DeFi Blockchain White Paper

https://DeFiChain.io

by

Dr. Julian Hosp
U-Zyn Chua

v.0.1 2019-10-14

Abstract: The DeFi Foundation is developing the DeFi Blockchain, a blockchain specifically dedicated to decentralized financial applications. By focusing on the functionality of the blockchain and dedicating it specifically to decentralized finance, the DeFi Blockchain provides unparalleled high transaction throughput, reduced risk of errors, and intelligent feature development specifically for the fulfillment of financial services on the blockchain.

This Document is not a Prospectus

This document does not constitute nor imply a prospectus of any sort. No wording contained herein should be construed as a solicitation for investment. Accordingly, this whitepaper does not pertain in any way to an offering of securities in any jurisdiction worldwide whatsoever. Rather, this whitepaper constitutes a technical description of the functionality of the Cake products and the development and distribution of the DeFi Blockchain.

This Document is not a Final Technical Specification

This document does not constitute nor imply a final technical specification of the DeFi Blockchain. Information presented on this whitepaper, technical or otherwise, is meant to outline the general idea of DeFi Blockchain, its design and its use-cases and is subject to change with or without notice. For the latest up-to-date technical specification, check out the documentation on the official website https://defichain.io

Executive summary

The cryptocurrency industry is based on a simple premise: people should be fully in control of their finances. While it seems like a simple and obvious statement, the current systems are far from providing financial services that are truly under the control of the people who use them. The mission of the DeFi Blockchain is to give people (and in the future, machines, and devices) seamless access to decentralized financial services.

For that purpose, we are introducing the DeFi Blockchain, a dedicated blockchain specifically for decentralized finance (DeFi) www.DeFiChain.io.

By dedicating the functionality of a blockchain specifically to decentralized finance, the DeFi Blockchain provides high transaction throughput, reduced risk of errors, and intelligent feature development specifically for the fulfillment of Satoshi’s original intent: To create a reliable alternative form of financial services built on top of Bitcoin.

Bitcoin, as described in the original Satoshi whitepaper, is designed as a form of digital cash, as a store and exchange of value. The evolution to Ethereum and smart contracts has allowed for tremendous new functionalities to be built on top of a blockchain, yet this development has come at a cost. The concept of one global operating system for everything has created a system that requires a complex codebase for smart contracts, slow throughput, and difficulty around the governance of the system.

The DeFi Blockchain approaches decentralized finance as a specific and critical segment of the blockchain community. DeFi is a dedicated blockchain that is optimized specifically for DeFi applications. The DeFi Blockchain is intentionally non-Turing-Complete and does not support any function, other than those needed for Decentralized Finance, resulting in a blockchain that provides higher throughput and better functionality specifically for dApps related to finance. The advantage of a non-Turing complete command set is that there is a much lower potential for coding errors of the type that have plagued Ethereum smart contracts such as with the DAO hack or the locked funds with Parity. While it is important that we have some smart contract languages that are Turing complete, in the area of finance, it is appropriate to restrict the capabilities of the language in favor of a more secure system with greatly-reduced attack vectors.

The Problem

Today, almost all financial services are run by banks. Investments, for example, by definition, is the use of capital to earn more capital. Investors use a bank to put their money into interest or dividend-making instruments in order to grow their wealth. The problems with financial services are increasingly becoming obvious to everyone: compounded costs due to middle(wo)men, slow transactions, delays for cross-border transactions, and inaccessibility to many sectors of the population. A myriad of fintech solutions have been brought in to improve the system, but fundamentally the underlying banking system is still in control, so fintech has brought only limited improvements.

Cryptocurrency and Decentralized Finance (DeFi) offer a way to start with a new system, circumventing the difficulties faced in changing the finance industry. While crypto has attracted billions in investments, decentralized financial services are lagging. When it comes to investment in cryptocurrency, crypto investors can buy and sell, but that’s it. The cryptocurrency itself cannot be invested in the same way fiat currency can be. Initial attempts to create peer-to-peer lending and asset tokenization so far have proven partial and unreliable, so investors have extremely limited options when it comes to an investment of their cryptoassets. The potential is enormous to provide financial services in crypto, the same way they are offered in fiat currency.

The Solution

The DeFi Blockchain is designed for investors in the cryptocurrency market who are looking to make their cryptocurrency work just like any other form of capital, such that they can ensure a return on investment in any market. The DeFi Blockchain is a dedicated non-Turing-complete blockchain, designed specifically for the decentralized finance (DeFi) industry. DeFi provides full functionality for this specific segment of the DLT community, sacrificing other types of functionality for simplicity, rapid throughput, and security.

The function set includes among others:

- Decentralized lending
- Decentralized wrapping of tokens
- Decentralized Pricing oracles
- Decentralized exchanges
- Transferable debts and receivables

- Decentralized Non-collateralized debt
- Asset tokenization
- Distribution of Dividends

Team

The DeFi Foundation is incorporated as a company limited by guarantee in Singapore which resembles a traditional foundation structure.

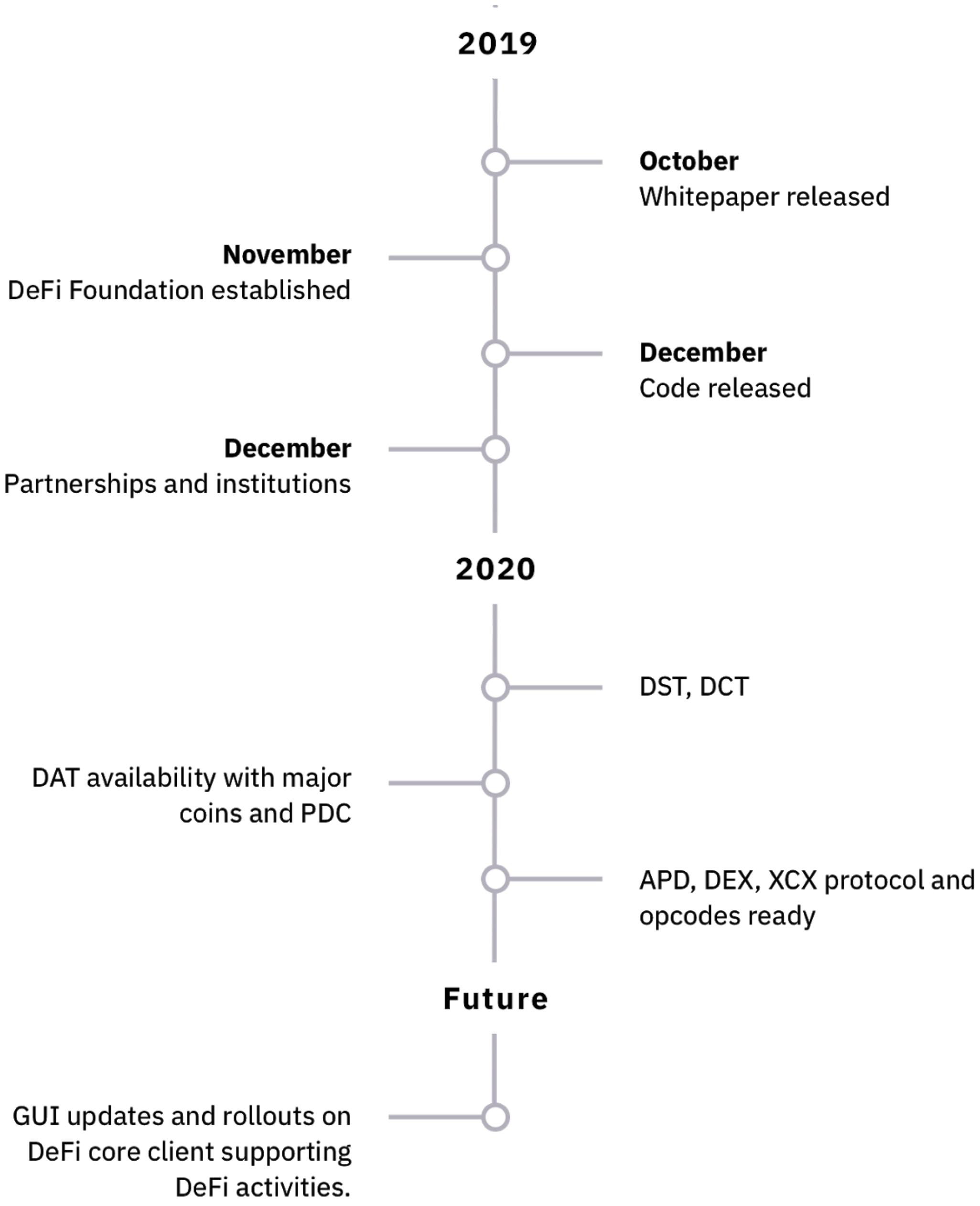
Dr. Julian Hosp, Chairman
https://www.linkedin.com/in/julianhosp/

U-Zyn Chua, Tech
https://www.linkedin.com/in/uzynchua/

John Rost, Finance
https://www.linkedin.com/in/john-rost-b70b0628/

Kenneth Oh, Legal
https://www.linkedin.com/in/kenneth-oh-840117158/

Timeline



2019

October
Whitepaper released

November
DeFi Foundation established

December
Code released

December
Partnerships and institutions

2020

DST, DCT

DAT availability with major coins and PDC

APD, DEX, XCX protocol and opcodes ready

Future

GUI updates and rollouts on DeFi core client supporting DeFi activities.

Background/Industry

DeFi's promises and challenges

Decentralized Finance promises to provide a variety of financial instruments without the need for middle(wo)men to ensure that the services are trusted. According to the OECD, financial services typically make up 20–30% of total service market revenue and about 20% of the total gross domestic product in developed economies.[1] This is an enormous industry dedicated to one thing: making sure that financial transactions are trusted. With the advent of blockchain, trustless systems and smart contracts can be used to replace much of the functionality of this industry, dramatically increasing the return on investment for the individual investor.

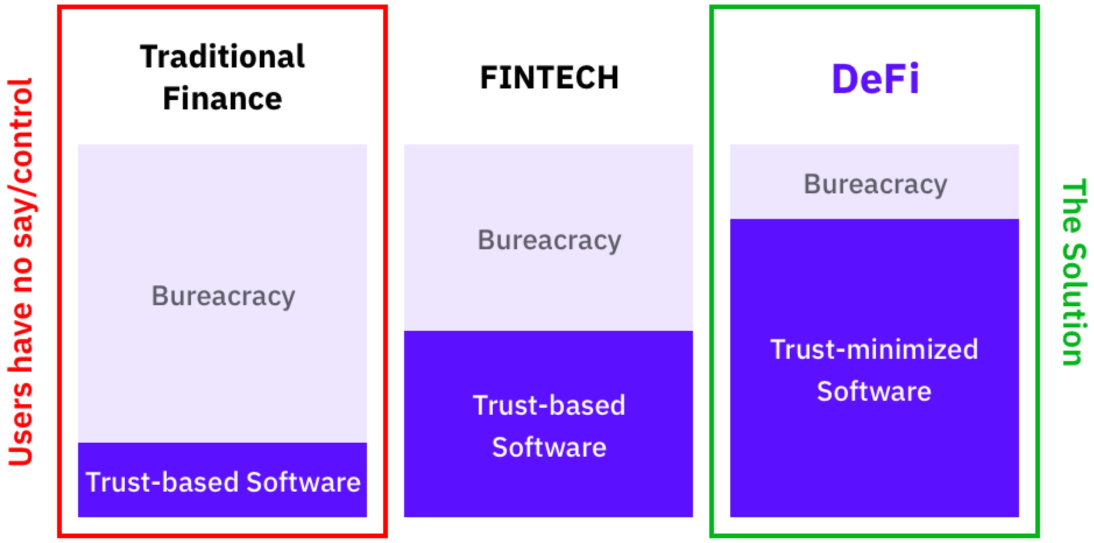
Financial services today are providing an important service, but at a very high cost, and despite many fintech developments, the following underlying issues persist:

- High transaction costs. Due to regulatory requirements, legacy systems with complex interoperability issues, and control by large institutions, transaction fees are high for the average user of banking and financial services. Services that require a broker are even more expensive, as agents and other types of middlemen are involved.
- Slow transactions, particularly for international transactions. Although theoretically, it should only take minutes for computers to transact, moving money from one institution to another can take hours within a country, and it can take days between countries.
- Lack of transparency and unfair advantages to large players. Financial instruments are complex and most people do not have access to the information that would allow them to make optimal decisions. Lack of transparency is one of the major factors that led to the 2008 financial crisis and in the short term, it always leaves smaller investors (the average person) at a disadvantage compared to institutional investors.
- Inaccessibility and/or higher cost to lower-income people. Financial services are simply not available in many geographies, and when they are, lower-income people are hit with even higher fees (percentage-wise) than average.

[1] https://www.investopedia.com/ask/answers/030515/what-percentage-global-economy-comprised-financial-services-sector.asp

- Despite legislation to reduce money laundering and related crimes, there is almost no evidence to suggest the current system or AML is, in fact, reducing money laundering.

Fintech has been attempting to address these problems, with some success. Fintech solutions such as online international transfer services, savings, and investment apps, and mobile money for underserved markets have begun to improve the situation. However, the change is incremental, and is still built on top of a system that fundamentally requires the overhead of agents to provide trust. While some of the costs can be reduced, fundamentally, fintech can't address the underlying issues of lack of transparency because it is dealing in the same financial instruments and going through the same major institutions as traditional finance.

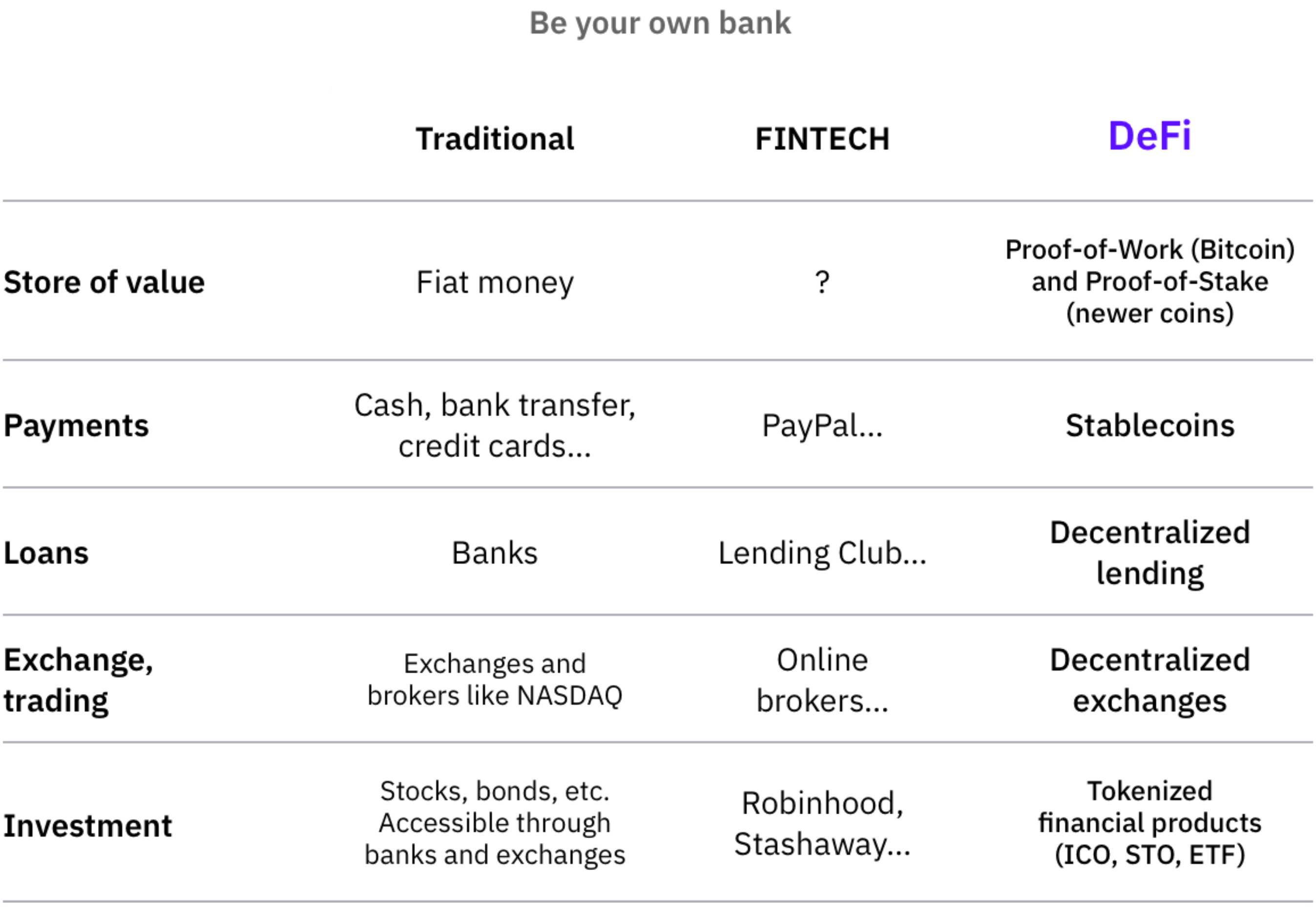


2019: DeFi – Decentralized Finance

For this reason, many investors have begun moving parts of their investments into cryptocurrency. Cryptocurrency, by definition has full transparency that traditional systems simply cannot provide. Furthermore, the amount of administration and bureaucracy required is minimal. Most of the activities that were carried out by agents can be written into the code in decentralized financial systems. Of course, there is still some overhead in creating and maintaining the code, as well as maintenance of the networks, but the amount of bureaucracy is minimal, eliminating much of the cost of transacting on these systems.

Despite the promise of decentralized finance, the technology is still nascent, and there are many opportunities to create a richer and more robust decentralized finance environment. To date, investors in cryptocurrency have extremely limited investment options. Promises of peer-to-peer lending platforms, asset tokenization and other types of blockchains have either failed to deliver, been hacked, or delivered a pared-down version of the original promise.

Today, almost universally, cryptocurrency investors have only one way to earn money on their capital: rise of the cryptocurrency asset. While in the short term, this may be a good investment, it’s not how currency is designed to work. The investment of capital should provide a return on investment, and cryptocurrency is designed to be like any other form of currency. Investors today want the possibility to lend, invest, and receive returns on their cryptocurrency investments. Well-designed DeFi platforms should allow the development of a variety of safe and secure financial instruments for the investment of cryptocurrency.



Be your own bank

	Traditional	FINTECH	DeFi
Store of value	Fiat money	?	Proof-of-Work (Bitcoin) and Proof-of-Stake (newer coins)
Payments	Cash, bank transfer, credit cards...	PayPal...	**Stablecoins**
Loans	Banks	Lending Club...	**Decentralized lending**
Exchange, trading	Exchanges and brokers like NASDAQ	Online brokers...	**Decentralized exchanges**
Investment	Stocks, bonds, etc. Accessible through banks and exchanges	Robinhood, Stashaway...	**Tokenized financial products (ICO, STO, ETF)**

The current DeFi state

The current state of Decentralized Finance (DeFi) is populated by general purpose blockchains, most of which provide Turing-complete command sets for the development of smart contracts on the chain. While appropriate for many programming languages, this dogmatic pursuit of Turing-complete smart contracts languages has resulted in a variety of problems when it comes to scalability, security and robustness of the blockchains.

- The sheer mass of dApps on networks such as Ethereum, EOS and TRON have potential (or proven) impact on other dApps on the network. The most obvious example was when CryptoKitties ground the Ethereum network practically to a halt. While some of the faster-throughput networks say this can’t happen, it will be some time before any other network reaches the critical mass of apps on Ethereum so that we can prove whether this is or isn’t the case.
- For serious financial type dApps, it’s important to know that the network is being maintained and managed in a responsible and secure manner. Having a blockchain that is swamped with games, gambling and other types of less “mission critical” apps will ultimately influence the development and direction of the blockchains. With governance models that allocate power to masternodes, dev groups, and token-holders, the core development team will ultimately be influenced by the biggest players. Decentralized Finance apps can’t afford the potential consequences of sharing a blockchain with anyone who chooses to use that operating system.
- Using Turing-complete command sets requires programmers to create complex programs to develop any kind of app. For example, to create a peer-to-peer lending contract on top of MakerDAO, a programmer requires approximately 2000 lines of code. Any bug in that code can cause loss of the funds, or some other consequence. Maintaining such a large code base intrinsically means larger chances for mistakes and a large attack surface for even simple apps.

The limitations of general-purpose blockchains for DeFi apps has opened up a market opportunity to serve this market. While cryptocurrency momentum has continued to rise, most of the current applications are still on Ethereum. Concerns about the network have already led some of the major projects to consider porting or working with alternative or additional blockchains.

DeFi’s current problems

- Finance dApps require reliability and do not want to be associated with blockchains that host apps such as betting, entertainment or other apps that may tarnish the reputation of a blockchain at any time.

- Sudden increases in volume of any dApp on a blockchain can potentially impact all the other dApps on that blockchain, either in terms of throughput, transaction price, or additional impacts, as seen with CryptoKitties on Ethereum.

- General-purpose blockchains require a large amount of coding to provide financial services, increasing the risk of hackability or bugs in the code.

- Functionalities that are basic requirements for financial services, such as multisig, are often difficult to implement or missing on general-purpose blockchains.

- Maintenance of a Turing-complete blockchain means that resources are not focusing on the areas valued by DeFi apps.

- Governance models of most of today’s blockchains are immature and showing signs of politicization, centralization and uncertainty. Without formal governance structures, the future of these blockchains is uncertain. Recent discussions of upgrades and forks in both Ethereum and Bitcoin have revealed the immaturity of these systems, and even the leader in governance, Aragon, showed the vulnerability of its on-chain governance system in the summer 2019 vote, where one large “whale” token-holder changed the outcome of several proposal votes at the last minute. Such vulnerabilities are unacceptable on blockchains dealing with finance.

- Regulatory standards and regulatory bodies that appropriately address the needs of natively cross-border currencies and financial instruments. Jurisdiction-based regulation, and regulation based on legacy technology is falling short of the needs of the DeFi industry. It is clear that a new legal and regulatory framework is needed to protect the rights of people using these systems.

- The blockchain industry itself has not shown the maturity to put in place its own standards bodies that will provide best practices or self-regulation in a way that would demonstrate the industry’s reliability for decentralized finance applications. To date, attempts at creating interoperability or self-regulation have been immature and have not resulted in leadership or standards that could be adopted by international bodies or serious regulators. The lack of self-regulation leaves the industry even more vulnerable to regulation from outside, making the environment risky for serious investors.

Consequences in the DeFi Market

- Multisig wallets are the best the industry has to provide when it comes to joint management of funds, and the solutions for multi-sig are, to some degree, kludges. Multisig tends to be leger-specific and not flexible for different scenarios. For example, in traditional finance, multi-signature accounts can assign signatories different levels of authority, or require different signatures for different transaction types and levels. Different chains take different approaches to adding multisig capabilities to their existing blockchains.
  - The BIP 11: M-of-N Standard Transactions is a Bitcoin Improvement Proposal (BIP)designed to add multisig support to Bitcoin blockchain.
  - Ethereum provides a Turing-complete command set for development of multisig on chain, leading to multiple entities providing multisig smart contracts. Bugs such as those in the Parity multisig (discussed below) have resulted in untold sums in lost funds.
- As a result of the complexity of the code required for multisig, in 2017, more than 150,000 ETH was lost to a hack in the Parity multisig wallet, due to an error in the code.[2] The referenced article notes ways in which this code bug could have been avoided, but it emphasizes the point that these complexities in coding cause many different attack vectors. An entire industry has sprouted up around smart contract auditing, because the situation is so vulnerable.
- In the largest industry hack (or bug?!), The DAO was drained of 3.6 million ETH due to a coding error in the smart contract holding all of the funds of The DAO.

One of the many results is that that the high risks get priced in to the underlying contracts leading to excessive costs for users, as can be seen when comparing rates from DeFi and non-DeFi examples. (For example 8% with decentralized DAI to 1.75% with centralized USDC (dated at the beginning of October 2019): https://deficompare.com/) Both coins represent 1 USD but the decentralized version ist 6.25% more expensive due to a priced in risk from the Ethereum contract.

The points described above are simply unacceptable for any type of financial transaction or investor. For that reason, it’s important to build dedicated services that will prevent such breaches, lower risks and thus cost. In the Blockchain world, having proper programming rules and reducing the attack vectors prevents this kind of attack.

[2] https://blog.zeppelin.solutions/on-the-parity-wallet-multisig-hack-405a8c12e8f7

Comparing existing DeFi alternatives

Bitcoin: Why Not?

Given our optimism on Bitcoin, the first question one might ask is why not develop DeFi using the Bitcoin Blockchain. While Bitcoin allows only basic smart contracts, some projects have begun developing workarounds. However, the transaction costs are restrictive on the Bitcoin chain, and we don't believe it is going to be appropriate for the speed required for financial transactions. The Bitcoin chain is currently working as designed as a store of value. In our opinion, sticking to that single purpose is the best use of the chain and it is proven over the last decade. Adding financial services into the main chain adds unnecessary complexity and may cause side effects both for DeFi and for Bitcoin that are undesirable. Furthermore, it is not something we think that the Bitcon governance is prepared to handle, and at some point, if the DeFi Blockchain requirements differed from those of the miners or developers on the Bitcoin chain, we would be subject to their decisions.

Turing-complete Solutions: Ethereum, EOS, Tron...

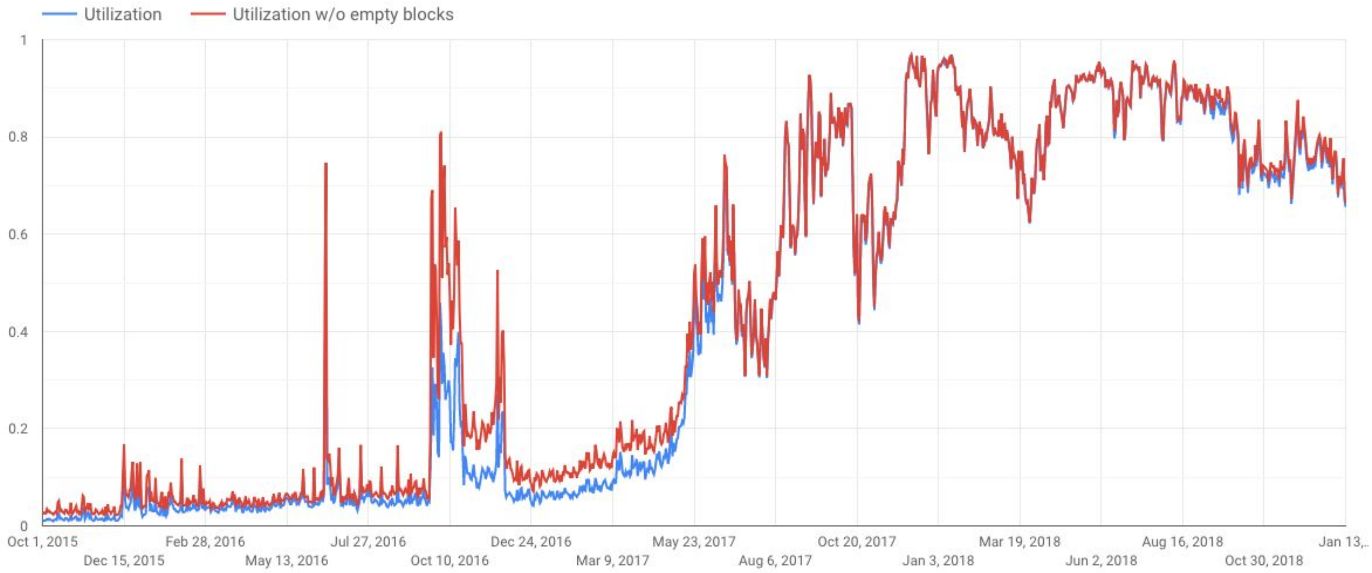
To date, a number of DeFi applications have been built on Ethereum, Tron, EOS and many other turing-complete chains. Since Ethereum has the biggest adoption it allowed the surfacing of issues that come with using a turing-complete blockchain for DeFi applications the fastest. The DAO hack was one of the first and most dramatic exposures of the vulnerability of using such a complex language. Anyone issuing a token on the network knows how difficult it is. Just to create and issue an ERC20 token can easily cost over 100,000 USD, considering the cost of smart contract auditing that is necessary for innovative solutions. Simply the fact that there's an entire industry built around "smart contract audits" should be enough to illustrate the problem. Despite the fact that ERC20 is the industry standard, it's still so easy to hack that it's impossible to issue even a simple token without getting a high-cost professional auditor as well as a programmer.

On an even more stark note, it's now possible to scan for exploitable code using automation, and a 2018 study managed to scan a million smart contracts, finding over 34,000 hackable smart contracts.[3] It's unfathomable that 3.4% of financial transactions would be vulnerable. While this

[3] https://arxiv.org/pdf/1802.06038.pdf

at the moment seems to be a problem mainly centered around Ethereum, we believe most other turing-complete chains will experience the same issues once more use cases get adopted on top of them.

The second problem stays mostly within Ethereum, which is the network's usage being already close to maximum capacity. It simply does not seem feasible to use the network for all of the decentralized finance applications. Ethereum's market cap is a tenth of that of Bitcoin. If the system is already near capacity, it's hard to see how it can manage the capacity of becoming a true DeFi network for the rest of the ecosystem. Something Vitalik has acknowledged in an interview: https://beincrypto.com/ethereum-founders-admit-never-designed-scalability/



Solution

Staying in the Bitcoin Ecosystem

The cryptocurrency market as a whole is difficult to predict. Most of the coins have become valueless, and it remains to be seen how the system will sustain itself after cash runs out from many of the major ICOs.

Despite this, our outlook on Bitcoin specifically is extremely optimistic. Over the last year, through market volatility, including instability in traditional financial markets, Bitcoin has retained its value, demonstrated its impermeability to attack and hackers, and gained increasing respect from traditional financial players.

Bitcoin is increasingly being seen as a store of value, and it is perceived as the standard by which other cryptocurrencies are measured. While people's portfolios vary widely, Bitcoin remains the standard currency that almost every crypto investor holds as a major part of their holdings. The tremendous community and ecosystem around Bitcoin bode well for its long-term viability as a store of value.

For that reason, creating decentralized financial services around Bitcoin represents a tremendous opportunity that has yet been untapped, partially because of the difficulty of creating smart contracts that work with the Bitcoin network, and partially because of the fractalization of the development community to many side projects. We believe this tendency of the development community to jump on the newest developments has drawn attention away from the real story: Bitcoin is here to stay.

Thus, we believe, building a DeFi Blockchain on top of Bitcoin would bring the best out of both worlds: Bitcoin's stability and immutability and DeFi-chain's scalability and functionality.

Building on Top of Bitcoin

One of the major challenges in new blockchains is creating the robust immutability available after a critical mass of users and blocks secure the chain. To provide immediate security and immutability of the blockchain, the DeFi Blockchain will be anchoring itself to the bitcoin blockchain. Every few minutes, the DeFi Blockchain saves its most recent Merkle tree to the Bitcoin blockchain, similar to how Rootstock (Turing Complete Smart contracts secured by Bitcoin https://www.rsk.co/) is planning on connecting to Bitcoin. In this fashion, the most recent chain is always fully secure and immutable, and can be checked against the most recent record anchored to Bitcoin. Over time, the DeFi Blockchain will space out the anchors at larger intervals. This anchoring mechanism ensures provably immutable records from day one and defends against attacks, hackers and vulnerabilities that can cause concern in emerging chains.

At the same time the DeFi Blockchain keeps its own consensus mechanism and function set, allowing for all those characteristics that Bitcoin does not inherently have. This is achieved by the DeFi Blockchain being a dedicated non-Turing-complete blockchain, designed specifically for the decentralized finance (DeFi) industry built on top of Bitcoin. The DeFi Blockchain provides full functionality for this specific segment of the DLT community, sacrificing other types of functionality for simplicity, rapid throughput and security.

The DeFi Blockchain utilizes a completely decentralized Proof-of-Stake mechanism allowing for:

- a massive scalable and energy conserving consensus.
- fast transactions and high security
- ability to create a variety of DeFi apps based on one chain, rapidly and with very low attack surface
- multi-token support on one chain through decentralized wrapped token technology.
- decentralized governance
- independence of other financial systems and financial instruments.
- fully liquid investments with no minimum size of investments, and no minimum lock-up periods

Unlike Ethereum or other turing-complete blockchains, the DeFi Blockchain is not a general-purpose blockchain, and commands outside the basic set of functions are not allowed. Limiting the allowed commands on purpose provides a dramatically reduced attack surface for smart contracts, eliminating the obvious breaches that are made possible when programmers need to design complex coding for these functions. The details of these will be described in the next section.

Benefits of the DeFi Blockchain: Summary

- Development of a variety of financial operations & vehicles for cryptocurrency economy.
- High throughput for all transactions
- Safer, more secure blockchain specifically for decentralized finance..
- Rapid development of dApps for decentralized finance.
- Peace of mind that the blockchain is not used for any types of non-financial dApps, thus decisions of Foundation and core developers are focused 100% on decentralized financial use-cases and nothing else.
- Rapid development of dApps with dedicated calls specifically for finance applications.
- Minimal attack surface of financial smart contracts developed on the platform.
- Reliable governance (off-chain and on-chain).
- Highly immutable – by periodic anchoring to Bitcoin blockchain.

Initial dAppSets

The initial function set includes:

- Decentralized lending
- Decentralized wrapping of tokens
- Decentralized pricing oracles
- Decentralized exchanges
- Transferable debts and receivables
- Decentralized non-collateralized debt
- Asset tokenization
- Distribution of dividends

This chapter provides an overview of each of these functions and the following chapter covers the technical details in how this is achieved.

Decentralized Lending

Decentralized lending allows individuals and groups to borrow and lend without the intervention of a bank. Through collateralized systems, decentralized lending on Ethereum reached over a quarter of a billion dollars in 2018.

All of these systems are based on Ethereum, meaning they are addressing only 15% of the market (based on market capitalization. The DeFi platform will be addressing the entire 100% of the market by leading with Bitcoin, but also including the entire market through wrapping and pooling as described below.

The major decentralized lending platforms (Compound, Dharma, dYdX, and Maker) provide lending at rates ranging from 0.5% through 6%. Because everything is managed through smart contracts, the overhead of banks is eliminated, and the platforms are able to provide much better rates than banks. As these types of decentralized lending services become safer, it’s likely the market will also see an increase in peer-to-peer lending opportunities through dedicated applications.

The power of decentralized lending lies in the market efficiencies available by eliminating the middlemen and administration involved in lending. Furthermore, with investors concerned about minimal or even negative interest rates, decentralized lending protects the investors from that potentiality, providing market rate interest while giving borrowers better rates than they can get in the existing financial markets. Given the magnitude of credit and the role it plays in the economy as a whole, decentralized lending offers the potential for many more initiatives to borrow money based on open markets and favorable conditions. Easier access to lending translates into a faster-growing economy.

Initial implementations of decentralized lending are fully collateralized, and because of the volatility of cryptocurrency, most platforms require double or more collateral on loans. This allows people to take loans based on cryptocurrency they hold. They can manage their cash flow problems without having to sell their crypto holdings, and meanwhile get favorable conditions on the loan.

Decentralized Wrapping of Tokens

An important issue for DeFi is the ability to work with a variety of cryptoassets, directly, on-chain. While the transaction on the chain is done via the native DFI token, the DeFi Blockchain can use Bitcoin, Ethereum, ERC-20, or any other cryptoasset through wrapping.

Wrapping allows the utilization of any digital asset such that the underlying asset is maintained, but it can transact on a different blockchain. The DeFi Blockchain provides a decentralized wrapping mechanism which allows the owner of the crytpoasset to maintain pegging to the asset and utilize a trustless wrapping mechanism that does not rely on any third party as a guarantor of the wrapping or asset. The wrapped tokens can be easily exchanged for their original value on their respective blockchain.

Creating a wrapped token on the DeFi Blockchain is a rewarded activity, such that there is incentive for cryptocurrency holders to create wrapped tokens on the DeFi network as a form of rewarded decentralized financial investment.

Wrapping is a key capability of DeFi due to the need for interoperability of different types of cryptocurrencies and assets. To date, there are no interoperability standards between different currencies, and the only way to interoperate between currencies is by using wrapping or collateralization, which has to be provided by a third party. The entire point of decentralization is that people do not need to trust an authority, yet, today that is the main way that investors can interoperate between Bitcoin and Ethereum without converting from one coin to the other. The Polkadot protocol provides a platform for the development of interoperable apps, but not specifically for DeFi. As a new protocol, it is yet to be seen how it will be leveraged.

Without wrapping, holders would need to convert their cryptoasset to the DeFi currency in order to use the services offered. Obviously, for most investors, that’s unacceptable. The investor has put their money into Bitcoin, or Ethereum, or whatever else, because that is the currency they want to hold. The main purpose of the DeFi Blockchain is to enable financial transactions in any type of crypto asset, such that people can use the assets and coins they hold, as currency for investment in other types of financial vehicles.

The decentralized wrapping function is crucial in allowing people to hold any asset and perform investments in another currency. So, for example, someone holding Bitcoin could make a loan to someone who wants to borrow ETH, or someone who wants to hedge against the cryptocurrency they have could do so using a wrapping function to use some of their assets to purchase options in other types of assets.

Decentralized Pricing Oracles

The DeFi Blockchain will include pricing oracles to collect data from outside blockchains. Oracles are used to collect data such as pricing of other cryptoassets.[4] Oracles are an important way for blockchains to collect accurate information from both other blockchains and from non-crypto markets.[5]

Participating as an oracle allows earning of tokens based on the accuracy of the oracles. The built-in oracle function will allow smart contracts to determine the number of oracles, consensus percentage, and the parameters for rewarding oracles for the data they provide.

Oracles are eventually meant to be decentralized. However, DeFi Blockchain will be launched with a few appointed trusted pricing oracles that periodically submit pricing data from trusted source onto DeFi Blockchain.

Decentralized Exchanges

The decentralized exchange function will allow atomic swap of cryptocurrencies in a peer-to-peer fashion.[6] The decentralized exchange function matches people for trading directly, without the need to buy and sell currency through an exchange. Using decentralized exchange reduces the risks associated with using exchanges, and ensures that the cryptoasset doesn’t leave the custodianship of the token-holders. It also removes the risk of custodianship from the exchange itself, because the mechanism is peer-to-peer based on an agreed-upon price or on the market price at the time of the exchange.

While a number of decentralized exchanges are available on the market today,[7] the DeFi Blockchain solution allows integration of atomic swap capabilities in third-party applications by creating a decentralized exchange as a service.

[4] https://cointelegraph.com/explained/blockchain-oracles-explained
[5] https://hackernoon.com/oracles-help-smart-contracts-resolve-subjective-events-d81639d8291c
[6] https://en.wikipedia.org/wiki/Decentralized_exchange

[7] https://coinsutra.com/best-decentralized-exchanges-dex/

Transferable Debts and Receivables

The DeFi Blockchain will offer a set of calls to work with transferable debts and receivables. In the centralized finance world, debts and accounts receivable can only be managed through financial institutions that handle loans. The lack of transparency of these transferable debts was one of the factors leading to the financial crisis of 2008.

For small and medium enterprises, this can be a particularly powerful tool. For example, Jane's widget factory supplies widgets to a large car manufacturer, but the car manufacturer pays for those widgets on a basis of invoice +60. Meanwhile, Jane has to pay for the materials to produce the widgets, and, of course, regular salaries to her workers on a monthly or weekly basis. The car manufacturer will pay the invoice, but not in time for Jane to pay all of her expenses. Without Defi, Jane needs to go to the bank and pay whatever interest rates they demand, because she has no alternatives. The transferable receivables function would allow anyone to offer Jane a loan based on the receivables. Since many people would be able to see that the car manufacturer is a low-risk customer, and that they will pay their invoices, anyone who wants can make an offer to Jane for a better rate than the bank, creating a competitive market for debts and receivables based on the real risk and market assessment of that risk. Jane now can get a loan with great rates, and the lenders, likewise get excellent returns on their loans, despite the fact that they are loaning the money for only 30-60 days.

Blockchain adds transparency to the exchange of debts and loans based on receivables or other types of financial promises. The DeFi Blockchain will include the capability for organizations to create smart contracts that allow straightforward investment in such assets, so that peer-to-peer loans can be made without the need for a financial institution to guarantee these types of financial assets.

Decentralized Non-Collateralized Debt

In the future, it will be possible to provide non-collateralized loans based on the reputation and other factors about borrowers. Through different forms of verifiable credentials, and records of an individual’s borrowing and repayment history, non-collateralized systems can be developed. Many of the identity solutions being developed today are looking at anonymous and pseudonymous reputation-reporting systems, based on a Decentralized Identifier (DID) issued by the individual, and Verifiable Credentials (VC) issued by known authorities who are reputable to provide information about the individual’s credit history.

The appropriate reputation based systems and risk assessment systems will need to be built out. While this will take time, perhaps years, it is foreseeable that this kind of system could supplement or replace today’s credit ratings scores.

Another potential application of this feature would be the ability to create non-collateralized decentralized stablecoins. The success of DAI and MakerDAO show the desirability of pegged stablecoins, yet the high level of collateralization is a deterrent to creating more such projects. It is feasible that through market mechanisms and staking, decentralized non-collateralized stablecoins can be created.

Asset Tokenization

Asset tokenization is the representation of an asset, such as real estate or company equity, in immutable tokens on the blockchain.[8] This particular area of decentralized finance has tremendous potential and is one of the most exciting areas of investment for holders of cryptocurrency.[9]

While several attempts have been made at asset tokenization in the blockchain space, most of them have pivoted and now provide services not directly related to asset tokenization (LAtoken, Etherparty). Tokeny and Tokenize-IT advertise themselves as tokenization platforms, but as of the writing of this paper, their processes are still fairly manual, and are heavily reliant on specific localities and regulatory requirements for those specific jurisdictions. Other blockchains, such as Tezos, have been mentioned as good platforms for asset tokenization, but, as with other multi-use blockchains, the Turing-complete set of commands will create complex smart contracts that are unnecessary when using the DeFi Blockchain.

The DeFi Blockchain will provide a module specifically designed for asset tokenization, and will be particularly easy to use to tokenize assets such as company equity, real estate, and other valued holdings.

Recently (October 2019), the Lichtenstein Blockchain law created the legal basis upon which any asset can be tokenized and legally bound to tokens or “containers” that represent the right to the asset. The law is precise in its wording, describing how a container issued by a trusted party now can hold the legal rights to the disposal over the asset. Disposal over the asset is distinct from ownership or rights to the asset, or even control as a specific concept. The careful wording of this law is a breakthrough for everyone in the world of asset tokenization, because it will now allow someone to go to a court of law with a token and expect to have legal legitimacy for assets that are tokenized (as long as the authority granting the token is recognized as a trusted authority to do so). It also opens up a space for the DeFi Blockchain to apply for this trusted status, such that the Asset Tokenization capability described here can be offered as a decentralized, legal and authorized capability that people can trust, without having to depend on any centralized authority.

[8] https://medium.com/@credits/tokenization-of-financial-assets-financial-blockchain-revolution-bc632e75c8

[9] https://www.forbes.com/sites/laurencoleman/2019/04/25/heres-why-interest-in-tokenizing-assets-is-starting-to-surge/#2ddeec4640a5

For more information on this law, please see Liechtenstein’s website at https://liechtensteinusa.org/article/liechtensteins-parliament-approves-blockchain-act-unanimously

Examples of assets people can now tokenize using the blockchain:

- Securities, such as ETF investing, stocks and shares.
- Shares in privately held companies.
- Energy and income generating devices, such as wind turbines, solar farms, satellites.
- Ownership in food means of production (new forms of cooperative farms where non-farmers could own food supply instead of commodities traded on exchanges)
- Self-driving cars, vending machines, ATMs pinball machines, and other types of revenue-generating self-regulating devices.
- DAOs (Distributed Autonomous Organizations).
- Small real estate investments (time shares, short-term rental apartments, etc.)
- Large real estate investments (airports, amusement parks, apartment complexes, business parks)

Distribution of Dividends

Any tokenized asset with return on investment can use the dividends distribution module to create smart contracts that pay out returns on the investment automatically. Using the DeFi Blockchain will allow a leap in the functionality of dividends distribution. It will be possible to implement models similar to today, where payouts are performed on a weekly, monthly, or quarterly basis, or models where payouts are on a daily, hourly or even minute-by-minute basis.

Distribution of dividends would be relevant in any type of tokenized asset, as described above. For example, today, a municipal government might do a bond issue to invest in a wind turbine to supply electricity. The government would take care of everything, and repay that bond according to the schedule. With distribution of dividends, the community could purchase the wind turbine directly, and distribute the dividends to the investors in the wind turbine. Instead of going through the administration required through the centralized authority (government), every citizen who wanted to could invest in that wind turbine, and dividends would be paid according to each person’s contribution to that investment. Eliminating overhead and fair distribution of profits would be major benefits for the community owning the wind turbine. In this case, the wind turbine is a public good, but it could also simply be a private investment.

Any private investment could be run this way: a pinball machine, self-driving taxi, real estate investment, etc. Automatic distribution of dividends reduces the need for administration and overhead, as well as eliminating uncertainty about payouts and control by a centralized authority.

The need for joint dividend investing is becoming increasingly relevant with IoT. Devices are able to create tremendous value. A self-driving car will be able to provide taxi services. Vending machines, sensors, satellites, etc., are all potentially revenue-generating devices that people can own together and share in the profit of together, yet until now the legal and financial complexity of doing so has been prohibitive. DeFi can simplify those processes.

Similarly, distribution of profits for a private company can be implemented. One of the first experiments in this area is a DAO (Distributed Autonomous Organization) called dOrg. dOrg is a collection of programmers (as well as a sales/operations team) who co-own their software house. Distribution of salaries is through a DAO that functions as a multi-sig, such that every 2 weeks, the whole organization submits their payment requests for work contracted, and the team votes to pass one anothers' salary requests. Inside dOrg, each person holds a "reputation" that represents the percentage of ownership each person has earned (they earn ownership according to the amount of work done since the inception of the company). But what will happen to the profit at the end of the year? Presumably, each individual will have to submit a request for their percentage of the profits, and everyone will have to vote on that, too, because the DAO does not allow for automated distribution of profits. Using the DeFi Blockchain, the team could easily implement a quarterly or annual function that would automatically distribute the profits of the company to each person, according to their holdings in the company. This scheme would work even for people who were active in the past, but are no longer active, so they aren't in the DAO any longer, but they still hold a percentage based on their past contributions. Other contributors might be an investor who puts money into the company, but does not participate.

The examples above seem logical and straightforward, but today are extremely time-consuming and complex. People who want to make an investment together in companies, real estate, or other income-deriving assets type of dividend distribution today is complex and requires a lot of manual calculations. Through the DeFi Distribution of Dividends functionality, it becomes not just simple, but automatic for companies to distribute dividends to equity owners.

The Blockchain

Design Parameters

Looking at the business requirements from the chapter before, the DeFi Blockchain needs to meet the following requirements:

1. Robust and secure: built on a proven and secure blockchain.
2. Fast and scalable.
3. Includes decentralized consensus mechanism.
4. Provides extensible smart contract support, without a Turing-complete instruction set.
5. As immutable as possible (Block anchoring enabled.) .

Each of these design principles is described in detail below.

1. Robust and Secure

Bitcoin Core is the most robust and longest running blockchain in the world. It has been operating with no disruptions since the genesis block in January 2009. Furthermore, from a security standpoint, Bitcoin core is has proven itself to be most secure blockchain with no security incidents, while securing the crypto asset with the highest valuation in the world, that is, Bitcoin (BTC). As of this writing, Bitcoin Core successfully secures $150 billion worth of crypto assets, or 68% of the crypto asset market capitalization.

The proven security and robustness of the Bitcoin Core made it the blockchain of choice for DeFi Blockchain base for extension. DeFi Blockchain is built based on a fork of Bitcoin Core 0.18, specifically v0.18.1.

The DeFi Blockchain will be written in C++, and the plan is to use other languages, such as Rust, in the future.

While the DeFi Blockchain is a new blockchain, basing it on a Bitcoin Core fork results in a chain that is easy to integrate with for exchanges and apps that support Bitcoin.

2. Fast and Scalable

One of the proven disadvantages of the Bitcoin blockchain has been the slowness of transactions on the chain. Furthermore, scalability has become an issue as the number of blocks on the chain increase.

In order to implement a blockchain with the required speed and scalability, the DeFi Blockchain fork of Bitcoin Core will include the following improvements:

- Block time: 30 seconds
- Block size: 16 MB

These improvements provide a transaction rate of over 2,200 transactions per second (tps) while maintaining manageable compute and bandwidth requirements to allow for decentralized operations of the DeFi Blockchain.

The following table compares Bitcoin and its forks, as well as Ethereum, to the DeFi Blockchain performance:

	Block time (s)	Block size (MB)	Tx block space (% of block size)	Min tx size (B)	Avg tx size (B)	Txs in a block (max)	Txs in a block (avg)	Max tps	Average tps
Bitcoin Core	600	1	98%	220	500	4,561.45	20,07.04	7.60	3.35
Bitcoin Cash	600	10	98%	220	500	45,614.55	20,070.4	76.0	33.45
Bitcoin SV	600	32	98%	220	500	145,966.55	64,225.28	243.28	107.04
DeFi Chain	30	16	98%	220	500	72,983.27	32,112.64	2432.78	1,070.42
	Block time (s)	**Gas limit**	**Tx block space (% of block size)**	**Min tx size (gas)**	**Avg tx size (gas)**	**Txs in a block (max)**	**Txs in a block (avg)**	**Max tps**	**Average tps**
Ethereum	13.5	10m0	100%	21k	60k	476.19	166.67	35.27	12.35

3. Decentralized Consensus Mechanism

Bitcoin Core is using Proof-of-Work (PoW) as the consensus mechanism. The DeFi Blockchain leverages the best aspects of PoW, that is, using hashing of the staking node's ID for block creation while focusing the majority of the consensus on Proof-of-Stake (PoS). The major improvement in the PoW mechanism for DeFi Blockchain is that staking nodes can run without investing in high-end servers and ultra-fast bandwidth connections. Thus, DeFi Blockchain is creating the potential for easier and faster decentralization of the mode ownership and infrastructure.

4. Non-Turing-complete Smart Contracts

Decentralized financial transactions are implemented through smart contracts. For example to ensure that borrowers repay lenders, smart contracts implement the conditions of lending in the code. For smart contract development, DeFi Blockchain will be adding opcode support for decentralized financial instruction sets. The DeFi opcode complements and works in tangent with the Script scripting language of the existing Bitcoin Core protocol.

The DeFi scripting language is called **Recipe,** denoting the language's role in describing and allowing for decentralized financial contracts.

Bitcoin Script instruction words usually start with the prefix OP_*. Recipe instruction words carry the prefix DF_*.

5. Immutable through Block Anchoring

While the common discussion of immutability is a binary conversation (a blockchain is either immutable or not), in fact, immutability is on a spectrum. The level of immutability of a blockchain is related to the cost of a rollback or "fork out" of mined blocks, also known as a 51% attack.

It takes time to amass significant miners or minters to make 51% attack costly enough that it is generally regarded as immutable, meaning that a new blockchain is automatically at a disadvantage when it comes to the immutability of the records. Some newer blockchains have been taking shortcuts to increase its immutability quality, typically by compromising on decentralization. For example, the chains may allow only delegated stakers chosen by the founders, or by making the blockchain permissioned instead of permissionless.

DeFi Blockchain aims to maintain decentralization quality while maintaining immutability. To do so, the DeFi Blockchain will anchor its block to Bitcoin blockchain every few blocks. This further enhances the immutability of DeFi Blockchain without any compromise to the decentralized nature of the chain..

Consensus Algorithm

Proof-of-Stake

DeFi Blockchain utilizes a Proof-of-Stake (PoS) algorithm similar to Bitcoin Core's original Proof-of-Work (PoW) mining algorithm. While DeFi Blockchain is choosing PoS over PoW, at the same time, DeFi technology retains the best of the tested and proven technologies that were developed in the Bitcoin Core blockchain.

Masternodes for Staking

To run a masternode (staking node), stakers must hold a fixed amount of DFI, initially set at 100,000. Masternodes on the DeFi Blockchain participate in active transaction validations and block creations.

Each staking node can perform only 1 hash per second, with the nonce from Bitcoin Core PoW algorithm replaced by a staker's UTXO.

A new block is mined if it satisfies the following condition:

```
SHA256({staker's UTXO}, {current timestamp, in seconds}, {stake modifier}) < {target}
```

The stakers check this requirement each second. If the block condition is less than the current target, then the stakers assemble and sign a new block.

Staker's UTXO require 20 confirmations before it can be accepted as a stake.

Stake Modifier

A stake modifier is a collective source of random entropy. Without a stake modifier, the future PoS kernel would be completely predictable. A good stake modifier needs to be neither predictable nor influance-able by stakers.

The DeFi Blockchain's staker modifier is set to be SHA256({previous stake modifier}, {masternode ID}).

Validation of Future and Past Headers

Unlike PoW, block header validation requires a stakes table. Headers get verified in batches before full blocks are downloaded, so the stakes table is used to verify future stakes.

To be able to verify future headers, the blockchain needs to apply an additional rule, so any change of the stakes database gets written right away, but takes effect only after 300 blocks. As a result, any node will be able to verify any block header against its current stake, if a block header isn't further in the future (or in the past) than 300 blocks.

Nothing at Stake Protection

For PoS blockchains, there's no limit to how many conflicting blocks a staker may sign. As a result, stakers may stake for every possible fork or branch, which weakens the finality of a PoS blockchain. This problem is known as a double-sign and is not possible in PoW blockchains, where a miner cannot mine all the possible branches without splitting mining capability. In PoW, this represents an intrinsic economic penalty. However, PoS blockchains cannot apply an inherent economic penalty for signing conflicting blocks on different branches.

Therefore, in order to enhance the finality of DeFi Blockchain, in PoS, it's necessary to detect double-signs and penalize them through an explicit mechanism.

Detection of Double-sign

Each block header has a sequence number as a number of blocks that a particular staker has minted before a particular block. If two blocks are minted with the same sequence number, it means that a staker has double-signed, even if the blocks have different ancestors, i.e. across branches.

During a block's generation, a staker has the right to include the double-sign proofs into his block header in exchange for only half of the penalty.

Double-sign Penalty

To be able to apply a penalty to stakers who double-sign, the DeFi Blockchain has to disallow immediate withdrawing of stake. Thus, when a deactivation transaction is confirmed, the DeFi

Blockchain requires 3000 blocks to pass. At a block time of 30 seconds, 3000 blocks is equivalent to 25 hours.

The double-sign penalty is 10 times the block rewards, deducted from the collateral. This also disqualifies the stakers from further staking immediately. The staker wanting to get back to staking has to re-put in fresh stake UTXO of 100,000 DFI. Running the official DeFi Blockchain node does not cause any unintentional or accidental double-sign. Double-sign happens only in cases of malicious intent.

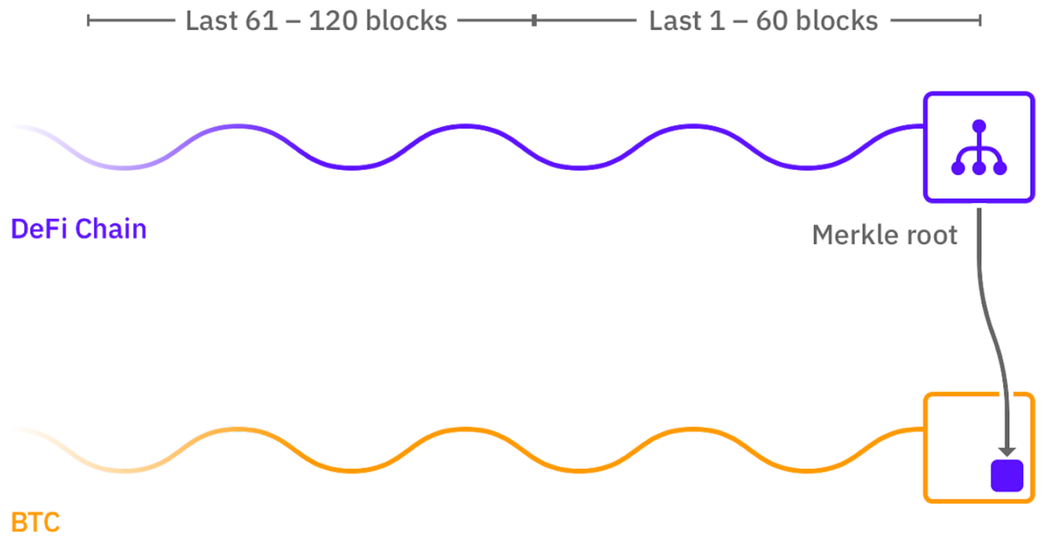
Time Drift Attack

The chain uses a maximum future block time of only approx. 5 seconds, to protect the chain from time drift attacks, where stakers set a block time too far ahead in the future, in order to claim a reward for themselves. . DeFi also uses NTP time synchronization to allow for ongoing adjustment to the block time.

Bitcoin Anchoring

DeFi Blockchain stakers publish blockchain block hashes periodically to the Bitcoin blockchain, providing public audit and block anchoring of the DeFi Blockchain to the strongest, most secure blockchain in the world.

Every 60 blocks (approximately 30 minutes), a staker gets the right to write the Merkle root of the previous block onto the Bitcoin blockchain. The information written is, specifically, the txid of the Bitcoin transaction, Bitcoin block header and Merkle proof containing the Merkle root onto the newly mined block. By doing so, the staker will be rewarded an extra block reward in DFI, incentivising nodes to regularly anchor all records to the Bitcoin blockchain.



The DeFi Blockchain node will include a built-in Bitcoin Simplified Payment Verification (SPV) client. SPV clients sync the Bitcoin blockchain by downloading only block headers which is sufficient information for nodes to add and validate the anchors.

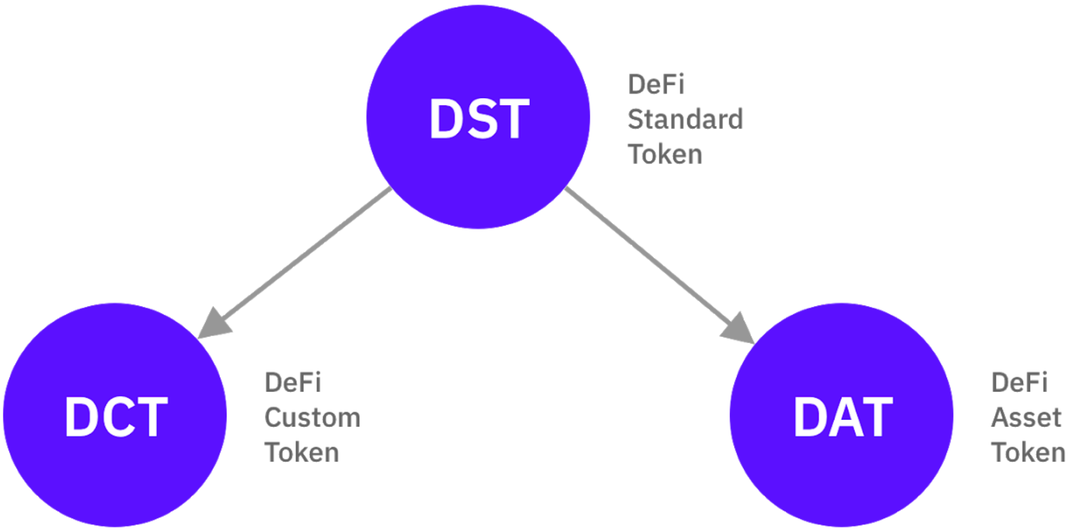
Tokenization as a DeFi Standard Token (DST)

The implementation of the features described in this whitepaper is performed with the use of standardized tokens. This chapter describes the mechanics of the tokens, interaction with other cryptoassets (tokens), and how they are used in the DeFi Blockchain.

Cross-chain Mechanics

DeFi Blockchain uses token standards to bring in external tokens to DeFi Blockchain in a trustless manner and allow trustless financial contracts and trading of all major cryptoasset tokens. The token standards are similar to ERC20 on Ethereum and Omni on Bitcoin blockchain. Through this standard, DeFi Blockchain allows tokenization of any assets.

On the DeFi Blockchain the standardized tokens are called DeFi Standard Token (DST). DST tokens are of two different types: DCT, created by users of the system, and DAT, which are asset-backed tokens created with the backing of cryptoassets.



DeFi Custom Token (DCT)

DCTs are custom tokens that can be created by any user to represent any project or set of smart contracts implemented on DeFi Blockchain. Any user can create such a DCT. To prevent abuse, creation of any proprietary DCT requires the user to lock up 1,000 DFI for the time that the tokens are issued. The DFI is returned when the tokens are revoked and the DCT is cancelled.

DCT tokens are not backed intrinsically by the DeFi Blockchain. They may be backed through an external mechanism, but it's essential to note that the DeFi Blockchain does not intrinsically back them. An example on the Ethereum blockchain would be DGX, which is an ERC20 token backed by gold. The Ethereum does not back DGX, although the token is created through ERC20. The Digix Foundation is accountable for the value of that token. Similarly, DCT is the DeFi parallel to ERC20 on Ethereum. Creation and issuance of tokens on DeFi is simplified and the potential for errors in the smart contract is eliminated, because creators of DCT can set only the parameters below, using an easy to use scripting interface.

DCT Parameters:

- DCT ID: <UDID> Unique blockchain identifier for the token.
- Name: <Token name> Name of the tokens.

- Symbol: The ticker symbol for the tokens. The DCT protocol will provide a reference for ensuring the choice will be a unique symbol.
- Decimal places: Divisible number of decimal places for the tokens. This cannot be changed once it is set.
- Total initial supply: Initial issue of tokens during the event generated.
- Initial distribution list: List of addresses for distribution of tokens.
- Minting support: yes/no
- Final supply limit (optional): Immutable total supply limit. If minting is supporting this will define the ceiling on how many tokens the token owner can mint in total (some may be reserved at this time). If this parameter is left blank, this is an unlimited supply token. This cannot be changed after the initial definition of the token.
- Tradeability: yes/no. This is a one-way switch allowing the token owner to transfer tokens during initial distribution period and also to decide when a token is tradeable/movable. To ensure the decentralized nature of DCT, once "tradeability" is set to yes, the owner is no longer able to reverse the tradability of a token. Typically, when creating a token, this should be turned to "no" until the initial distribution is confirmed to be accurate.

Using this interface, there is no need to have a smart contract developer, and there is no need for a security audit.

DeFi Asset Token (DAT)

DeFi Asset Tokens (DATs) are backed in a decentralized manner. DATs on the DeFi Blockchain are tokens and crypto assets external of the DeFi Blockchain, such as:

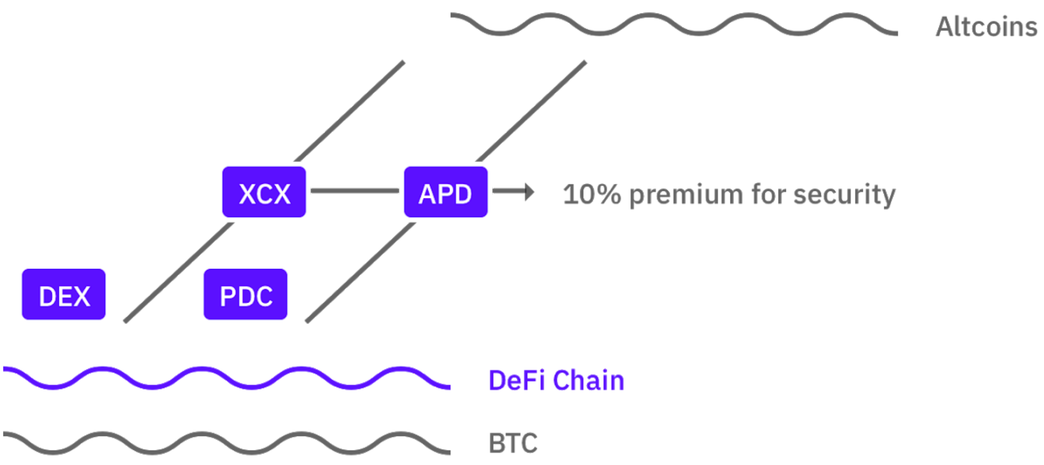
- DBTC, backed by BTC
- DETH, backed by ETH
- DXRP, backed by XRP
- DUSDT, backed by USDT
- DBCH, backed by BCH, etc.

New DATs are introduced to the system through voting by masternodes. This ensures that only assets that gather the most interest amongst DeFi Blockchain users get introduced.

Mechanism of DATs

1. PDC - Personalized Debt Contract
2. APD - Asset Peg Depository
3. DEX - Decentralized Exchange
4. XCX - Cross-chain Exchange
5. Pricing contract

DAT Overview



Personalized Debt Contract (PDC)

A Personalized Debt Contract (PDC) is designed to allow the owner of the PDC to take a collateralized loan against collateral locked in the PDC. Each PDC is unique to every owner (address) on the DeFi Blockchain.

Any user can open a PDC on DeFi Blockchain, free of charge. The user who opens a PDC owns a specific PDC. This ownership is transferable.

Once a PDC is opened, DFI can be sent to fund the PDC collateral. Once a PDC is funded, it allows the owner to take out a loan by minting DATs up to a certain collateralization ratio. The minimum collateralization ratio can be adjusted by the DAO and starts at 150%. In other words, $1,500 worth of collateral (in DFI), allows the PDC owner to take out a maximum of $1,000 in loans.

Minted DATs are subject to a floating borrowing rate. A PDC has no expiry date. The owner is able to take out a loan for as long as they desire, as long as the collateralization ratio stays above 150% at all times.

Collateralization ratio = Collateral / (Loan + accrued interest)

If a PDC falls below the 150% collateralization ratio at any point in time, a PDC's collateral is liquidated via Decentralized Exchange (DEX) to pay off accrued interest. There will be an additional 15% liquidation penalty to discourage PDCs from having to be liquidated. It is the responsibility of the PDC owners to monitor the collateralization ratio to prevent an unwanted liquidation.

If a PDC is close to minimum collateralization ratio, the owner must take one of the following steps to prevent liquidation and having to incur 15% liquidation penalty:

1. Deposit more DFI into the PDC, thereby increasing its collateral and collateralization ratio.

2. Pay back some of the loan (or accrued interest), thereby decreasing the PDC's loan amount and increasing its collateralization ratio.

Closing a PDC entitles its owner to get back all 100% of its collateral. To close a PDC, the owner has to pay back the loan in full, plus the accrued interest in its entity in the DAT (e.g. DBTC). Upon liquidation of the loan, the minted DAT is burned, and the initial minted DAT and the interest will be converted into DFI via the DeFi DEX described in this paper.

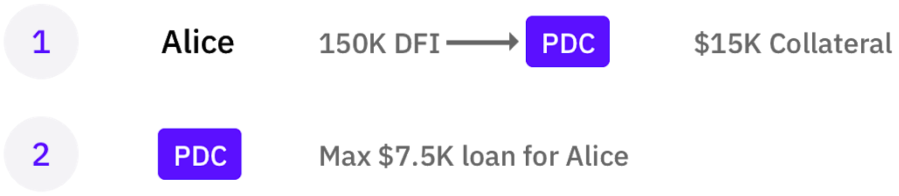
While this concept is not new to the DeFi system, what is novel is the possibility to collateralize with literally any asset due to the DeFi Blockchain's nature.

1. Alice opens a PDC and funds it with 150k DFI.
2. With DFI at $0.10 spot rate, Alice's PDC now has $15,000 worth of collateral.
3. At the minimum collateralization ratio of 150% she can take out a maximum of $10,000 worth of DBTC, which is pegged to BTC spot price via the later described APD.
4. Since the DBTC loan via PDC accrues interest, and DBTC and the DFI price fluctuate, Alice decides to only take out $5,000 worth of DBTC, i.e. 0.5 DBTC, giving her PDC a collateralization ratio of: 15000/5000 = 300%, well above 150%.
5. Over-collateralization allows for some room for price movements of DBTC. If the BTC price increases to $15,000, Alice's loan of 0.5 DBTC would now be worth $7,500. Her PDC now has

a collateralization ratio of: 15000/7500 = 200%, still above 150%, so liquidation would not be triggered even in the case of this type of price shift.

6. The interest rate for each DAT loan differs. Assuming the DBTC loan rate is 5% annually, taking out a loan for a year, in order to close her PDC and to fully redeem her initial 150k DFI, Alice has to pay back 0.5 DBTC * 1.05 = 0.525 DBTC by the end of the year.

PDC



Asset Peg Depository (APD)

The Asset Peg Depository's (APD) role is to maintain the price guarantee of a DAT to its actual asset, e.g. DBTC to BTC, DETH to ETH, etc.

APDs are not personalized and act as depositories that collectively hold all collaterals from PDCs.

An APD sets the base buy and sell price of a DAT on a DEX at an 1:1.1 rate (10% premium), as long as the APD has enough collateral/DAT in its depository to cover it.

- DFI: $0.10
- BTC: $10,000
- ETH: $200

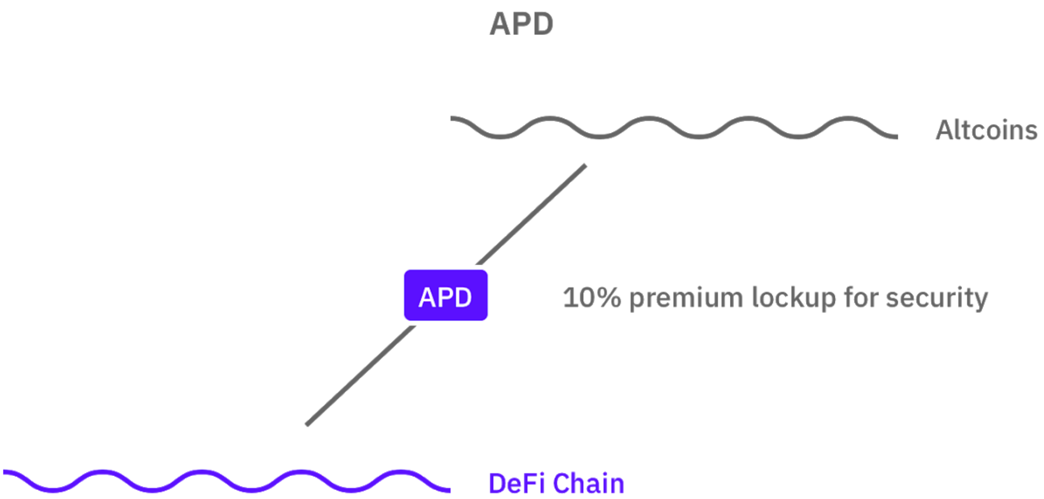
An APD starts out with no DATs but DFIs as collateral for PDCs. As long as there are enough DFIs in an APD, the APD would list the following buy orders on the DEX:

- Buy DBTC at 110,000 DFI (i.e. $11k worth)
- Buy DETH at 2,200 DFI (i.e. $220 worth)

If DBTC and/or DETH are sold to an APD, the APD would list the following, as long as there are DBTC/DETH in its holding:

- Sell DBTC for 110,000 DFI (i.e. $11k worth)
- Sell DETH for 2,200 DFI (i.e. $220 worth)

Regardless of buys or sells, APD trades are always feeless on DEX to APD, as the non-APD party has to pay the fees.



Decentralized Exchange (DEX)

The DeFi internal DEX provides decentralized trading for all DeFi tokens and DFI itself, which means that all tokens: DFI and DCT (DAT and DCT) can be listed on the DeFi Blockchain DEX. DEX will initially launch with DFI as the base trading pair, providing markets such as DBTC/DFI, DETH/DFI, DUSDT/DFI, etc. With increasing volume, other base trading pairs can be introduced, subject to a DAO approval, providing markets such as DETH/DBTC, DFI/DUSDT, etc.

Asset Peg Depositories also participate on DEX automatically as described above, setting a base price for DATs.

Cross-chain Exchange (XCX)

A user holding DBTC might be interested in holding of actual BTC instead of a DeFi pegged BTC token (DBTC).

The DeFi Cross-chain Exchange (XCX) allows anyone to do exactly that. XCX allows listing of DATs with its native tokens, e.g. DBTC for BTC, DETH for ETH, DXRP for XRP.

XCX orders contain several parameters that can be freely decided by the market marker (first lister of an order). For selling of DBTC for BTC (i.e. someone who's interested in receiving actual BTC), the parameters are:

- Amount: Amount of DBTC to be locked up for BTC.
- Premium: Amount a market taker (in this case buyer) stands to make from this trade. (Premium is listed per unit amount, thus allowing for partial fulfillment of trade orders. Together with expiry, it can also be considered as lending interest to the buyer.)
- Expiry: Time when the contract expires. Unlike PDC, XCX has a mandatory expiry date.
- Native token address: Address to send BTC to for executing the contract.

Example:

Alice has 1 DBTC and wants 1 BTC so she can trade on a centralized exchange.

Bob has 1 BTC that he does not need for 1 month, hoping to generate some lending interest during that period of time.

1. Alice lists the following XCX order:
    - Amount: 1 DBTC/BTC
    - Premium: 8,000 DFI
    - Expiry: December 31, 2019 – approx. 1 month.
    - Address: Alice lists her BTC deposit address
2. Bob accepts the offer by sending a transaction on the DeFi Blockchain.
3. Bob receives a confirmation on the DeFi Blockchain that his order is accepted. In case there are multiple order acceptance transactions.
4. Bob sends 1 BTC to Alice's BTC deposit address as listed in the XCX order and sends a transaction on the DeFi Blockchain with the BTC txid as receipt. Bob also specifies a receiving BTC address on the same transaction for Alice to repay the 1 BTC later on.
5. Multiple DeFi Blockchain stakers with BTC bridges confirm that Bob has indeed sent the amount as agreed and the that the txid is valid.
6. XCX's premium of 8000 DFI is instantly released to Bob. Bob can do what he wants with the DFI straight away with no strings attached. It is Bob's to keep for this trade.

Now, Alice has 1 BTC and Bob has 8000 DFI. Alice also has 1 DBTC locked up on XCX order and Bob is the beneficiary of that BTC. Note that the beneficiary of an XCX is transferable, i.e. Bob is able to sell the XCX with Alice to a third party (this allows for decentralized debt selling and tokenization of receivables).

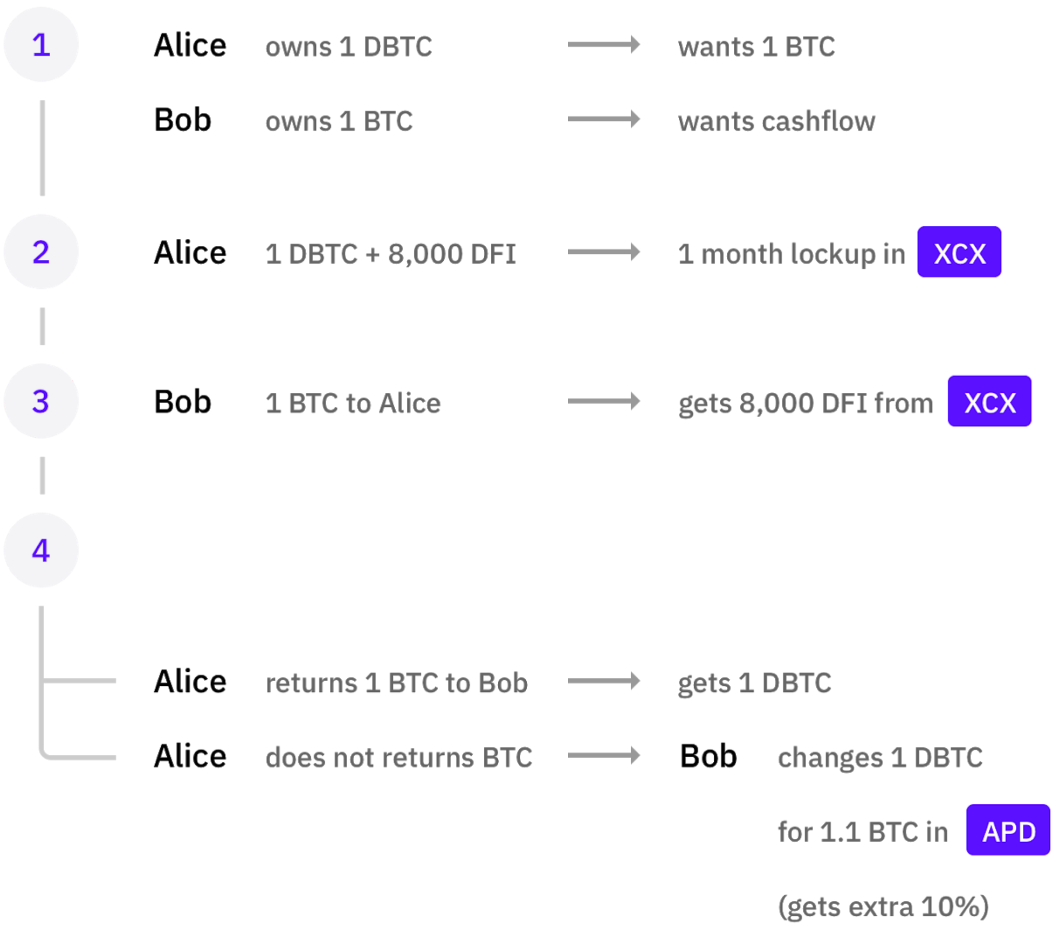
Should Alice wish to redeem her 1 DBTC from the XCX before the time is up, Alice will send Bob the 1 BTC she borrowed earlier to Bob's address specified in the XCX and send the acknowledgement on the DeFi Blockchain. Upon confirmation by stakers with a BTC bridge, the XCX contract now closes and Alice gets her 1 DBTC back, having paid 8,000 DFIs as interest.

Bob gets his 1 BTC back (keeping his 8000 DFI as lending interest).

Should Alice wish not to redeem the XCX before the expiry, Bob gets to keep Alice's 1 DBTC.

Alice gets to keep the 1 BTC (minus 8000 DFI interest) and Bob now gets 1 DBTC (plus 8000 DFI interest). If Bob has no interest in DBTC and wishes to get his BTC back, he can sell the 1 DBTC on the DEX via the APD and receive a 10% additional premium that is locked up in the APD.

XCX


1
Alice owns 1 DBTC → wants 1 BTC
Bob owns 1 BTC → wants cashflow
2
Alice 1 DBTC + 8,000 DFI → 1 month lockup in XCX
3
Bob 1 BTC to Alice → gets 8,000 DFI from XCX
4
Alice returns 1 BTC to Bob → gets 1 DBTC
Alice does not returns BTC → Bob changes 1 DBTC
for 1.1 BTC in APD
(gets extra 10%)

Pricing Contract/Oracle

A Pricing Contract is a smart contract on DeFi Blockchain allowing multiple trusted and appointed parties to submit periodic price feeds of DATs and DFI.

Multiple Pricing Contract oracles are chosen by the DeFi DAO (explained in the next chapter).

Use Case Examples

Following are examples of how the technical implementations of the DeFi Blockchain can be used. This is just a list of examples. Many other applications can be implemented as well.

Leveraging a Long Position

1. Alice has 100k DFI. She likes the prospects of DFI and wants to leverage her position.
2. Alice opens a PDC on the DeFi Blockchain and takes out a loan in DUSDT.
3. Alice sells DUSDT for more DFI.

Thus Alice can obtain a compounded long position on DFI without putting in extra money.

Shorting a Coin

1. Bob wishes to short coin XXX. Bob has DFI.
2. Bob opens PDC on DeFi Blockchain, takes out a loan in DXXX.
3. Bob can now either sell DXXX for DFI or DUSDT on DeFi DEX, or convert DXXX via XCX to sell XXX on a non-DeFi-internal exchange.
4. Once Bob wishes to close his short position, Bob buys back XXX (or DXRP) from the market, hopefully at a lower rate, closes his PDC and thus completes his short of XXX.

Getting a Loan (Borrowing)

1. Charlie has DFI, but he needs short-term cashflow of another coin XXX. Charlies does not want to sell DFI for it nor does he want to spend fiat money to buy this coin.
2. Charlie takes a loan via PDC on DeFi Blockchain for DXXX and converts it to XXX.
3. Once he wishes to settle his loan, Charlie simply purchases XXX/DXXX and close his PDC.

Lending a Coin for Cashflow

1. Dave has BTC that he does not need in the short-term. Dave wishes to generate some interest (cashflow) by lending BTC.
2. Dave lists BTC on XCX specifying his BTC amount, desired premium (interest rate) and expiry (period that he does not need his BTC).
3. Once a counterparty takes up Dave’s listing, Dave receives an instant premium in DFI.
4. Upon expiry, Dave would either receive his BTC back, or receive DFI that are worth 10% more than his original BTC as he would redeem them from the ADP, where a 10% premium is locked up.

DFI token

The DFI token will be the integral unit of account in the DeFi Blockchain ecosystem.

The DeFi Foundation located in Singapore will be issuing the DeFi utility token, DFI, capped at 1,200,000,000 (1.2 billion) for throughout its lifetime. There will only ever be 1.2 billion DFIs created.

DFI is divisible up to 18 decimal places.

DFI Token Utility

- DFI is used for fee payment for all transactions and smart contracts on the DeFi Blockchain.
  - Fee payment for decentralized exchange transactions
  - Fee payment for token transfers
- Fees payment for DeFi activities:
  - DEX fees
  - XCX fees
  - PDC interests payment
  - etc.
- Collateral for borrowing of other cryptoassets on the DeFi Blockchain.
- 100,000 DFI is required to run a staking node for the DeFI Blockchain.
- 1,000 DFI is required to create a DCT. This is refundable upon destruction of the DCT.
- 500 DFI is required to submit a proposal for DFI the community budget. This is non-refundable.

Fees from DeFi Activities

Fees from DeFi activities on the DeFi Blockchain are burned and redistributed through new token minting over a period of time as laid out below. This ensures that DeFi stakers enjoy the benefits of earning rewards from facilitating trustless DeFi trades on DeFi Blockchain in a fair manner.

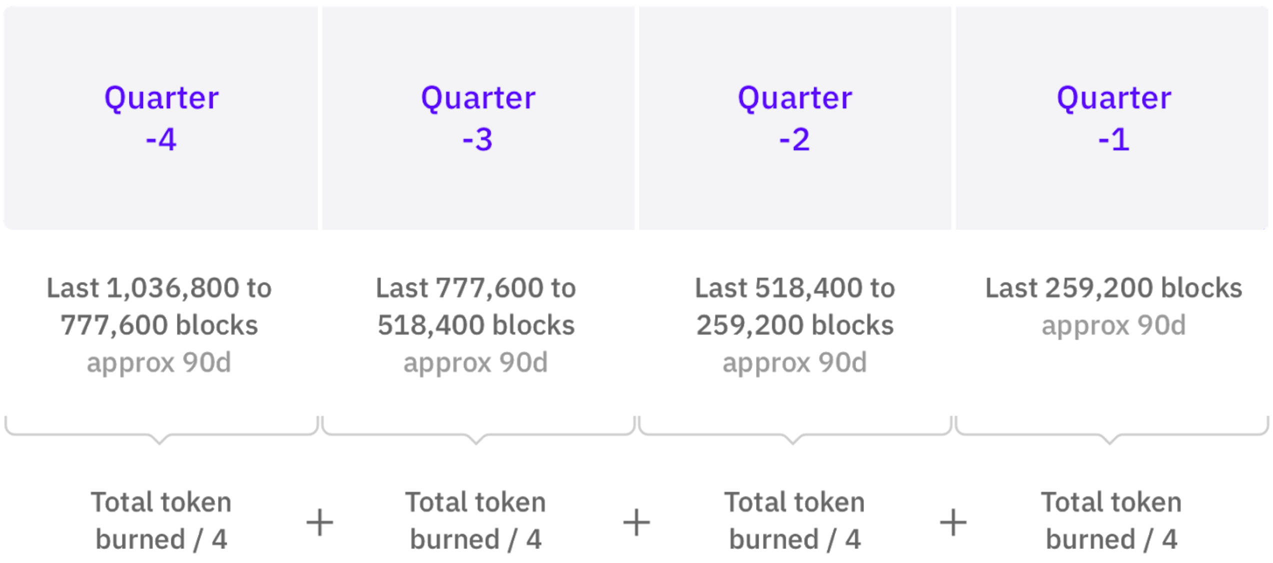
Rewards from minting a block on DeFi Blockchain are calculated as:

1. Underlying block reward schedule (see distribution schedule) +

2. Burned token redistribution schedule

The burned token redistribution schedule is determined automatically every 259,200 blocks (approx. every 90 days) and works as follows:

Burned Token Redistribution



Quarter -4

Last 1,036,800 to 777,600 blocks approx 90d

Total token burned / 4

+

Quarter -3

Last 777,600 to 518,400 blocks approx 90d

Total token burned / 4

+

Quarter -2

Last 518,400 to 259,200 blocks approx 90d

Total token burned / 4

+

Quarter -1

Last 259,200 blocks approx 90d

Total token burned / 4

Burned token redistribution for the next 259,200 blocks =

1. (Total token burned from the last 259,200 blocks [Quarter -1]) / 4 +
2. (Total token burned from block -518,400th to -259,200th block [Quarter -2]) / 4 +
3. (Total token burned from block -777,600th to -518,400th block [Quarter -3]) / 4 +
4. (Total token burned from block -1,036,800th to -777,600th block [Quarter -4]) / 4

Masternodes

DeFi is a Proof of Stake blockchain. Initially, 100,000 DFI allow the owner to own a staking node. The returns for staking will decrease over time, as the volume and number of transactions compensates for the reduction in per-transaction staking rewards.

Nodes are entitled to:

- Periodic staking rewards as described later in this chapter.
- Submission of votes to key decisions that govern DeFi Blockchain in the governance system.
- Submission of votes on how the DFI community budget is being allocated and distributed.

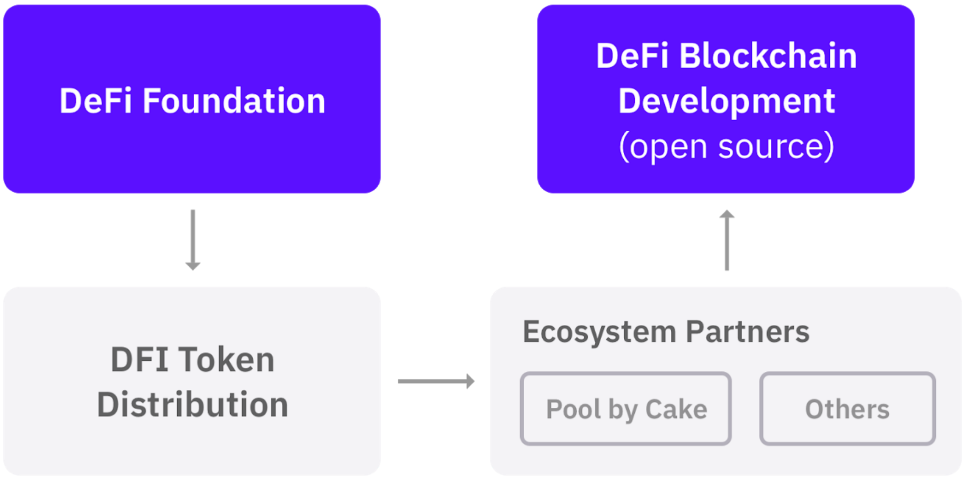
Governance

The DeFi Foundation located in Singapore is responsible for issuance of tokens and is governed by an independent board. This board will be governed by the DeFi masternodes by on the one hand voting on its members but also giving directives on key decisions.

For clarification and transparency, Cake Pte Ltd is a private company located in Singapore. Cake Pte Ltd is an initial contributor as part of the ecosystem's partners to creating services on the DeFi Blockchain.

The DeFi Foundation awards tokens to users and groups to speed up adoption (see the section on initial token distribution and marketing). The Foundation is tasked with boosting the ecosystem, bringing in ecosystem partners, directing the development of the tools for ecosystem partners, and other activities to increase the number of ecosystem partners.

Governance



Community Development Fund

The DeFi Foundation will create a community development fund with up to 10% of the block rewards under management. This percentage can be updated by submitting a DAO proposal that will be voted on my all masternodes. Community development funds were popularized by DASH[10] and are used in some selective DAOs today. The community will determine the use of these funds for development, marketing, or research that forwards the DeFi community. DFI masternodes vote for projects they like and the highest voted proposals every month will be funded.

It costs 500 DFI to submit a budget proposal and a proposal can be submitted by anyone. This fee is burned and non-refundable regardless of whether the budget is approved. Budgets are proposals which receive a net total of yes votes equal to or greater than 10% of the total possible votes (for example over 448 out of 4480). Budgets can be nullified at any time if vote totals (cast or re-cast) fall below the approval threshold. Budgets are processed (paid) in order of yes minus no votes. More popular budgets get payment priority. Voting happens on a monthly basis but can be changed by a masternode vote.

For governance decisions, only the Foundation may submit proposals. Proposals are voted in similar way as DAO budget proposals except that decisions will be honored via simple majority vote.

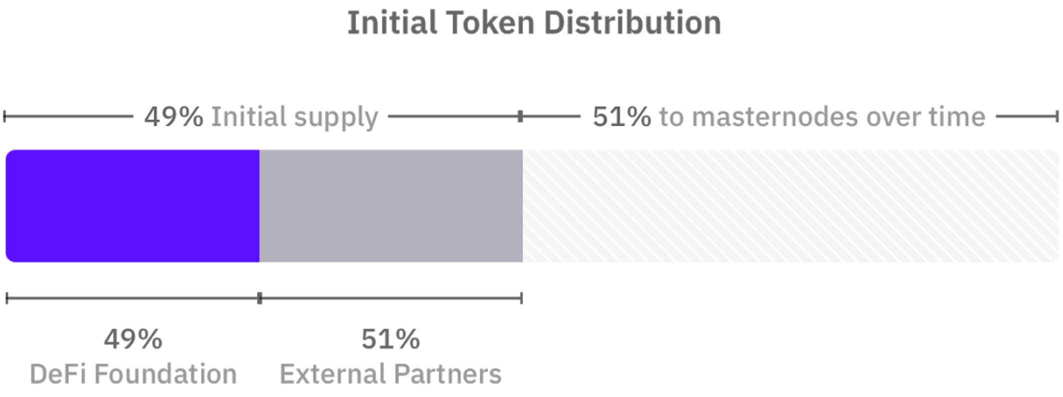
[10] https://docs.dash.org/en/stable/governance/understanding.html

Initial Token Distribution

Of the roughly 1.2 billion DFI tokens 49% will be issued to the DeFi Foundation at the start. The rest will be issued to Masternode holders over time.

Of the 49% initially issued DFI tokens, 49% will be kept by the DeFi Foundation. The rest may be distributed or sold to accredited investors, large funds and institutions, collectively known as external partners, to fund the initial development of the DeFi Blockchain. In order to decentralize the holdings of DFIs as much as possible the DeFi foundation may not keep more than 49% of all initially issued tokens. The use of potential proceedings of the tokens will be decided by the DeFi Foundation board but will exclusively be directed towards the adoption and development of the DeFi Blockchain.

For any avoidance of doubt, there will NOT be a public ICO.



Further tokens will only ever be received through staking, which is described in the next chapter.

Token Issuance Schedule via Staking

The DeFi Blockchain is initially launched with a 200 DFI block reward, of which 10% goes to the community fund. The Foundation pledges to guarantee this 200 DFI block reward for at least 1,050,000 blocks since the the first genesis block, so approximately 1 year.

Subsequently, block rewards will be adjusted through governance vote. The Foundation also further pledges that there will never be more than 1,200,000,000 (1.2 billion) DFI in circulation, unless until the DAO governance votes to change this limit. Therefore DFI is a deflationary utility token.

The proposed staking schedule for the first 10 years is according to the following table:

Year	Start of year token in circulation	% of supply staked	Block reward	Targeted new token %	Targeted new token	Staking return %	Actual new token	End of year token in circulation	% of cap	New token for year
1	490,000,000	95%	200	20.000000%	98,000,000	42.91%	210,240,000	700,240,000	58.35%	210,240,000
2	700,240,000	85%	150	13.333333%	93,365,333	22.52%	157,680,000	857,920,000	71.49%	157,680,000
3	857,920,000	75%	100	8.888889%	76,259,556	12.25%	105,120,000	963,040,000	80.25%	105,120,000
4	963,040,000	70%	70	5.925926%	57,069,037	7.64%	73,584,000	1,036,624,000	86.39%	73,584,000
5	1,036,624,000	70%	50	3.950617%	40,953,047	5.07%	52,560,000	1,089,184,000	90.77%	52,560,000
6	1,089,184,000	70%	40	2.633745%	28,686,328	3.86%	42,048,000	1,131,232,000	94.27%	42,048,000
7	1,131,232,000	70%	25	1.755830%	19,862,510	2.32%	26,280,000	1,157,512,000	96.46%	26,280,000
8	1,157,512,000	70%	20	1.170553%	13,549,295	1.82%	21,024,000	1,178,536,000	98.21%	21,024,000
9	1,178,536,000	70%	10	0.780369%	9,196,928	0.89%	10,512,000	1,189,048,000	99.09%	10,512,000
10	1,189,048,000	70%	5	0.520246%	6,185,973	0.44%	5,256,000	1,194,304,000	99.53%	5,256,000

Acquiring DFI Tokens

DFI tokens will be issued only to the users of the DeFi Blockchain or partners with an interest in utilizing and participating in the ecosystem. There will be NO public sale or public token offering. Following are the only ways to get DFI tokens:

- Institutional investors, accredited investors and funds who are interested in the use of the DeFi Blockchain can contact the DeFi founders at (partners@defichain.io).
- Over time, DFI will be available on staking platforms (such as www.CakeDeFi.com) and on selected exchanges.
- The DeFi foundation will issue airdrop tokens for users of the DeFi Blockchain. (Hodlers and other market makers).
- The DeFi foundation gives grants to developers who are developing functionality for the DeFi Blockchain or dApps to run on the blockchain.

DeFi-Foundation

The DeFi Foundation is incorporated as a company limited by guarantee in Singapore which resembles a traditional foundation structure.

Dr. Julian Hosp - Chairman

- https://www.linkedin.com/in/julianhosp/
- Serial entrepreneur, author and international blockchain expert
- European Union Blockchain Workgroup Advisor
- Raised close to 100M USD in the cryptocurrency space
- Led teams of over 100 employees

U-Zyn Chua - CTO

- https://www.linkedin.com/in/uzynchua/
- Experienced blockchain engineer
- Singapore Smart Nation Fellow – blockchain research for government
- Successfully launched dozens of blockchain projects

John Rost - Financial Advisor

- https://www.linkedin.com/in/john-rost-b70b0628/
- Vast financial knowledge and exit from large insurance company in the US

Kenneth Oh - Legal Advisor

- https://www.linkedin.com/in/kenneth-oh-840117158/
- Helped to setup 100s of crypto projects in Singapore

Marketing

Target Market

Unlike most other DeFi-focused initiatives, the DeFi Blockchain being built on top of Bitcoin can harness almost the entire crypto market without being limited to “smaller” chains like Ethereum etc. Thus, as of publication, the target market for the DeFi Blockchain are over 60-80 million cryptocurrency owners and we can expect that hundreds of millions of other users will join in the future. This group of investors is investing and holding cryptocurrency due to the returns as well as their belief in the future of the industry. As investors, they have widely done well with the rise in many of the cryptoassets, however, they are not able to use their holdings in order to get better returns. Providing DeFi services will allow these investors to hold the coins they believe in, and increase their holdings over time based on investments that go deeper than just currency trading.

Go-to-market Strategy

The initial DeFi Blockchain team is made up of some of the top names in the cryptocurrency industry, people who have made a name for themselves not just by delivering on their promises, but by creating a following. The team has built up a variety of marketing channels and has an established following on social media, wide distribution of books in the area of cryptocurrency, and deep contacts within the cryptocurrency industry.

With the experience of building up social media followings of hundreds of thousands of users in the course of just a few years, the team plans to leverage their current followers and bring them onto specific channels that will be the domain of the DeFi Blockchain. The team will build up a complete marketing engine and staff, using the same proven competence they displayed in the past.

Unlike other blockchains, the DeFi Blockchain will be balanced between marketing and technology expertise. Building the best network is only half of the job. DFI holders can rest assured that the marketing team has the proven experience in building up a marketing engine that is required for product success and that the tech team will be able to deliver on the roadmap.

Partnerships

The DeFi Foundation will be tasked with assessing applications from ecosystem partners and providing foundation grants in the form of DFI tokens to developers and contributors to the DeFi Blockchain. Many open source projects and blockchain developers today are looking for the right blockchain project in order to develop their DeFi applications, and the prospect of a dedicated DeFi Blockchain, backed by industry leaders is appealing.

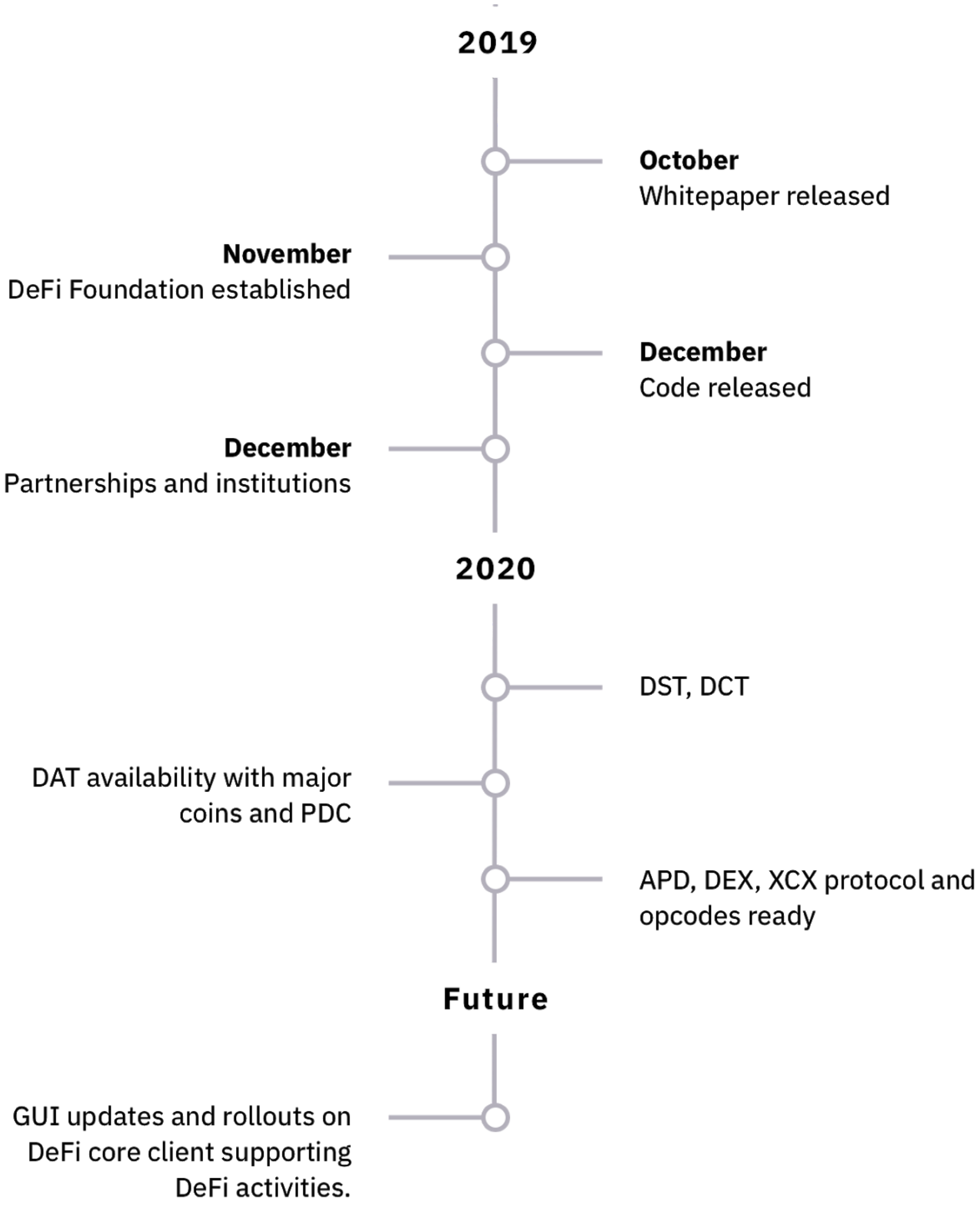
The DeFi Foundation will undertake a variety of efforts to choose the best projects for the expansion of the DeFi Blockchain:

- Creation of a formal application process so that worthy projects can apply for airdrop or foundation grants for their development
- Approaching developers in the ecosystem who are doing DeFi dApps on other blockchains, and providing grants for them to develop their dApps on DeFi.
- General marketing to get the word out about the availability of DeFi foundation grants to fund worthy projects.

Every project on the DeFi Blockchain will naturally bring it its own users and put effort towards marketing of the project, adding users and hodlers to the DeFi Blockchain.

partners@defichain.io

Roadmap and Milestones



2019

October
Whitepaper released

November
DeFi Foundation established

December
Code released

December
Partnerships and institutions

2020

DST, DCT

DAT availability with major coins and PDC

APD, DEX, XCX protocol and opcodes ready

Future

GUI updates and rollouts on DeFi core client supporting DeFi activities.

A Glimpse into the Future

Building on top of the DeFi Blockchain will lead to some of the most exciting benefits not only for first-world areas, but moreover also all those that need decentralized finance the most. For example, imagine Anna, who owns a small business in a developing economy, but who doesn't have a traditional bank account. She uses mobile money and digital currencies to run her business, accepting payments through mobile--which makes perfect sense, because nobody in her province uses cash or credit cards. Anna uses the DeFi Blockchain to take out a loan when one of her suppliers pays late, saving her business. In the old days, she would have simply gone out of business, because no bank would loan money to her. Anna also invests wisely. When she is paid by the supplier, she immediately moves the cash into various tokenized assets to avoid the hyperinflation and instability of her national government's currency, and on top of that, she is able to earn interest.

Anna creates a group of local businesspeople, and together they pool funds to help other entrepreneurs in their village. They purchase office space, solar panels, and a satellite to create a business center. The group uses DeFi to eliminate the overhead of complex legal contracts between them. They receive automatic dividends when the business center profits. Some of them reinvest in a delivery drone which charges for its services, and distributes the income to the investors. Others invest in sensor equipment that test local soil conditions, and sell the data to commodity markets. All of the sensors work independently and charge independently, and the investors simply reap the profits, all calculated automatically on the DeFi Blockchain.

Now, 5 years after her initial use of DeFi, Anna is able to take out a loan with no collateral, based on her long-term record of smart investments and returning loans on time, as well as assessment of her industry from trusted oracles. It's a win-win situation. The lenders come from all over the globe, from people who want to diversify their investment portfolio to developing economies. The lenders don't have to worry about the complexity of cross-border transactions or legal requirements. They escape the banking systems of their own countries, which moved to zero and negative-interest rates on savings. Now, these regular investors can be assured of returns on investments based on Anna and people like her, who run great businesses and can provide returns on people's investments.

This is what the DeFi Blockchain is all about - To make the world a better place!