

# DeFi: Opportunities and Risks

Campbell R. Harvey  
Duke University and NBER

# Times have changed

- Bitcoin was once thought of as a method for criminal transactions or a “fraud”



JPMorgan Chase & Co. Chief Executive Officer Jamie Dimon said he would fire any employee trading bitcoin for being “stupid.”

# JP Morgan joins bitcoin bandwagon



The price of the digital asset has risen by as much as a quarter this week amid signals that it is becoming mainstream and is being accepted by big financial institutions

ERIC GAILLARD/REUTERS

Share    

Save 

Bitcoin enjoyed another boost yesterday at the end of a record-breaking week as the world's largest investment bank outlined plans to trade it.

larvey 2022

# THE WALL STREET JOURNAL.

## FINANCIAL TIMES

### Coinbase Fetches \$85 Billion Valuation in Market Debut

### Coinbase coins it on Nasdaq

Cryptocurrency exchange is first major bitcoin-focused company to test U.S. public market



#### Coinbase's recent growth



# Duke University's Early Coinbase Investment Could Now Be Worth \$500M: Sources



# Setting

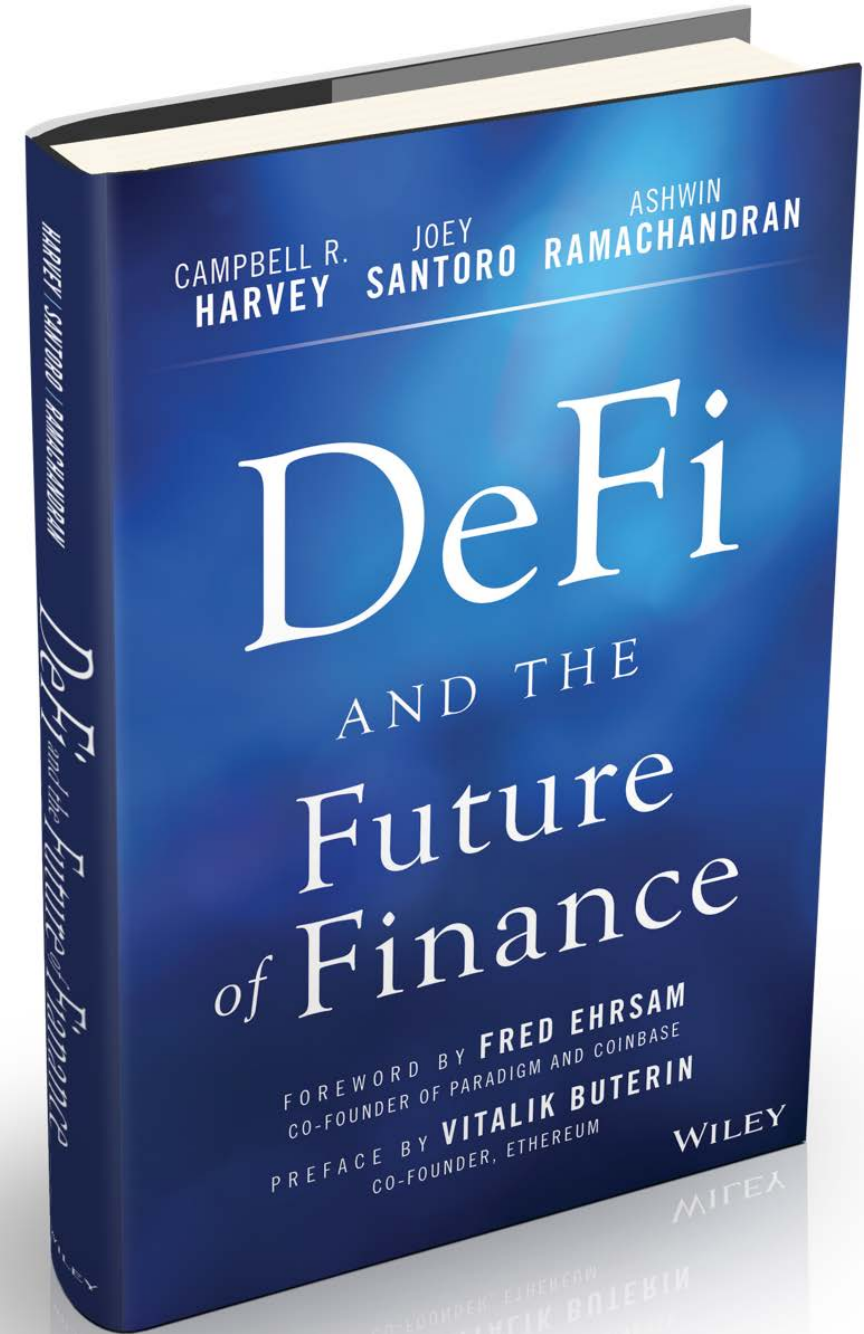
- But there is far too much attention paid to bitcoin
- Many are familiar with the asset – few understand it
- There is something else, largely under the radar, that has little to do with bitcoin: Decentralized Finance or DeFi
- Word cloud from my course

Asymmetric-key-cryptography  
Scaling-risk AMM Proof-of-stake  
Yield-farming Vertical-scaling DEX Nonce  
Sharding Slashing KYC Address  
Vampirism Mint Invariant DAO  
Schelling-point-oracle Direct-incentive  
Optimistic-rollup Halting-problem Testnet ERC  
EOA Airdrop Fork Oracle  
Keeper Smart-contract  
Double-spend Gas Hexadecimal Burn Miner PoS  
Defi-Legos Consensus-protocol Layer Utility-token  
Flash-swap Horizontal-scaling Miner-extractable-value  
Flash-loan PoW IDO Contract-account dApp  
Node Vault Stablecoin Router-contracts Symmetric-key-cryptography  
Digest Impermanent-loss  
Bonding-curve Governance-token  
Hash Proof-of-work Staking DeFi

# What is DeFi?

- “DeFi or decentralized finance seeks to build and combine open-source financial building blocks into sophisticated products with minimized friction and maximized value to users using blockchain technology. Given it costs no more to provide services to a customer with \$100 or \$100 million in assets, we believe that **DeFi will replace all meaningful centralized financial infrastructure in the future**. This is a technology of inclusion whereby anyone can pay the flat fee to use and benefit from the innovations of DeFi.”

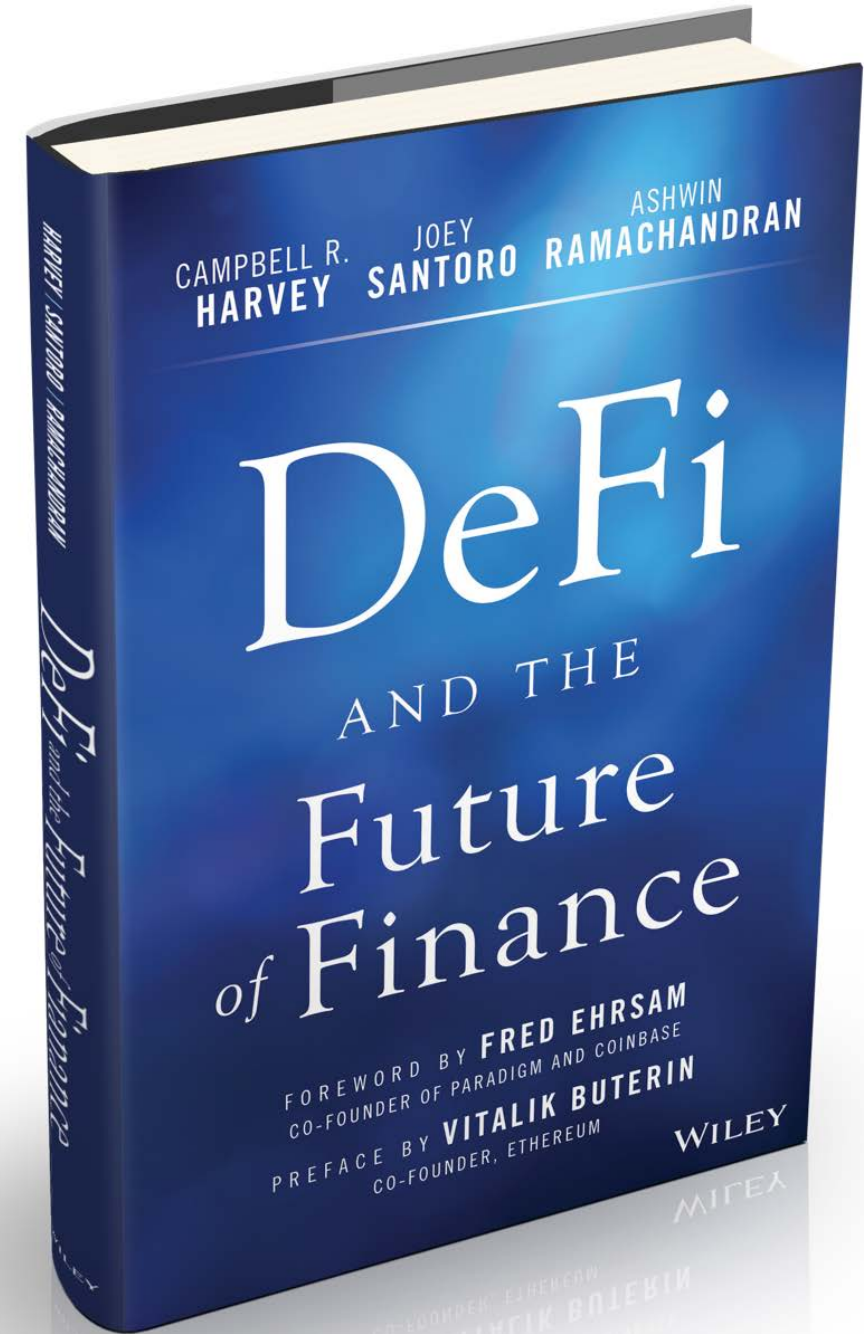
Campbell R. Harvey 2022





# What is DeFi?

- “DeFi is fundamentally a competitive marketplace of decentralized financial applications that function as various financial “primitives” such as exchange, save, lend, and tokenize. These applications benefit from the network effects of combining and recombining DeFi products...”

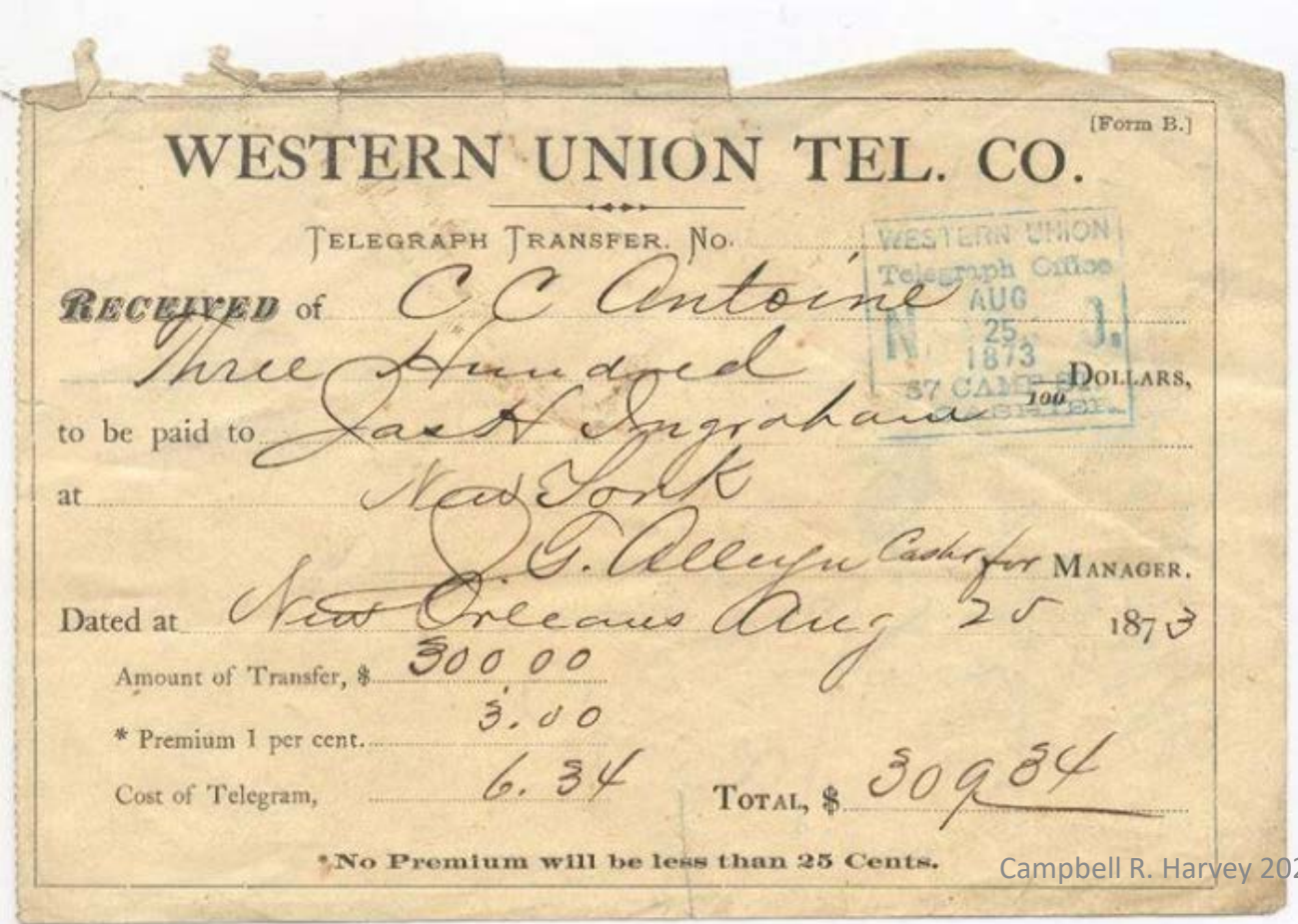


# Problems DeFi attempts to solve

- **Inefficiency**
- Limited access
- Opacity
- Centralized control
- Lack of interoperability

# Problems DeFi attempts to solve

- First Western Union money transfer



# Problems DeFi attempts to solve

- First Western Union money transfer

[Form B.]

**WESTERN UNION TEL. CO.**

TELEGRAPH TRANSFER. No. \_\_\_\_\_

RECEIVED of *C. C. Antoine*

*Three Hundred*

to be paid to *Jas H Ingraham*

at *New York*

Dated at *New Orleans Aug 25 1873*

*J. G. Alley* Cashier for MANAGER.

Amount of Transfer, \$ *300 00*

\* Premium 1 per cent. *3.00*

Cost of Telegram, *6.34* TOTAL, \$ *309 34*

WESTERN UNION  
Telegraph Office  
AUG 25 1873  
37 CENTS  
100

DOLLARS,

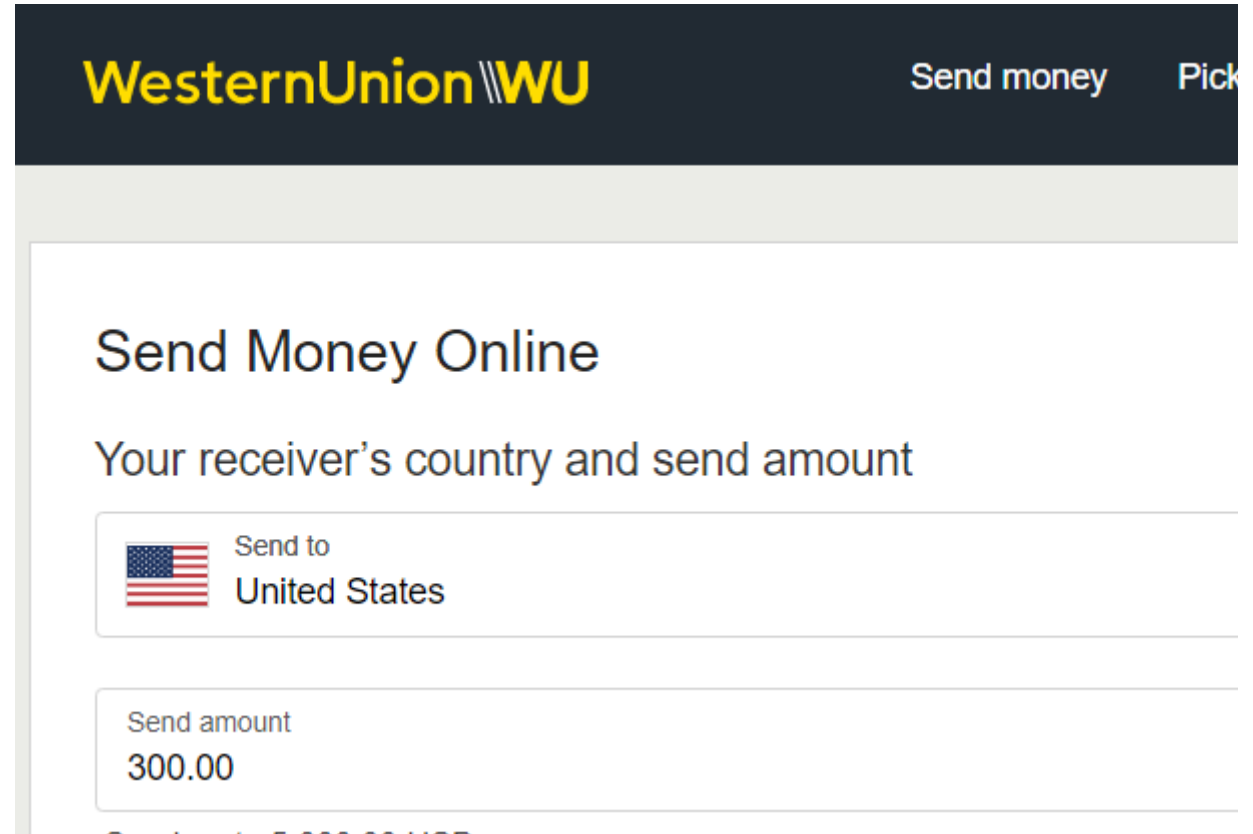
\*No Premium will be less than 25 Cents.

3% fee – nothing changed in 150 years!

# Problems DeFi attempts to solve

## *2021 e-Money*

- Today Western Union money transfer



The screenshot shows the Western Union website's 'Send Money Online' interface. At the top, the Western Union logo is on the left, and 'Send money' and 'Pick' are on the right. Below the header, the main heading is 'Send Money Online'. Underneath, it says 'Your receiver's country and send amount'. There are two input fields: the first is labeled 'Send to' and contains 'United States' with a US flag icon; the second is labeled 'Send amount' and contains '300.00'.

# Problems DeFi attempts to solve


## *2021 e-Money*

- Today Western Union money transfer

How would you like to pay? <sup>31</sup>

Pay online


Pay cash in-store



**Credit Card**

---


In minutes<sup>1</sup>  
Fee<sup>2</sup> 54.50 USD



**Debit Card**

---

In minutes<sup>1</sup>  
Fee<sup>2</sup> 47.00 USD



**Bank account**

---

0-4 Business days<sup>1</sup>  
Fee<sup>2</sup> 11.00 USD

# Problems DeFi attempts to solve

## *2021 e-Money*

- Today Western Union money transfer

Summary	
Transfer amount	300.00 USD
Transfer fee <sup>2</sup>	+ 47.00 USD
Promo discount	<a href="#">Apply promo</a>
Transfer total	347.00 USD
<hr/>	
Total to receiver	300.00 USD
<hr/>	
Service time: <sup>1</sup>	In minutes

<https://www.westernunion.com/us/en/web/send-money/start?ReceiveCountry=US&ISOCurrency=USD&SendAmount=300&FundsOut=AG&FundsIn=DebitCard>

# Problems DeFi attempts to solve

- **Inefficiency**

- High volume and low frictions (no 300bp swipe fee)
- Trade with peers via dApps
- Smart contracts available to anyone (who pays gas fee)
- Little organizational overhead (contracts reused)
- No settlement delays
- Forking makes it easy to improve



# Problems DeFi attempts to solve

- Inefficiency
- **Limited access**
- Opacity
- Centralized control
- Lack of interoperability

# Problems DeFi attempts to solve

- **Limited access**

- 1.7b unbanked – many more “underbanked”
- Many small businesses are forced to resort to credit card borrowing – because banks not interested in going through the loan process
- Savings rates are negligible and loan rates too high
- DeFi offers yield farming
- DeFi offers flash loans
- DeFi offers IDOs
- Democratization of finance

# Problems DeFi attempts to solve

- Inefficiency
- Limited access
- **Opacity**
- Centralized control
- Lack of interoperability

# Problems DeFi attempts to solve

- **Opacity**

- Senator Elizabeth Warren:  
*“DeFi refers to a fast-growing and highly opaque corner of the cryptocurrency market”*

ELIZABETH WARREN  
MASSACHUSETTS

COMMITTEES:  
BANKING, HOUSING, AND URBAN AFFAIRS  
ARMED SERVICES  
FINANCE  
SPECIAL COMMITTEE ON AGING

United States Senate

UNITED STATES SENATE  
WASHINGTON, DC 20510-2105  
P: 202-224-4543

2400 JFK FEDERAL BUILDING  
15 NEW SUDBURY STREET  
BOSTON, MA 02203  
P: 617-565-3170

1550 MAIN STREET  
SUITE 406  
SPRINGFIELD, MA 01103  
P: 413-788-2690

[www.warren.senate.gov](http://www.warren.senate.gov)

July 26, 2021

The Honorable Janet Yellen  
Secretary  
United States Department of Treasury  
1500 Pennsylvania Avenue, N.W.  
Washington, D.C. 20220

Dear Secretary Yellen:

I am writing to you in your capacity as Chair of the Financial Stability Oversight Council (FSOC) regarding the need for a coordinated and cohesive regulatory strategy to mitigate the growing risks that cryptocurrencies pose to the financial system. FSOC is responsible for identifying and responding to emerging risks to financial stability, and I am pleased to see that the Council has begun devoting more attention to this critical issue.<sup>1</sup> I urge FSOC to act with urgency and use its statutory authority to address cryptocurrencies' risks and ensure the safety and stability of our financial system.

# Problems DeFi attempts to solve

- **Opacity**

- However, smart contracts are transparent
- All parties aware of capitalization of counterparties
- It is the current system that is opaque. We rely on regulators and they have a dubious track record.

# Problems DeFi attempts to solve

- Inefficiency
- Limited access
- Opacity
- **Centralized control**
- **Lack of interoperability**

# Problems DeFi attempts to solve

- **Centralized control**

- Concentrated banking, exchange and insurance sectors exert market power in traditional finance.
- The community of stakeholders or even an algorithm can control parameters of a DeFi dApp (if admins have control over certain parameters, everyone knows that).
- Flaws will be “forked away”
- DAOs controlled by governance tokens

# Problems DeFi attempts to solve

- Inefficiency
- Limited access
- Opacity
- Centralized control
- **Lack of interoperability**



# Problems DeFi attempts to solve

- **Lack of interoperability**

- Traditional financial products are difficult to integrate with each other, (e.g., wire transfer), in many cases cannot be recombined
- Ease of composability of DeFi products, aka DeFi Legos

# Risks

- Smart contract risk
- Governance risk
- Oracle risk
- Scaling risk
- DEX risk
- Custodial risk
- Environmental risk
- Regulatory risk

# Risks: Smart contract risk

## *New attack vector*

- Public blockchains are open systems.
- Anyone can view and interact with code on a blockchain after the code is deployed. You don't need to "hack" into system to see code.
- Given that this code is often responsible for storing and transferring blockchain native financial assets, it introduces a new, unique risk.
- This new attack vector is termed *smart contract risk*.
- New companies have arisen with single goal of auditing.

# Risks: Smart contract risk

## *Sources of risk*

- Smart Contract risk can take the form of a logic error in the code or an economic exploit in which an attacker can withdraw funds from the platform beyond the intended functionality.

# Risks: Smart contract risk

## *Logic error*

- The error can take the form of any typical software bug in the code.
  - Example: some rounding in a contract. Code says to pay out 14 ETH – but only 13.99999999 are in the contract. Transaction fails because of insufficient funds.
  - Dangers include the draining of funds in a contract
  - It is also possible that tokens are functionally locked within the protocol. Informally these are known as “bricked” funds and cannot be recovered.

# Risks: Smart contract risk

## *Example: Economic exploit*

- An economic exploit would be more subtle.
- For example, let's assume a contract takes the role of an exchange between two tokens. It determines the price by looking at the exchange rate of another similar contract elsewhere on chain and offering that rate with a minor adjustment.
- If the oracle exchange is illiquid, the exploiter could sell on the illiquid exchange driving the price down, and then buy cheaply on the liquid exchange.

# Risks: Smart contract risk

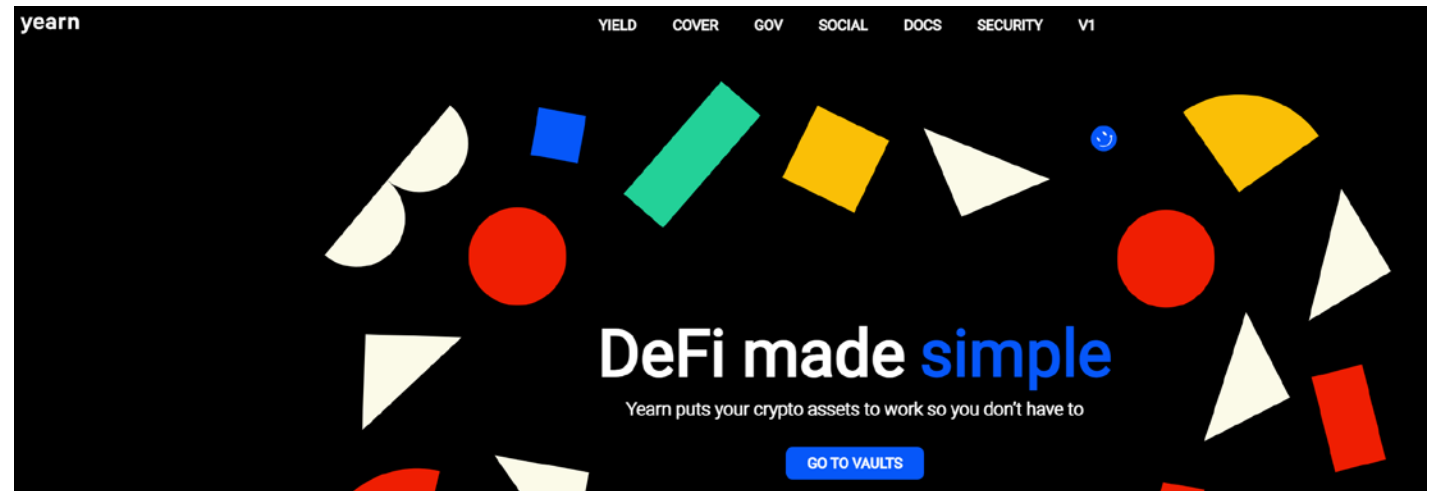
*Example: Economic exploit – flash attack*

- Economic exploits become even trickier when considering that flash loans essentially allow any Ethereum user to become financially equipped for a single transaction.

# Risks: Smart contract risk

## *Yearn.finance*

- Yearn.Finance is a yield aggregator, through which users can deposit funds in pools — or vaults — which are then deployed to other DeFi protocols in an effort to generate yields for those depositors.
- Complex exploit with over 160 nested transactions



## Yearn Finance suffers exploit, says \$2.8 million stolen by attacker out of \$11 million loss



by Michael McSweeney

February 4, 2021, 5:38PM EST · 1 min read

February 3, 2021



# Risks: Smart contract risk

**\$200m Flash loan – with no collateral**

Interacted With (To):

- Contract [0x62494b3ed9663334e57f23532155ea0575c487c5](#) ✓
- TRANSFER 215,035.171940600397346616 Ether From [Wrapped Ether](#) To → [0x62494b3ed9663334e57f23...](#)
- TRANSFER 215,035.171940600397346616 Ether From [0x62494b3ed9663334e57f23...](#) To → [Compound Ether](#)
- TRANSFER 215,035.171940600397346616 Ether From [Compound Ether](#) To → [0x62494b3ed9663334e57f23...](#)
- TRANSFER 215,030.171940600397346616 Ether From [0x62494b3ed9663334e57f23...](#) To → [Wrapped Ether](#)
- TRANSFER 5 Ether From [0x62494b3ed9663334e57f23...](#) To → [Yearn \(yDai\) Exploiter](#)

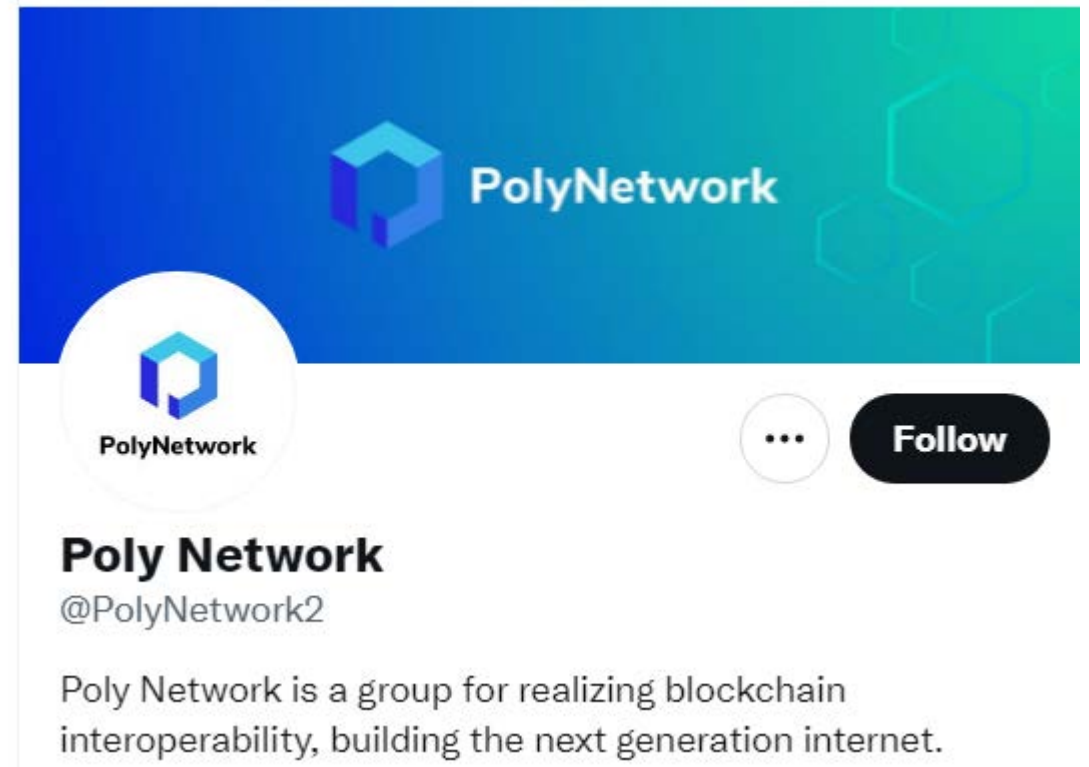
Transaction Action:

- Borrow 116,920.396944223800915079 Ether From [dYdX](#)
- Supply 215,035.171940600397346616 Ether To [Compound](#)
- Borrow 126,945,116.6393679705276416 [DAI](#) From [Compound](#)
- Borrow 134,000,000 [USDC](#) From [Compound](#)
- Repay 126,945,116.6393679705276416 [DAI](#) To [Compound](#)
- Repay 134,000,000 [USDC](#) To [Compound](#)
- Withdraw 215,035.171940600397346616 Ether From [Compound](#)
- Swap 153,258.252632 [USDT](#) For 93.30329749673893679 Ether On [Uniswap](#)
- Flash Loan 98,114.774996376596431537 Ether From [Aave Protocol V2](#)
- Repay 116,920.396944223800915081 Ether To [dYdX](#)

# Risks: Smart contract risk

## *Poly Network*

- “Poly Network, a protocol for swapping cryptocurrency, including [bitcoin](#), announced on Tuesday that it was hacked, resulting in the loss of \$611 million. The hack is suspected to be the largest fraud in “decentralized finance,” or DeFi, in history.”



NEWS

**Newsweek**

## **\$611 Million in Cryptocurrencies Stolen in Massive Hack**

BY **EMMA MAYER** ON 8/10/21 AT 12:16 PM EDT

# Risks: Smart contract risk

## *Poly Network*

- To exploit or not to exploit? That is the question.



# Risks: Smart contract risk

🔍 Search

**Bloomberg**

August 26, 2021

Cryptocurrencies

## **Victim of Biggest DeFi Hack Says All Funds Have Been Returned**

By [Olga Kharif](#)

August 26, 2021, 1:12 PM EDT



**Poly Network** @PolyNetwork2 · Aug 26

...

Yay! [#PolyNetwork](#) has completed the recovery of all [#PolyNetworkExploit](#) affected user assets. (approx. worth \$610M)

[#PolyBridge](#) has now restored cross-chain functionality for a total of 59 assets. Other advanced functions will be gradually restored.

# Risks: Smart contract risk.

## *Summary*

- Not all smart contracts are smart
- Once contract is deployed, it cannot be “fixed”

# Risks: Governance risk

## *What is governance risk?*

- For some protocols, such as Uniswap, programming risk is the sole threat to the protocol because the application is autonomous and controlled by smart contracts.
- Other DeFi applications rely on more than just autonomous computer code.

# Risks: Governance risk

## *What is governance risk?*

- For example, MakerDAO, the decentralized credit facility, is reliant on a human-controlled governance process that actively adjusts protocol parameters to keep the system solvent.
- Many other DeFi protocols use similar systems and rely on humans to actively manage protocol risk.
- This introduces a new risk, *governance risk*, which is unique to the DeFi landscape.

# Risks: Governance risk.

## March 13, 2021 \$TSD governance attack

- Hacker amasses governance token
- Devs held only 9% of governance
- Hacker votes to mint him/herself 11.5 quintillion \$TSD
- Hacker dumps 11.8 billion on Pancakeswap DEX

### ← Thread



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

A malicious attacker has just utilized \$TSD DAO to mint 11.8 billion tokens to his own account and sold all to Pancakeswap. Here is what happened:

1. Due to long Debt phase, people unbond from DAO because they no longer have rewards from expansion..

22

103

193



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

2. Dev account has only 9% of the DAO. We failed once when proposing the Implementation to enable the crosschain bridge. In this case, Dev account does not have enough stack to vote against the attacker.

1

3

20



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

3. What has been done by him? He gradually bought \$TSD at low price to accumulate until he has more than 33% of the DAO. Then he proposed an Implementation and voted for it. Because he possess enough stack to finish the voting process, the Implementation went through successfully

6

16

40



**True Seigniorage Dollar** @TrueSeigniorage · Mar 13

In the Implementation, the attacker added code to mint for himself 11.8 billion \$TSD. Then he sold all of the tokens to Pancakeswap. That's sad, it is an attack but it is how a decentralized DAO works.

5

9

63



Campbell R. Harvey 2022

<https://twitter.com/trueseigniorage/status/1370956726489415683?lang=en>

43



# Risks: Oracle risk

## *What is oracle risk?*

- Oracles are one of the last unsolved problems in DeFi and are required by most DeFi protocols in order to function correctly.
- Fundamentally, oracles aim to answer the simple question: How can off-chain data be securely reported on chain?
- Without oracles, blockchains are completely self-encapsulated and have no knowledge of the outside world other than the transactions added to the native blockchain.

# Risks: Oracle risk

## *Highest risk*

- Oracles, as they exist today, represent the highest risk to DeFi protocols that rely on them.
- All on-chain oracles are vulnerable to front-running, and millions of dollars have been lost due to arbitrageurs.
- Additionally, oracle services, including Chainlink and Maker, have suffered crippling outages with catastrophic downstream effects.
- Until oracles are blockchain native, hardened, and proven resilient, they represent the largest systemic threat to DeFi today.

# Risks: Scaling risk

## *What is scaling risk?*

- Ethereum and other “Proof of Work” (the consensus mechanism) blockchains have a fixed block size.

# Risks: Scaling risk

## *What is scaling risk?*

- Ethereum is currently limited to a maximum of 15 TPS.
- Yet, almost all of DeFi today resides on this blockchain.
- Compared to Visa, which can handle upward of 65,000 transactions per second, Ethereum is capable of handling less than 0.1% of the throughput.
- Ethereum's lack of scalability places DeFi at risk of being unable to meet requisite demand.

# Risks: Scaling risk

## *Proof of Stake*

- One actively pursued solution to the problem is a new consensus algorithm, *Proof of Stake*.
- Proof of Stake simply replaces mining of blocks (which requires a probabilistic wait time), with staking an asset on the next block, with majority rules similar to PoW.
- *Staking*, an important concept in cryptocurrencies and DeFi, means a user escrows funds in a smart contract and is subject to a penalty (*slashed funds*) if they deviate from expected behavior.

# Risks: Scaling risk

## *Vertical scaling*

- Vertical scaling centralizes all transaction processing to a single large machine – or a small number of machines.
- This centralization reduces the communication overhead (transaction/block latency) associated with a PoW blockchain such as Ethereum, but results in a centralized architecture in which one machine is responsible for a majority of the system's processing.
- Some blockchains, such as [Solana](#), follow this approach and can achieve upward of 50,000 TPS.

# Risks: Scaling risk

## *Horizontal scaling = sharding*

- Horizontal scaling divides the work of the system into multiple pieces, retaining decentralization but increasing the throughput of the system through parallelization.
- *Ethereum 2.0* takes this approach in combination with a Proof of Stake consensus algorithm.
- Ethereum 2.0's technical architecture differs drastically from vertically scaled blockchains such as Solana, but the improvements are the same. Ethereum 2.0 uses horizontal scaling with multiple blockchains and can achieve upward of 50,000 transactions per second.

# Risks: Scaling risk

## *Layer 2*

- *Layer 2* refers to a solution built on top of a blockchain that relies on cryptography and economic guarantees to maintain desired levels of security.
- Transactions can be signed and aggregated in a form resistant to malicious actors.
- This removes the constraints of a fixed block size and block rate, allowing for much higher throughput. Some layer-2 solutions are live today.



# Risks: Scaling risk.

## *Scaling problem*

- As long as DeFi's growth is limited by blockchain scaling, applications will be limited in their potential impact.

# Risks: DEX risk

## *What is DEX risk?*

- The DEX landscape on Ethereum consists of two dominant types, Automated Market Makers (AMMs) and order-book exchanges.
- Both types of DEXs vary in architecture and have differing risk profiles.
- Risks include: smart contract risk, illiquidity and slippage, impermanent loss for liquidity providers, as well as other risks

# Risks: Custodial risk

## *What is custodial risk?*

- Cryptocurrency ownership is guaranteed by the possession of a private key – a long random number that cannot be guessed. For Bitcoin and Ethereum, the private keys are 256 bits or 64 hexadecimal characters.
- Private keys are used via a digital signature algorithm to sign transactions. Hence, you need your private key to “spend”.
- Custodial risk is when you lose your private key.
- Both individual users and institutions (corporations, endowments, etc.) are subject to custodial risk.

## Risks: Custodial risk

*The New York Times*

# *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes*

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left to figure out a password that is worth, as of this week, about \$220 million.

<https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html>



# Risks: Custodial risk

## *Users face a choice*

- Users have a choice between custodial and non-custodial wallets
  - Custodial Wallet (Third Party Custody): 3rd party holds access to private keys
    - E.g., Coinbase, Binance
    - Users are subject to KYC/AML regulation
  - Non-Custodial Wallet (Self-Custody) : User has full control of keys
    - E.g., Hardware wallet, Web wallet (Metamask – keys stored in browser), Desktop wallet (Electrum – stored on machine), Mobile Paper wallet

# Risks: Environmental risk

*Proof of Work is very energy intensive*

- ETH and BTC's greatest strength is also its greatest weakness

Bitcoin electricity consumption, TWh (annualised)

Select an area by dragging across the lower chart



<https://cbeci.org/>

# Risks: Environmental risk

## *Issues*

- I calculate the marginal carbon offset cost of a new bitcoin is \$4,000.
- There are two important qualifiers here. First, what if that bitcoin is traded?
  - The \$4,000 should not apply to every trade. So the trading volume needs to be taken into account.
- Second, what if I choose to buy a bitcoin that was mined in 2012 where the carbon footprint (assuming the same carbon cost) was likely only a few cents.
  - There are 18m bitcoin and most of them mined in the period where very little energy was needed.

# Risks: Environmental risk

## *Proof of Work and Proof of Stake*

- Unlikely that BTC will shift from PoW to PoS (the miners would not support the move because the value of their equipment would go to zero)
- ETH will transition to PoS. It is a question of “when” not “if”
- What if investors purchased carbon offsets? How would be think about valuing those offsets



Risks: Environmental risk

*Issues:*

*Carbon offset*

Cryptocurrencies

## Bitcoin ETF Pledges to Reduce Carbon Footprint by Planting Trees

By [Michael Bellusci](#)

August 27, 2021, 9:22 AM EDT

► Accelerate to link the number of trees planted to asset flows

Calgary-based Accelerate, which offers alternative ETF products, pledges to plant 3,450 trees for every C\$1 million (\$788,200) invested into its carbon-negative Bitcoin ETF, estimating this will result in the sequestration of about 1,000 tons of carbon dioxide. Exchange traded crypto funds have been approved in Canada, though not in the U.S.

Note very close to my calculation.

$788,200 / 60,000 = 13 \text{ BTC}$

$13 \text{ BTC} * 83 \text{ tons} = 1,079 \text{ tons}$

Planting trees likely cheaper than carbon offset credits

# Risks: Regulatory risk

## *KYC/AML*

- DeFi in the cross-hairs of the SEC right now
- China bans crypto transactions
- Major centralized spot and derivatives exchanges, previously ignored by the CFTC, have recently been forced to comply with [KYC/AML compliance orders](#), and DEXs appear to be next.
- Already, several decentralized derivatives exchanges, such as dYdX, must geoblock US customers from accessing certain exchange functionalities.

# Risks: Regulatory risk

FTX SERVICES AND FTX TOKEN (FTT) ARE NOT AVAILABLE IN THE UNITED STATES OR OTHER PROHIBITED JURISDICTIONS.



MARKETS

OTC

FTT

HELP

Search market

FTT

SRM

BTC

ETH

Prediction

NEW

New Stocks

NEW

Futures

Spot

Stocks

Leveraged Tokens

Volatility

Prediction

Fiat

Recent



GME/USD

258.000 -14.00%

24h volume  
\$501,009

GameStop (GME) is a tokenized stock. Learn more about FTX tokenized stocks [here](#).

Outside U.S. Market Hours

GME/USD

5m



Compare



Indicators



Save



Orderbook

Grouping None

258.000

Bid Size (GME)	Bid Price (USD)	Ask Price (USD)	Ask Size (GME)
4.02	253.675	258.000	10.00
126.30	253.650	259.100	0.01
1.00	253.525	261.200	0.01
0.04	253.500	263.200	0.01
0.01	253.000	265.300	34.48
1.40	252.000	266.400	0.15
2.01	251.000	266.875	3.98
2.00	250.400	266.900	10.00
6.03	250.000	267.000	98.93
45.61	249.425	267.300	0.01
0.01	248.900	269.000	1,772.90

Market Trades

Price (USD)

Size (GME)

Time



# Risks: Regulatory risk

- **Balancing act**

- Too much regulation drives innovation offshore – too little regulation leads to consumer exploitation
- New technology is complex
- Difficult for regulator to invest time to understand
- Even if they are trained, their knowledge quickly becomes stale
- Difficult for regulators to recruit talent that understands space.

# Conclusions

- I would argue that finance has been operating with a similar model over the past century (commercial banks, central banks, stock exchanges, brokers, insurance, ...)
- Current wave of fintech just improves the current CeFi and is likely fleeting

# Conclusions

- I would argue that finance has been operating with a similar model over the past century (commercial banks, central banks, stock exchanges, brokers, insurance, ...)
- Current wave of fintech just improves the current CeFi and is likely fleeting
  - ***“The current fintech, like Stripe and Plaid, is like putting lipstick on a pig.”*** Fred Ehrsam, March 9, 2021 guest lecture

# Conclusions

Less than 1%  
into this  
disruption  
but ...

### Comparing the Cryptocurrency Universe to Banks



Source: <https://coin.dance/>, Standard & Poors, Bloomberg

# Conclusions

- This innovation draws on parts of computer science (e.g., cryptography and distributed systems) and other fields such as game theory and finance and is developing into a fundamental and interdisciplinary area of science and engineering its own right.
- Future generations will be jealous of your opportunity to get in on the ground floor of this new area—analogous to getting into the Internet and the Web in the early 1990s.
- I cannot overstate the opportunities available to someone who masters this material—current demand is much, much bigger than supply.



# Conclusions

- We are now seeing the scaffolding of a new city that reinvents finance. It is just a matter of time for the legacy players – and they know it.
- Millenia ago, we started out with peer to peer market exchange - barter. We have come full circle. All assets, physical and virtual will be tokenized.

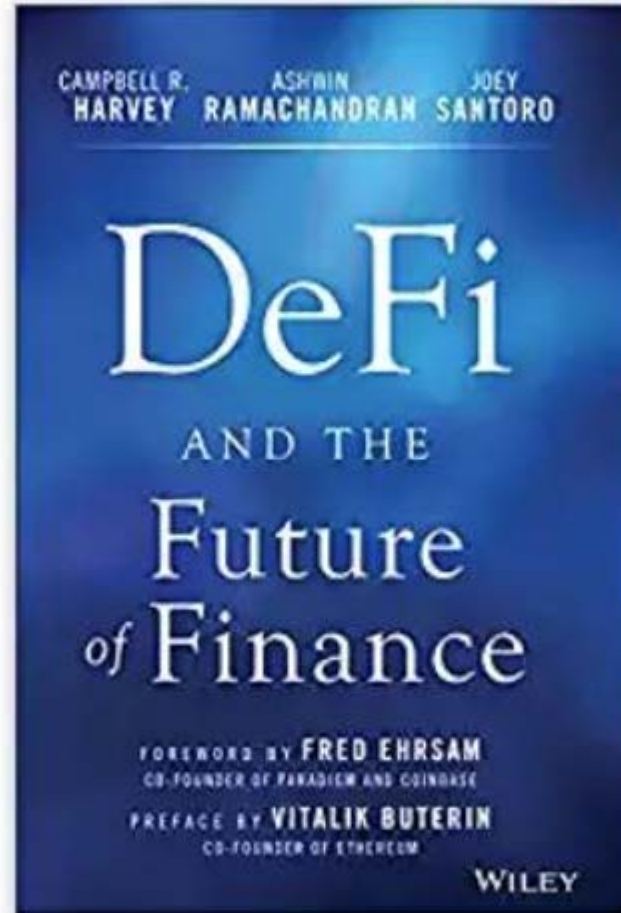
# Conclusions

- Investors should not fool themselves. I have heard so many times: “We are not exposed to crypto.”
- Even though your portfolios might have no direct investments in DeFi, you are exposed in a negative way
- DeFi has the potential to substantially disrupt or eliminate many of the companies in your current portfolio

#1 Best Seller in Business Finance

Look inside ↓

Released Fall 2021



ISBN-13: 978-1119836018

ISBN-10: 1119836018

Campbell R. Harvey 2022

[https://www.amazon.com/DeFi-Future-Finance-Campbell-Harvey/dp/1119836018/ref=sr\\_1\\_3](https://www.amazon.com/DeFi-Future-Finance-Campbell-Harvey/dp/1119836018/ref=sr_1_3)

# Contact: Follow me on LinkedIn

<http://linkedin.com/in/camharvey>

cam.harvey@duke.edu

@camharvey

SSRN: <http://ssrn.com/author=16198>

ETH: camharvey.eth



METAMASK: **0xff65F352156D2c69F9AbbF1AEF18E6d85314Ecce**