BNC.
bravenewcoin.com

NOV
2020

TECHEMY
CAPITAL

NON FINANCIAL RISKS IN DEFI:
Identifying key Non-Financial risks in Decentralized Finance on the Ethereum Blockchain

A report by Xavier Meegan

TECHEMY GROUP RESEARCH 2020

Contents

Executive Summary

This report identifies and defines non-financial risks for Decentralized Finance (DeFi) on the Ethereum blockchain. DeFi can be based on any permissionless smart contract platform. This report focuses on DeFi on the Ethereum blockchain. Ethereum is an open-ended, decentralized, blockchain-based, public software platform that facilitates peer-to-peer contracts, known as Smart Contracts, as well as Decentralized Applications, known as Dapps.

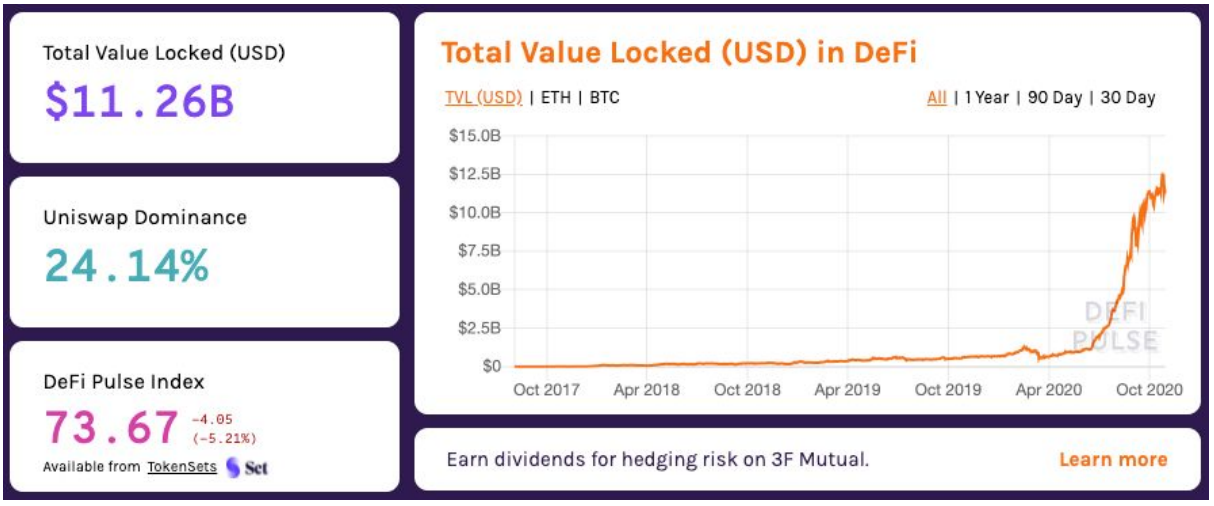
Non-financial risks for Decentralized Finance (DeFi) on Ethereum:

- Scalability Risk
- Smart Contract Vulnerability Risk — General
- Smart Contract Vulnerability Risk — Re-Entrancy Vulnerability
- Smart Contract Vulnerability Risk — Unhandled Exceptions Vulnerability
- Smart Contract Vulnerability Risk — Integer Underflow / Overflow Vulnerability
- Smart Contract Vulnerability Risk — Transaction Ordering Dependency Vulnerability
- Smart Contract Vulnerability Risk — Timestamp Dependence Vulnerability
- Smart Contract Vulnerability Risk — Upgradeable Smart Contract Vulnerability
- Oracle Risk
- Design Risk
- Composability Risk
- Centrality Risk
- Economic Incentive Risk
- Financial Illiteracy Risk
- Regulatory Risk
- Finality Risk
- Disclosure Risk

What is DeFi?

Decentralized Finance applications (herein called "DeFi") have experienced exponential growth in 2020 with a boom in the value of DeFi tokens and their protocols. DeFi can be described as the transformation of traditional financial products into new products that operate without a central intermediary via smart contracts on a blockchain.

The value of DeFi locked on the Ethereum blockchain has grown from $4 in August 2017, to $11.26B at the end of October 2020. Types of DeFi applications are wide-ranging. Some popular DeFi applications include lending, stablecoins, decentralized exchanges (DEXs), derivatives, synthetic assets, insurance, and asset management.



Value has grown from $4 in August 2017, to $11,260,000,000 as of October 29, 2020. Source: Defipulse.com

DeFi is attractive to users as it offers yields (returns) unobtainable in traditional finance. In the past year, DeFi has enjoyed a meteoric rise, grabbing headlines as it has seen yields obtained by investors in excess of >1000% annualized per year, just by depositing tokens into protocols. This is in comparison to the barely above 0% that one can earn by depositing cash into a bank.

Lending protocols, in particular, are an attractive alternative to traditional finance. Many countries around the world are entering into negative interest rate environments, accelerated by COVID-19. DeFi, on the other hand, can offer users in excess of 20% on stablecoin deposits (a.k.a. assets that exist on the blockchain and are pegged 1:1 with various real-world fiat currencies i.e. USD).

	Compound v2	Aave Lend	dYdX Lend	Fulcrum	Nuo
DAI	3.03%	3.93%	10.09%	14.2%	4.65%

Lending Rates as of November 9, 2020 — Source: Defirate.com/lend/

In traditional financial theory, investors can expect higher returns on financial instruments that are considered risky.

Traditionally, cryptocurrencies (more specifically tokens), which live on a blockchain, have been considered extremely risky investments. Tokens were once used as a store of value or for utility. Now they are being used to help the governance of DeFi protocols. For example, when a DeFi protocol such as a lending platform generates a fee when an investor wants to borrow from a liquidity pool, that fee can now be distributed directly back to the token holder. For the first time in the short history of crypto assets, we are seeing tokens that can be properly valued based on revenue and future growth, the same valuing mechanism seen in the equity markets.

DeFi can be based on any permissionless smart contract platform. This report focuses on DeFi on the Ethereum blockchain.

Ethereum is an open-ended, decentralized, blockchain-based, public software platform that facilitates peer-to-peer contracts, known as Smart Contracts, as well as Decentralized Applications, known as Dapps.

Ethereum has many Dapps that exist on its blockchain. A Dapp can be created and used in any industry vertical — e.g. health, energy, supply chain, gaming, or social networks. More recently, there has been a surge in the creation of Dapps in the financial vertical on Ethereum. As mentioned previously, a Dapp is a decentralized application and therefore a Dapp that lives in the financial vertical is itself DeFi. When the crypto market crashed on Black Thursday in March 2020, the worst vertical of Dapps to suffer from the collapse in prices was DeFi.

What separates DeFi from traditional finance?

DeFi is permissionless, composable, transparent, censorship-resistant, decentralized, accessible, and flexible.

DeFi is essentially finance without an intermediary (e.g. there is no reliance on a third party to be the escrow of any value). The most important aspect of DeFi, when compared to its traditional counterpart, is its permissionless and accessible nature.

Many products in traditional finance are limited in terms of who can access them. These investments are limited to accredited investors, which automatically excludes most of the world's population. DeFi disrupts this model, as anyone with an internet connection can connect to DeFi protocols. Anyone on earth, with as little or as much money as they wish, has the freedom to invest in financial products of their choosing, no permissions needed. Crucially, they remain the custodian of their own funds, thanks to the public key cryptography properties of the blockchain.

As we have discussed, while DeFi offers many benefits, it also introduces a range of inherent risks. Because it is a financial market, DeFi faces the same financial risks that have been well covered in existing financial theory (e.g. market risk, credit risk, liquidity risk, and operational risk). These risks are well understood and it is common practice for a company to employ a financial risk manager to deal with these kinds of risks. What separates DeFi from traditional finance, however, are the inherent risks it is exposed to as a direct result of its reliance on its infrastructure layer, the Ethereum blockchain.

The rest of this report will summarize the key non-financial risks in the Decentralized Finance ecosystem on the Ethereum blockchain.

In the DeFi ecosystem, most participants are aware of a range of risk factors, but there is no standardized identification or explanation of these risks for a potential investor to access. All of the work done so far in DeFi risk management is fragmented and based on opinion, rather than research and evidence.

As a result of thorough qualitative research, I have identified twelve key non-financial risks in Decentralized Finance.

List of DeFi Risks

Scalability Risk

Scalability risk is the risk that Ethereum could experience network congestion resulting in higher gas fees and failed transactions.

A DeFi application might not work as intended when network congestion is high, in particular, if it has a reliance on oracles (more about this in the definition of oracle risk).

Scalability risk is simply the risk that a DeFi protocol will malfunction if there is too much stress on the network. Currently, there are a limited amount of transactions that can be added to any single block on a blockchain. Miners have the power of choosing which transactions will make it into those blocks. If there are too many transactions being requested of validators (miners) on Ethereum, miners will simply choose the transactions that have a higher transaction fee attached to them to publish on the blockchain first, and get to transactions with lower fees attached to them later — dependent on network demand. Traders might not be able to transact with DeFi protocols if they are unaware of the current fees that miners require for transactions. We saw this happen on Black Thursday in March 2020, when actors in MakerDAO (liquidators) could not access auctions to bid on collateral, resulting in collateral being sold for free — because economic actors within the protocol could not access it (from not sending high enough transaction fees that miners demanded arbitrarily from an extreme peak in network activity).

Scalability risk is also the risk that Ethereum itself will not scale properly for DeFi protocols to be able to function sustainably over time. If network activity is too high (as it has been recently) it deters smaller investors and removes the 'accessible' aspect of DeFi — because smaller investors are earning rewards that are less than the fees required to obtain them. Not only does scalability risk impact investors, but it also impacts protocols (e.g. MakerDAO).

Smart Contract Vulnerability Risk — General

To understand this risk one must understand what smart contracts are. A smart contract is a piece of code that runs on a blockchain to autonomously facilitate, execute, and enforce the pre-defined terms of an agreement without an intermediary.

Smart contract vulnerability risk is the risk that an attacker could find a way to drain funds from a smart contract due to the code being written incorrectly, or an attacker using a known attack vector to exploit the functionality of a smart contract.

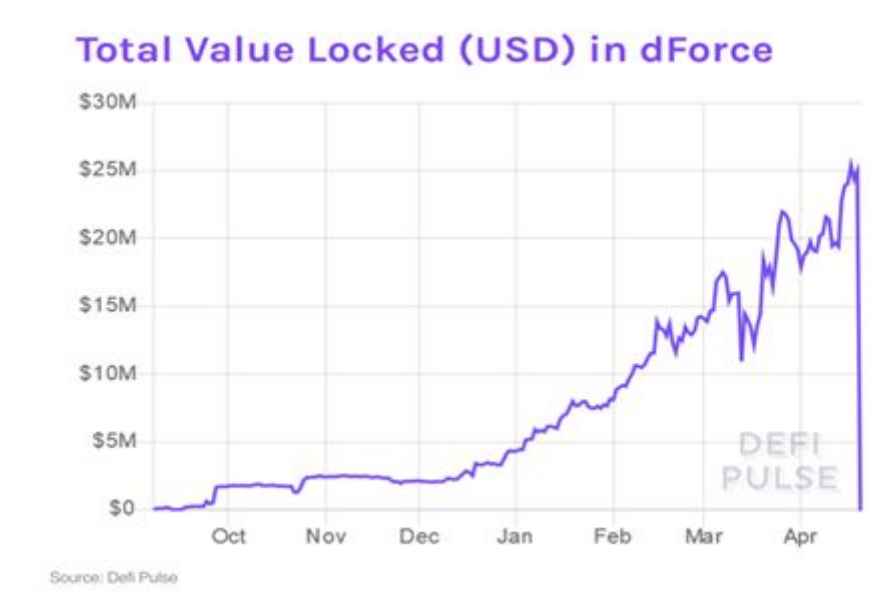
I have identified 6 key smart contract vulnerabilities.

Smart Contract Vulnerability Risk — Re-Entrancy Vulnerability

Re-entrancy occurs when a contract sends ETH before updating its internal state. Imagine someone asking a bank teller at a bank to give them $500. It is impossible to ask for $500, receive the $500, and keep receiving $500 with the bank teller never updating the person's account balance.

This is not the case with Ethereum smart contracts. It is possible to keep requesting ETH before the smart contract (teller) has updated its internal state of whether it has sent ETH or not. The biggest smart contract vulnerability in history was a target of a re-entrancy vulnerability (The DAO, $60 million, 2016).

This vulnerability is much less common today, but not non-existent. A few months ago, an attacker drained $25 million from dForce smart contracts by exploiting this vulnerability.



A re-entrancy vulnerability attack — Source Defipulse.com

Smart Contract Vulnerability Risk — Unhandled Exceptions Vulnerability

In Solidity (the programming language for writing smart contracts on Ethereum), not all failed "calls" raise an exception. Some examples of exceptions occurring in Solidity include when there is not enough gas to execute an operation, the call stack limit has been exceeded, or some unexpected system error occurs due to the node of the user performing the call. Some low-level operations in Solidity such as send, which is used to send ETH, do not throw an exception on failure, but rather report the status by returning a boolean (a true or false output of whether ETH has been sent). This can be a problem if a smart contract has a function where funds aren't sending and a developer/user is unaware of the ETH not sending (from not checking the boolean return properly and thinking ETH has been transferred as they have not received an exception as to why they wouldn't have).

Smart Contract Vulnerability Risk — Integer Underflow / Overflow Vulnerability

The incorrect smart contract integer underflow/overflow vulnerability occurs when a computed value is too large for the type attached to the value. Imagine a car odometer. A car odometer can reach 999999 before it resets to 000000. Smart contracts on Ethereum operate in much the same way. In layman's terms, imagine a 'type' in solidity. The Ethereum Virtual Machine (EVM) has integer data types that are designated with bit-level specification; e.g. "uint8" for an 8-bit unsigned integer, or "uint256" for a 256-bit unsigned integer. The bit-level specification of integers causes value storage limitations. Let's use the example of an overflow with a uint256 value that is equal to the integer 100. If a smart contract has an operation where the user tries to subtract 105 from the value of 100, instead of it being equal to -5, it will reset to the highest number of that value (like a car), being 100.

```
function overflow(uint fee) {
  uint amount = 100;

  // underflows if fee > 100
  amount -= fee;

  // tries to send a large value
  // and fails on underflow
  msg.sender.send(amount);
}
```

This means that an exploiter could potentially overflow their account address with the maximum value by exploiting this vulnerability (unless the developer has ensured this cannot occur).

Smart Contract Vulnerability Risk — Transaction Ordering Dependency Vulnerability

Transaction-ordering dependency occurs when two dependent transactions invoke the same contract and are part of the same block. This is the risk that transactions will be

ordered differently from how a user expects. This is because in blockchain, two transactions can be sent to the mempool/tx-pool within a block and the order in which they arrive does not matter. As mentioned earlier, miners are the ones who determine which transactions actually make it to the blockchain and in what order. They have the freedom to choose the order of the transactions in a block. There can be financial incentives to manipulate transaction ordering on a blockchain that a miner may wish to exploit. This type of vulnerability is known as front-running and is a serious concern in DeFi, especially in Decentralized Exchanges (DEXs).

The risk of the front-running vulnerability being exposed in DeFi is becoming more prevalent with the introduction of flash loans. Flash loans are a new kind of financial innovation in DeFi. A flash loan is a loan that is only valid within one blockchain transaction, which is essentially non-collateralized, risk-free debt. Flash loans are atomic, either a loan is made with the principal and interest being paid back to the creditor at the end of a block, or it reverts back to its original state if the borrower fails to pay back the principal and interest required by the protocol within the same block. In essence, flash loans may make DeFi more accessible than ever. Investors can make trades with no upfront capital needed. The issue here is that DeFi investors/traders/arbitrageurs have more tools at their disposal to make trades with the introduction of flash loans, except ultimately, miners are the ones that choose which transactions are published on the blockchain. Recently, there have been instances of arbitrageurs making profitable trades using flash loans, only for miners to profit from the trade (with no intellectual thought needed) by simply copy and pasting the transaction and paying a higher gas price for it to receive the profit instead of the arbitrager.

> $950,000 — That's the arbitrager profit made from exploiting different price feeds and liquidity pools on bZx in early 2020 — inflating prices to evade oracles then longing and shorting on different exchanges — what if it was front-ran?

Smart Contract Vulnerability Risk — Timestamp Dependence Vulnerability

If a contract uses the block.timestamp (or now) global variable as a triggering condition for executing a critical operation (e.g. a money transfer) or as a source of randomness, it can be manipulated by a malicious miner. Essentially, it is important to watch out for smart contracts that rely on the (now) variable in smart contracts — it can give miners an unfair advantage.

Smart Contract Vulnerability Risk — Upgradeable Smart Contract Vulnerability

The upgradeable key risk is the risk that an administrator can upgrade a smart contract and change the behavior that a user expects.

This is also a type of design risk. Currently, the majority of popular DeFi protocols have some form of centralized control that enables 'administrator' addresses to intervene in powerful ways (e.g. pausing the system, blacklisting addresses etc). Existing techniques to upgrade smart contracts have flaws that increase the complexity of the smart contract significantly and ultimately introduce more smart contract vulnerabilities. If contracts can be upgraded, it juxtaposes against what DeFi strives to become, financial products with no intermediary.

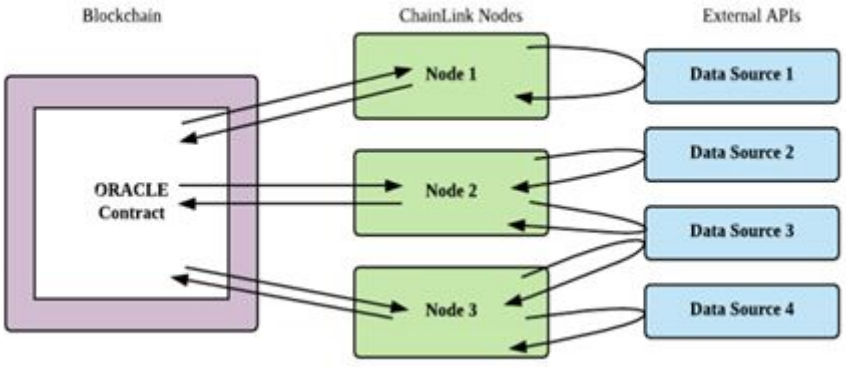
Oracle Risk

Oracle risk is the risk a smart contract could receive dishonest input about off-chain values due to the manipulation of information from the provider, or an oracle does not update a smart contract with off-chain information as fast as an application expects it to (related to scalability risk).

Oracles are often needed in DeFi because blockchains are incapable of considering any information 'off-chain'. This concept is referred to as the 'oracle problem'. Oracles are a middle layer — fed data by APIs that relay the data onto the blockchain. An oracle

connects a blockchain (with no knowledge of the outside off-chain world) to knowledge of the outside world (e.g. the temperature). Oracles can be centralized or decentralized. Even if a blockchain reaches consensus on how a transaction (e.g. a smart contract) is passed between addresses by an agreeance from nodes, the nodes that accept the transaction as valid have no way of identifying if a transaction includes valid metadata (e.g. information about the outside world like the temperature). Oracles are relied upon in DeFi, especially for financial information from the outside world (e.g. the price of the USD). The Ethereum blockchain has no way of knowing what the price of USD is at any particular time because it only understands transactions. Many DeFi protocols rely on oracles which determine pay-outs. An oracle could have reason to manipulate data to receive an unfair payout by feeding inaccurate data into the blockchain (e.g. through smart contracts) if the logic within a smart contract relies on the data being a certain value.

> US $37,000,000 — Synthetix used a centralized oracle that incorrectly priced Korean Won by x1000 in 2019, an arbitrager noticed the incorrect price feed and netted $37 million making trades with the inflated price.



How Chainlink tries to solve the oracle problem to provide correct inputs of off-chain information into the blockchain — Source: Chainlink

Design Risk

Design risk is the risk that a flaw will cause the protocol to behave differently than intended leading to failure.

A DeFi protocol with a high level of security and risk mitigation can be compromised if it adds a new smart contract or token to its protocol that has a different level of security. This is particularly relevant in DeFi, as the composability of DeFi is a strong selling point, meaning that DeFi platforms often integrate code made by others with their own code. The risk of this is that third parties might start using underlying code made by other DeFi platforms that do not work well within their own platform as the platform is not designed properly for integrations or new standards.

Composability Risk

Composability risk is the risk that a DeFi platform is reliant on another DeFi platform operating properly for its own platform to function correctly.

Composability risk is related to design risk. Composability is a system design principle that enables applications to be created from component parts. Composability is often referred to as “money lego” in the DeFi ecosystem as code can be selected and assembled in multiple combinations. DeFi developers can easily use and build on top of existing protocols because most DeFi protocols are open-source for anyone to use. Due to its open-source nature, a relatively large number of DeFi protocols integrate components made by third parties in the making of their own protocol. DeFi protocols benefit from composability as it contributes to faster innovation in the space (ie network effect and open-source code), but it results in higher levels of interdependency between platforms (causing greater amounts of composability risk). The interdependency of all DeFi platforms makes it highly exposed to systemic risk as the fall of one could lead to the fall of many. The current interconnectedness of DeFi is extremely similar to how traditional finance was before the Global Financial Crisis (GFC) in 2007–08. Pooling risk in different products and the rehypothecation of collateral and fractional ownership that is happening in DeFi right now, is the exact

same financial engineering that led to the GFC in 2008. DeFi is at risk of the same financial crisis its underlying technology was created to prevent.

Centrality Risk

Centrality risk is the risk a DeFi protocol relies on a centralized intermediary which could result in a central point of failure.

There are three types of centrality risk.

1. Upgradeable Smart Contract Centrality Risk
2. Centralized Stablecoins in DeFi Centrality Risk(USDT,USDC,DAI)
3. Reliance on Infura as a Node Infrastructure Operator Centrality Risk

Upgradeable Smart Contract Centrality Risk has been mentioned already.

Centralized Stablecoins Centrality Risk is the risk that major stablecoins in DeFi do not function as a user intends them to due to central points of failure of the stablecoin.

DeFi has contributed to the rise in stablecoin minting in recent times. As mentioned previously, investors can receive high yields by depositing cryptocurrencies in DeFi. An attractive cryptocurrency to deposit in lending protocols are stablecoins (to reduce volatility risk). The issue in DeFi is that it strives to be decentralized, yet most of the tokens that are used in DeFi protocols are centralized. In particular, USDT and USDC are stablecoins that are minted by a centralized third party. USDT and USDC are popular stablecoins in DeFi which are supposedly backed 1:1 with USD at a bank. The problem here is DeFi investors have to rely upon a centralized third party to stay true to their word that the stablecoin has value off-chain. We know this is not the case though, as it has been revealed that USDT (Tether) stablecoin reserves are only backed 74% to each token that exists on the blockchain. Doing the maths, with about US $20 billion in circulation of USDT right now, if there was a huge bank run for any reason (even external to DeFi) on Tether, about 25% of Tether held by investors would be worthless in real-life or US $5 Billion. USDC is another centralized stablecoin issuer that has the ability to blacklist addresses that hold USDC if they deem suspicious

activity — as a DeFi investor we again have to rely upon this central third party not to do that. Finally, DAI, the stablecoin that is supposed to be Decentralized, can be minted by depositing USDC as collateral. DAI, like DeFi, strives to be Decentralized — however the more aspects of incorporating centralized third parties (e.g. using USDC for collateral) that DeFi investors have to rely upon, the more DeFi is exposed to centrality risk.

Finally, we have **Reliance on Infura as a Node Infrastructure Operator Centrality Risk**.

The Infura IaaS (infrastructure-as-a-service) by ConsenSys, provides Ethereum clients running in the cloud, so users do not have to run a node themselves to work with Ethereum (which is expensive). Infura provides enormous value to the development community by removing the cost and time investment that is necessary to sync and run an Ethereum node that would otherwise put DeFi development out of reach for many. If a DeFi protocol relies on Infura to communicate with the blockchain then it creates a single point of failure as Infura's service could introduce bugs or become unavailable for whatever reason, crippling the ability for DeFi protocols relying on Infura to function properly. In addition, any DeFi protocol using Infura removes the core benefits of a Decentralized application (e.g. being unstoppable, censorship resistant and trustless). Infura is operated by a single provider — the Ethereum development studio ConsenSys– and relies on cloud servers hosted by Amazon. As such, concerns exist that the service represents a single point of failure for the entire network. In an ideal world, every decentralized application would run their own node to mitigate this risk.

> An estimated 63% of the Ethereum community use Infura as their preferred method of interacting with the blockchain. What are the consequences if Infura does not function as expected one day?

Economic Incentive Risk

Economic incentive risk is the risk that economic incentives that encourage network participants to perform certain actions could fail to encourage the right behavior or not be sufficient enough, leading to other users being adversely impacted.

The top 10 DeFi protocols (by value locked) all have their own utility token — which governs how a protocol works. Some users of DeFi protocols (e.g. liquidity providers) do not necessarily hold or need to hold the native DeFi utility token to interact with a DeFi protocol. The risk is that DeFi utility token holders (governors of DeFi protocols) could vote for something in the future that negatively impacts users of the DeFi protocol that do not hold the native DeFi utility token. Holders of DeFi utility tokens can vote on any number of proposals and their vote is weighted by the amount of the native DeFi utility token in % of circulation — like in traditional votes with stocks. The risk is that proposals are voted in at any time by those that hold utility tokens (govern DeFi protocols) which negatively affect users (e.g. there is a hard-cap on interest rates for borrowing within a DeFi protocol, which could negatively affect investors that do not hold the native token of the protocol). Any number of risks could be thought of if a native token creates proposals that contribute to network participants behaving maliciously for financial gain.

Financial Illiteracy Risk

Financial illiteracy risk is the risk that a platform has been developed by someone with no financial background.

Programmers attempting to express traditional financial products via code in smart contracts often have no financial background. This is in contrast to traditional finance, where traditional financial products are traded by institutions and created by financial engineers with certification. DeFi strives to be more accessible to the global community and is open to anyone to build products. A serious risk of this is that developers might create a DeFi product having no financial knowledge about the financial implications of the product they are creating and have users invest in the

product without considering the risks. This risk can also go the other way, as there can be a Technology Illiteracy Risk in DeFi, when someone with a financial background develops a poorly designed protocol that may be vulnerable to attacks.

Regulatory Risk

Regulatory risk is the risk that a DeFi protocol is affected by new regulation. This could be a new law that affects how a DeFi protocol operates or even a new law that effectively shuts down a DeFi protocol.

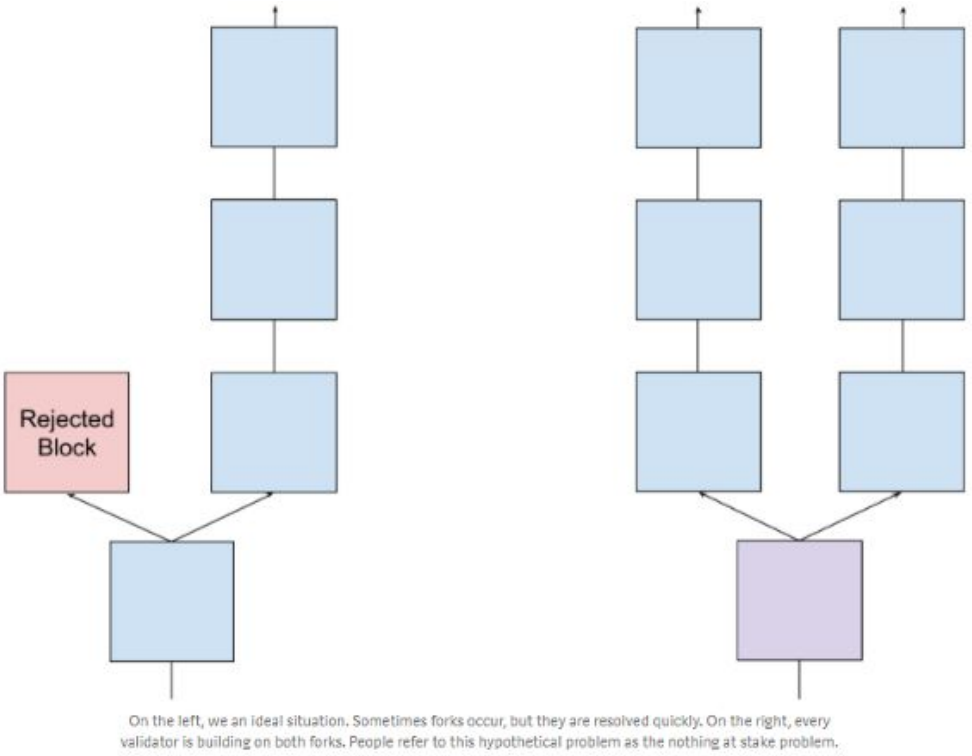
In general, the greatest amount of regulatory attention so far has focused on traditional concerns of investor and customer protection, particularly in the case of cryptocurrencies and Initial Coin Offerings (ICOs), not on DeFi. DeFi is so innovative that it currently operates in a regulatory grey area, as no regulator in any jurisdiction has attempted to regulate how DeFi is used in any way. In DeFi, there is no accountability or governing body overseeing how protocols are functioning and making sure they are compliant so user funds are not at risk. Regulatory risk is a critical risk of DeFi right now, as at any point if a regulator decides that DeFi investing is becoming out of control or finds too many users have funds at risk, the regulator can enforce measures which ban populations of countries from interacting with DeFi platforms.

Finality Risk

Finality risk is the risk that the Ethereum blockchain will fork, resulting in the creation of two different chains (resulting in DeFi assets being available on two or more chains, not one).

Currently, the consensus algorithm (the algorithm that nodes use to compete to publish blocks and the protocol used to agree on the validity of blocks being published) used on Ethereum is proof-of-work. Compared to a traditional database, public blockchains that use proof-of-work as consensus, such as Bitcoin and Ethereum, have a possibility of being reversed, a probability that often decays with time but which is never zero. Meaning transaction finality is probabilistic. For any given block, there is

always the possibility that someone will create a longer chain by reordering previous blocks in their favor and ignoring the true chain. It is a risk for DeFi users that an event such as a 51% attack could result in one chain continuing and one chain forking into a new direction. In essence, financial players want transactions to be final. They do not want the possibility of their transaction reversing, or their assets to be made available on two chains continuously, which is always a risk using public blockchains such as Ethereum. Supposedly, the consensus that Ethereum is attempting to transition to currently — 'proof-of-stake' (PoS), will mitigate finality risk as it gives transactions higher chances of being probabilistically final. However, Ethereum's transition to proof-of-stake adds a huge uncertainty to the Ethereum blockchain itself, let alone its impact on DeFi. The transition to proof-of-stake known as Ethereum Casper or Ethereum 2.0. The transition will be an enormous security test for ETH and could make it more vulnerable to attacks and manipulation (by validators of the network i.e. stakers), and more exposed to complicated forks than it was with its original proof-of-work consensus. A classic example of this is a USD stablecoin backed 1:1 with USD reserves at a bank. The stablecoin now exists on one chain, hence its value is true to real-life, but what about if the chain does fork and the asset is available on both chains? It only has one true value that exists off-chain, so how is this determined on-chain? How does this impact investors?



Nothing-at-stake — Will proof-of-stake mitigate finality risk or amplify it? — Source vitalik.ca

Disclosure Risk

Disclosure risk is the risk that a DeFi protocol has not disclosed a full list of risks a DeFi user could experience while using the platform.

There is always a risk to a DeFi user that the user's chosen platform has not adequately disclosed the results of its auditing reports. Not only that but even if a DeFi platform has been audited, it might have been audited prior to a protocol upgrade, where new vulnerabilities could have been introduced. As we know there is no accountability of DeFi platforms (due to the regulatory grey area), therefore DeFi protocols might have an incentive to not disclose all risks of their platform if they think they can fix issues without the public knowing whilst continuing to receive funds.

Risk of more Risks

The risk of more risks is the risk of new risks being found in the DeFi ecosystem that are not yet known.

As this article has outlined, there are many risks and each risk affects individual platforms differently. Innovation in DeFi is rapidly accelerating and new products are being created that appear to defy the laws of finance itself i.e. with flash loans (no collateral and risk-free, win-win situation to arbitrage). New financial products that are not yet existent in the DeFi ecosystem include asset management, asset issuance, and open market platforms, all of which are being created now and likely to exist in the future. These alone will come with their own risks that could be specific to how that platform operates. As we are constantly seeing new financial products and mechanisms created in DeFi, it is likely that these will introduce new risks that are not mentioned in this paper and are impossible to forecast.

Conclusion

This paper represents my subjective initial research into identifying the non-financial risks apparent in DeFi on the Ethereum blockchain. This work is intended to contribute to the DeFi risk management conversation. Proper risk management when interacting with DeFi protocols is a necessary step on the path towards mainstream adoption. I invite anyone with an interest in the risk management area of DeFi to reach out to me if you have questions, comments, theories, or ideas related to this area.

If you would like to read further about my work — please see the following link for a more in-depth analysis of the risks with examples and evidence available at: https://www.researchgate.net/publication/344689196_Identifying_Key_Non-Financial_Risks_in_Decentralized_Finance_on_Ethereum_Blockchain

Author Bio

Xavier Meegan

If you would like to contact me regarding this work, I can be reached at my email — or alternatively, you can connect with me on LinkedIn.

Connect on LinkedIn:

linkedin.com/in/xavier-meegan-65344b145/

Email: xave.meegan@hotmail.com

Special thank you to those who assisted me with my research and made themselves available for communication regarding this work. In particular to Paul Salisbury and Donn Krassiyenko from Techemy Capital, Jordan Lyall and Jack Clancy from ConsenSys, Hugh Karp from Nexus Mutual, Felix Lutsch from Chorus One, Marouane Hajji from Unslashed, and my supervisor Massimo Morini (BANCA IMI S.P.A., Algorand) for his great discussions on the direction of my work.

Special thank you also to those in the DLT team at ING who assisted with the formatting for the release of this work, including Mariana Gomez de la Villa, Tommy Koens and Gamze Tillem.