INVESTIN: World's most secure and transparent platform to invest in.

Anas Abdul Khader
anas.khader@protonmail.com
www.investin.pro
14/07/2020

Abstract: A trustless platform that allows anyone to invest without giving away custody of the asset to any manager/trader who trades it for profit. Smart contracts written using a Turing-complete programming language govern the terms of exchange and allow investors to have full control over their assets while allowing a defined control to world's best managers/traders who invest and make money for respective investors. The system being on blockchain allows full anonymity/transparency to both traders/managers and investors, thus removing the need for any third party to audit and verify the transactions as the contracts inherit all the security features of the blockchain and keep executing the defined immutable code as long as the network remains live.

1. Introduction

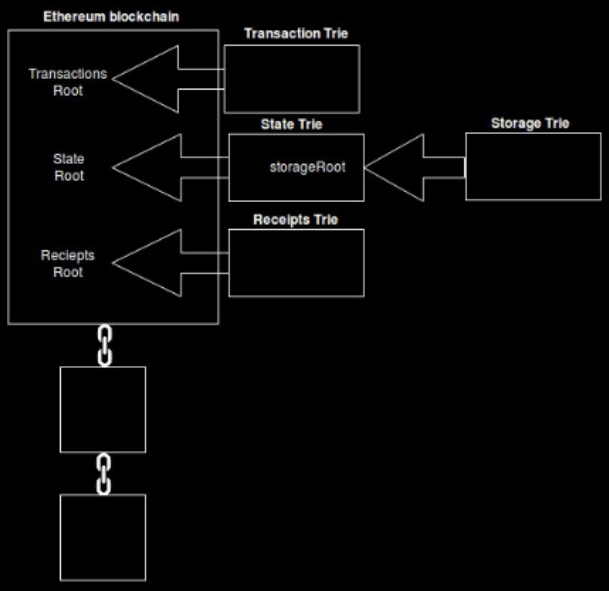
The era of trusting financial institutions and corporations solely due to their legacy and heritage is a thing of the past, with the emergence of open source technologies it is time societies acknowledge the fact that any entity that guarantees transparency can become a trustworthy business that many can count on. Investment funds/hedge funds have been running for the past century on an outdated system of building trust among their clients/investors by reporting great numbers in profits year on year, the money invested in the fund is controlled by fund managers and big corporations who oversees the investments in assets and acts to protect people's blind trust in such entities. Governing agencies around the globe spend millions of taxpayers money to run independent regulatory bodies to keep a check on the behavior of these funds and to keep them from committing fraud and duping their clientele's investments. Yet, we find many cases where the fund goes bankrupt, and there is no accountability for the loss. This arrangement of trust is hurting the future of free markets where anyone could invest and earn profits without fearing betrayal. It's sincerely tough to trust anyone with one's hard-earned money by just signing on papers.

Reliability, security and anonymity are things which all individuals yearn in the world of finance. To fill this need for a trustless system a platform built on immutable smart contracts is proposed, where no human interference is warranted. The platform maintains consensus based on cryptographic proofs instead of trust, allowing any two willing parties to transact directly with each other for a mutually agreed duration without

having to give away the custody of their assets. With the emergence of blockchains being completely trustless and immutable, its matter of a time many tasks that included a human to oversee would be replaced by smart contracts that run on top of these blockchains. The core components utilized in building the architecture of the proposed platform are described in detail in the following sections with an assumption that the reader is familiar with the functioning of blockchain.

2. Smart contracts

A smart contract is an immutable set of code that constitutes a set of rules agreed upon by two or more parties to govern the transactions based on the predefined criteria. Upon execution, it validates the criteria dynamically and executes the transactions to produce the desired output. This allows decentralized automation by facilitating the verification and enforcement of the underlying agreement. This allows us to exchange anything of value including money, shares, property etc, in a transparent peer-to-peer manner eliminating the need for a middleman and keep the system conflict-free. These assets can be deposited and redistributed among the participants according to the rules of the contract.



Data stored on block header

Smart contracts boast many features among them the most important are discussed below:

a. Trust
The properties of transparency and security in a smart contract makes it trustworthy for businesses and clients. It eliminates the possibility of manipulation as well as manual errors and establishes confidence in the execution of the defined business logic. Upon validation of all the conditions, the contract automatically execute the predefined transactions. This unique feature of the contracts prove its capability to significantly lessen obfuscations over legal contracts and the requirement of collateral as a judicial guarantee. Self-executing smart contracts allow parties to commit and bind by the terms and conditions described prior to its implementation.

b. Tamper proof
A smart contract is coded in an explicitly detailed form. The code that holds all the terms and conditions once deployed will be immutable, which means it can never be changed and no one can tamper with it. Any necessary condition that's left out of the contract might result in an error while execution and no new condition could be incorporated once the execution starts.
Due to this, the smart contract becomes a comprehensive agreement which once deployed on the blockchain will keep executing the written set of code. Any discrepancy in the state of terms and condition set at deployment won't be editable by any unknown parties other than owner themselves.

c. Security
Smart contracts being on blockchain inherit all the cryptographic features of the blockchain they are deployed on. The blockchains rely heavily on cryptography to achieve their data security. In this context, the so-called cryptographic hashing functions are of fundamental importance. Hashing is a process whereby an algorithm(hash function) receives an input of data of any size and returns an output (hash) that contains a predictable and fixed-size byte code.
Therefore, the hash of each block is generated based on both the data contained within that block and the hash of the previous block. These hash identifiers play a major role in ensuring blockchain security and immutability. The specifics are beyond the scope of this paper, in essence, asymmetric cryptography prevents anyone but the private key holder from accessing funds stored in a crypto wallet/smart contract, thus keeping those funds safe until the owner decides to spend them (as long as the private key is not shared or compromised).

d. Transparency
One of the basic characteristics of blockchain technology which is also shared by smart contracts is transparency. As previously stated, smart contracts are filled with terms and conditions in absolute detail which can be checked by the parties involved in the agreement over a transaction.

This eliminates the chance of dispute and issues at the later stages as the terms and conditions are thoroughly checked and put into place only when all the participants agree to those. This trait of smart contracts allows the involved parties to ensure transparency during transactions.

Ethereum state transition function

3. Platform

The market place for people who want to invest grows every day yet the facilitators have been shrinking and consolidating. The average investor needs to go through the tedious process of finding a legit fund which can guarantee them returns and put their faith in agencies governing these funds to effectively police them from running away with all the money invested with them, the investors also need to acquire specific knowledge on rules and regulations under the law of the residing country for being invested in global markets and many investors wouldn't qualify to invest due to their inability to understand and have less capital. Given the above barriers and many uncertainties/anxieties in the investor's mind, the capital that could be added to the market is shrinking.

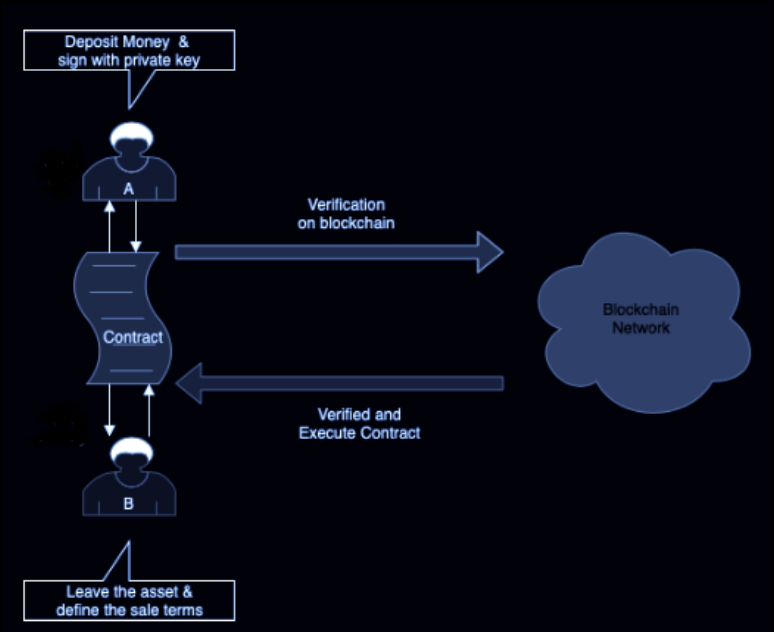
The platform would be built on the ethereum blockchain and deployed through smart contracts written in solidity, these contracts will be secure and audited by the best auditing firms prior to deployment, ensuring no fallbacks or errors or mismanagement that can occur when these contracts handle investor's tokens. These contracts together will act as a protocol and would process requests through specified conditions they are coded in. Any fund manager/trader will be able to deploy a contract to start their fund using the protocol and that contract will act as fund managers/traders vault where any investor looking to invest can send their tokens. On a successful transaction from an

investor to fund manager/trader's address the investor will receive an ERC 721 token which are non-fungible tokens deployed on ethereum blockchain based on the Ethereum improvement proposal (EIP) 721. These erc 721 tokens will act as a deposit receipt/form of agreement that investor holds in their wallets for their investment sent to the contract and whenever the investor wills to withdraw their investment they can simply send this token to contracts address which will process the token and verify the amount invested for the token bearer and send back the amount invested plus the profits made on the amount for the duration it was being traded with, back to investors wallet.

The protocol will never allow direct custody of assets to the fund manager/trader trading using the amount, it will only process the buy/sell signals and trade accordingly, the protocol will also have a risk defined approach on the maximum drawdown that will be allowed on the total capital that is being used to trade by the relevant fund manager/trader, which will further ease the anxiety of investors of losing their money in hands of rogue traders or due to unknown trading errors. Inherently the investor will always have control over their assets invested as they can withdraw the tokens anytime and can also keep tabs on the performance of fund manager/trader through the platform's website. The profits/losses made by fund manager/trader will be exact as these trades will be on the blockchain and these trades will be verifiable by anyone whose willing to do so and the platform's user interface shall only aggregate performance data from the blockchain as well, thereby removing any chance of bloating up fake results which is possible on centralized platforms.

The protocol will handle revenue model as well and would be making decisions based on the performance of fund manager/trader, the initial management fee which will be defined by fund manager/trader will be deducted and sent to their relevant address when an investor sends the tokens to the contract while the performance fee will only be given if the fund manager/trader meets the average profit targets that they promise while deploying these contracts through the platform. The platform will deduct a fee for handling the transactions and to keep the system running the protocol will deduct a small fee if the fund manager/trader meet their targets on the amount invested by investors. Hence the platforms survival will be on the fund managers/traders making profits for investors invested with them.

The protocol will ease the onboarding experience of investors by allowing them to send their tokens from their wallets to fund manager/trader's contract address deployed by the protocol without registering anywhere or revealing their identities and will always have the risk defined for the amount invested. The users who don't have wallets would be able to create it by using a two-step process of signing up on the website to assign a wallet linked to their email accounts which will allow them to have no risk of losing the wallet due it to being linked to their email accounts and can recover using the email account if they lose or forget the wallet created using the platform's website.



Working of the contract

4. Trading engine

Ethereum is a public blockchain designed to be transparent, all the transactions are mined on-chain and broadcasted on the whole blockchain which helps in many aspects but making everything open to all halters many possible use cases for business solutions to be deployed using these contracts. Hence, it's necessary for the platform to integrate some of the advanced protocols built on native blockchains to run the trading engine. Some of the key integrations are listed in the following sections.

a. Decentralized exchanges

A decentralized exchange is an exchange market that does not rely on a third-party service to hold the customer's funds. Instead, trades occur directly between users (peer-to-peer) through an automated matching process.
All decentralized exchanges feature on-chain settlement. On-chain settlement is a necessary element that enables users to eliminate the need to trust a centralized party (such as a centralized exchange) to control user assets, settle trades, and ensure that account balances are correct. On-chain settlement helps users publicly verify on the ledger that their trades were settled according to their desired terms. The performance of any decentralized exchange is limited due to the latency involved in securely confirming a transaction on the underlying chain. Therefore, the speed of confirming a transaction on a distributed ledger network is the bottleneck for the mass adoption of decentralized exchanges.

b. Rollup

Trading requires high-speed execution and liquidity, which is simply not possible on the current network as ethereum blockchain can handle less than 15 transactions per second, hence high latency can seriously hamper general trading using any decentralized exchange. To overcome issues of speed and security we use rollups that are transactions done on side-chain with much higher speeds and processed later on the main chain.

Rollup is a layer 2 blockchain technology which scales ethereum smart contracts to handle 100 – 2000 transactions per second (TPS). Its major advantage over other solutions is the fact it enables Turing-complete smart contracts on layer 2 using Optimistic Virtual Machine (OVM) without compromising any security and also reduces the cost of user transactions. There are two types of rollup: Optimistic and ZK Rollup. Rollup works similar to Plasma in the sense both scale ethereum by moving transactions off-chain onto a layer 2 sidechain which is secured by the mainnet i.e. layer 1. Both solutions deploy smart contracts to the mainnet which hold all the funds deposited into the sidechain and proof of the current state of the sidechain. Sidechain users and operators maintain the sidechain and ensure valid state transitions are committed to the mainnet contract. The method of submitting state transitions (or new sidechain blocks) differs between Rollup and Plasma. While both concepts offer great solutions for our platform, we look forward to the development being done in both fields and plan to take upon the most viable solution to our use and deploy using such layer 2 technology.

Trading is an art of having edge over the markets due to which the fund manager/ trader's transaction cannot be relayed on the blockchain, as malicious parties can front-run these orders and profit off by market-making/arbitraging when these orders are filled on decentralized exchanges on mainnet, which will hurt the profitability and compound to major losses if not handled well. Some well-versed actors can also subscribe to transactions of profitable traders and trade based on the positions they see on the blockchain, this will hurt the business model. To counter such problems without losing the security of the main chain we shall use layer 2 based decentralized exchanges which won't transmit the trades as soon as the trades are taken, these rollups will batch the transaction and transmit on the main chain after a certain period of time allowing traders/managers to take positions beforehand and later their position can be known.

5. User experience

Blockchains with their inherent features are high-level concepts that require a high degree of knowledge in both computer sciences and cryptography to understand. Hence it's difficult to produce an understanding of what goes on, when a contract on the blockchain is executed to an average user and doesn't make sense to put it into words unless they are investors in such technology. The only way to make global adoption possible for this machine level language-cum-immutable-cum-Turing complete technology is by easing the onboarding experience for users and let them experience the advantage of trustless environments that can be achieved. Our mission as blockchain developers/enthusiasts would be to excel at making such user interfaces possible and provide a great value proposition to everyone.

Hence this user experience with blockchain technology will constitute the version 3 of the internet which can be named as Web 3, the essential mission of web 3.0 would be to provide a user-friendly interface for people who do not know much about working of blockchain and encourage them to accept this powerful technology. As a result this will create many businesses that need no third party/centralized authorities to administer or handle complex banking/financial instruments, validate agreements or policies, verify authenticity, et cetera.

Conclusion

The protocol proposed will be able to handle the complex task of administering large sums of asset and allow any number of fund managers to access those assets to make intelligent investment decisions without risking or building a trustful relationship with investors, this kind of instruments will propel the finance industry to new heights and We envision the platform referred to as Investin, will help transform the investment industry and set a new standard on how business is conducted.

References

1. https://bitcoin.org/bitcoin.pdf
2. https://ethereum.org/whitepaper/
3. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
4. https://stanford-jblp.pubpub.org/pub/deconstructing-dex/release/1
5. https://medium.com/coinmonks/smart-contract/home
6. https://kauri.io/what-is-web-30/2678d5d36f5c45f981e482de289ce154/a
7. https://aantonop.com/books/
8. https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6
9. https://z.cash/technology/zksnarks/
10. https://semaphore.appliedzkp.org/howitworks.html
11. https://arxiv.org/pdf/1905.08833.pdf