EN

NOWP

UTXO DeFi

A Case Study

nowput.finance

Written by: David Owen Morris
Designed & edited by: Paul William Mills & Zlata Amaranth
Developed by: Wang Xiao Yu & Zhu BaJie 007

nowput.finance

In simple terms, UTXO DeFi rejects the idea that a user has to interact directly with extra code within a smart contract to participate in decentralized finance, also known as DeFi. The main issue in DeFi or CeFi (centralized exchanges) is trust.

Trust can be structured somewhat like a sandwich:

DeFi	*CeFi*
Immutability of the blockchain the service is hosted on.	*Exchange will permit you to continue depositing and withdrawing funds.*
Code of the token you use for the service.	*Code of the token or coin you fund the platform with.*
Code of the contract you interact with.	*Non transparent market data used to execute your option.*
The source of the data for that contract.	*No insider tracks for counter trading.*
The execution of the contract in a timely manner (not being front run)	*No magical tokens from thin air to pad exchange books.*

UTXO DeFi structure changes the complexity of the trust sandwich drastically by reducing the number of trusted layers, with several particularly egregious when it comes to trust.

UTXO DeFi
Immutability of the blockchain the service is hosted on.
The opensource matching engine in common coding language used to match data to trades.
Payments being made hourly after transaction confirmation.

nowput.finance

How is this done?

Rather than forcing users to send tokens to a smart contract or make a deposit into an account with little control, UTXO DeFi encourages the use of transaction tagging by locking into specific addresses to clearly signal participation in what is offered at that address, removing two levels of trust in potential code errors with DeFi along with CeFi depositing issues.

Why a tagged transaction instead of tokens and contracts or having an account?

Simply put, the need to trust the two levels of code for the token and the contract disappears along with the knowledge of where your funds go if deposited into a centralized exchange.
In terms of security in UTXO DeFi, there is inherent protection from the host blockchain which means to attack the funds (which can be 100% cold), an attack on the native chain is needed. For Bitcoin, Litecoin and Bitcoin Cash, this is an incredibly costly endeavor, additionally for chains like Raptoreum, Firo or Comodo this is an impossibility due to technical innovations such as chainlocks or distributed/delegated proof of work aka Dpow.

But can someone hack the deposit addresses?

Unlike current DeFi smart contracts or exchange wallets, UTXO deposit wallets can be kept 100% cold and offline until payment wallets need refilling or transactions need signing and broadcasting. These can be kept offline and distributed away from the host and also applies to exchange cold wallets while eroding the transparency which UTXO DeFi technology offers.

Can someone attack and spoof data feeds?

Yes, but just like 51% attacks, it is extremely costly to do and difficult with distributed feeds from the same source. As payments are on the hour after transaction, an attack would have to be performed for an extended period of time on all routes into the matching engine. By adding a single private data feed as a sanity check, it becomes a very complex exercise.
The goal isn't to be immune, but to generate an environment where there is no gain carrying out such an attack. This is easily achieved with option size limits and a spam filter.

Can someone attack payout addresses?

Yes, but the same applies to the payout addresses as the deposit addresses: they can be used for offline signing of alternatively broadcast transactions.

The main issue lies with hot payout wallets. This can be remedied by involving PSBT which forces an attacker into targeting multiple locations vastly increasing the complexity. Additionally we can strengthen this when combined with non node wallets also performing PSBT.

Why Isn't it perfect?

This is as secure, trust-less and as transparent as any top tier blockchain development will allow on the market today.

Banks close daily at the moment, EVM DeFi contracts get hacked or ‘rugged’, and centralized exchanges also get hacked, embezzled and also exit scam.

The only risk here are open positions in the deposit addresses for up to two hours.

What can you do with this system and what are you aiming to develop for it?

The possibilities are endless but an initial few spring to mind let’s examine each in some detail and their advantages and disadvantages over traditional implementations of these offerings.

nowput.finance

“Binary options” aka “up/down options” or “fast hedges” or “betting on prices”

Binary options match a desired duration of option to a price feed in a transparent manner.

Traditionally, this has been achieved on centralized platforms while requiring accounts and making use of third party code to fund, or third party services such as Perfect Money/Paypal etc; making the whole process opaque. Additionally a user is also required to trust that the price feed used to set the option against is honest.
On top of that, users have no knowledge of being counter traded by the platform offering the options.
Adding further insult to injury, users have no guarantees of being able to withdraw funds without additional fees.

With DeFi, the situation is somewhat better but still not ideal as price oracles can rely on centralized aggregator services for price data feeds meaning users are being served delayed data on many markets for short durations options/hedging limiting the use case, allowing bad actors the ability to execute flash loan attacks.

Solidity based contract code funded by tokens still promotes an unhealthy environment by opening up the possibility of exploits or ecosystem infrastructure losses.

UTXO DeFi is in this case a far superior option as it alleviates most, if not all of these issues.
Transactions are secured by proof of work on nearly unassailable blockchains without the need for any additional code.
ZMQ notifications allow for the opening of near instantaneous positions, and when combined with appropriate transaction tagging, users have full certainty of participation.
Data freshness for short term options is no issue as users can go directly to varying market sources and offer options against those verifiable feeds which ensures that the issuing platform can not countertrade you other than placing live orders.
Furthermore, it can provide market makers on centralized exchanges additional hedging tools otherwise unavailable.

nowput.finance

Predictions Markets

Prediction markets match the outcome of a future event to a pool of funds.

On centralized platforms, prediction markets require user accounts while using third party code for tokens for funding, or third party services like Payzaa and Skrill etc making the process opaque. Additionally users are required to trust that the event feed used to set the option against is honest and have no way of knowing if they are being countered by the platform offering the predictions pool.
While just to exacerbate things, users have no guarantee of withdrawing funds without additional fees or to the desired service if depositing with one, but would like to be paid out on another.

On DeFi the situation is slightly improved, however not ideal as in many cases, event oracles rely on centralized aggregator services for data feeds meaning users are served late data allowing for bad actors to perform flash loan attacks.
A problem with using contracts for speculators on who scores the first goal during a football match is the lag from the event, which is often televised live to the data aggregator and then to the oracle and finally to the contract. This may be countered with delayed payments or not taking additional contracts after the start of the event, however, the more elements users need to add to the contract, the greater the attack surface.

The combination of Solidity contract code funded by issued tokens allows for an unhealthy combination which opens up the possibility of exploits or losses in ecosystem infrastructure.

UTXO DeFi offers a better user experience by allowing near-to-real-time participation in events with set durations. This is done without adding the risk of complex contracts and oracle solutions to the mix, while reducing risk when compared to both DeFi and the majority of centralized options. The ability to keep wallets ‘cold’ apart from the payout process; additionally mitigates further risk by reducing the potential for many security issues.

Dex Implementations

The use case is slightly more murky here with several working dex models namely EVM, SOL and Atomic Swap. The EVM dex's mainly allow swap trades vs liquidity pools, and the SOL dex's function like centralized exchanges with limit / market / stop / trailing stop order types. The same goes for atomic swap based dexes such as Komodo's Atomic Dex or Particl's marketplace.

There are some drastic differences between the different types of dex implementations here and what that means for the different scenarios.

EVM based chains require that all traded assets be tokenized on the chain of which the DEX is native to and in many cases do not support limit orders but rather swaps against a specified liquidity pool. This leaves users with very little granular control of their trades and are placed in a position in which they have to trust chain code, two sets of token code, dex code, without failing to mention liquidity pool code. This builds a seriously unappetizing sandwich.
Additionally, users also have to compete with frontrunning, mev extraction, lp draining and a multitude of additional issues.
This leaves first and second generation EVM dexes with a relatively limited but workable use case.

SOL dexes have the same requirements and are otherwise similar to EVM dexes save that they offer a fuller range of order types.

Atomic swaps directly between two chains as implemented on Komodo's Atomic dex, offer the greatest degree of flexibility and possible combination of pairs, as the wallets are all self custodial with the respective coin teams running the support infrastructure. This is the best most decentralized option for dex trading.

UTXO DeFi can utilize swap dexes in a manner similar to how first generation EVM swap exchanges work but with one major difference, the ability to place limit orders.
Users would also be able to place funds in a liquidity/payout pool earning a proportional share of fees earned by the swap exchange.
The main advantage to this approach is all but a smaller payout pool can be kept 100% cold at all times minimizing potential wallet attack issues.
This is a huge difference compared to EVM dexes where frontrunning MEV and LP draining are just some of the issues users have to accept and deal with.
Canceling an order or withdrawing funds from the LP on the dex/swap would involve sending a signed message from the same sending address, this is clunky and not the most user friendly, however it is still well within the comparable range of the LP withdrawal procedures on EVM or SOL dexes.

Can we go beyond this?

Yes, that is certainly possible and the Nowput team will publish additional use cases as the chain matures.

Summing it all up!

UTXO DeFi is a viable option worth exploring and developing as it allows DeFi or DeFi like functions directly on native UTXO based chains, saving users fees from wrapping and bridging onto other networks. Due to FTX and a number of DeFi hacks, the security standpoint is as relevant as it will ever get, and we can conclude that for the range of functions we have explored, there is a significant mitigation of most security risks currently associated with participating in the overall cryptocurrency marketplace.
One of the main improvements is that users do not have to access a high risk web wallet through their browser. Users will be able to trade directly from their hardware or electrum wallets which support op_return messaging.

So, “Out with the new and back in with the old till there is something that requires we go beyond it!”

David Owen Morris
June 2023

EN

nowput.finance

NOWP

keeping it green

Contact : Angel@nowput.finance

Written by: David Owen Morris
Designed & edited by: Paul William Mills & Zlata Amaranth
Developed by: Wang Xiao Yu & Zhu BaJie 007