderchain controller contract provides external interfaces for investors and fund managers/pro traders to interact with the protocol. Investors will deposit and withdraw their investment to a fund via this interface. Fund managers interact with it to manage their portfolios or configure properties of a fund. The Trading System

contract defines the structure of a fund, managing its share issuance and redemption. It's designed so that a fund and its shares can be traded in any NFT decentralized exchange. It helps reduce the costs of liquidating assets in a redemption process and give more flexibility to investors. Fund assets are stored in a System Vault contract which doesn't allow any direct request from external accounts to transfer assets out. Assets can only be spent following a set of rules in 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. Investors will interact with this contract to buy and sell shares of a fund. To secure assets in a vault, only internal requests from this contract are permitted to interact with the System Vault contracts. 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 a fund and their permissions, as well as provides computation for tracking a fund value and its share price.

4. Trading System Contract

Each trading system/fund is a Non-Fungible Token (NFT) following EIP-1155 smart contract standard. EIP-1155 allows the protocol to issue an amount associated with a token id which will be used as a number of shares for an investment. This will power the Traderchain protocol to provide two significant features. 1) Allow investors to buy and sell shares of a trading system similar to the shares of a mutual fund. 2) Allow investors to trade the shares on a NFT exchange similar to how an ETF does. We call it the share conversion mechanism and here is how it works. Once an investor sends his investment to a fund, he will receive a number of shares that will be 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. 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 exchange them for their investment back. In this redemption process, Traderchain protocol will liquidate a portion of fund assets via a DEX into the base cryptocurrency and send it back to investors. Also at the same time, it will burn those disposable shares to make sure the share price of a system unchanged.

5. System Vault Contract

A new instance of the System Vault contract will be created for each fund in order to hold the fund assets separately for the purpose of better security and easier auditability. Investors can only deposit and withdraw their assets to the vault via the share conversion mechanism explained above. There is no external interface exposed in the vault contract that allows a user to interact with the vault directly. Fund managers/pro traders can only request to use vault assets for trading operations following their trading systems, but they can never withdraw or use the assets for any other purposes. This is totally different with the traditional asset management in which a bank can lend out money and keep only a fractional reserve in their balance sheets. The assets in the vault are always fully reserved and available for withdrawal anytime by the share owner, thus investors and fund managers will have no concern about the fund insolvency. The performance of a fund is dependent on the manager's skills and the effectiveness of his trading system, not by 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. A high liquidity stablecoin like DAI or USDC will be set as default. Following are 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 realtime or at a cutoff time.

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

Pros
- The value of an investment can follow the portfolio performance in realtime.
- Fund managers don't need to manage asset allocation for each new investment.
- Simple to implement.
- It works for small funds which have a few investments and a small number of assets.
- The protocol doesn't 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: A new investment and estimated fees from an investor will be held until a cutoff time, e.g. the end of day. 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 used for asset liquidation procedures.

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

Cons
- Investors need to wait until cutoff time to receive shares.
- Managers need to manage asset allocation for new investment at cutoff time.
- More complicated to implement.
- Small funds which have a few investments per day don't have much benefit.

- The protocol needs to hold fees for deferred allocating transactions.
- Hard to estimate 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. Investors can receive the benefit of diversification in 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 efficiency and liquidity for the fund's shares in which investors don't need to liquidate their assets reserved in vault to receive the capital which costs more transaction fees in case the fund is well diversified.

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

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

Friend groups of 2-20 people

Today, 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 doesn't lose the group's money. 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 want to invest into NFTs together have a lot of investing power given cumulative capital that could be pooled together. However, they suffer from slower decision-making, challenges with ownership tracking, legal considerations and managing members over time. Traderchain Manager DAO will streamline group decision-making quickly on chain before transactions. Ownership tracking and contribution 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. A vault that stores assets for each fund is protected behind a controller contract layer that makes sure the fund is secure and is only used for the transactions under the preset consensus between all participants. Also, as funds are implemented following the EIP-1155 standard, it gives fund managers and investors a very flexible and automatic solution to exchange the fund value for an investment. Not only can investors contribute and withdraw an investment anytime, but also they can exchange the fund shares in any NFT exchange for many benefits such as saving loading fees or seeking income from an arbitrage. Our system is decentralized from the bottom up with its liquidity provider layer built on top of decentralized exchanges to make sure all transactions are transparent and auditable. All participants are confident in their investing and trading decisions when interacting with the protocol knowing that they don't need to trust on any intermediaries because all outcomes are governed by immutable smart contracts on a blockchain.

References

- Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf
- Ethereum Whitepaper: https://ethereum.org/en/whitepaper/
- Uniswap Whitepaper: https://uniswap.org/whitepaper-v3.pdf
- Fractional Reserve Banking: https://en.wikipedia.org/wiki/Fractional-reserve_banking
- Reserve Requirements: https://www.federalreserve.gov/monetarypolicy/reservereq.htm
- FDIC Designated Reserve Ratio: https://www.fdic.gov/resources/deposit-insurance/deposit-insurance-fund/dif-fund.html
- Financial Crisis of 2007: https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%932008
- EIP-1155: Multi Token Standard: https://eips.ethereum.org/EIPS/eip-1155
- Decentralized Finance: https://en.wikipedia.org/wiki/Decentralized_finance
- Squads, example of DAO funds: https://docs.prysm.xyz/getting-started/who-is-using-squads