TOFU PROJECT

Cost-effective DeFi

TofuPanda
panda@tofudefi.com

October 11, 2020

Abstract

Decentralized finance, also known as DeFi, is a fast-growing sector of the cryptocurrency industry. While cryptocurrency coins create a decentralized store of value independent from any government or central bank, DeFi creates decentralized financial instruments independent from traditional financial institutions.

At the moment, the vast majority of DeFi applications are built on the Ethereum blockchain. Unfortunately, the Ethereum Network has become overloaded. As a consequence, Ethereum network transaction fees have surged and hit all-time high recently. This issue limits further use and development of DeFi applications on this blockchain.

This paper intends to propose a solution that can address arising issues by utilizing the TRON blockchain. TRON is a blockchain-based decentralized platform focused on smart contracts and high performance. The TRON network is capable of handling about 2000 transactions per second, making it suitable to build cost-effective DeFi solutions.

1 Introduction

Since the summer of 2015, those with a pulse on the digital currency industry have eagerly watched the development of next-generation cryptocurrency platform Ethereum[1]. From a technical perspective, Ethereum is an open source, globally decentralized, computing infrastructure that executes programs called smart contracts[2].

The goal was to create a set of tools that developers could use to move the internet away from an information network characterized as centralized, controlled, and disproportionately profitable for only a few large companies. Instead, with decentralized systems like Ethereum the command and control functions of the internet can be redistributed and redeployed for greater access and security.

1.1 What is Decentralized Finance (DeFi)?

DeFi is a shortened form of "decentralized finance" which generally refers to the digital assets and financial smart contracts, protocols, and decentralized applications (DApps) built on top of blockchain platforms like Ethereum, TRON or EOS. Technologies like the internet, cryptography, and blockchain give us the tools to collectively build and control a financial system without the need for central authorities.

Although it is still small compared to the global economy, DeFi has seen rapid growth in 2020. In early 2019, there were only $275 millions of crypto collateral locked in the DeFi economy. By February 2020, that number had grown to $1 billion, and it has continued to grow impressively throughout the year, hitting $3 billions by mid-July, and more than $9 billions by mid-September.

Most DeFi platforms take the form of decentralized applications, known as dApps. These dApps use a series of smart contracts to automate financial transactions, making them faster, more efficient, and often more affordable than their centralized counterparts. Likewise, because dApps are governed by computer code, which is inherently neutral, there is no issue of bias.

The most popular types of DeFi applications include:

- Decentralized exchanges
- Stablecoins
- Lending platforms
- Prediction markets

One of the most notable projects in DeFi space recently is Uniswap[3]. Uniswap is a decentralized exchange and automated market maker protocol[4] built on Ethereum smart contracts. Users can buy and sell ERC-20 tokens and supply liquidity in order to earn exchange fees.

At this moment, most applications that call themselves “DeFi” are built on top of the Ethereum blockchain. Even though Ethereum has progressed significantly since 2015 and became standard in the area of decentralized finance and smart contracts, it has an issue with further development of cost-effective decentralized applications.

2 Scalability problem

At the moment, Ethereum is struggling with crippling congestion. The blockchain utilization is currently over 96 percent, making it costly to run applications and use.

Like Bitcoin, the main reason for the Ethereum scalability problem is the network protocol that each node in the network has to process each

transaction. Ethereum implements a slightly modified version of the proof-of-work (PoW) consensus mechanism[5]. Every Ethereum node has to verify that the miners' work is valid and keep an accurate copy of the current network state. This greatly limits the transaction processing capability. Currently, it can only process 12-15 transactions per second[6].

This issue significantly limits development and usage of decentralized applications on Ethereum blockchain. The average fee paid by Ethereum users per one transaction have reached a new record average of over $10.33 recently[7].

As the DeFi ecosystem continues to grow, the urgency for scaling solutions that can ensure network usability continues to rise.

3 Possible solutions

3.1 Ethereum 2.0

Ethereum 2.0 is a long-planned upgrade to the Ethereum network which promise to reduce energy consumption, allow the network to process more transactions, and increase security. Technically speaking, Ethereum will become a proof-of-stake[8] blockchain and introduce shard chains[9]. Ethereum 2.0 is regarded as the long-term solution that can bring stability to the network, and the long-awaited upgrade is set to be released in 2020.

While the initial release of Ethereum 2.0 is a noteworthy event, it will not bring immediate changes. The first iteration will serve as a testing ground for what will eventually become the only Ethereum. This change is estimated to take from one to two years. In fact, Ethereum's creator, Vitalik Buterin, recently admitted that the team underestimated how long the sharding and proof-of-stake features that characterize Ethereum 2.0 would take to develop.

3.2 Second layer networks

Second layer solutions aim to provide all, or most of the functionalities and security of their underlying blockchain without using it, or more accurately, using it in a different way. The idea behind second layers is that you can combine many bilateral transactions together and only settle the net exchange on the first layer periodically. This theoretically would substantially reduce the number of transactions on the first layer.

This can be helpful in the short-term, as it relieves the Ethereum network of congestion, and in the long-term, keeps the blockchain free of "unnecessary" transaction history.

The concept of second-layer networks is not new, nor is it unique to Ethereum. Bitcoin itself is no stranger to congestion and scalability issues. RSK[10] and the Lightning Network[11] are examples of such solutions. Today, there are a few independent projects that leverage this same concept in

order to provide an immediate solution for Ethereum's scalability problems as well as a better ecosystem for the DeFi industry.

But layer-two solutions are complex and difficult to develop because they walk a very thin line between security and convenience. Blockchain networks are safe because every single transaction is recorded on an immutable ledger, however, these solutions bypass this constraint.

Another problems with second layer solutions are lack of interoperability and liquidity fragmentation. First layer solutions can interact with each other in a straight way. This allows developers to build new DeFi solutions on top of existing ones. Such cooperation can generate synergy effects and strengthen the whole DeFi ecosystem on the main blockchain.

3.3 Alternative blockchains

Since 2015, many developers have indeed taken the opportunity to build their own engines, most often designed to overcome the same issues that Ethereum 2.0 is seeking to solve and even more, in some cases. We will review most notable competitors.

RSK

Rootstock (RSK) is a smart contract platform compatible with Ethereum that is connected to the Bitcoin blockchain through sidechain technology. RSK was launched in late 2017 and caused much excitement around the platform's promise to bring smart-contract functionality to Bitcoin. Furthermore, with the capacity for many hundreds of transactions per second, it was one of the first real threats to Ethereum in terms of scalability. RSK has capability of processing about 400 transactions per second which is better compared to Ethereum, but there are alternatives with capability of processing more than 1,000 transactions per second.

And since RSK doesn't have its own token and hasn't launched any kind of crowdfunding, it does not have the massive funds at its disposal that alternatives have.

EOS

EOS is a blockchain designed to compete with Ethereum and was promoted as "Ethereum Killer". Like Ethereum, it supports smart contracts and distributed applications, while also providing high transaction throughput, free transactions, and improved performance. EOS relies on delegated proof-of-stake (DPoS) consensus[12]. Stakeholders continuously elect 21 block producers, who process transactions and make governance decisions.

EOS uses WebAssembly (WASM) to develop smart contracts. While WASM is not a programming language, but it will give developers to code in the language of their choice and compile into a bytecode that can run

on a supported browser. Even though WASM has some advantages for developers, at the moment, main language for developing smart contracts in EOS is C++ which is notoriously known for its steep learning curve. It also means that EOS smart contracts are not compatible with Ethereum.

Another issue with EOS is spam transactions. Currently, EOS team claims that their blockchain is able to process 50,000 transactions per second. EOS does not charge transaction fees to end-users. Instead, dApp developers must stake EOS to reserve resources such as RAM, CPU, and network. Then, they can use those resources to reserve bandwidth for their DApp transactions. In theory, these limitations should prevent "spam" transactions from overloading the blockchain, but in reality, issues still arise.

Even though EOS is more efficient system than Ethereum, it implements different economy model. Both blockchains have vastly different communities and are used for different kinds of applications. Migration of Ethereum's smart contracts to EOS will require additional resources.

Cardano

Cardano has been one of the most hotly anticipated rivals to Ethereum for some time. The platform was developed by one of the original co-founders of Ethereum, mathematician Charles Hoskinson, who left Ethereum in 2014 and subsequently founded IOHK, the company building Cardano.

Cardano blockchain and its advanced Proof-of Stake consensus algorithm, Ouroborous, the first peer-reviewed consensus algorithm in the crypto space. At the moment Cardano can process about 1,000 transactions per second.

IOHK, the company behind the Cardano, has announced the launch of the Ouroboros Hydra protocol which is the second layer solution on top of the Cardano first layer where PoS consensus is used. IOHK explained that the this scaling protocol will enable Cardano to handle up to 1 million transactions per second, but it's still under development.

Cardano has chosen Haskell and Plutus as their languages of choice. Haskell will be used to code Cardano, while Plutus will be used for the smart contract creation. Both of them are functional languages. Even though functional languages exist for several decades and became quite popular last few years, they are rather complex to learn compared to imperative languages. All traditional programming languages like C++, Java, and even Solidity are imperative programming languages. Ethereum's first language for smart contracts was LLL, a functional programming language, with Lisp-like syntax. But it didn't become popular and was superseded by Solidity as main language for smart contract development in Ethereum. So, it means that Cardano smart contracts are not compatible with Ethereum and developers will need to migrate their code to new language which is error prone process.

TRON

An early rival to Ethereum, Tron launched in 2017. Under the leadership of Justin Sun, the platform made strides with its acquisition of BitTorrent. In March 2019, Tether announced it was launching a TRC-20 version of USDT. Within six months, Tron-based USDT had grown to 12% of the total coins in circulation, due to Tron's superior throughput compared with Ethereum.

The TRON code base was originally a fork or copy of Ethereum and it uses a fork of the Solidity smart contract language, which was the programming language developed for and most popularly used on Ethereum. As a result, Ethereum smart contracts and token standards are compatible with the TRON ecosystem.

The main technical difference with Ethereum is that TRON uses a different consensus mechanism for adding and verifying transactions on its network. As EOS, TRON uses Delegated Proof-of-Stake with 27 elected Super Representatives who produce blocks for the network. This consensus mechanism allows TRON to achieve capability to process about 2000 transactions per second.

3.4 Conclusion

Of course this is not full list of potential Ethereum competitors. There are other blockchains like Tezos, NEO, Cosmos, Waves, etc. But if we talk about cost-effectiveness we should consider at least two things. One of them is scalability and low transaction fees. Another is development costs.

Ethereum was the first platform to build smart contracts and dApps and there are plenty of code for it. Any new platform which introduce new tools and languages to create smart contracts will struggle to surpass Ethereum by this criteria. Keeping all this in mind we believe that only TRON is suitable to build cost-effective DeFi solutions at the near future. It can process up to 2,000 transactions per second and it's compatible with Ethereum. It's much easier to migrate from Ethereum to TRON compared to any other blockchain platform.

4 TofuBridge

Alternative blockchain platforms provide better transaction speed and lower fees, but Ethereum has first-mover advantage. Numerous cryptocurrency projects were launched based on Ethereum platform and ERC20 tokens in the last several years. Even now, when there are a lot of alternatives, many new projects decide to launch their dApps and tokens on Ethereum blockchain. One of the reasons for this is liquidity. In a liquid market, assets can be easily converted with minimal slippage. Liquidity is the key driver for the adoption and user growth for DeFi projects.

But if your dApp is transaction intensive, Ethereum does not seem to be a good choice. Let's consider Uniswap case. The number of daily transactions on the Ethereum network related to Uniswap's V2 Router contract only reached a new all-time high of 198,643 on September 2 with 10,540 ETH paid in fees which was about $5 millions at that moment. Meanwhile, average TRON's transaction fee is about $0.02 now, so 200k transactions will cost its users about $4,000.

The TofuBridge will allow transfer of tokens between Ethereum and TRON blockchains by collecting tokens on the one blockchain while issuing wrapped tokens on the other. This approach is suitable for projects that have a token in only one of these blockchains. Original tokens sent to TofuBridge contract on the one blockchain will become collateral for wrapped tokens issued on the other.

Let's consider that Alice wants to trade BAT ERC-20 tokens on TRON blockchain with lower fees. She sends her BAT tokens to TofuBridge smart contract in the Ethereum network and specifies her TRON address as a parameter. After her transaction was confirmed on Ethereum network she can receive wrapped BAT tokens on the TRON network and trade them or stake in liquidity pools on the TRON network.

If, some time later, Bob bought a large number of wrapped BAT TRC-20 tokens and he can't sell them for a reasonable price on the TRON network because there is not enough liquidity at the moment, he can send his tokens to TofuBridge contract on the TRON blockchain to redeem original BAT ERC-20 tokens on the Ethereum network and sell them.

5 TofuOracles

Trust is a fundamental concept that represents the level of risk to individual users of a system, where the higher the trust, the lower the risk assessment of the extent of potential damage in the event of attack is.

The process of cross-chain transfer should be trust-less. One external data source can maliciously or accidentally behave in a way that could compromise security of the system, either by reporting incorrect information or due to being subjected to censorship, blocking or filtering data, or any other external interference. It is the diversification of data sources that can help to increase the resilience of a system to the described threats.

The TofuOracles are set of independent oracles in both blockchains providing a reliable connection to the external data from real world and alternative chains to maintain Tofu services. We will utilize Gravity protocol[13] to achieve that. Users will need to pay a transfer fee to cover the expenses related to interaction with oracle contracts.

6 TofuSwap

TofuSwap is a protocol for automated token exchange on the TRON network. With TofuSwap users can swap between any two supported tokens by paying a 0.3% swap fee. It can be achieved in two ways:

- Direct exchange if there is a liquidity pool for the exact same pair and it offers the best price;
- Routed trades across several liquidity pools if possible

Each liquidity pool holds reserves of two TRC-20 tokens and issues an TRC-20 pool liquidity token as a proof of proportional ownership of the underlying reserves.

TofuSwap based on the same idea as Uniswap, but with some modifications and improvements. The original idea of Uniswap protocol is that smart contracts hold reserves of various tokens and trades are executed directly against these reserves. Prices are set automatically using constant product market maker mechanism, which keeps overall reserves in relative equilibrium:

$$b_{eth} * b_{tkn} = const$$

where b_{eth} – balance of ETH,
b_{tkn} – balance of ERC-20 token.

By using a simple constant-product invariant, Uniswap was able to create lightweight and gas-efficient contracts. Simplicity and gas-efficiency are very important properties for smart contracts executed on the Ethereum network because of high gas prices, but, at the same time, they are significant limitations for developing more sophisticated logic which can benefit users and liquidity providers. Fortunately, these limitations are not so restrictive on the TRON network.

Several improvements were introduced so far. On of them is StableSwap protocol by Michael Egorov[14] which introduced new formula for mean-reverting assets like stable tokens. Stableswap protocol combines the constant-sum invariant $x + y = const$ with the constant-product invariant $x * y = const$, based on the pool imbalance ratio χ:

$$\chi D^{n-1} \sum_i b_i + \prod_i b_i = \chi D^n + \left(\frac{D}{n}\right)^n$$

where b_i – balance of i-th asset,
D – sum of all balances of before swap,
χ – imbalance coefficient.

StableSwap provides a mechanism to create cross-markets for stable tokens in a way which could be called "Uniswap with leverage". It is a fully autonomous market maker for stable tokens with very minimal price slippage. Also it's an efficient "fiat savings account" for liquidity providers. This approach was implemented by Curve project on the Ethereum network. We will use this approach for stable token swaps.

Another improvement of constant product approach is an idea of using virtual balances in automated market maker smart contracts to mitigate front-running issues which was originally proposed by Vitalik Buterin[15].

When a user broadcasts an Ethereum transaction, it doesn't become part of the blockchain until a miner includes it in a block. This process can take from a few seconds to several minutes. During this time, other network participants can profit from their knowledge of the future inclusion of the transaction at the user's expense. This is called front-running. Even though, TRON blockchain is faster than Ethereum, front-running is still possible.

Virtual balances allows to blunt the price impact of the short-term trading volume slippage. This approach helps to reduce the impact of front-running and redistributes profits from arbitrageurs to liquidity providers.

We follow all the latest developments and research[16] relentlessly and will use them in our products to deliver cost-effective services to all our users.

7 TofuDeFi Token

TofuDeFi token (TOFU) is an TRC-20 asset that empowers community governance of the Tofu Project. Holders of TOFU tokens will be able to debate, propose, and vote on all changes to the TofuSwap and TofuBridge protocols.

TOFU token does not in any way represent any shareholding, participation, right, title or interest in any company or legal entity. TOFU will not entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore, Hong Kong or any relevant jurisdiction. TOFU tokens may only be utilized on the Tofu platform, and ownership of TOFU carries no rights, express or implied, other than the right to use TOFU as a mean to enable community governance of the Tofu Project platform and protocols.

7.1 Distribution

The total supply of TOFU token is 100,000,000 tokens. The distribution of the total TOFU supply is as follows:

- 30% will be sold in three public token sales

- 40% will be distributed between liquidity providers and traders within next 3 years
- 20% will be reserved for TOFU team for continued development and support
- 8% will be sold to private buyers
- 2% will be distributed between TOFU ambassadors

7.2 Governors

Governors are individuals who have 100,000 TOFU or more. Governors will be able to:

- Initiate community votes on new protocol changes
- Add new tokens to default list of tokens on the TofuSwap
- Promote their tokens on our website

References

[1] Ethereum Foundation. Ethereum webpage. https://ethereum.org/.

[2] https://en.wikipedia.org/wiki/Smart_contract.

[3] Hayden Adams, Noah Zinsmeister, Dan Robinson, Uniswap v2 Core, March 2020. https://uniswap.org/whitepaper.pdf.

[4] Mohsen Pourpouneh, Kurt Nielsen, Omri Ross, Automated Market Makers, July 2020. https://econpapers.repec.org/paper/foiwpaper/2020_5f08.htm.

[5] Bitcoin Wiki: Proof-of-Work.

[6] Brian Wu, Ethereum Blockchain Performance and Scalability, December 2019 https://blog.bybit.com/uncategorized/ethereum-blockchain-performance-and-scalability/.

[7] Coindesk: Ethereum Transaction Fees Set a Record Once Again as DeFi Becomes Even Pricier, September 1, 2020.

[8] Bitcoin Wiki: Proof-of-Stake.

[9] Alexander Skidanov, Detailed overview of Ethereum 2.0 shard chains: Committees, Proposers and Attesters, October 2018.

[10] Sergio Demian Lerner, RSK: Bitcoin Powered Smart Contracts, October 2015. https://www.rsk.co/Whitepapers/RSK-White-Paper-Updated.pdf.

[11] Joseph Poon and Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, January 2016. https://lightning.network/lightning-network-paper.pdf.

[12] Daniel Larimer, DPOS Consensus Algorithm - The Missing White Paper, May 2017. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper.

[13] Gravity: a blockchain-agnostic cross-chain communication and data oracles protocol, August 2020. https://arxiv.org/abs/2007.00966

[14] Michael Egorov, StableSwap - efficient mechanism for Stablecoin liquidity, November 2019. https://www.curve.fi/stableswap-paper.pdf.

[15] Vitalik Buterin, Improving front running resistance of x*y=k market makers, March 2018. https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281.

[16] Yongge Wang, Automated Market Makers for Decentralized Finance (DeFi), September 2020. https://arxiv.org/abs/2009.01676

8 Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. The opinions reflected herein are subject to change without being updated.