Econ 101 Economic Principles

DeFi and the Future of Finance

Prof.CAMPBELL R. HARVEY

Professor of Finance, Fuqua School of Business, Duke University

Research Associate, National Bureau of Economic Research in Cambridge, Massachusetts.

Fellow, American Finance Association

Host: Prof. Luyao Zhang | Ph.D.

Assistant Professor of Economic, Social Science Division
Senior Research Scientist, Data Science Research Center
Duke Kunshan University

Time: Sep. 27th , Monday

9:00 –10:15 AM Durham/PM Kunshan

Zoom ID: 972 8882 9573

DUKE KUNSHAN
Office of Undergraduate Studies

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.”

https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin

THE TIMES

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.

https://www.thetimes.co.uk/article/jp-morgan-joins-bitcoin-bandwagon-vl6s5vcb2

THE TIMES

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.

https://www.thetimes.co.uk/article/jp-morgan-joins-bitcoin-bandwagon-vl6s5vcb2

THE WALL STREET JOURNAL.

Coinbase Fetches $85 Billion Valuation in Market Debut

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

https://www.wsj.com/articles/coinbase-shares-surge-in-trading-debut-11618421619

FINANCIAL TIMES

Coinbase coins it on Nasdaq

https://www.ft.com/content/5e26e64d-c617-4e15-94d5-331b82adb96c

CRYPTOCURRENCIES

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

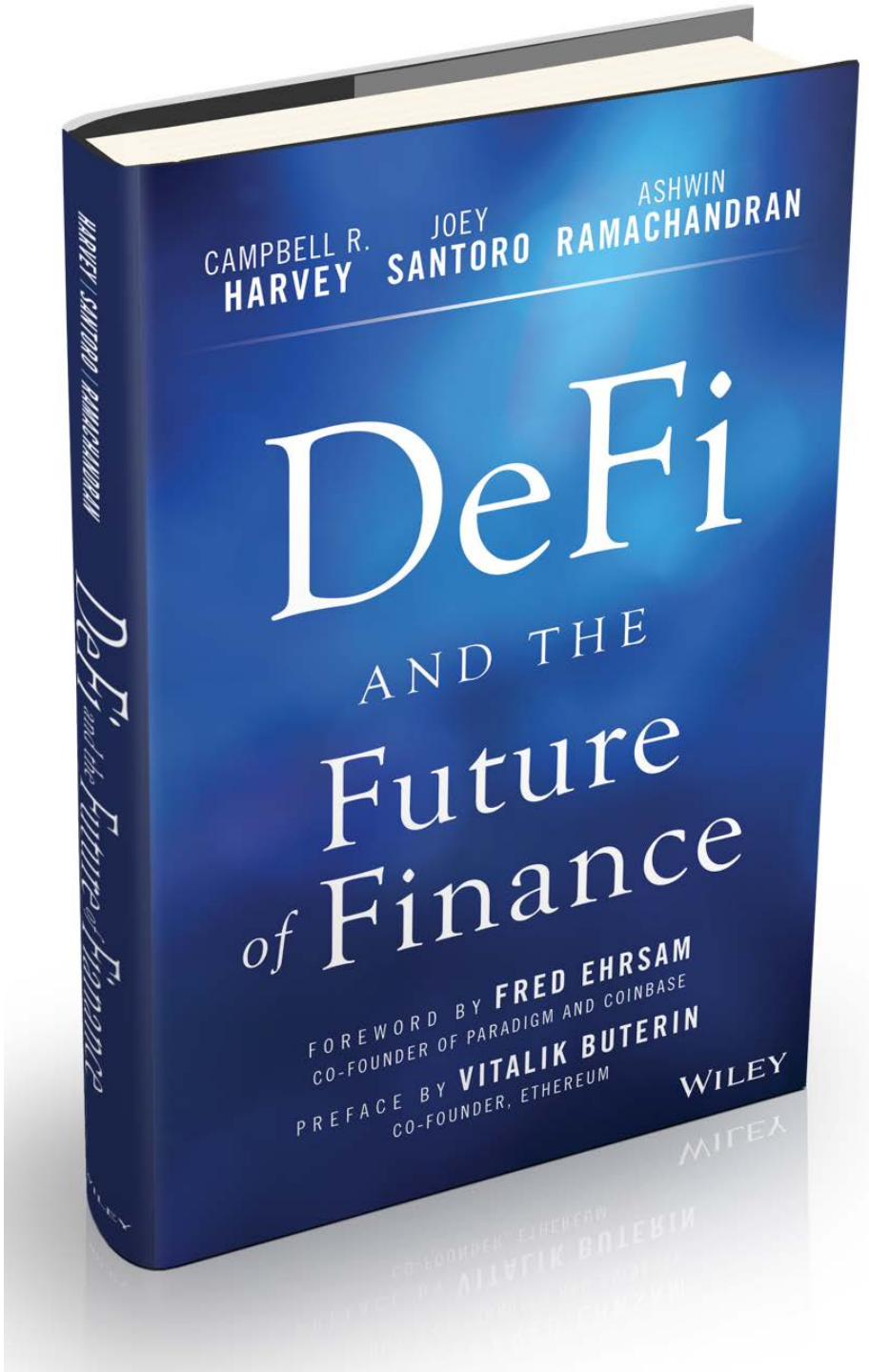
Setting

- 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
Schelling-point-oracle
Direct-incentive
DAO
Halting-problem
Testnet
ERC
Optimistic-rollup
EOA
Airdrop
Fork
Keeper
Smart-contract
Oracle
Double-spend
Gas
Hexadecimal
Burn
Miner
PoS
Mainnet
Defi-Legos
Consensus-protocol
Layer
Utility-token
Flash-swap
Horizontal-scaling
Miner-extractable-value
Flash-loan
dApp
PoW
IDO
Contract-account
Node
Vault
Stablecoin
Router-contracts
Symmetric-key-cryptography
Digest
Impermanent-loss
Bonding-curve
Governance-token
Hash
Proof-of-work
DeFi
Staking

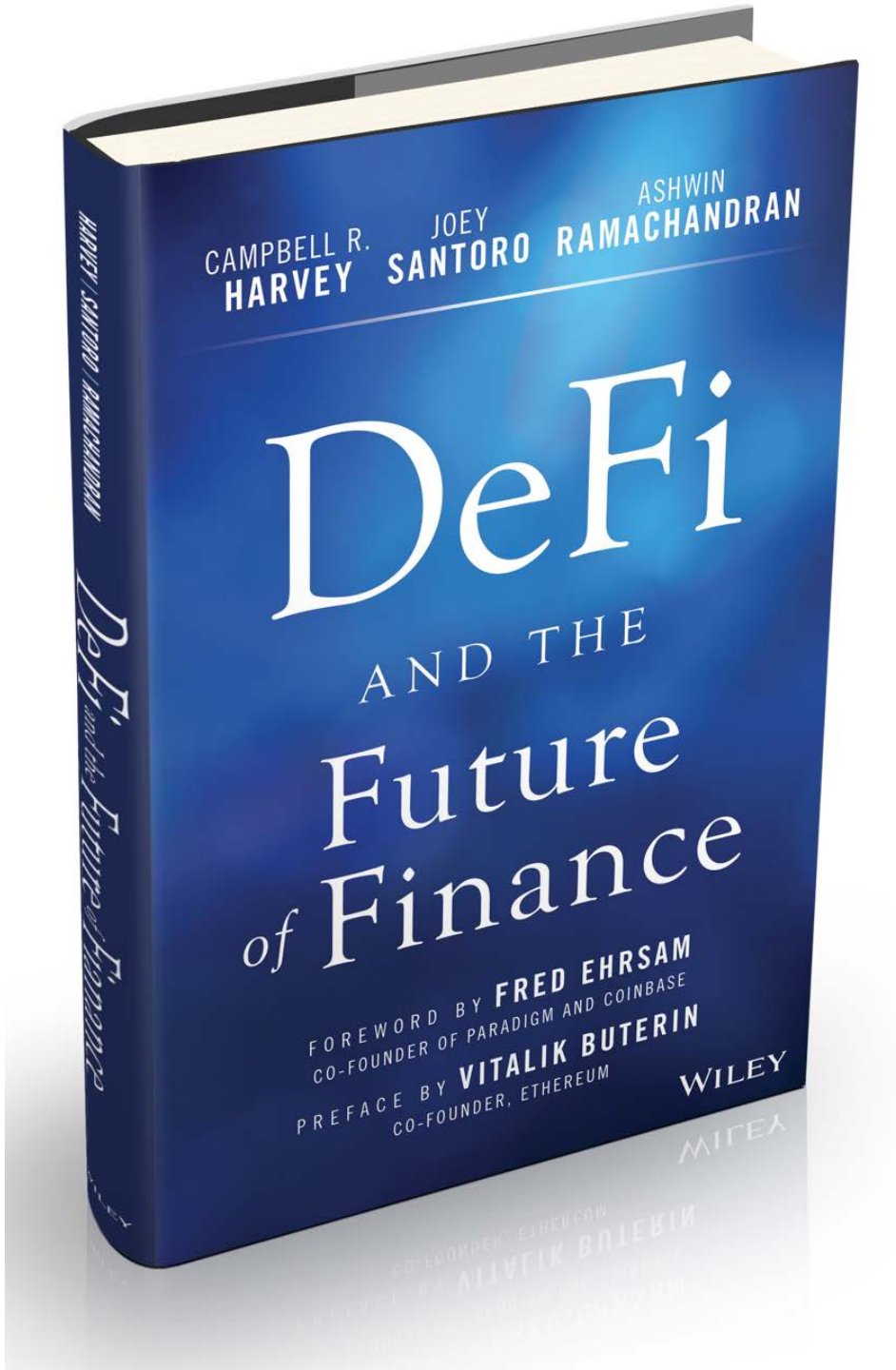
What is DeFi?

- "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."



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…"

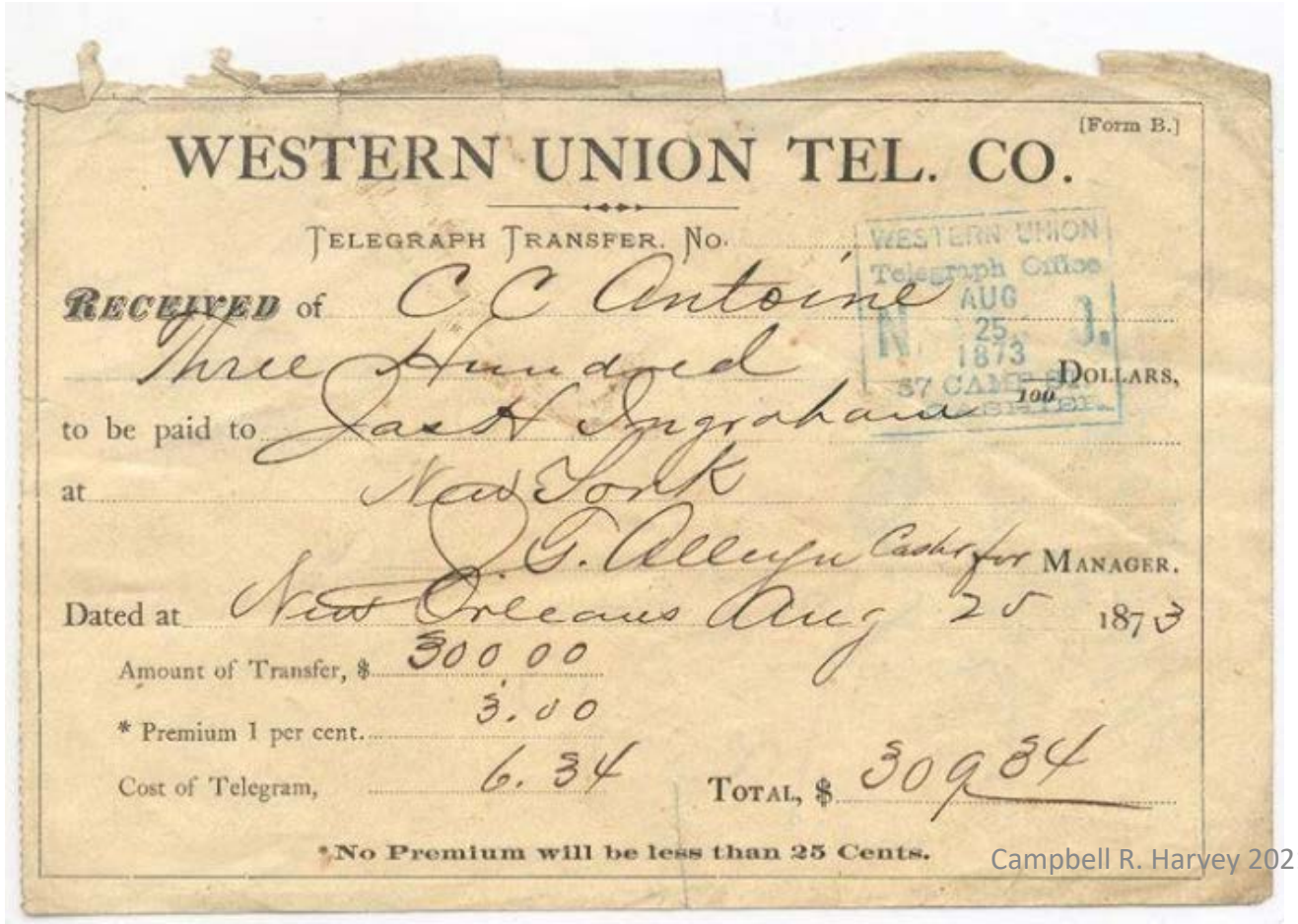


Problems DeFi attempts to solve

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

Problems DeFi attempts to solve

- First Western Union money transfer



[Form B.]

WESTERN UNION TEL. CO.

TELEGRAPH TRANSFER. No.

WESTERN UNION Telegraph Office AUG 25 1873 37 CANAL STREET

RECEIVED of C C Antoine

Three Hundred 100 DOLLARS,

to be paid to Jas H Ingraham

at New York

J. G. Allen Cashr for MANAGER.

Dated at New Orleans Aug 25 1873

Amount of Transfer, $ 300 00

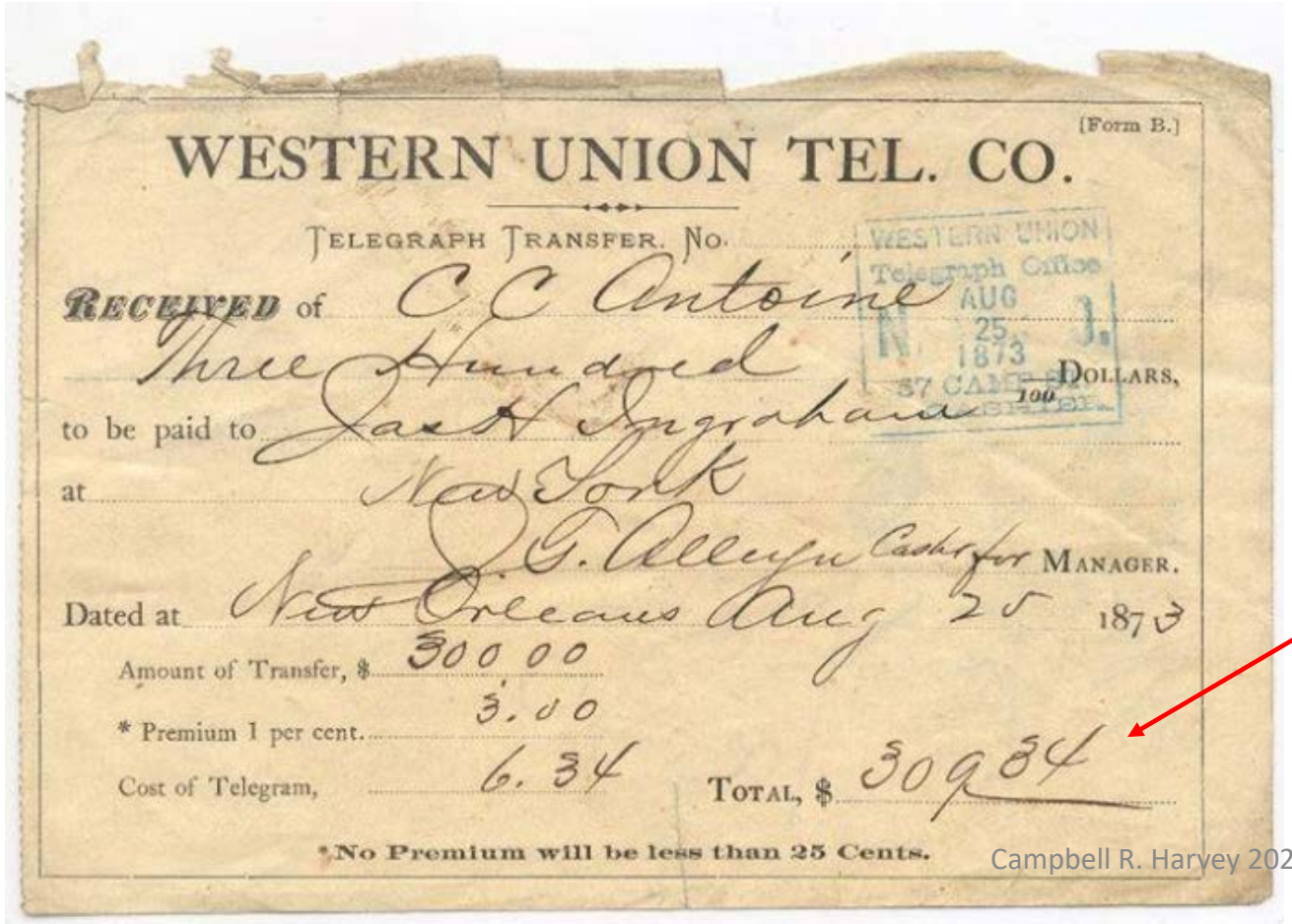
* Premium 1 per cent. 3.00

Cost of Telegram, 6.34 TOTAL, $ 309 34

*No Premium will be less than 25 Cents.

Problems DeFi attempts to solve

- First Western Union money transfer



[Form B.]

WESTERN UNION TEL. CO.

TELEGRAPH TRANSFER. No.

WESTERN UNION Telegraph Office AUG 25 1873 37 CANAL STREET

RECEIVED of C C Antoine

Three Hundred 100 DOLLARS,

to be paid to Jas H Ingraham

at New York

J. G. Allen Cashr for MANAGER.

Dated at New Orleans Aug 25 1873

Amount of Transfer, $ 300 00

* Premium 1 per cent. 3.00

Cost of Telegram, 6.34

TOTAL, $ 309 34

*No Premium will be less than 25 Cents.

3% fee – nothing changed in 150 years!

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

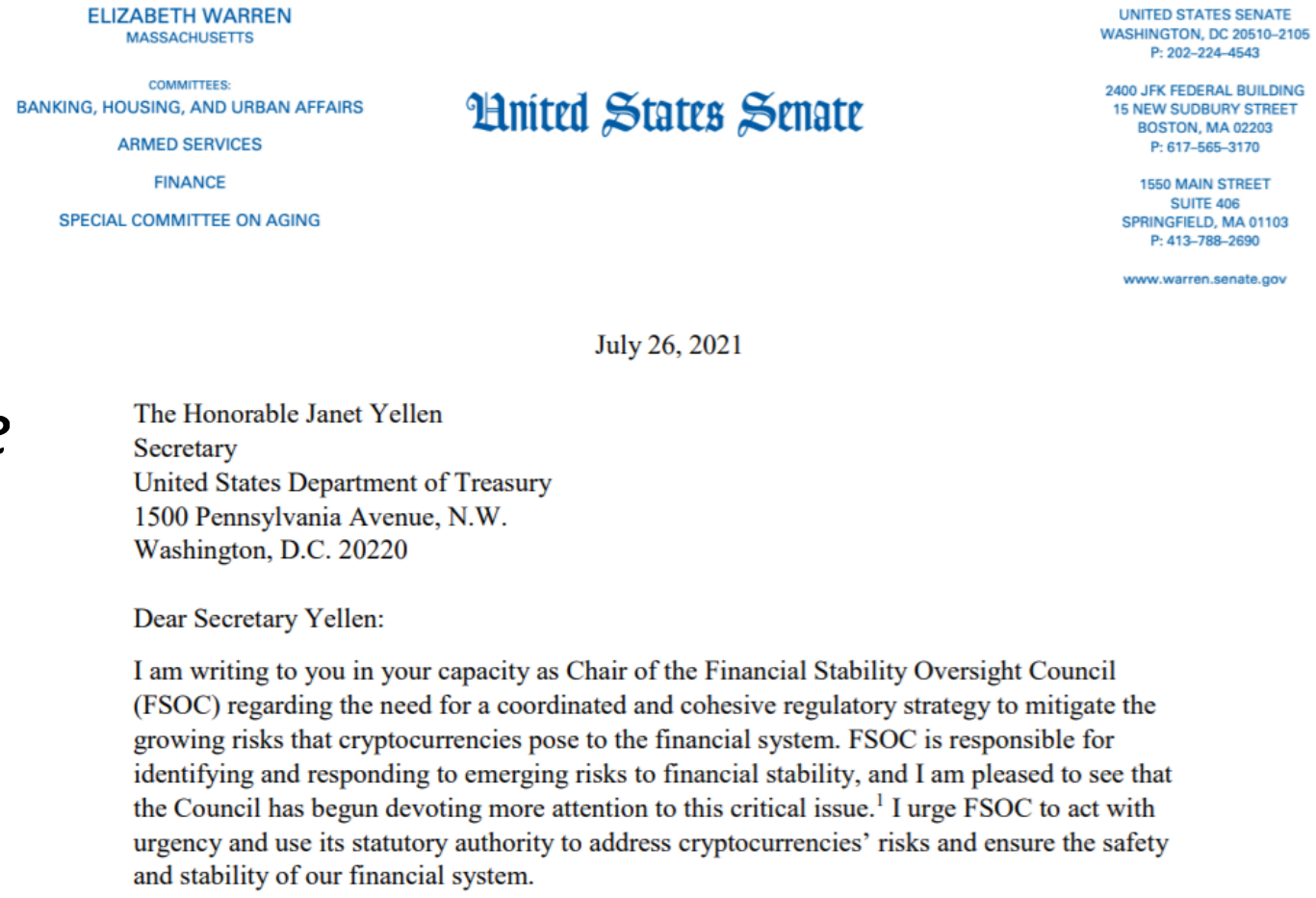
- **Limited access**
  - 1.7b unbanked – many more “underbanked”
  - Many small businesses are forced to resort to credit card borrowing – because banks not interested in going through the loan process
  - Savings rates are negligible and loan rates too high
  - DeFi offers yield farming
  - DeFi offers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

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.[1] 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.

https://www.warren.senate.gov/imo/media/doc/FSOC%20Crypto%20Letter%2007.26.2021.pdf

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

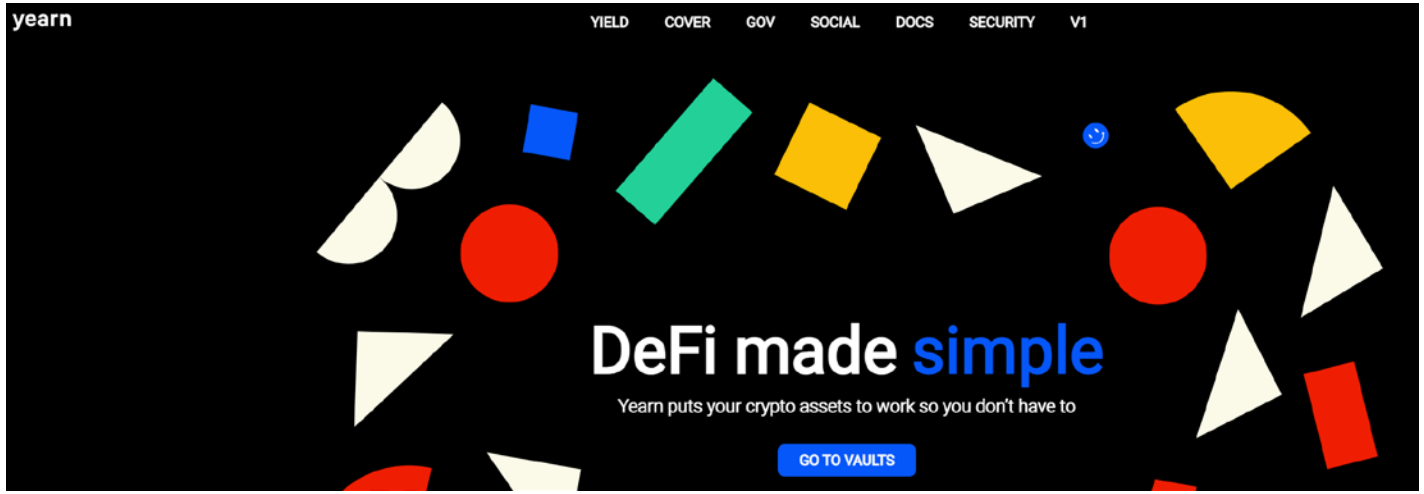
Example: Economic exploit – flash attack

- 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

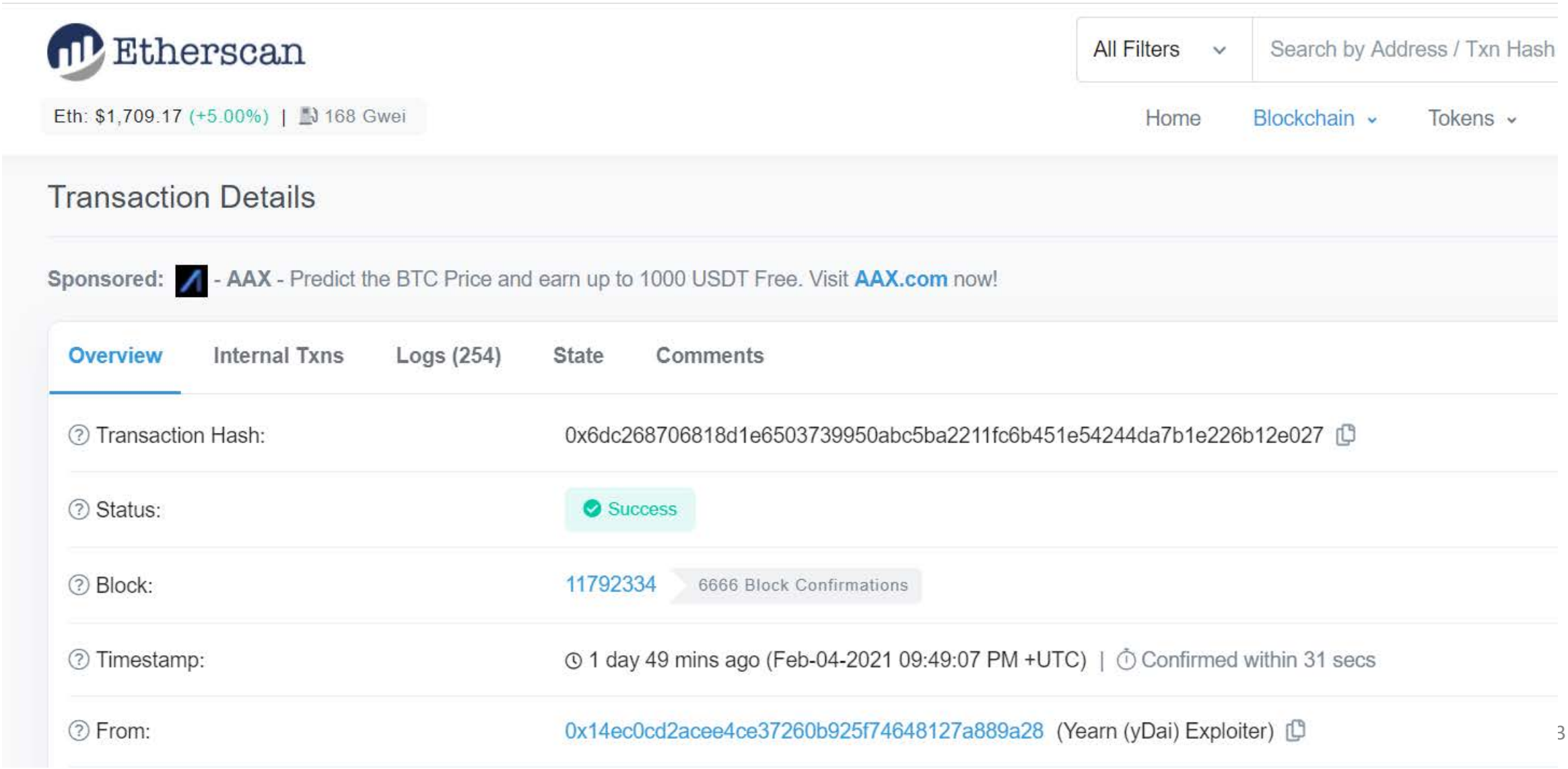
by Michael McSweeney

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

February 3, 2021

https://www.theblockcrypto.com/linked/93818/yearn-finance-dai-pool-defi-exploit-attack

Risks: Smart contract risk



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

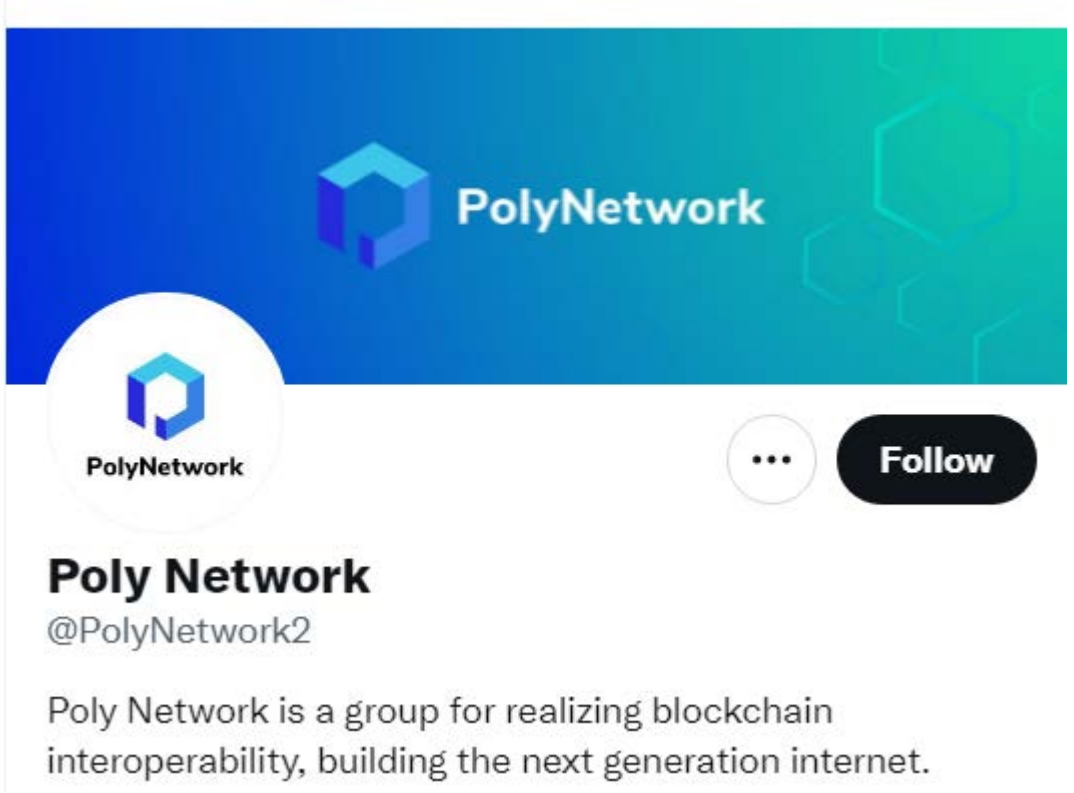
161 token transfers. Just displaying the first 10.

https://etherscan.io/tx/0x6dc268706818d1e6503739950abc5ba2211fc6b451e54244da7b1e226b12e027

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

https://www.newsweek.com/611-million-cryptocurrencies-stolen-massive-hack-1617999

Risks: Smart contract risk

Poly Network

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

Risks: Smart contract risk

August 26, 2021

Search

Bloomberg

Cryptocurrencies

Victim of Biggest DeFi Hack Says All Funds Have Been Returned

By Olga Kharif

August 26, 2021, 1:12 PM EDT

https://www.bloomberg.com/news/articles/2021-08-26/victim-of-biggest-defi-hack-says-all-funds-have-been-returned

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

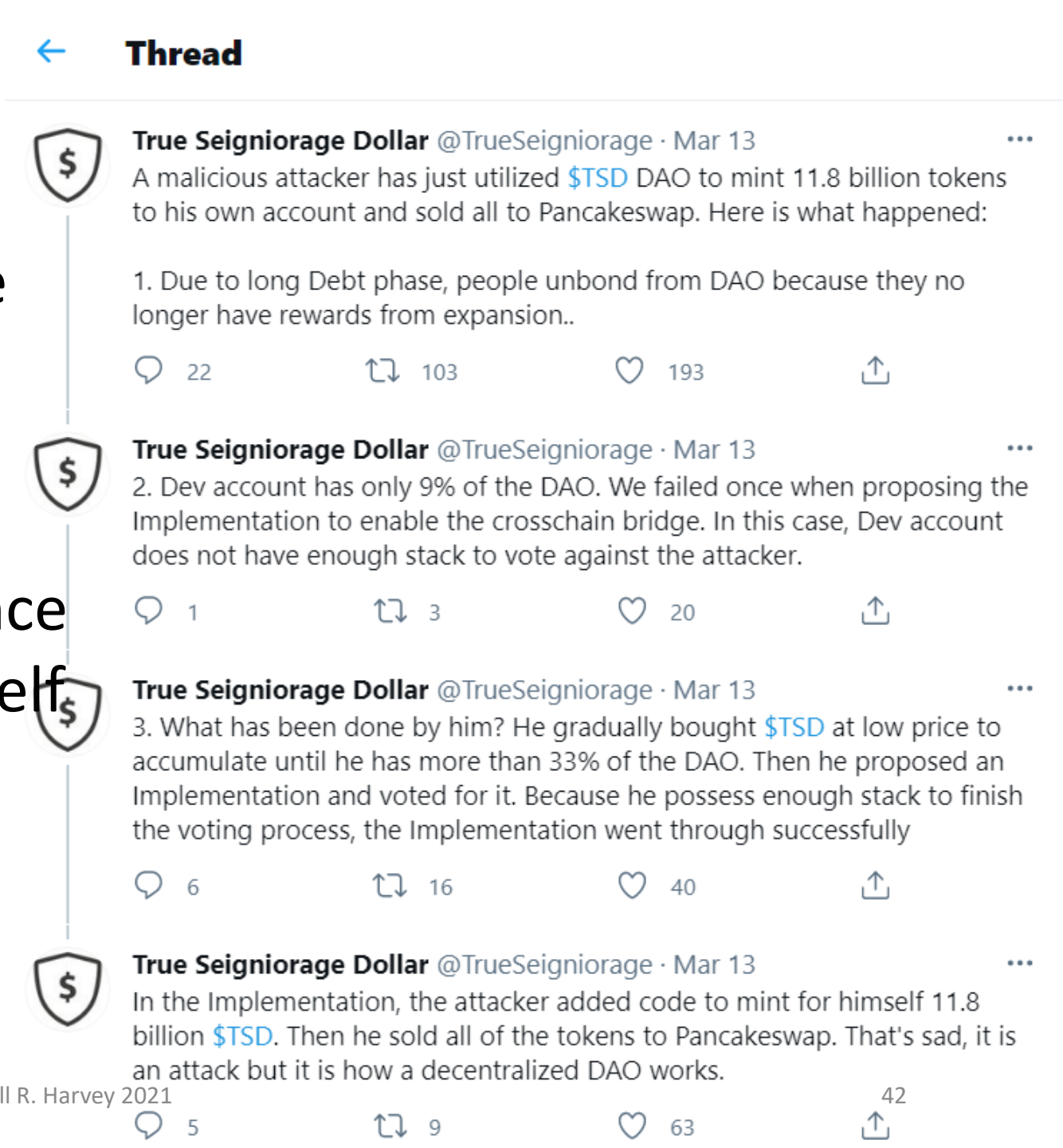
What is governance risk?

- 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



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

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: DEX risk

AMM DEX

- AMMs, however, are the most popular DEX to date, because they allow users to trustlessly and securely exchange assets, while removing traditional counterparty risk.
- By storing exchange liquidity in a trustless smart contract, AMMs give users instant access to quotes on an exchange pair.

Risks: DEX risk

CFMM DEX

- Uniswap is the best-known example of an AMM, also known as a Constant-Function Market Maker (CFMM).
- Uniswap v2 relies on the product of two assets to determine an exchange price. Balancer generalizes to multiple assets. Uniswap v3 recently introduced.
- The amount of liquidity in the pool determines the slippage when assets are exchanged during a transaction.

Risks: DEX risk

CFMM DEX

- CFMM liquidity providers (LPs) earn yield by depositing assets into a pool, because the pool takes a fee for every trade (LPs benefit from high trading volume).
- This allows the pool to attract liquidity, but exposes LPs to smart contract risk and impermanent loss.

Risks: DEX risk

On-chain order-book DEX

- On-chain order-book DEXs have a different but prevalent set of risks.
- Expensive to do everything on chain.
- Order-book DEXs are often forced to rely on a single market maker for each asset pair.

Risks: DEX risk.

Off-chain order-book DEX

- These exchanges function by settling all position entries and exits on chain, while maintaining a limit-order book entirely off chain.
- This allows the DEX to avoid the scaling and UX issues faced by on-chain order-book DEXs.

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

Retail Users

- Retail 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: 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

Delegating custody

- If you delegate the ownership of your private keys, say to an exchange, there is risk the exchange will be hacked and the keys stolen.
- Exchanges keep most of the private keys in "cold storage" (either on a drive not connected to the Internet or hard copy in a physical vault)
- Some exchanges, like Coinbase, are insured. However, the insurance is only as good as the health of the insurer.

Risks: Custodial risk.

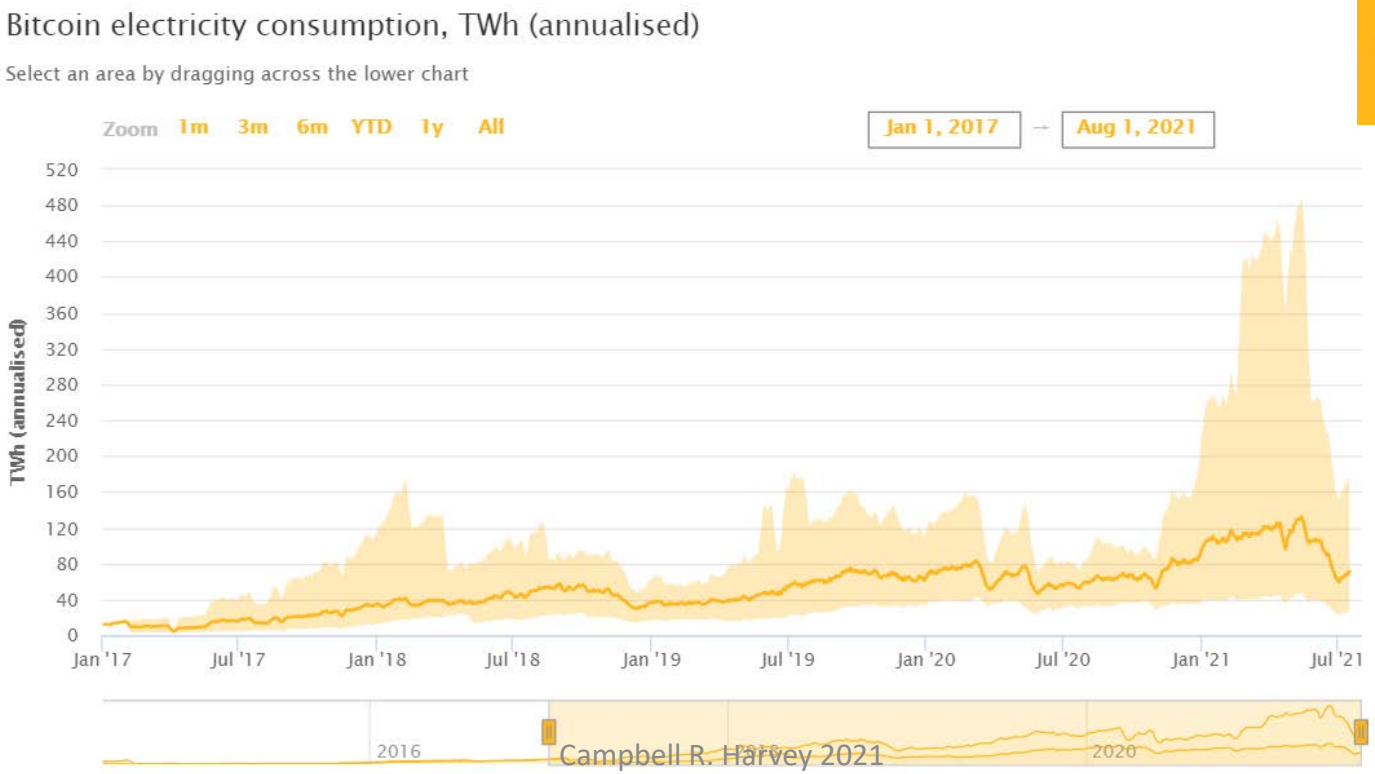
Example of Infrastructure - Splitting keys

- Companies like BitGo offer multi-signature solutions
- Three keys:
  - Owner has two keys and BitGo holds one.
  - 2 of 3 keys can be used for a transaction
  - A hack of BitGo's key is useless because a single key cannot spend
- If a user loses one key, there is a backup

Risks: Environmental risk

Proof of Work is very energy intensive

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



UNIVERSITY OF CAMBRIDGE Judge Business School | Cambridge Centre for Alternative Finance

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

Search **Bloomberg**

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 BTC

13BTC * 83 tons = 1,079 tons

Planting trees likely cheaper than carbon offset credits

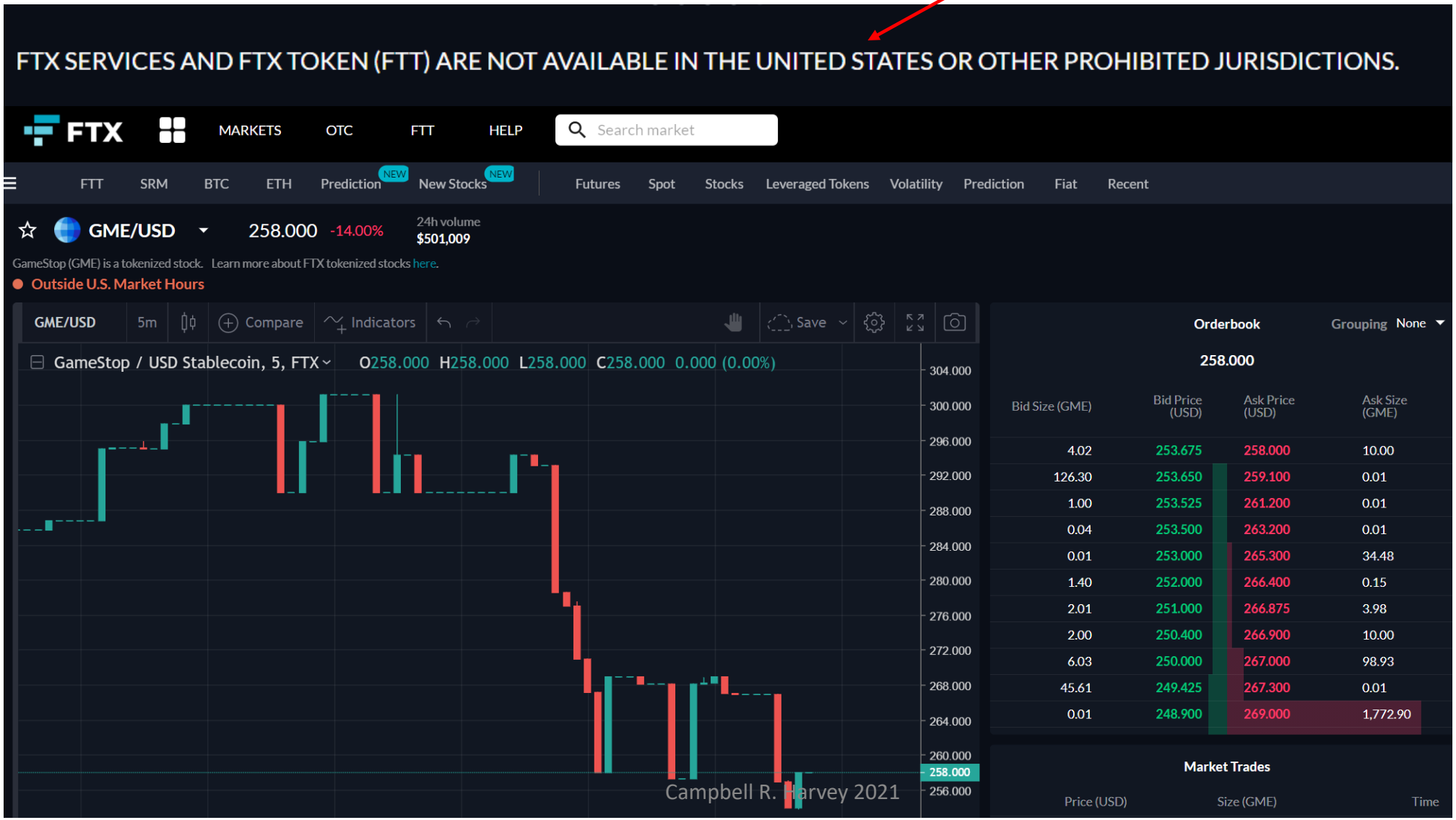
https://www.bloomberg.com/news/articles/2021-08-27/bitcoin-etf-pledges-to-reduce-carbon-footprint-by-planting-trees?sref=H1RVk7ry

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



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.

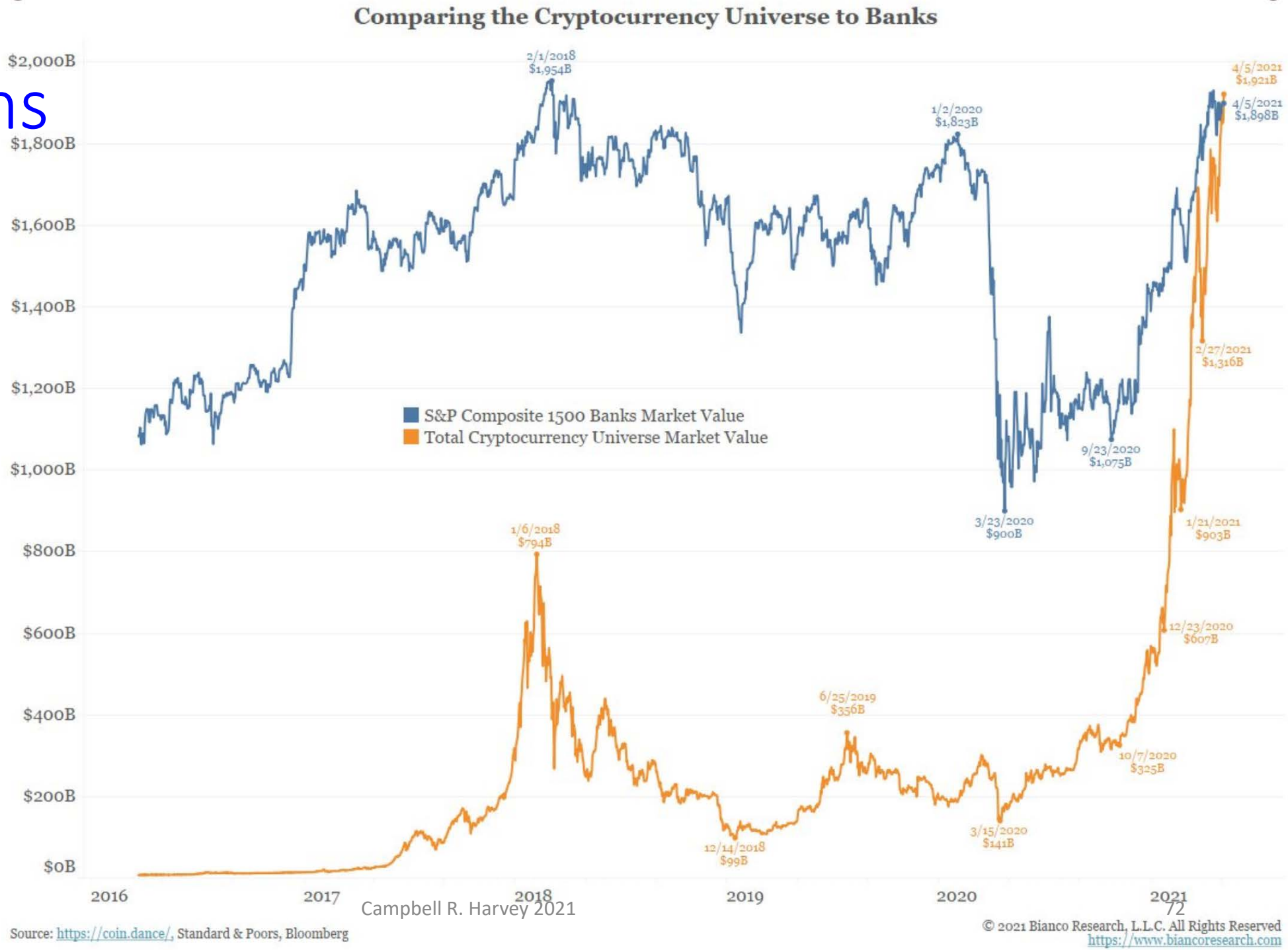
Conclusions

- 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



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.

https://timroughgarden.github.io/fob21/l/l1.pdf Based on Tim Roughgarden's opening lecture

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.

Questions

1. Tianyu Wu

DeFi risk in Flash-Loans

In your book DeFi and the Future of Finance, you mentioned that one of the emerging DeFi applications, flash-loans, could highly reduce the risk of default when borrowing or lending on a decentralized platform. However, a potential risk in the smart contract risk might allow users to take advantage of arbitrage opportunities. Will you think of the risk as an illegal frontrunning behavior, or an acceptable arbitrage behavior?

Questions

2. Xinyu Tian

Metaverse

With the development of Augmented Reality (AR) technology, the concept of Metaverse has absorbed people's attention nowadays. The CEO of Facebook, Mr. Mark Zuckerberg described the Metaverse as a world with a maximalist, interconnected set of experiences straight out of SciFi. And Metaverse will definitely be an interactive space for DeFi. What are the new opportunities and risks for DeFi in the Metaverse?

Questions

3. Haoxin Yu

DeFi Risk Measurement

The last chapter of your book DeFi and the future of finance illustrate DeFi risk such as smart contract risk and governance risk intuitively. It inspired me to conduct relative research on measuring these risks. I am wondering which of these risks you elaborate on can be quantified?

What are the most important risks?

Questions

4. William Zhao

Governance Policy on DeFi

The central bank of China recently declared that all cryptocurrency transactions are illegal, while the SEC in the U.S. is considering broadening the definition of "security" to include cryptocurrency in its regulation. These moves coincide with the regulatory risk you mentioned in your book. If you were a policy maker, how would you regulate cryptocurrencies?

Questions

5. Zesen Zhuang

Software developing for DeFi

DeFi is booming today, with a wide range of dApps deployed on blockchain supporting its ecology and development. Given the current blockchain infrastructure, what do you think will be the bottleneck that will limit the next step in the development of DeFi applications?

Legal

Questions

6. Ray Zhu

Cryptocurrency as legal tender

EL Salvador became the first country to accept Bitcoin as legal tender about two weeks ago. Also on the same day, BTC crashed to its lowest in a month. This reminds me of the volatility risk, regulatory risk, privacy debate, and all other negative sides of a cryptocurrency you mentioned in your coursera course. People from EL Salvador also complained about the high cost of converting BTC into the USD, which is high at 10%. What do you think about adopting cryptocurrency as a legal tender?

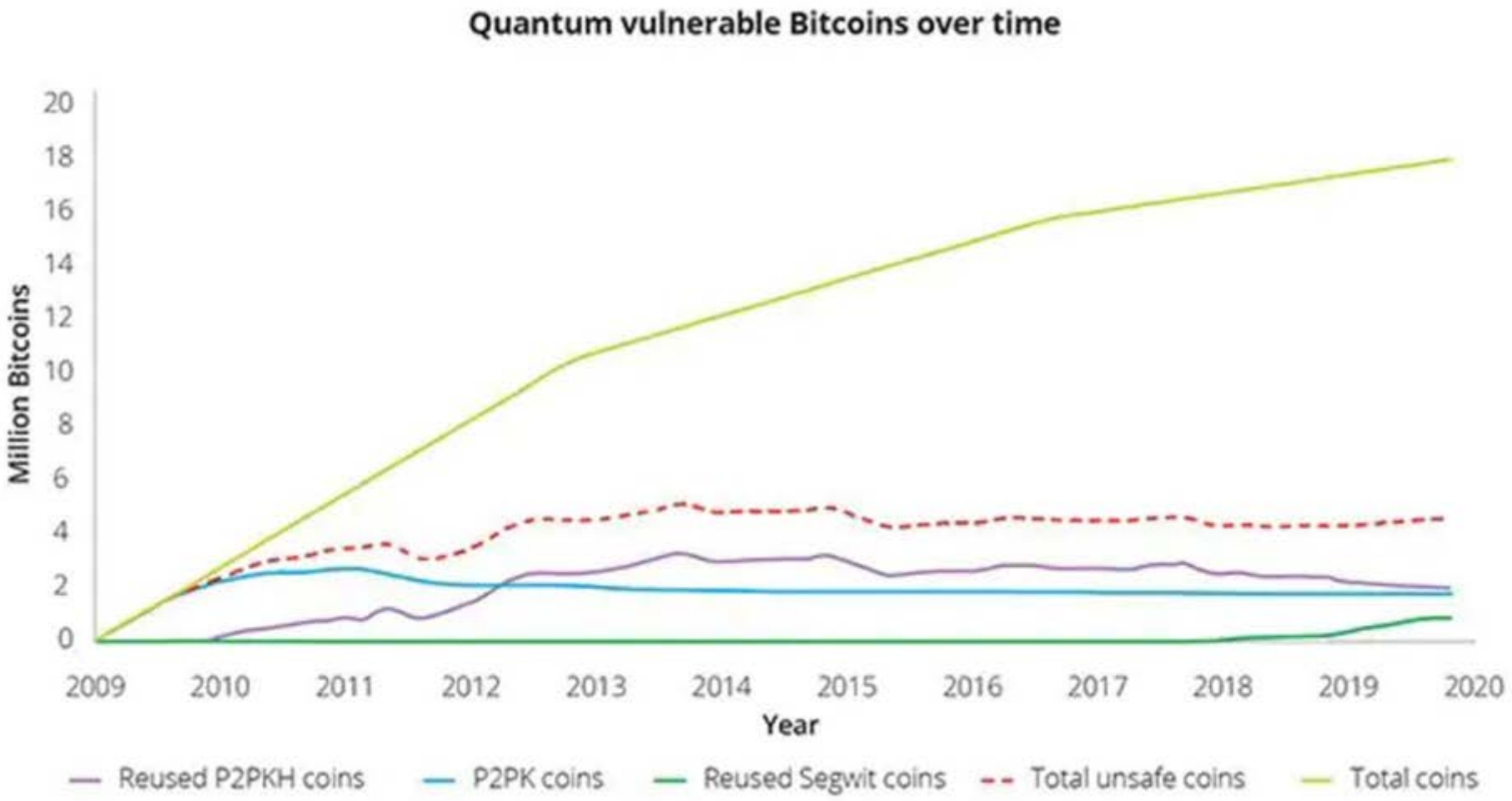
Layer 2

Questions

7. Yufan Zhang

Quantum Computing for DeFi

In the AMA interview published on SciEcon-AMA, you mentioned two courses you teach at Duke. One of them is Tech-driven Transformation and Business, where topics related to blockchain like quantum computing and brain-machine interface (BMI) are introduced. What's your take on the potential impact that quantum computing can play on the DeFi and some other fields based on blockchain?

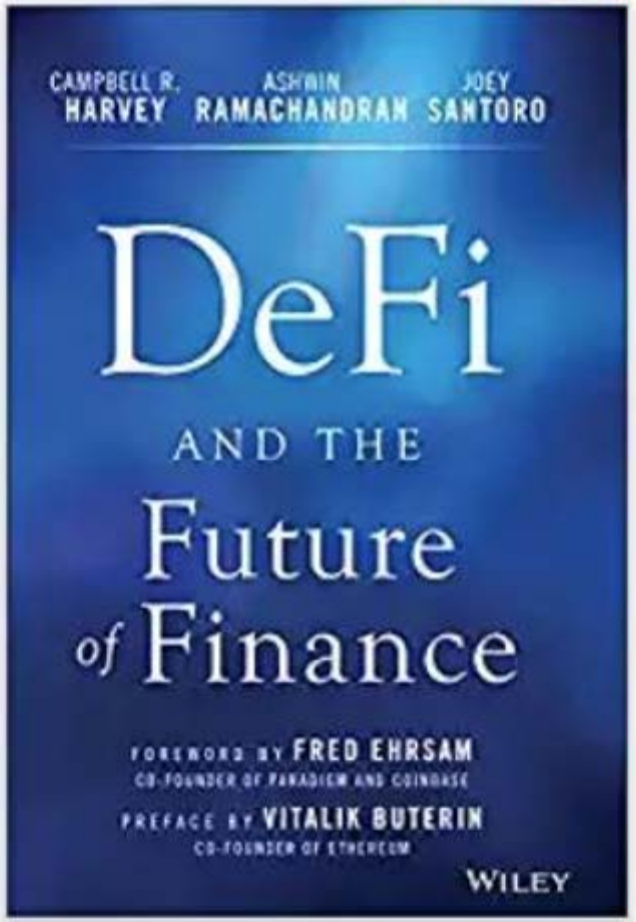


https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

Released Fall 2021

#1 Best Seller in Business Finance

Look inside ↓



ISBN-13: 978-1119836018
ISBN-10: 1119836018

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

PGP: E004 4F24 1FBC 6A4A CF31 D520 0F43 AE4D D2B8 4EF4

Supplementary (only if needed)

Cash is anonymous

- 80.2% of the value of US currency is in $100 bills
- Large denomination bills method of choice for criminal activity

El Chapo's cash stash

https://www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm