DeFi: New Risks Require New Regulation

Greg Hopper

Presentation to Office of Financial Research Advisory Committee

Nov 8, 2022

What Crypto Sector Does This Presentation Cover?

- In this presentation, we discuss the risks and regulatory strategy involving decentralized protocols
- The analysis and proposals in this presentation do not necessarily apply to centralized institutions, such as traditional exchanges or bank-like entities, that trade crypto
- We also do not discuss stablecoin risks and proposed regulation, since that is a separate complicated topic that requires its own treatment

Competing Visions of DeFi Regulation

This View Seems to Be Gaining Steam…

- DeFi has no obvious use cases still and so digital assets are unmoored from any economic fundamentals, making them highly volatile and speculative
- Risk profiles in DeFi are largely the same as in conventional finance
- Similar risk profiles means that most of DeFi is covered by the current regulatory apparatus
- Need for limited additional statutory authority from Congress to cover the remaining uncovered pieces
- DeFi must be aggressively regulated now using current law and practices to protect the public and to prevent potential systemic risk interaction with the conventional financial sector

We discuss the alternative perspective in this presentation

But There is An Alternative Perspective

- DeFi is still in early stages but has the potential to dramatically improve the efficiency of and access to financial services, if it can solve its technical and risk management challenges
- Risks in DeFi are mostly different from those in conventional finance
- As a result, current regulatory rules and requirements are not well suited to protect the public in DeFi transactions, since they are aimed at the wrong risks and can also create perverse incentives
- Need for substantial new authority from Congress to properly regulate DeFi
- DeFi needs proper regulation or it will never gain widespread adoption from consumers or institutions
- Regulatory policy should therefore be designed to
  - control the new risks present in DeFi in order to protect the public and prevent systemic risk
  - provide an environment in which the technology can develop and flourish

Outline

- There are new risks in DeFi that are fundamentally different from the most important risks in conventional finance
  - identity risk
  - algorithmic liquidity risk
  - smart contract risk
  - oracle risk
  - legal risk
  - wrong way risk
  - custody risk
  - bridge risk (also systemic)
  - protocol risk (also systemic)
- These new risks imply that systemic risk and a crypto financial crisis will be fundamentally different from historical banking or financial crises
  - but a crypto financial crisis could be the catalyst of a financial crisis in the conventional banking system
- Recent case studies illustrate many of these risks in action
- Since current regulatory rules cover risks different from DeFi risks and may also create perverse incentives when applied to DeFi, a new legal and regulatory regime is required
- Recommendations for a new DeFi legal and regulatory regime

Identity Risks

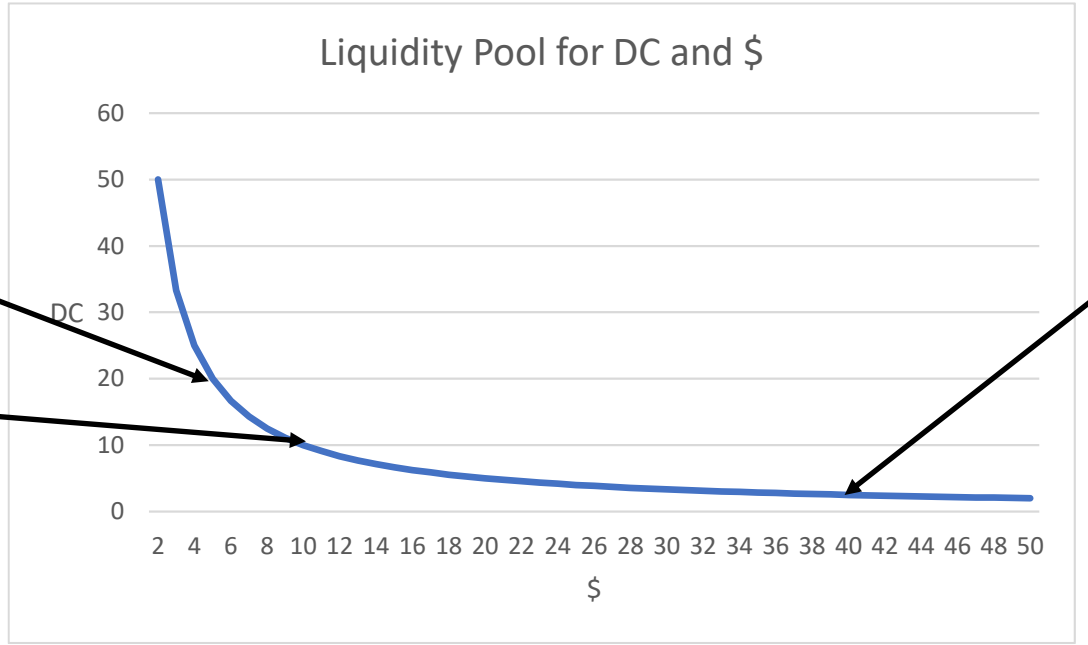
- Blockchains are pseudonymous rather than anonymous and every transaction is public, transparent, and preserved permanently
- On the other hand, there are cryptographic methods that allow complete anonymity on blockchains
- These two aspects of blockchains imply identity risks
  - risk that transactions intended to be kept private become public
  - risk that attacker can use different pseudonyms (but with same identity) to manipulate a DeFi protocol
  - risk that criminals hide their identity to commit crimes or evade legal requirements and regulations
- These identity risks may conflict: the risk that criminals can hide their identity can be mitigated by increasing the risk that private transactions will be made public
- There are potential technical solutions that can resolve the conflict

Algorithmic Liquidity Risk

- An Automated Market Maker (AMM) is a DeFi protocol that provides liquidity if a trader wants to exchange one asset for another
- Unlike a conventional exchange that matches buyers and sellers, an AMM uses an algorithm to determine the price
- The simplest AMM is a constant product AMM that requires that if there are R_x digital coins DC in the pool and R_y stablecoins then any trades must satisfy R_x x R_y=c
- In the example below, we set c = 100

1 At this point, there are 20 DC and $4.5 in the liquidity pool

2 If you want to buy DC for $, then if you put in to the liquidity pool $5.5 (going from $4.5 to $10, then you can remove 10 DC (20 DC – 10 DC). Price was $5.5/10 DC = $0.55/DC



3

- In this range, DC is very illiquid. The same $5.5 would allow withdrawal of 0.3 DC, implying a price of $18.2/DC
- The Mango Market exploit, discussed later, used the illiquidity of an AMM to drive up the price of MNGO
- Very large price increases are possible with AMMs
- Depends on algorithm and reserve ratios

Smart Contract Risk

- A smart contract is simply a computer program that runs on a virtual machine on the blockchain
  - a virtual machine is a computer that runs computer programs just like a desktop computer would except that the computer itself is implemented in software running on the blockchain
- Smart contracts implement the financial services of DeFi such as AMMs, Decentralized Exchanges (DEX), money market funds, lending protocols, and derivative contracts
- A smart contract can do the same things any computer program can do but it can also manipulate the native digital currency on the blockchain
- Because smart contracts are computer programs, they have the same risks as any computer program—bugs or mistakes in the program logic
  - however, because smart contracts are open source and can be inspected by anyone, bugs and logic mistakes are much easier to find and exploit than in conventional software
  - In addition, smart contracts are much harder to fix than conventional software since the code may in fact be locked down partially or completely, so that the software can't be repaired quickly or at all
- The open source nature of smart contracts has an additional vulnerability in that anyone can write a contract, regardless of programming skill or experience
- Important smart contracts should undergo a rigorous independent audit before deployment and on an ongoing basis
- Smart contracts should also be stress tested

Oracle Risk

- Smart contracts can only know what is on the blockchain and cannot know anything about the outside world
- Because smart contracts may need external information, such as prices on an exchange or that a payment was made somewhere else, they need some mechanism to feed that information to them
- Oracles provide that service to smart contracts
- An oracle is an important potential source of risk management failure in a smart contract
- Oracle data must be accurate, reliable, and timely or the smart contract can either fail or be hacked
- Oracle risk management best practices
  - data sources should be high quality with high uptime, speed, and accuracy guarantees
  - oracles should be responsible for performing due diligence on the quality and accuracy of the data by getting more than one data source and checking for outliers and incorrect values
  - oracles should not have a single point of failure in their design
  - strong oracle cyber security practices very important to avoid being hacked
  - oracle design and practices should be transparent
  - oracles should tailor their practices to specific smart contracts they service
- Important for smart contract developers to perform a risk management audit and due diligence on potential oracles

Legal Risk

- Because there is no clear legal and regulatory structure governing DeFi around the world, legal and regulatory risk is huge
- If someone exploits a smart contract but does nothing deceptive, what are the civil and/or criminal penalties?
- Who would have standing to sue in any case?
- DeFi practitioners have found that they can write a smart contract, develop a platform, or trade crypto and be surprised later on that they are the subject of civil or criminal actions
  - the CFTC recently brought enforcement actions against those who participated in the governance protocol of Ooki DAO (Decentralized Autonomous Organization—an association defined by a smart contract)
  - Do Kwon, the developer of the Terra stablecoin system that collapsed, had criminal charges filed against him in South Korea and is also the subject of an Interpol red notice
  - One of the Tornado Cash developers, Alexey Pertsev, was arrested in the Netherlands on suspicion of facilitating money laundering
  - Mango Markets settled privately with the person who exploited their protocol; it's very common for DAOs to settle with hackers and attackers since there is no clear legal enforceability
- Very important to manage legal and regulatory risk by knowing all potential laws and regulations that could apply (even if it is not clear that they do apply) and stringently following them

Wrong Way and Custody Risk

- Although wrong way risk occurs in conventional finance, it can be much more prevalent in DeFi
- Wrong way risk arises because of the correlation of major crypto tokens under stressed conditions and because insurance and capital funds are often denominated in crypto
- Custody risk occurs because ownership of digital assets requires that a private key—essentially a piece of data that records ownership of crypto—be safeguarded
- If a private key is lost, the crypto assets that it corresponds to are lost forever
- Custody risk must be carefully controlled by custodians such as centralized exchanges—if the keys are lost or stolen, customer funds cannot be retrieved
- Solutions for custody risk are being developed but none have gained dominance yet

Bridge Risk

- A crypto bridge is an application that allows two blockchains to transfer crypto tokens by allowing the blockchains to communicate, exchange data, and execute instructions
- Bridges are popular because they allow tokens on one blockchain to be traded on a different blockchain that has some advantages over the first blockchain, such as lower fees
- Bridge security is inherently difficult and is probably the biggest security challenge in DeFi currently
  - security of tokens depends on the protocol of the blockchain native to the token
  - when the tokens are mirrored on another blockchain by transfer over a bridge, they are less secure since they are secured by the protocol of the foreign blockchain, while the original asset is secured by its native blockchain
  - bridges do not have the same security guarantees as blockchains
- Bridges also could introduce systemic risk
  - if there are many bridges between a number of blockchains, an attack on one blockchain could produce contagion that would threaten the security of a number of other blockchains at the same time, producing a crypto financial crisis

Protocol Risk

- Protocol risk refers to the risk that the security of the blockchain could be compromised by an attack
- A 51% attack is a well-known protocol risk in Bitcoin for example
- Blockchain protocols could also be threatened by a denial of service attack, a failure to reach consensus, or a hard fork (a decision by the chain to split off into two separate chains that are incompatible with each other)
- Studying the security guarantees of particular blockchains is very import
- As recommended later, regulatory authorities may want to stress test particular blockchains or the entire DeFi economy as part of a systemic risk management program

Case Study: Mango Market Exploit on Oct 11,2022

Mango Market is a decentralized exchange (DEX) running on the Solana blockchain

1

Approx 5 mil USDC → Deposited as margin to buy perpetual swaps on MNGO/USDC with 4X leverage

Approx 5 mil USDC → Deposited as margin to sell perpetual swaps on MNGO/USDC, taking other side of long position

2

Drove up MNGO/USDC substantially by buying MNGO for USDC on DEXs with thin liquidity and whose prices fed the oracles monitored by the Mango Market DEX to value the perpetual swaps

3

As the long perpetual swaps went into the money, withdrew excess margin and used funds to continue to drive up MNGO/USDC

4

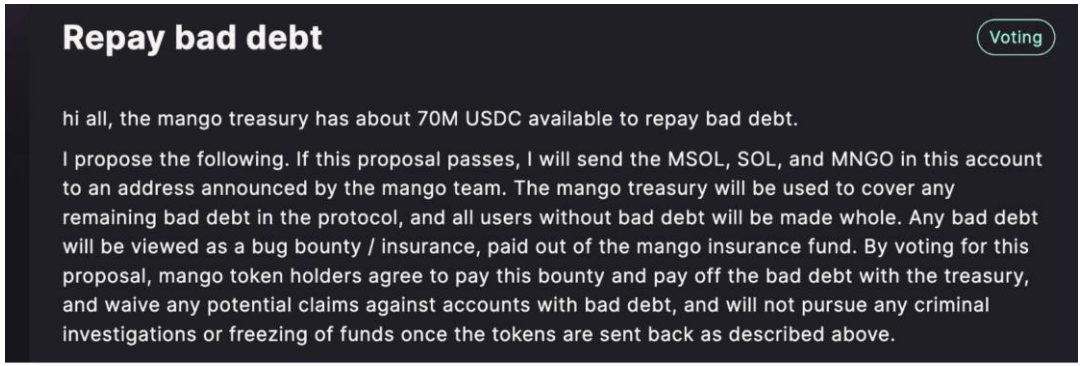
Having pushed MNGO/USDC up and therefore value of long position substantially, borrowed $120 million in various digital tokens collateralized by unrealized gains, and removed tokens from platform

Long Account:+$120 million

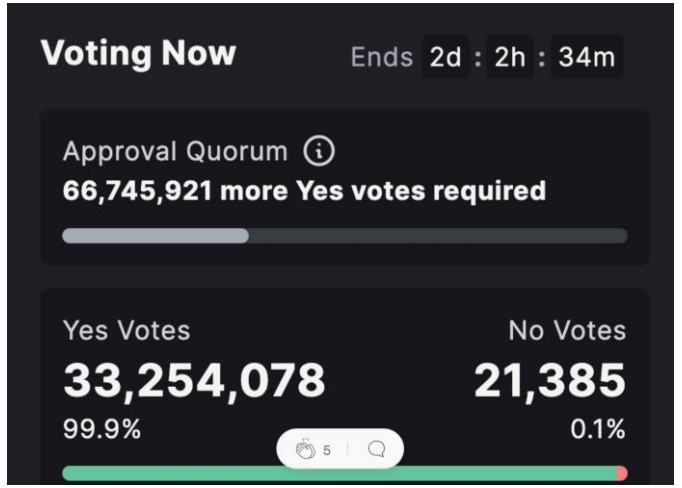
Short Account: -$115 million

5

Managed potential civil and criminal legal risk by making governance proposal to Mango Market DEX



6



Once the governance proposal was approved by the DEX, collected approximately $37 million as "bug bounty"

Risk Management Failures In Mango Markets Step by Step

1. Identity Risk: smart contract code failed to identify that the same agent was on both sides of the perpetual swaps
2. Algorithmic Liquidity risk: How much a thinly traded token's price rises depends on the algorithm of the AMM
3. Oracle risk: Oracle performed no risk management or due diligence on MNGO/USDC price feed to detect price manipulations
4. Smart Contract Risk: algorithm allowed borrowing against unrealized gains and removing the borrowed assets from the platform
5. Legal Risk: "code is law" view provides no clear recourse in civil law and criminal penalties are highly uncertain. The person who claimed responsibility for the Mango Markets exploit commented on twitter: "I believe all of our actions were legal open market actions, using the protocol as designed, even if the development team did not fully anticipate all the consequences of setting parameters the way they are."
6. Wrongway Risk: Mango Markets insurance fund was denominated in MNGO, which had crashed after the exploit, rendering the insurance fund insolvent

Risk Management Solutions To Prevent Mango Markets Exploit Step by Step

1. Identity Risk: In the absence of a digital identity solution, have dedicated risk management team carefully examine vulnerability to Sybil attack (multiple traders with the same underlying identity)
2. Algorithmic Liquidity risk: Stress test Automated Market Maker algorithm for liquidity supply under adverse conditions
3. Oracle risk: Have dedicated risk management team perform due diligence on all oracles used by the smart contracts. Require independent validation or audit of oracle before use.
4. Smart Contract Risk: Independent risk team review of algorithm. Carefully review leverage and margin requirements. Stress test the smart contract
5. Legal Risk: Write a legally enforceable contract expressing the intent of the smart contract logic and require all users to sign contract before using the platform.
6. Wrongway Risk: Always denominate capital or insurance funds in a robust stablecoin backed by real assets

How Do You Stress Test A Smart Contract?

- Smart contract developers should perform a suite of stress tests once their DEXs or AMMS are of sufficient size
- Smart contracts are computer programs that run on a virtual machine on the blockchain
- As a consequence, unlike in financial stress tests, a smart contract's behavior is deterministic and predictable with certainty
- A stress testing model would consist of a custom built virtual machine that imitates exactly the virtual machine on the blockchain
- Scenarios would be stressed market inputs that are run through the smart contract running on the custom virtual machine
- Scenarios could reveal risks that would need to be addressed by changing the smart contract logic
- Stress tests of the larger DeFi protocols should be risk management best practice

Recent Examples of Crypto Bridge Exploits

BNB Bridge Exploit (Oct 6, 2022)

- Very subtle cryptographic bug allowed attacker to forge messages on the internal bridge between Binance Chain and Binance Smart Chain (BSC)
- Attacker minted 2 million BNB and then deposited them in the Venus protocol, a DEFI automated money market on the BNB Chain
- Attacker then attempted to move minted assets across bridges to other chains
- Binance quickly shut down BNB Chain, but attacker was still able to remove approximately $100 million

Wormhole Bridge Exploit (Feb 2, 2022)

- The wormhole bridge allows transfers between Solana and Ethereum blockchains
- For example, wormhole would allow you to lock ether in a smart contract on Ethereum, then credit those Ethereum on Solana
  - the Ethereum are “wrapped” on Solana and can be traded on Solana with its lower fees
- Exploiting a bug, the attacker convinced the wormhole to credit 120K ETH on Solana, and then bridged back 93,750 ETH to Ethereum before the attack was discovered

Risk Management Lessons From Bridge Exploits

- Bridges are probably the hardest risk management problem in DEFI currently
- Risk management actions that could mitigate the risk include
  - Independent audits to verify code and cryptographic integrity
  - Vigorous monitoring of transactions in real time to uncover abnormal or suspicious activities (e.g. a DEFI version of an AML-like program)
  - Bridge withdrawal lockup periods that get longer as the size of the bridged transaction increases
  - Capital fund (or independent insurance) denominated in a stablecoin backed by real assets to maintain bridge operation in the event of an attack
- Bridges also can introduce systemic risk, which will be discussed in the section on systemic risk and crypto financial crises

Case Study: Tornado Cash Sanctioned By OFAC

- The U.S. Treasury's Office of Foreign Assets Control (OFAC) added 45 Ethereum addresses to the list of Specially Designated Nationals (SDN) in August 2022
- The Ethereum addresses correspond to smart contracts running on Ethereum that make up part of the Tornado Cash protocol
- Tornado Cash is a smart contract application that allows users to transact privately on Ethereum
- Applications such as Tornado Cash helps DeFi users manage identity risk but worsens identity risk for regulators and law enforcement
- On Ethereum and other smart contract blockchains, addresses correspond to both accounts and smart contracts, i.e., computer programs that run on the blockchain
- The OFAC sanction is notable in that it sanctions smart contract addresses, i.e., software itself, rather than just account addresses that are owned by persons
- Sanctions of privacy smart contracts are not a general solution to the identity risk problem, since they make privacy on blockchains more difficult, reducing the chance of more widespread use of digital assets and services
- The technical solution to the digital identity risk problem already exists, and is an integral component of Tornado Cash—zero knowledge proofs

What is A Zero Knowledge Proof?

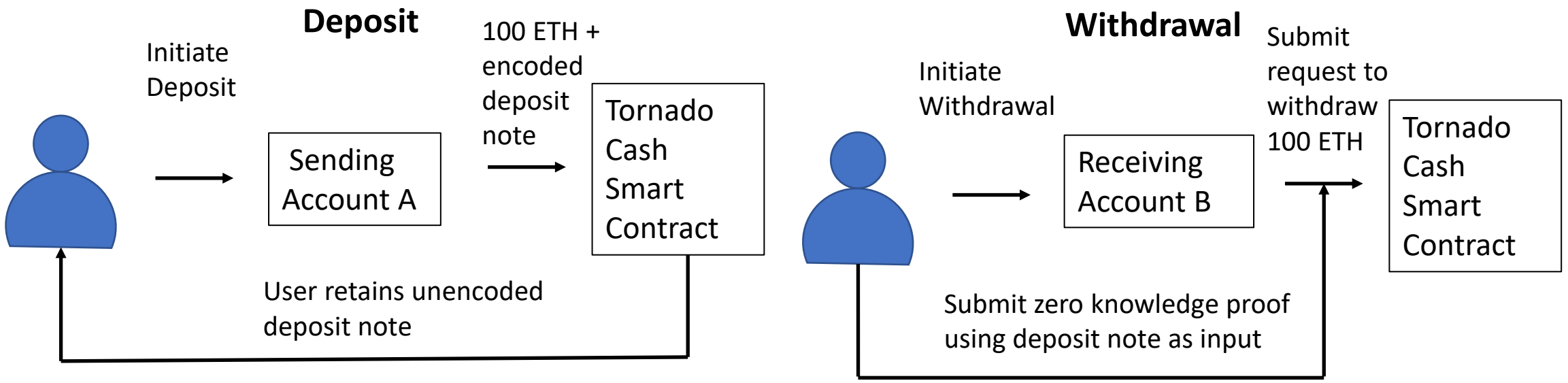
- A zero knowledge proof is a cryptographic proof that some fact is true without revealing any other information other than that the fact is true
- Relevant zero knowledge proofs for DeFi that communicate essential information while maintaining privacy include
  - my income is at least 75K, (but I won't say what it is)
  - I am over the age of 18 (but I won't reveal my age)
  - I am not on a list of sanctioned persons (but I won't tell you who I am or where I live)
- How are zero knowledge proofs possible? We illustrate with a simple example to convey the intuition.

How can A, the prover, prove to B, the verifier, that 2 balls have different colors without revealing the colors?

Zero Knowledge Protocol

1. B puts on a blindfold and then A puts a ball in each of B's hands. B then randomly shuffles the balls behind his back and puts one ball in each hand.
2. B then shows the balls to A and challenges him to say whether the balls have changed hands. If they are really the same color, A has a 50% chance of getting it right
3. B then randomly shuffles the balls behind his back again and then challenges A to state whether the balls have changed hands. A now has a 25% chance of getting both guesses right if the balls are the same color
4. B keeps repeating the experiment until the probability is so low that A is randomly guessing that B must conclude the balls are indeed a different colors, but he does not know what colors

How Tornado Cash Works

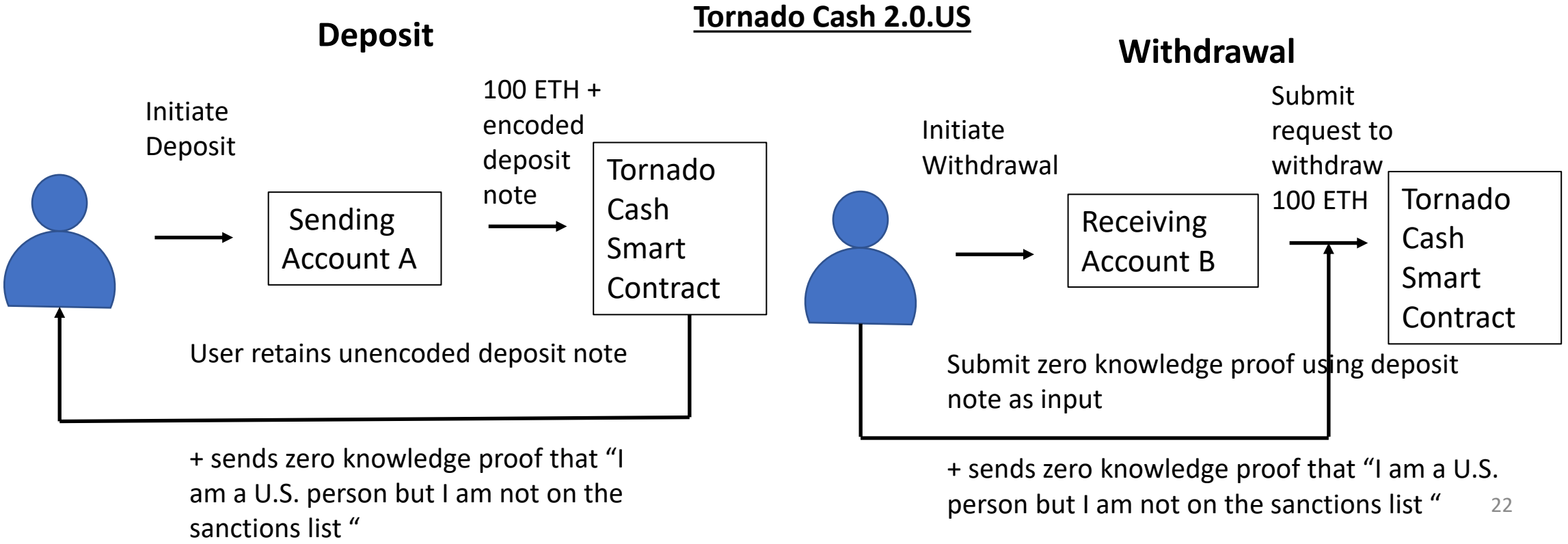


- User keeps the unencoded deposit note secret
- He will later use the deposit note to prove to the Tornado Cash smart contract that he deposited 100 ETH without revealing his identity
- Smart contract keeps encoded deposit note on file
- All users must deposit the same amount of ETH—100 ETH in this example—to increase security

- Smart contract verifies that the zero knowledge proof proves that the user previously deposited 100 ETH without revealing which sending account the 100 ETH came from
- The smart contract also disables the ability of the user to withdraw 100 ETH again so that fraudulent multiple withdrawals are prevented
- Thus, users can transact privately on Ethereum using Tornado Cash

Risk Management Lessons For Identity Risk

- Smart contract privacy applications can be modified in principle to protect user privacy while satisfying legal and regulatory requirements
- Applications like Tornado Cash would have to have an additional zero knowledge routine that would verify the proof of "I am a U.S. person but I am not on the sanctions list"
- Management of digital identity, however, will likely require additional legislation and regulatory rules



Trust in People vs Trust in Software Protocols

- Conventional finance relies fundamentally on trust in people whereas DeFi relies on trust in the software protocol
- The regulatory problem in conventional finance is that people may not be trustworthy and therefore must be governed by regulatory rules
  - securities must be registered to ensure that the promoters disclose all relevant information to investors
  - exchanges must be regulated since they are run by people, the software used is closed source, and therefore the rules of the exchange need to be disclosed to prevent fraud, mistaken trades, or market manipulation
- The trustworthiness of people is largely irrelevant in DeFi since everything is open source software and all relevant facts are already transparent and disclosed
- Although DeFi lacks the fundamental regulatory problems of conventional finance, it has a host of new risks that do need to be regulated
- However, the current regulatory environment given its statutory foundation is not set up to do that
- Application of current rules to an area to which they don't apply will miss the risks that are present and also may create perverse incentives

Is The Howey Test Applicable to DeFi?

- In 1946 in SEC v W.J. Howey Co, the Supreme Court laid out the canonical four-part legal test to determine if something is a security. To be a security requires
  - an investment of money
  - in a common enterprise
  - with the expectation of profit
  - derived from the efforts of others
- Most crypto securities (including NFTs) could be argued to meet this test, implying that smart contracts that implement exchanges, money markets, or derivatives would be subject to the same rules that standard securities must follow
- However, whether crypto securities satisfy the Howey test is irrelevant to the point of the Securities Act of 1933, which is to 1) insure that investors receive all significant information, financial or otherwise, before deciding to purchase a security and 2) that fraud and misrepresentations are prevented
- Digital tokens and smart contracts are simply open source software—all information about the tokens or exactly how the exchanges work is already revealed in the code
- The Securities Acts of 1933 and 1934 are designed to mitigate the risks associated with trust in people
- DeFi, as already discussed, has completely different risks

Application of Conventional Regulatory Rules Can Create Perverse Incentives

- Ethereum recently changed its consensus mechanism from proof of work to proof of stake
- Using proof of stake, it could be argued that Ethereum now satisfies the Howey test and has become a security
- Nonetheless, Ethereum works exactly the same as before under proof of stake—it's now just much more efficient and much more climate-friendly
- But as a security Ethereum and the DeFi ecosystem around it would incur new reporting and other regulatory requirements, disincentivizing proof-of-stake over proof-of-work
- In contrast, proof-of-work digital assets, such as bitcoin, would continue to be legally classified as commodities
- New legislation would likely be necessary to regulate proof-of-work digital assets, since regulatory authority of the spot commodities market is limited
- Having a 2-tier regulatory system would mean that the regulatory rules are not technology- nor risk-invariant
- Digital assets that behave exactly the same way and have the same risk profile under different consensus mechanisms would be treated differently under the current legal view that a digital asset is either a commodity or a security

Current Regulatory Rules Could Miss Potential Systemic Risk in Crypto

- Fundamentally, financial crises in the conventional financial system arise because of a sudden lack of trust coupled with some weakness in financial institutions (e.g, under-capitalization or poor risk management)
  - a run on a bank is a loss of trust that the bank can satisfy its obligations, which is generally sparked by some weakness in the bank's management or practices
  - the 2008 financial crisis started as a run on the repo market, precipitated by general concerns about the health and risk management practices of financial institutions
  - The recent financial crisis in the crypto markets was confined to centralized institutions—the DeFi segments did not have a financial crisis
- Blockchains are designed to shift trust from faith in people or institutions as in the conventional financial system to faith in a software protocol
- As a result, a DeFi financial crisis will not look like a conventional financial crisis
- A DeFi financial crisis would result from a loss of faith in the underlying blockchain protocols that is systemic
- One way that could happen is if a protocol attack occurred on one blockchain that is bridged into a number of other chains
- The bridges could introduce contagion across blockchains, which could eventually spill into the banking system in the off-ramps
- Current regulatory statutes do not seem to provide authority to deal with potential systemic risks

Recommended Legal and Regulatory Policy

- Even if is true that DeFi has a new set of risks and therefore needs updated legislation to properly regulate it, is it really feasible that Congress pass new legislation given that DeFi is a new, complex technology that is developing and changing very fast?
- If Congress can't write legislation expeditiously, shouldn't the regulatory community proceed by applying existing law, however inadequate, rather than leaving the sector unregulated?
  - in other words, even if the second view on page 3 is correct about the facts, isn't the first view the practical solution, if sub-optimal?
- This is the dilemma the industry and regulatory community have been confronting
- One way out of this dilemma is to put the burden on the industry to develop appropriate risk management standards and rules, since the industry has the needed expertise
- Congress could employ the Self-Regulatory Organization (SRO) model in which it would be up to the DeFi industry to set rules and regulations, establish risk management best practices, and set standards that promote ethical behavior and adherence to laws and regulations
- Congress could set up an additional SRO, similar to FINRA, that would regulate the industry, reporting to one or more regulatory agencies
- The regulatory agencies would have to review and approve all rules, policies, and risk management standards
- The following recommendations are grounded upon the SRO model

Recommendations

Recommendation 1: The DeFi industy should set up a standards committee (SRO) that would define best practices for risk management of DeFi projects that would explicitly target identity risk, algorithmic liquidity risk, smart contract risk, oracle risk, wrong way risk, custody risk, bridge risk, and protocol risk. The rules would also define standards for independent validation. The standards committee should have a certification process for DeFi projects and should disclose to the public which projects have been certified. In addition, the standards committee should write rules that guide how blockchains and other layers should govern smart contracts that would be certified to run on their platform. Smart contracts or other projects that can be used to violate or avoid laws should not be certified.

To make sure rules are being enforced, Congress should set up a Self Regulatory Organization (SRO) similar to FINRA which would report to one or more of the existing regulatory authorities. The task of the SRO would be to monitor compliance with the rules and standards proposed by the standards committee, to audit DeFi protocols, and to issue findings if a deficiency is found in the rules and standards themselves or in their application. All rules and standards proposed by the standards committee would be reviewed and approved by the governing regulatory agencies. The new SRO would be financed by fees levied on DeFi projects so that tax payers would not incur any cost.

Recommendations

Recommendation 2: As part of that SRO legislative package in Recommendation 1, regulatory authorities should be given the mandate and budget to measure potential systemic risk in DeFi by running CCAR-like stress tests. In contrast to systemic regulatory stress tests required by Dodd Frank in which banks run stress tests designed by regulators, in DeFi regulators could design and run the stress test themselves. Because DeFi is completely open and smart contracts run deterministically, it would be possible for regulators to create models that would allow realistic simulation of systemic risk scenarios, something regulators would have liked to do for the conventional financial system, but which has not been possible for practical reasons. Initially, these scenarios would be run for information and research purposes, but later on as the technology matures, Congress may grant authority for regulators to intervene if systemic risks develop.

Recommendation 3: Since new legislation for digital assets currently viewed as spot commodities is necessary in any event, lawmakers should take the opportunity in the SRO legislation to avoid the arbitrary distinction between commodities and securities in the crypto context and create a common regulatory platform by defining a new asset class, algorithmic assets, that would cover the gamut of digital assets in a uniform fashion. Federal legislation on algorithmic assets should be made consistent with proposed amendments to the Uniform Commercial Code, specifically the new Article 12 and amendments to Article 9, which provide the ability to perfect a security interest in digital assets and to provide negotiability of digital assets. The states should codify these UCC amendments into state law and in addition consider providing a new legal person status for Decentralized Autonomous Organizations (DAOS) so that they would have some of the legal characteristics of corporations.

Recommendations

Recommendation 4: Regulatory authorities should provide notice and extensive comment periods before taking enforcement actions in order to tailor their policies better to the risks inherent in the crypto sector
Recommendation 5: To balance legitimate privacy interests with the need to prevent money laundering and criminal activities, regulators should publish a proposed policy for how privacy applications could be designed and used legally. The policy should reflect the capabilities of the current cryptographic technology. For example, regulatory rules in the DeFi context should be stated as much as possible in terms that could be verified by a zero knowledge protocol in a smart contract. Rules could also specify what tools should be made available. Tornado Cash already has a compliance tool that allows a user to decode his deposit slip to prove the source of funds upon a legal request from law enforcement or regulatory authorities. Is that tool sufficient or is something else or more needed? If the DeFi industry does set up a standards committee, regulators could work with it to define the rule.