DeFi and the Future of Finance:
6. Risks

Campbell R. Harvey
Duke University and NBER

Outline

- Smart contract risk
- Governance risk
- DNS attack
- Oracle risk
- Scaling risk
- DEX risk
- Custodial risk
- Regulatory risk

Risks

A new set of risks

- While DeFi can eliminate counterparty risk, as with any innovative technology, the innovations introduce a new set of risks.
- In order to provide users and institutions with a robust and fault-tolerant system capable of handling new financial applications at scale, we must confront these risks.
- Without proper risk mitigation, DeFi will remain an exploratory technology, restricting its use, adoption, and appeal.

Risks: Smart contract risk

Hack

- Over the past decade, crypto-focused products, primarily exchanges, have repeatedly been hacked.
- Whereas many of these hacks happened because of poor security practices, they demonstrate an important point: software is uniquely vulnerable to hacks and developer malpractice.
- Blockchains can remove traditional financial risks, such as counterparty risk, with their unique properties, but DeFi is built on code.

Risks: Smart contract risk

Attack vector

- This software foundation gives attackers a larger attack surface than the threat vectors of traditional financial institutions.
- Public blockchains are open systems.
- Anyone can view and interact with code on a blockchain after the code is deployed.
- 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*.

Risks: Smart contract risk

Audit

- DeFi's foundation is public code known as a smart contract.
- The implementation is new to mainstream engineering practice. Practices that will help reduce the risk of smart contract bugs and programming errors are still under development.
- The recent hacks of The DAO, DForce and bZx demonstrate the fragility of smart contract programming.
- Auditing firms, such as Quantstamp, Trail of Bits, and Peckshield, are emerging to fill this gap in best practices and smart contract expertise.

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.
- The former can take the form of any typical software bug in the code.

Risks: Smart contract risk

Example: Logic error

- Suppose we have a smart contract which is intended to be able to escrow deposits from a particular ERC-20 from any user and transfer the entire balance to the winner of a lottery.
- The contract keeps track of how many tokens it has internally, and uses that internal number as the amount when performing the transfer.
- The bug will belong here in our hypothetical contract.

Risks: Smart contract risk

Example: Logic error

- The internal number will, due to a rounding error, be slightly higher than the actual balance of tokens the contract holds.
- When it tries to transfer, it will transfer “too much” and the execution will fail.
- If there was no failsafe put into place, the 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.
- There would be no explicit failure in the logic of the code, but rather an opportunity for an economically equipped adversary to influence market conditions in such a way as to profit inappropriately at the contract's expense.
- 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.

Risks: Smart contract risk

Example: Economic exploit

- The other exchange is playing the role of a price oracle
- The possibility for an economic exploit arises when the oracle exchange has significantly lower liquidity when compared to the primary exchange
- A financially equipped adversary can purchase heavily on the oracle exchange to manipulate the price, then proceed to purchase far more on the primary exchange in the opposite direction to capitalize on the price movement. The net effect is that the attacker was able to manufacture a discounted price on a high liquidity exchange by manipulating a low liquidity oracle.

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.
- Special care must be used when designing protocols such that they cannot be manipulated by massive market volatility within a single transaction.
- An economic exploit which utilizes a flash loan can be referred to as a *flash attack*.

Risks: Smart contract risk

Example: Economic exploit – flash attack

- A series of high profile flash attacks were executed in Feb 2020 on bZx Fulcrum, a lending market similar to Compound.
- The attacker utilized a flash loan and diverted some of the funds to purchase a levered short position, with the remainder used to manipulate the price of the oracle exchange which the short position was based on.
- The attacker then closed the short at a profit, unwound the market trade and paid back the flash loan. The net profit was almost $300,000 worth of funds previously held by bZx, for near zero upfront cost.

Risks: Smart contract risk

The DAO and DForce

- The classic failure of a smart contract was The DAO
- A similar failure occurred recently with DForce.

Risks: Smart contract risk

SLOCK.IT

The DAO

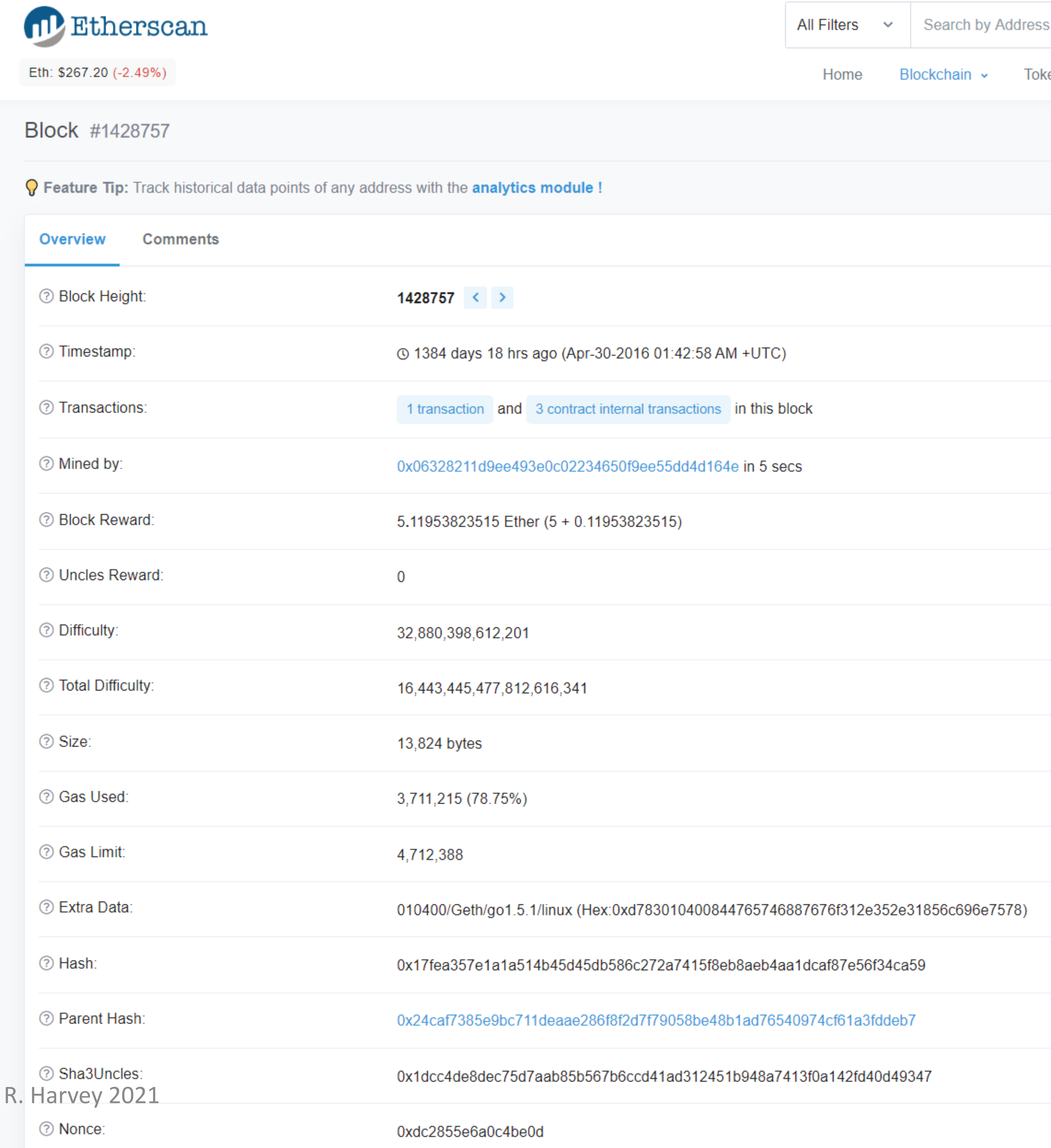
- Purpose: Venture Capital Fund for blockchain based investments that would be directed by investors (owners of the DAO token)
- Smart contract on Ethereum blockchain designed by Slock.it
- Vision: no management structure, no Board of Directors, no employees
- Code was open-source
- The DAO was stateless – (not tied to any country) – so not obvious how it would (or could) be regulated

Risks: Smart contract risk

The DAO

- Launched –April 4-April 30, 2016 on Ethereum block 1428757 with a crowdsale to fund the organization.
- Ether value about $150 million by May 21 (about 14% of all ether at the time).
- DAO tokens were traded on various exchanges by May 28
- Early example of tokenizing ether

Risks: Smart contract risk

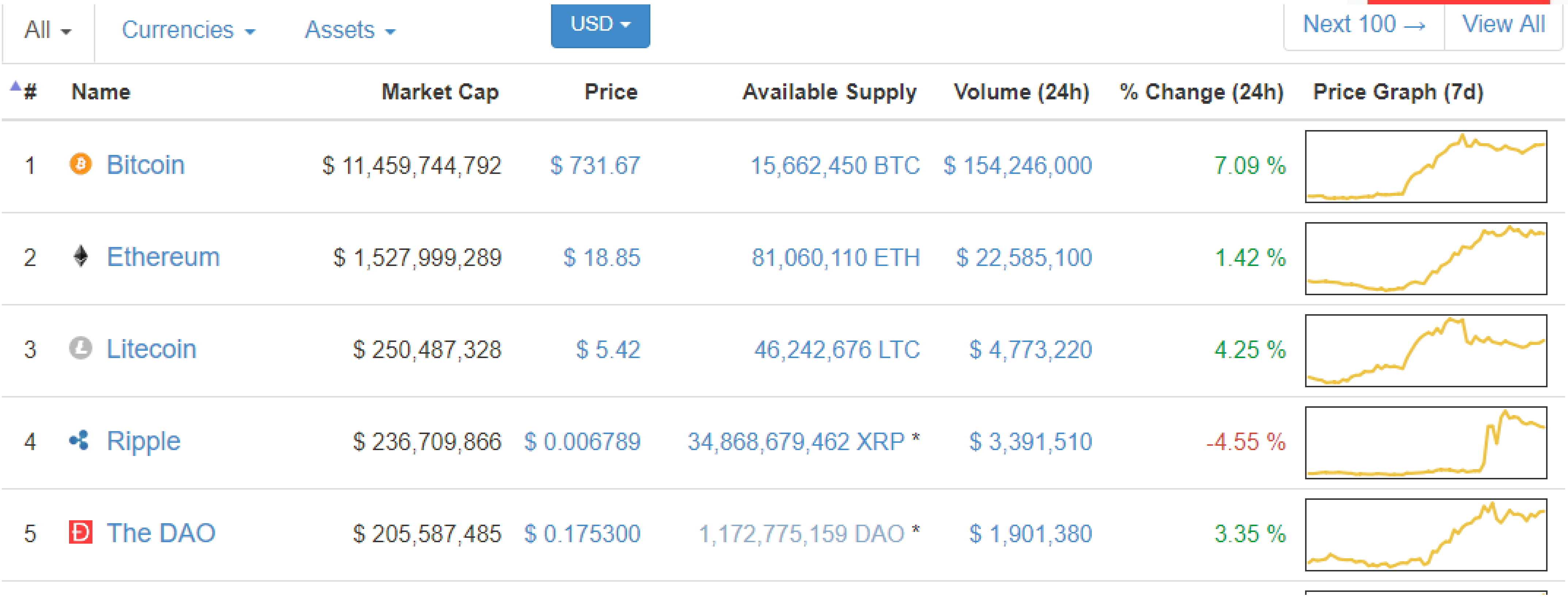


Block #1428757

Feature Tip: Track historical data points of any address with the analytics module !

Block Height:	1428757
Timestamp:	1384 days 18 hrs ago (Apr-30-2016 01:42:58 AM +UTC)
Transactions:	1 transaction and 3 contract internal transactions in this block
Mined by:	0x06328211d9ee493e0c02234650f9ee55dd4d164e in 5 secs
Block Reward:	5.11953823515 Ether (5 + 0.11953823515)
Uncles Reward:	0
Difficulty:	32,880,398,612,201
Total Difficulty:	16,443,445,477,812,616,341
Size:	13,824 bytes
Gas Used:	3,711,215 (78.75%)
Gas Limit:	4,712,388
Extra Data:	010400/Geth/go1.5.1/linux (Hex:0xd783010400844765746887676f312e352e31856c696e7578)
Hash:	0x17fea357e1a1a514b45d45db586c272a7415f8eb8aeb4aa1dcaf87e56f34ca59
Parent Hash:	0x24caf7385e9bc711deaae286f8f2d7f79058be48b1ad76540974cf61a3fddeb7
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Nonce:	0xdc2855e6a0c4be0d

Risks: Smart contract risk



#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 11,459,744,792	$ 731.67	15,662,450 BTC	$ 154,246,000	7.09 %	
2	Ethereum	$ 1,527,999,289	$ 18.85	81,060,110 ETH	$ 22,585,100	1.42 %	
3	Litecoin	$ 250,487,328	$ 5.42	46,242,676 LTC	$ 4,773,220	4.25 %	
4	Ripple	$ 236,709,866	$ 0.006789	34,868,679,462 XRP *	$ 3,391,510	-4.55 %	
5	The DAO	$ 205,587,485	$ 0.175300	1,172,775,159 DAO *	$ 1,901,380	3.35 %	

June 16, 2016

Risks: Smart contract risk

Reentrancy Bug

- June 9, 2016, two developers reported that most ethereum based contracts that managed funds were vulnerable to a bug that could empty funds.
- June 12, 2016 Stephan Tual, founder of Slock.it reported that The DAO code was not vulnerable to this exploit.

Risks: Smart contract risk

Reentrancy Bug

- Crucial part of code had two lines in the wrong order (allowing withdrawal of ether repeatedly before checking if the attacker was entitled to withdraw)
- Suppose you have $100 in a bank account. Think of bringing the bank teller a stack of $100 withdrawal slips and the teller gives you $100 for each one until the bank runs out of money. At that point, they register the $100 debit and have no idea you took everything.

https://github.com/ethereumbook/ethereumbook/blob/develop/appdx-forks-history.asciidoc

Risks: Smart contract risk

The DAO

- June 17, 2016 The DAO attacked and user gained access to about $50 million of ETH (30% of ether in the contract)
- Simultaneously, another group, Robin Hood Group (RHG), used the same exploit (but promised to return all ether to the original owners) (they got the remaining 70%)

https://github.com/ethereumbook/ethereumbook/blob/develop/appdx-forks-history.asciidoc

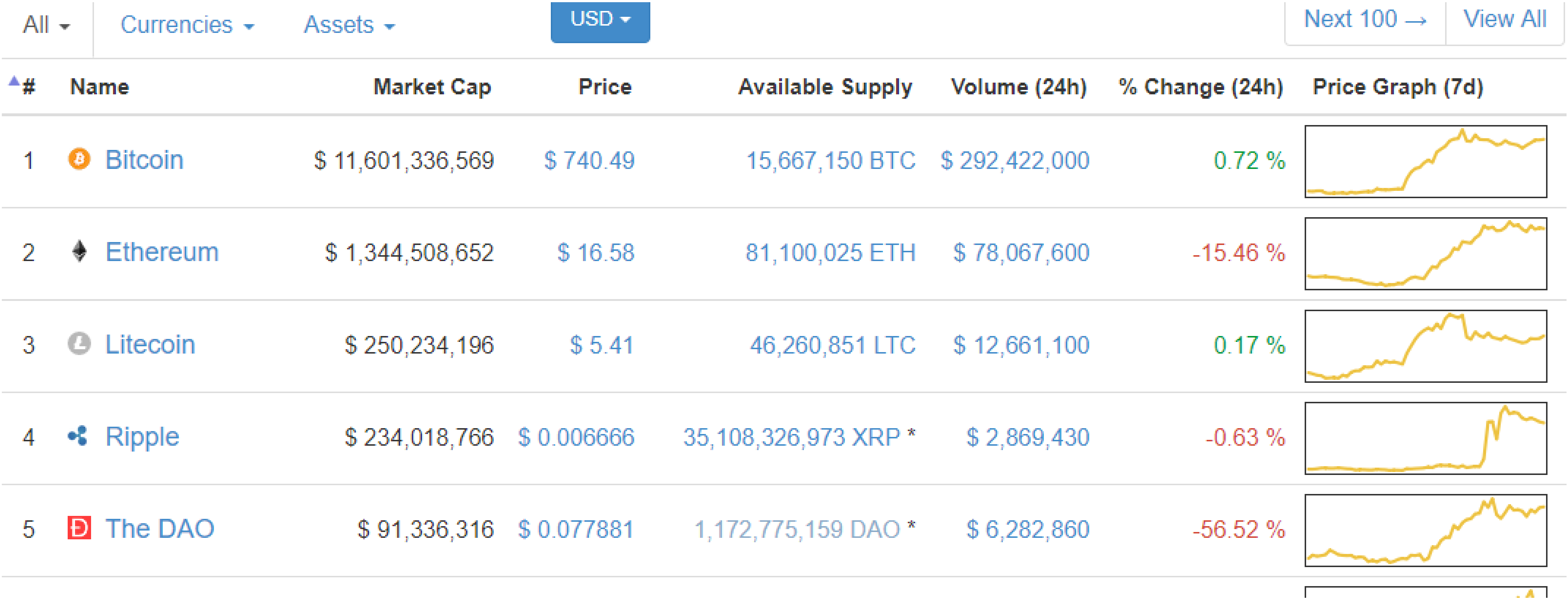
Risks: Smart contract risk

The DAO

- Funds put in a 28-day holding period (as per the contract) before they could be withdrawn
- Community debated what to do with a July 20 deadline (end of 28-day period): should they rewrite history by hard forking?

https://github.com/ethereumbook/ethereumbook/blob/develop/appdx-forks-history.asciidoc

Risks: Smart contract risk



#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 11,601,336,569	$ 740.49	15,667,150 BTC	$ 292,422,000	0.72 %	
2	Ethereum	$ 1,344,508,652	$ 16.58	81,100,025 ETH	$ 78,067,600	-15.46 %	
3	Litecoin	$ 250,234,196	$ 5.41	46,260,851 LTC	$ 12,661,100	0.17 %	
4	Ripple	$ 234,018,766	$ 0.006666	35,108,326,973 XRP *	$ 2,869,430	-0.63 %	
5	The DAO	$ 91,336,316	$ 0.077881	1,172,775,159 DAO *	$ 6,282,860	-56.52 %	

June 17, 2016

Risks: Smart contract risk

The DAO

- July 20, 2016 hard fork at block 1,920,000 and rewrote history returning the DAO directed ether to the investors
- The old protocol became Ethereum Classic (ETC) preserved history (and immutability property). RHG now needs to return 70% of the ETC to the original investors

Ethereum (ETH)

Ethereum Classic (ETC)

Risks: Smart contract risk

The DAO is a security

- July 26, 2016 The SEC rules that DAO tokens were “securities” subject to federal securities laws.
- *…issuers of distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. Those participating in unregistered offerings also may be liable for violations of the securities laws. Additionally, securities exchanges providing for trading in these securities must register unless they are exempt. The purpose of the registration provisions of the federal securities laws is to ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for investors' protection.*

https://www.sec.gov/news/press-release/2017-131

Risks: Smart contract risk

Hard forks vs. soft forks

- Soft forks are relatively minor software changes
- Soft forks are software upgrades that are backward compatible with previous versions
- Nodes do not need to upgrade to new version to form consensus

Risks: Smart contract risk

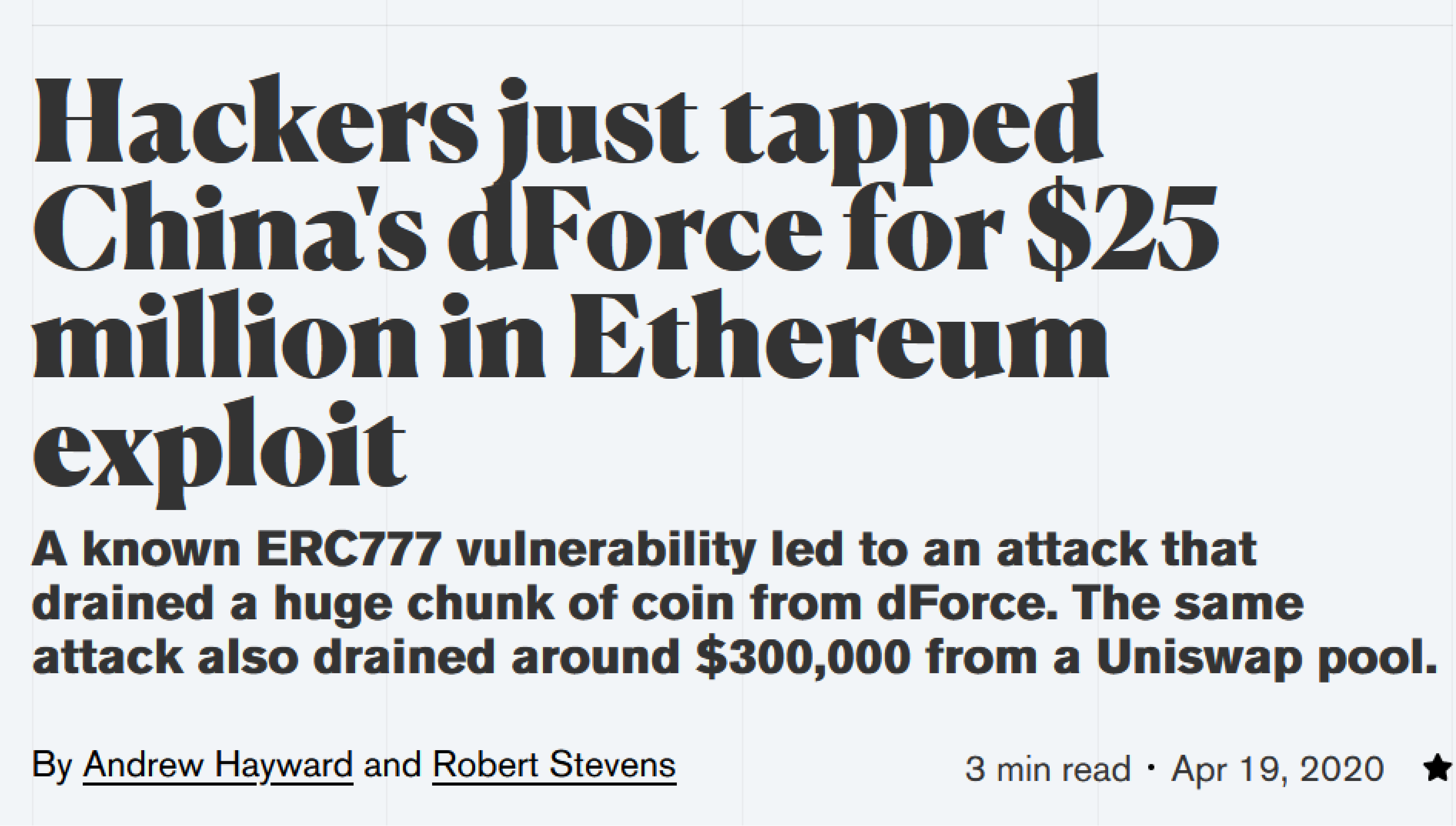
Hard forks vs. soft forks

- Hard forks are major software changes
- Hard forks are not backward compatible with previous versions
- Nodes need to follow new rules for consensus
- Hard forks can be planned (Constantinople) or contentious (ETC)

https://www.mycryptopedia.com/hard-fork-soft-fork-explained/

Risks: Smart contract risk

Risk events



Hackers just tapped China's dForce for $25 million in Ethereum exploit

A known ERC777 vulnerability led to an attack that drained a huge chunk of coin from dForce. The same attack also drained around $300,000 from a Uniswap pool.

By Andrew Hayward and Robert Stevens

3 min read · Apr 19, 2020

Risks: Smart contract risk

Risk events: DForce

- "DForce, a Chinese decentralized finance protocol, today lost $25 million worth of its customers' cryptocurrency due to a well-known exploit of an Ethereum token.
- The money was drained this morning from the contracts of Lendf.Me, a lending protocol that's part of dForce, a collection of DeFi protocols.
- The site for Lendf.Me is now offline and its smart contracts have been paused. The funds were sent to DeFi lending protocols Compound and Aave. Stani Kulechov, founder and CEO of Aave, told *Decrypt* that around $10 million of the funds were sent to his protocol."

Risks: Smart contract risk

Risk events: DForce

- The hack is linked to a well-known Ethereum exploit that was yesterday used to drain more than $300,000 from decentralized exchange Uniswap.
- Uniswap smart contracts containing imBTC—an Ethereum-based, tokenized version of Bitcoin that's run by TokenIon—were drained. Lendf.Me integrated imBTC in January.

Risks: Smart contract risk

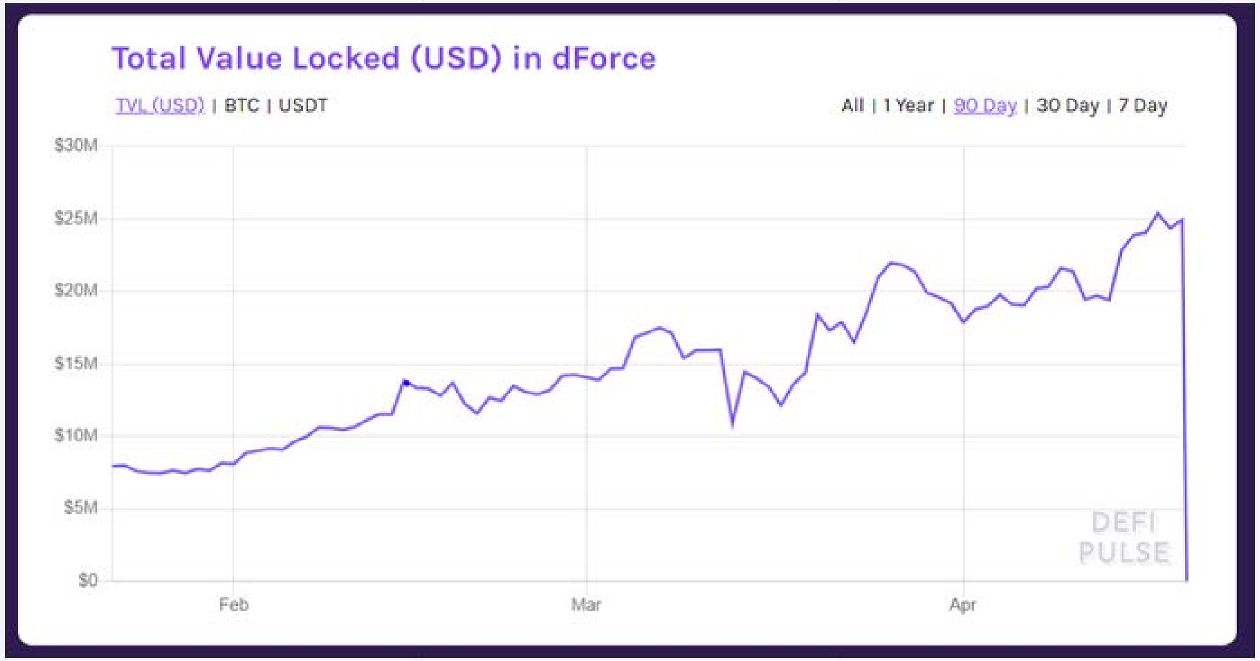
Risk events: DForce

- The Uniswap attack took advantage of a known vulnerability that concerns the ERC777 token standard.
- Due to the way Uniswap smart contracts are set up, a hacker could continually withdraw ERC777 funds from Uniswap before the balance updated, gradually draining the contracts of imBTC.
- The dForce hack, though entirely separate from the Uniswap hack, is suspected to use the same exploit.

Risks: Smart contract risk

Risk events: DForce

- In a bizarre twist, the hackers returned $126,014 back to Lendf.Me with a note saying, "Better luck next time," according to *Chain News*.



The smart contract for dForce was drained. (Source: DeFiPulse)

Risks: Smart contract risk

Risk events: DForce

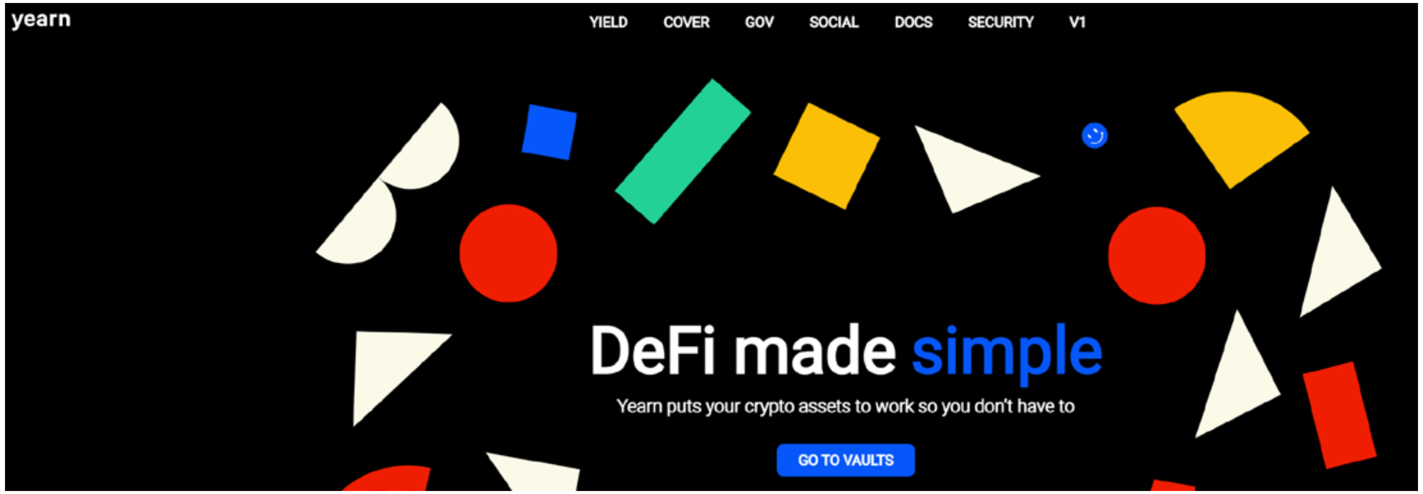
- "Robert Leshner, the CEO of Compound, claims that Lendf.Me had appropriated its code, which was open-source.
- A report from *The Block* in January found that the term "Compound" appeared four times in dForce's contract.
- "If a project doesn't have the expertise to develop its own smart contracts, and instead steals and redeploys somebody else's copyrighted code, it's a sign that they don't have the capacity or intention to consider security," tweeted Leshner."

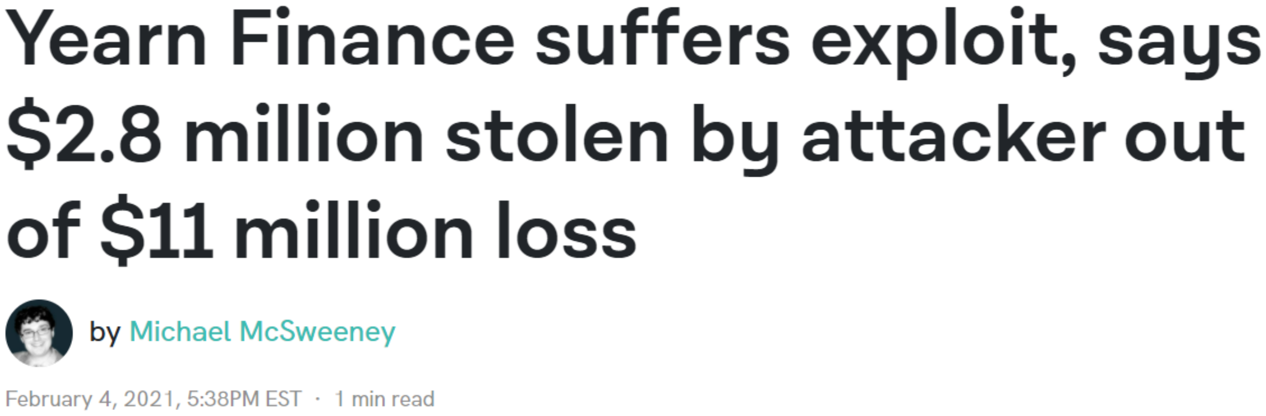
https://decrypt.co/26033/dforce-lendfme-defi-hack-25m

Risks: Smart contract risk

Yearn.finance

- "Yearn.Finance is a so-called 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.





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

by Michael McSweeney

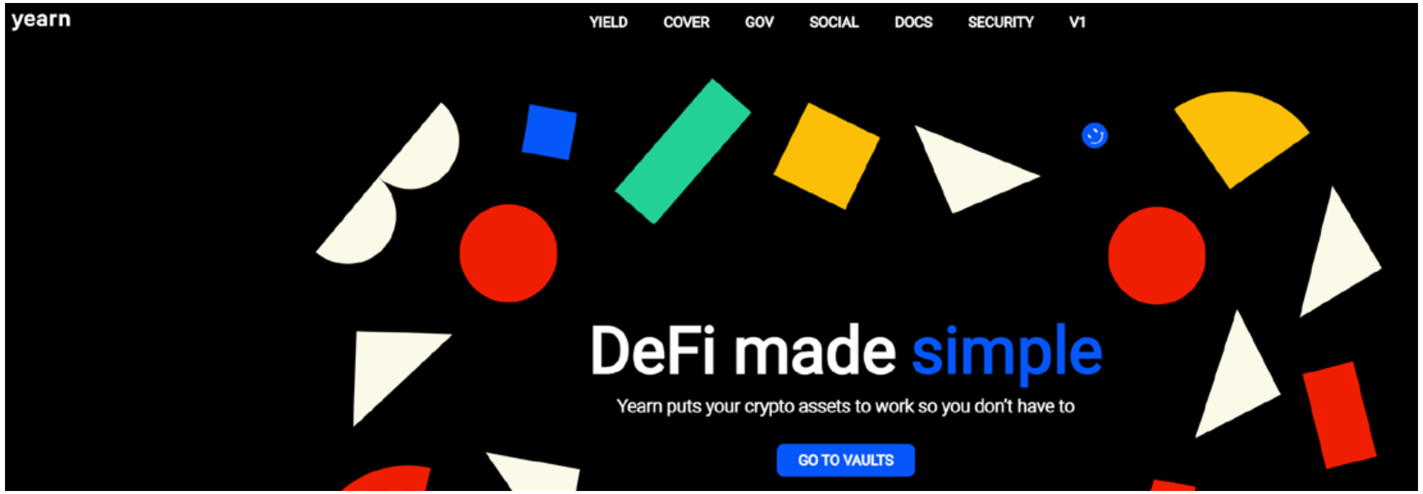
February 4, 2021, 5:38PM EST · 1 min read

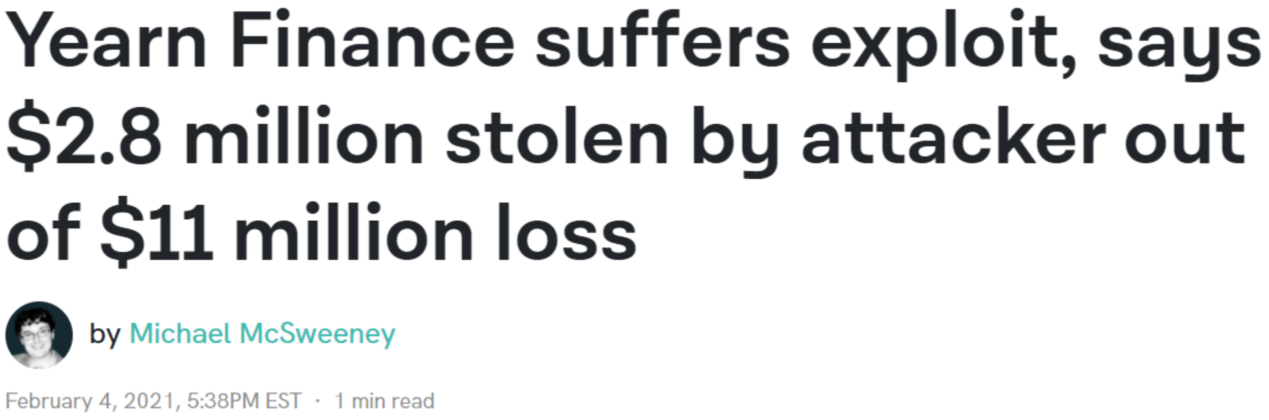
https://www.theblockcrypto.com/linked/93818/yearn-finance-dai-pool-defi-exploit-attack

Risks: Smart contract risk

Yearn.finance

- “Stani Kulechov, the founder of DeFi platform Aave, later tweeted out the transaction at the heart of the exploit, involving numerous DeFi protocols and more than $5,000 worth of ETH-denominated gas fees.”
- Complex exploit with over 160 nested transactions





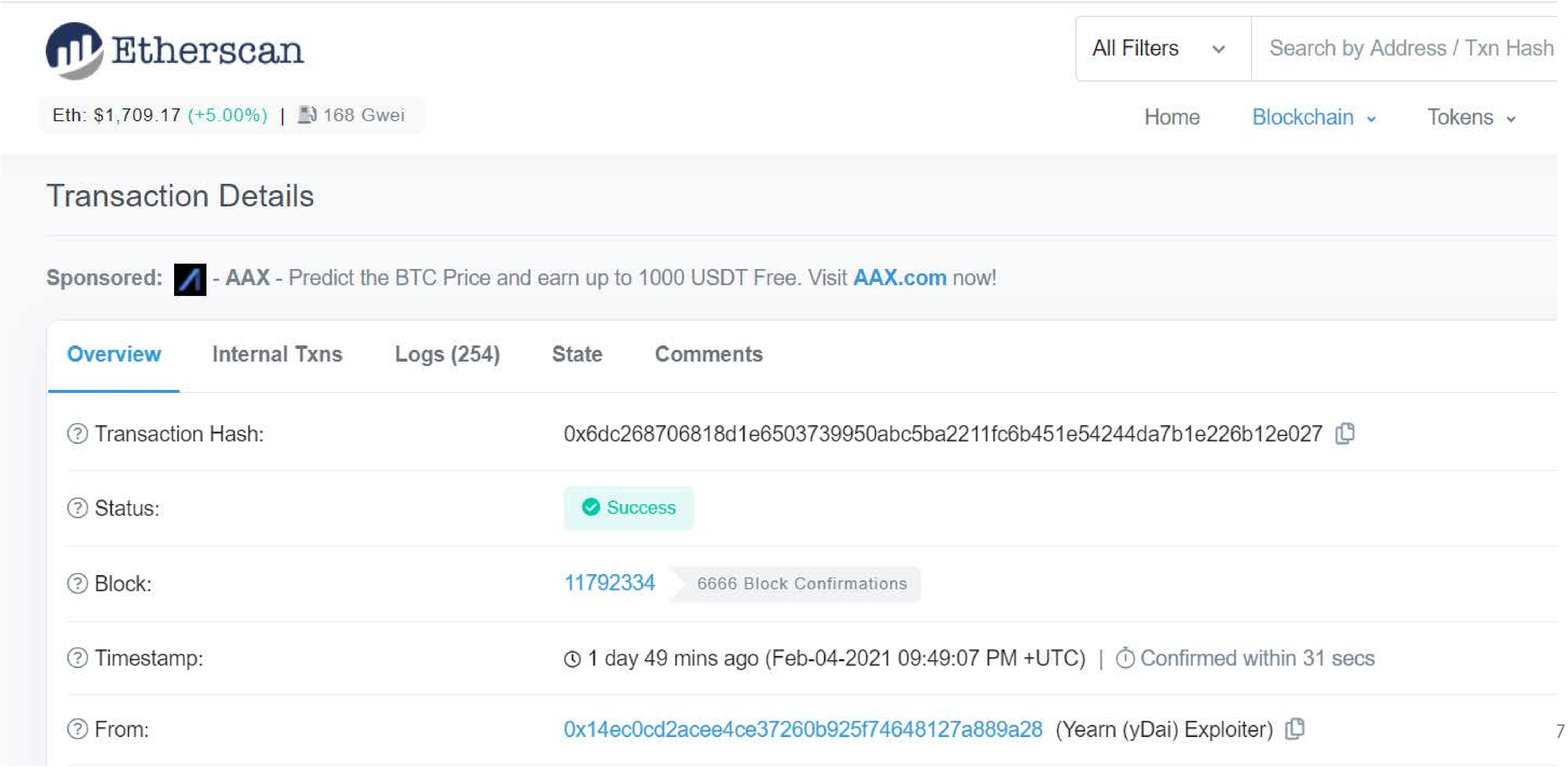
Yearn Finance suffers exploit, says $2.8 million stolen by attacker out of $11 million loss

by Michael McSweeney

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

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

Risks: Smart contract risk



Eth: $1,709.17 (+5.00%) | 168 Gwei

Transaction Details

Transaction Hash: 0x6dc268706818d1e6503739950abc5ba2211fc6b451e54244da7b1e226b12e027

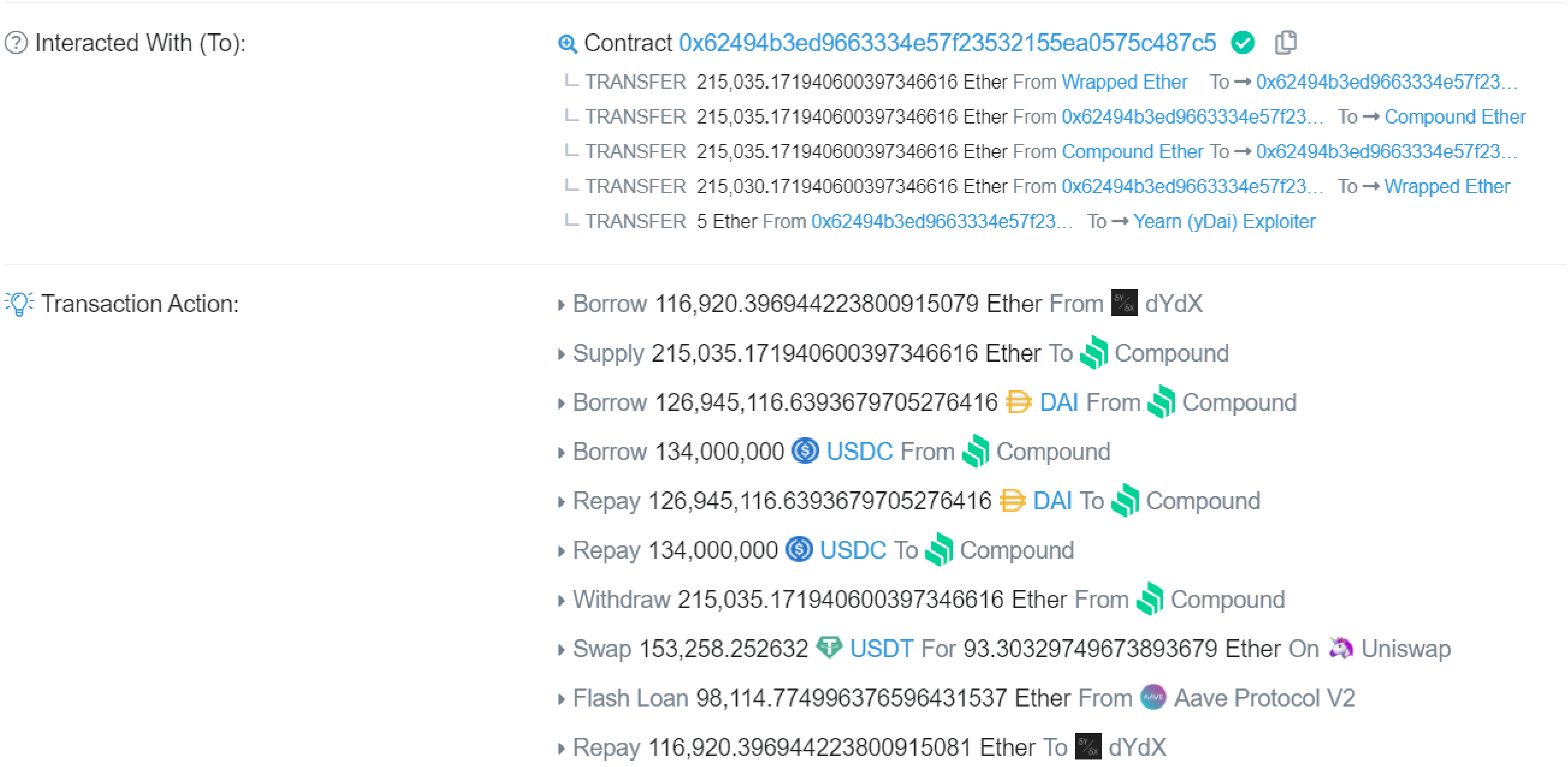
Status: Success

Block: 11792334 6666 Block Confirmations

Timestamp: 1 day 49 mins ago (Feb-04-2021 09:49:07 PM +UTC) | Confirmed within 31 secs

From: 0x14ec0cd2acee4ce37260b925f74648127a889a28 (Yearn (yDai) Exploiter)

Risks: Smart contract risk



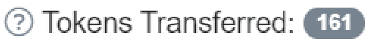
Interacted With (To): Contract 0x62494b3ed9663334e57f23532155ea0575c487c5

- 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:

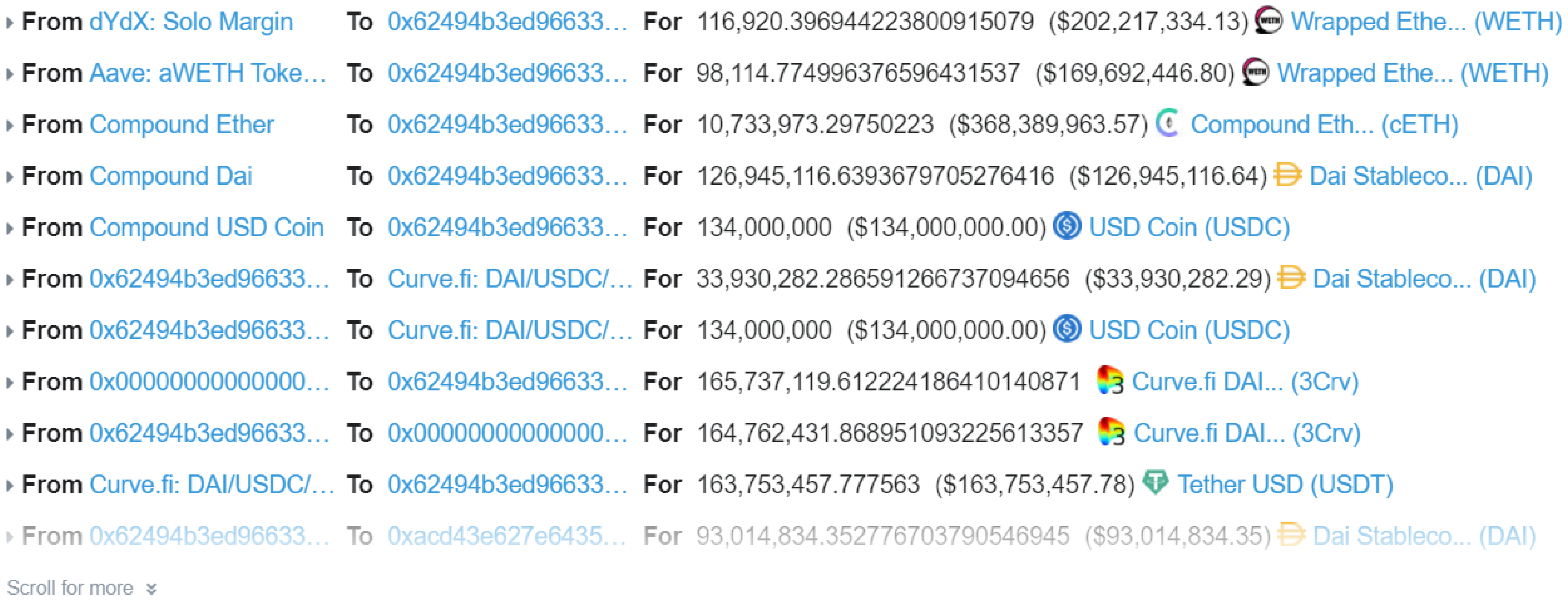
- Borrow 116,920.396944223800915079 Ether From dYdX
- Supply 215,035.171940600397346616 Ether To Compound
- Borrow 126,945,116.6393679705276416 DAI From Compound
- Borrow 134,000,000 USDC From Compound
- Repay 126,945,116.6393679705276416 DAI To Compound
- Repay 134,000,000 USDC To Compound
- Withdraw 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



Tokens Transferred: 161

161 token transfers. Just displaying the first 10.



From	dYdX: Solo Margin	To	0x62494b3ed96633…	For	116,920.396944223800915079 ($202,217,334.13)	Wrapped Ethe... (WETH)
From	Aave: aWETH Toke…	To	0x62494b3ed96633…	For	98,114.774996376596431537 ($169,692,446.80)	Wrapped Ethe... (WETH)
From	Compound Ether	To	0x62494b3ed96633…	For	10,733,973.29750223 ($368,389,963.57)	Compound Eth... (cETH)
From	Compound Dai	To	0x62494b3ed96633…	For	126,945,116.639367970527641 6 ($126,945,116.64)	Dai Stableco... (DAI)
From	Compound USD Coin	To	0x62494b3ed96633…	For	134,000,000 ($134,000,000.00)	USD Coin (USDC)
From	0x62494b3ed96633…	To	Curve.fi: DAI/USDC/…	For	33,930,282.286591266737094656 ($33,930,282.29)	Dai Stableco... (DAI)
From	0x62494b3ed96633…	To	Curve.fi: DAI/USDC/…	For	134,000,000 ($134,000,000.00)	USD Coin (USDC)
From	0x00000000000000…	To	0x62494b3ed96633…	For	165,737,119.612224186410140871	Curve.fi DAI... (3Crv)
From	0x62494b3ed96633…	To	0x00000000000000…	For	164,762,431.868951093225613357	Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USDC/…	To	0x62494b3ed96633…	For	163,753,457.777563 ($163,753,457.78)	Tether USD (USDT)
From	0x62494b3ed96633…	To	0xacd43e627e6435…	For	93,014,834.352776703790546945 ($93,014,834.35)	Dai Stableco... (DAI)

Scroll for more

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

Risks: Smart contract risk

Summary

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

Other attacks

- Origin (reentrancy) November 2020: https://www.theblockcrypto.com/post/84804/defi-protocol-origin-attack-7-million-lost

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 described earlier, 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

Protocol governance

- Protocol governance refers to the representative or liquid democratic mechanisms that enable changes in the protocol.
- To participate in the governance process, users and investors must acquire a token that has been explicitly assigned protocol governance rights on a liquid marketplace.
- Once acquired, holders use these tokens to vote on protocol changes and guide future direction.

Risks: Governance risk

51% (or less)

- Governance tokens usually have a fixed supply that assists in resisting attempts by anyone to acquire a majority (51%), nevertheless they expose the protocol to the risk of control by a malicious actor.
- The founders often control traditional fintech companies, which reduces the risk of an external party influencing or changing the company's direction or product.

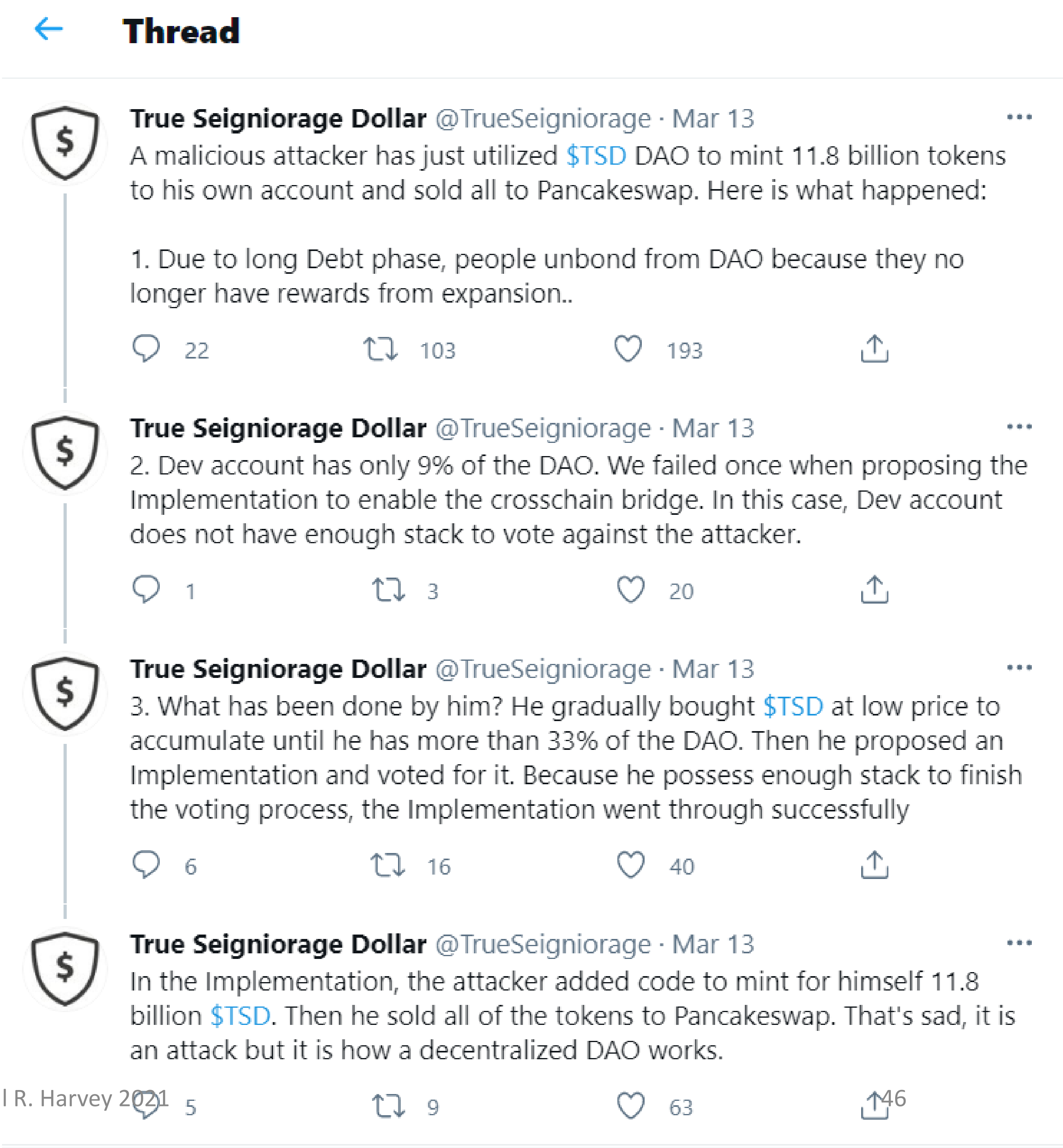
Risks: Governance risk

51% (or less)

- DeFi protocols, however, are vulnerable to attack as soon as the decentralized governance system launches.
- Any financially equipped adversary can simply acquire a majority of liquid governance tokens to gain control of the protocol and steal funds.
- We have not yet experienced a successful governance attack on any Ethereum-based DeFi project, but little doubt exists that a financially equipped adversary will eventually attack a protocol if the potential profit exceeds the cost of attack.

Risks: Governance risk

March 13, 2021 $TSD governance attack



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..

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.

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

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.

Risks: DNS attack

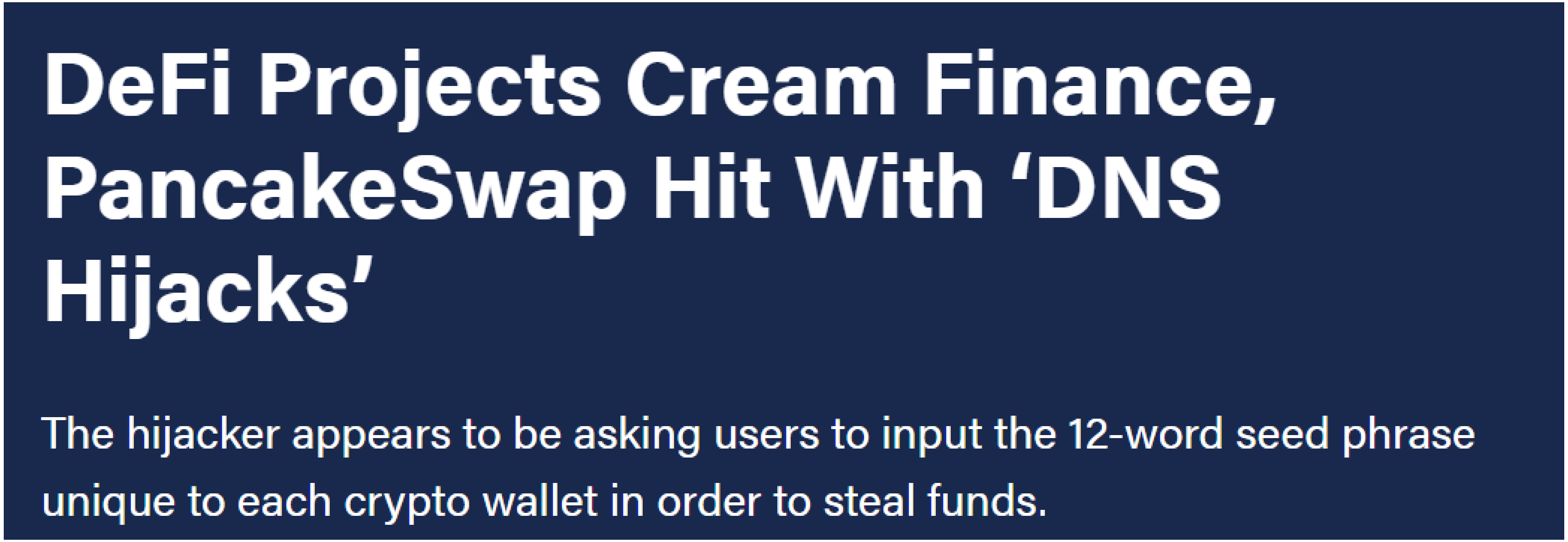
DNS

- Hacker takes over domain name service and tricks user into giving private key

Risks: DNS attack

coindesk

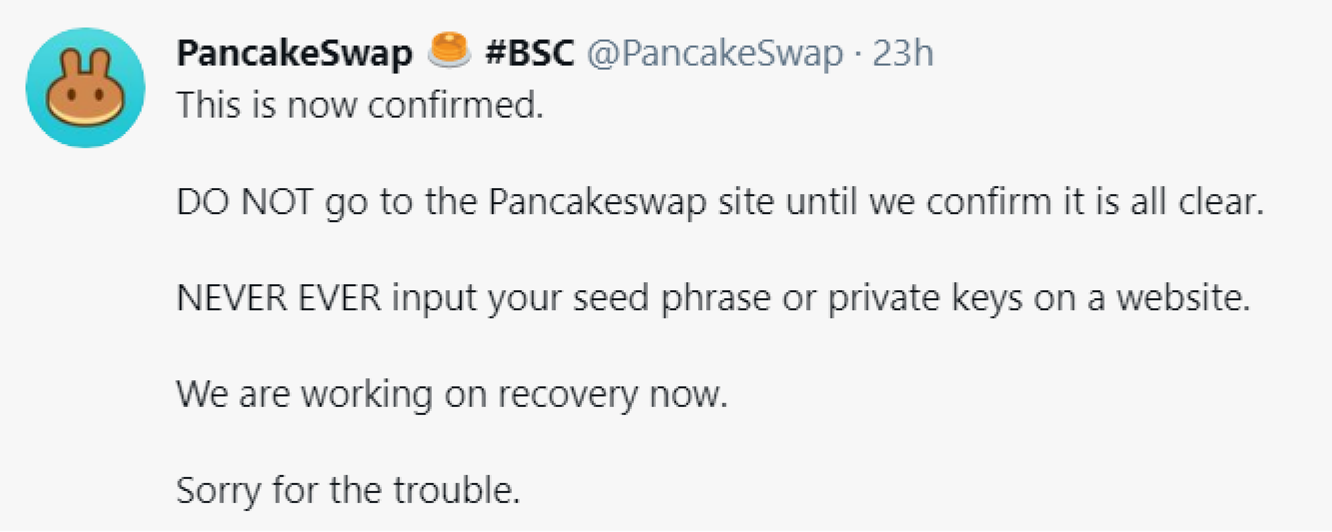
March 15, 2021



DeFi Projects Cream Finance, PancakeSwap Hit With 'DNS Hijacks'

The hijacker appears to be asking users to input the 12-word seed phrase unique to each crypto wallet in order to steal funds.

Risks: DNS attack



PancakeSwap 🥞 **#BSC** @PancakeSwap · 23h

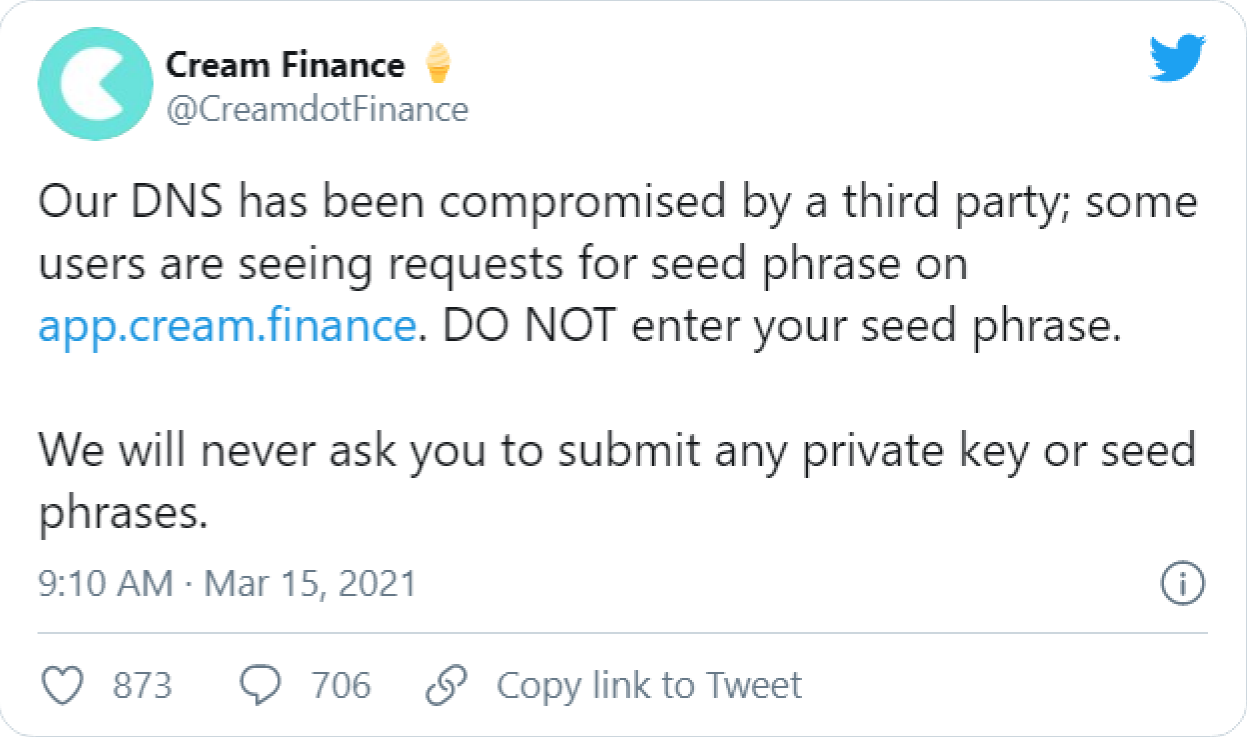
This is now confirmed.

DO NOT go to the Pancakeswap site until we confirm it is all clear.

NEVER EVER input your seed phrase or private keys on a website.

We are working on recovery now.

Sorry for the trouble.



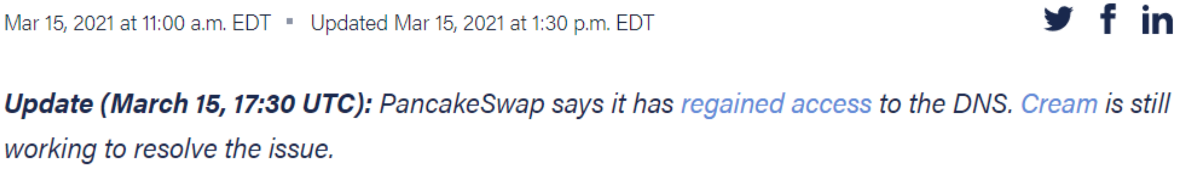
Cream Finance 🍦
@CreamdotFinance

Our DNS has been compromised by a third party; some users are seeing requests for seed phrase on app.cream.finance. DO NOT enter your seed phrase.

We will never ask you to submit any private key or seed phrases.

9:10 AM · Mar 15, 2021

♡ 873 706 Copy link to Tweet



Mar 15, 2021 at 11:00 a.m. EDT • Updated Mar 15, 2021 at 1:30 p.m. EDT

***Update (March 15, 17:30 UTC):** PancakeSwap says it has regained access to the DNS. Cream is still working to resolve the issue.*

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

What is oracle risk?

- Many DeFi protocols require access to secure, tamper-resistant asset prices to ensure that routine actions, such as liquidations and prediction market resolutions, function correctly.
- Protocol reliance on these data feeds introduces *oracle risk*.
- If an oracle's *Cost of Corruption* is ever less than an attacker's potential *Profit from Corruption*, the oracle is extremely vulnerable to attack.

Risks: Oracle risk

Types: Shelling-point oracle

- This oracle relies on the owners of a fixed-supply token to vote on the outcome of an event or report the price of an asset.
- Examples of this type of oracle include Augur and UMA.
- While Schelling-point oracles preserve the decentralization components of protocols that rely on them, they suffer from slow times to resolution.

Risks: Oracle risk

Types: API oracle

- These oracles are centralized entities that respond asynchronously to requests for data or prices.
- Examples include Provable, Oraclize, and Chainlink. All systems relying on API-based oracles, must trust the data provider to respond accurately to all queries.

Risks: Oracle risk

Types: Application-specific oracle service

- This type of oracle is used by Maker and Compound.
- Its design differs based on the requirements of the protocol it was developed for.
- For example, Compound relies on a single data provider that the Compound team controls to provide all on-chain price data to the Compound oracle.

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?

- As we have discussed, Ethereum and other “Proof of Work” (the consensus mechanism) blockchains have a fixed block size.
- For a block to become part of the chain, every Ethereum miner must execute all of the included transactions on their machine.
- To expect each miner to process all of the financial transactions for a global financial market is unrealistic.

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

What is scaling risk?

- Much effort is focused on increasing Ethereum’s scalability or replacing Ethereum with an alternative blockchain that can more readily handle higher transaction volumes.
- To date, all efforts have proven unsuccessful.

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

Proof of Stake risks

- An example of malicious behavior includes voting for multiple candidate blocks.
- This action shows a lack of discernment and skews voting numbers, and thus is penalized.
- The security in PoS is based the idea that a malicious actor would have to amass more of the staked asset (ether in the case of Ethereum) than the entire rest of the stakers on that chain.
- This is infeasible in Ethereum and hence results in strong security properties similar to PoW.

Risks: Scaling risk

Vertical scaling

- Vertical scaling centralizes all transaction processing to a single large machine.
- 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

Horizontal scaling = sharding

- The development of Ethereum 2.0 has been delayed for several years, but its mainnet, which will contain a basic blockchain without any smart contract support, may go live in 2021.
- Ethereum 2.0 has not yet finalized a functional specification for sending transactions between its horizontally scaled blockchains.

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, but are not directly posted to the blockchain unless there is a discrepancy of some kind.
- 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

Optimistic rollup

- As Ethereum’s transaction fees have risen to record levels, layer-2 usage has remained stagnant.
- The space has been developing slowly and many live solutions lack support for smart contracts or decentralized exchanges.
- One solution in development is an *Optimistic Rollup.*
- An optimistic rollup is a process in which transactions are aggregated off-chain into a single digest that is periodically submitted to the chain over a certain interval.

Risks: Scaling risk

Optimistic rollup

- Only an aggregator who has a bond (stake) can combine and submit these summaries.
- Importantly, the state is assumed to be valid unless someone challenges it.
- If a challenge occurs, cryptography can prove if the aggregator posted a faulty state.
- The prover is then rewarded with a portion of the malicious aggregator’s bond as an incentive (similar to a Keeper mechanism).

Risks: Scaling risk

Optimistic rollup

- Optimistic rollups have yet to deliver functional mainnets and require expensive fraud proofs as well as frequent rollup transaction posting, limiting their throughput and increasing their average transaction costs.
- Many approaches aim to decrease the scalability risks facing DeFi today, but the field lacks a clear winner.
- 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 relies on the product of two assets to determine an exchange price.
- The amount of liquidity in the pool determines the slippage when assets are exchanged during a transaction.

Risks: DEX risk

CFMM DEX

- CFMMs such as Uniswap optimize for user experience and convenience, but sacrifice absolute returns. 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

CFMM DEX

- Impermanent loss occurs when two assets in a pool have uncorrelated returns and high volatilities.
- These properties allow arbitrageurs to profit from the asset volatilities and price differences, reducing the temporary returns for LPs and exposing them to risk if an asset moves sharply in price.
- Some AMMs, such as Cap, are able to reduce impermanent loss by using an oracle to determine exchange prices and dynamically adjusting a pricing curve to prevent arbitrageurs from exploiting LPs, but impermanent loss remains a large problem with most AMMs used today.

Risks: DEX risk

On-chain order-book DEX

- On-chain order-book DEXs have a different but prevalent set of risks.
- These exchanges suffer from the scalability issues inherited from the underlying blockchain they run atop of, and are often vulnerable to front running by sophisticated arbitrage bots.
- Order-book DEXs also often have large spreads due to the presence of low-sophistication market makers.
- 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

- Several decentralized exchanges use an entirely off-chain order book, retaining the benefits of a noncustodial DEX, while circumventing the market making and scaling problems posed by on-chain order-book DEXs.
- 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, but also presents a separate set of problems around regulatory compliance.

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

Types of Custodianship

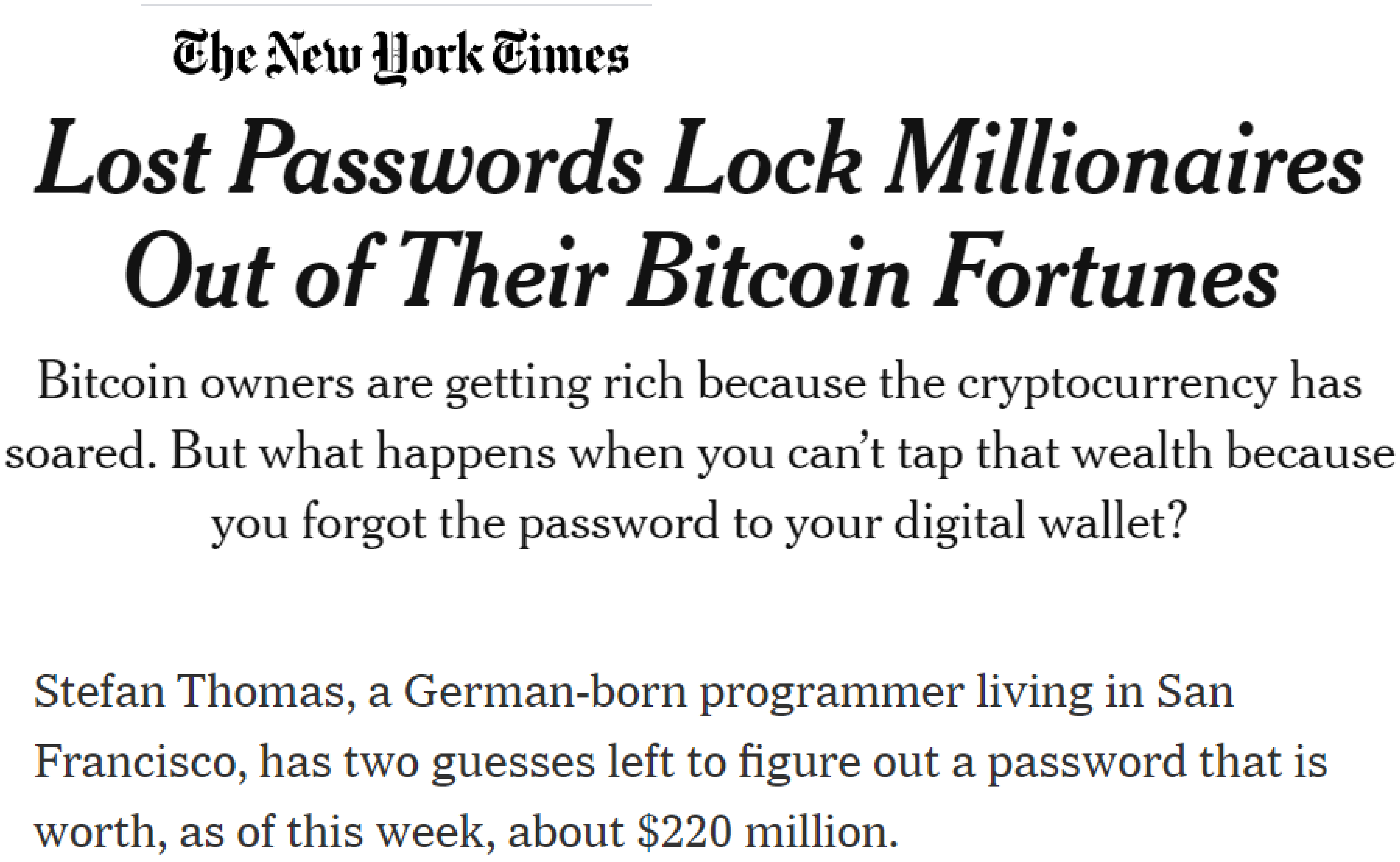
- Self-Custody: Build our own solution
  - In-house or commercial solutions that store crypto assets
  - Solely responsible for assets and not insured against unexpected events
- Partial Custody: Your own wallet + external solution
  - Includes 2-FA and multi-signature solutions (e.g., BitGo)
  - Aligns with needs of retail and high net-worth clients
- Third-party Custody: Hire a managed solution
  - Fully maintained by service provider(s)
  - Aligns with needs of institutions, needed by regulatory bodies

Risks: Custodial risk

Retail Users

- Retail users have a choice between custodial and non-custodial wallets
  - 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
  - Custodial Wallet (Third Party Custody): 3rd party holds access to private keys
    - E.g., Coinbase, Binance
    - Users are subject to KYC/AML regulation

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

Exchange Hacks

- Several exchanges have been hacked, highlighting the security risk of cryptocurrencies
  - Mt. Gox (2011-2014) - 850k Bitcoin
  - Bitfloor (2012) - 24k Bitcoin
  - Bittfinex (2016) - 120k Bitcoin
  - Coincheck (2018) - 523 million NEM (Worth $500 million at the time)
  - Binance (2019) - 7k Bitcoin
- Stolen cryptocurrency is often not completely recovered

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

Infrastructure by Custodians

- Wallet
  - Hot – Internet-connected solutions; fast and frictionless
  - Cold - Air-gapped or internet-isolated solutions; slower but very secure
- Storage Mechanism
  - Software – Digital platforms storing data on the internet or a network segment
  - Hardware – Specially built electronic devices storing data (e.g., Hardware Security Modules)
- Access Protocols
  - Multi Party Computation – Single signature computed by a distributed set of users
  - Multi-Sig – Uses multiple signatures from distinct private keys to secure a wallet

Risks: Custodial risk

BitGo

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: Custodial risk

Concerns around custodianship

- Latency vs Speed
  - Trading at low latency = having fast access to funds
  - But this raises questions around security and proper verification
- New Coins
  - Custodians don't support all newly invented coins for compliance
  - Some coins are offered in some countries and not in others
- Staking
  - Transaction validation on a PoS chain, can be done independently or through a custodian
  - Choose custodian wallet for staking based on proper care and due-diligence

Risks: Custodial risk

Top Custodians

- Coinbase Trust
- Bitgo
- Fidelity Digital Assets
- Bakkt Warehouse
- Kingdom Trust
- Several Banks looking into developing solutions – ING, BBVA, Northern Trust

Institutions looking into Crypto

- Facebook
- Visa
- PayPal
- Mastercard
- Goldman Sachs
- IBM

https://medium.com/blockchain4all/leading-us-based-crypto-custodian-providers-for-institutional-clients-3ba9b8683c6d#:~:text=Who%20are%20the%20leading%20crypto,the%20world's%20largest%20crypto%20custodian.
https://finance.yahoo.com/u/yahoo-finance/watchlists/top-crypto-bets/

Risks: Custodial risk

Regulatory Environment

- In the past, a lack of custody solutions has been a main reason why hedge and mutual funds could not invest in crypto
- Legal and regulatory environments for custodians and institutions have not been clearly defined
  - Custody Rule of Investment Adviser Act of 1940 – Institution with $150 million AUM needs a licensed custodian
- Federally charted banks are allowed to provide crypto custodial services

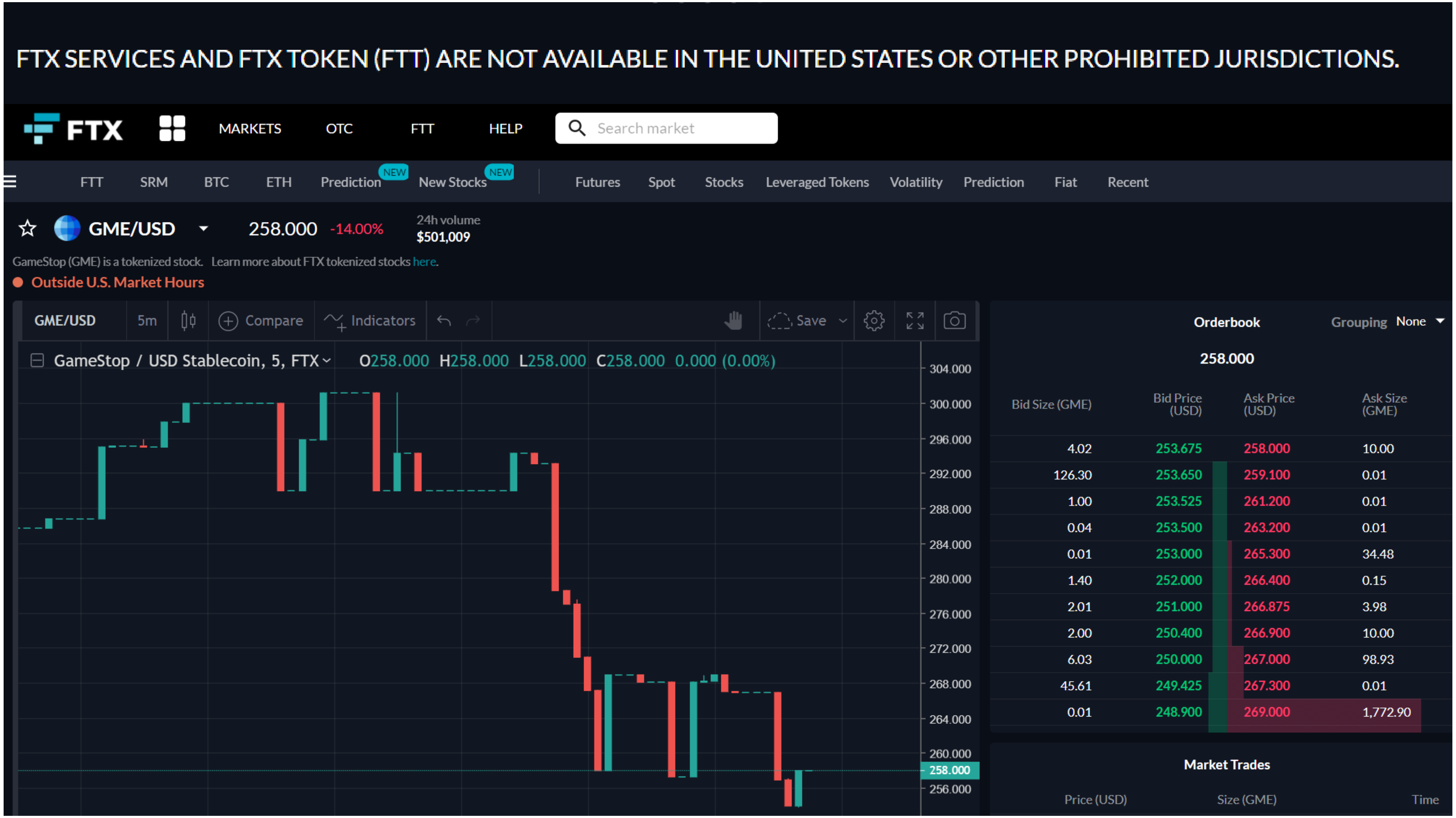
https://www.coindesk.com/sec-qualified-custodian-statement
https://www2.deloitte.com/us/en/pages/audit/articles/cryptocurrency-custody-regulations-from-occ-deloitte-us.html

Risks: Regulatory risk

KYC/AML

- 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.

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

GameStop / USD Stablecoin, 5, FTX O258.000 H258.000 L258.000 C258.000 0.000 (0.00%)

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

Basis

- A well known algorithmic stablecoin project known as Basis was forced to shut down in December of 2018 due to regulatory concerns.
- A harrowing message remains on their home page for future similar companies:
  - "Unfortunately, having to apply US securities regulation to the system had a serious negative impact on our ability to launch Basis...As such, I am sad to share the news that we have decided to return capital to our investors. This also means, unfortunately, that the Basis project will be shutting down."

Risks: Regulatory risk

Governance tokens

- Governance tokens, released by many DeFi projects, are also facing increasing scrutiny as the SEC continues to evaluate if these new assets will be regulated as securities.
- For example, Compound, the decentralized money market on Ethereum, recently released a governance token with no intrinsic value or rights to future cash flows.
- Doing so allowed Compound to avoid the SEC’s securities regulation, freeing the company from security issuance responsibilities.

Risks: Regulatory risk

Money-transmitter laws

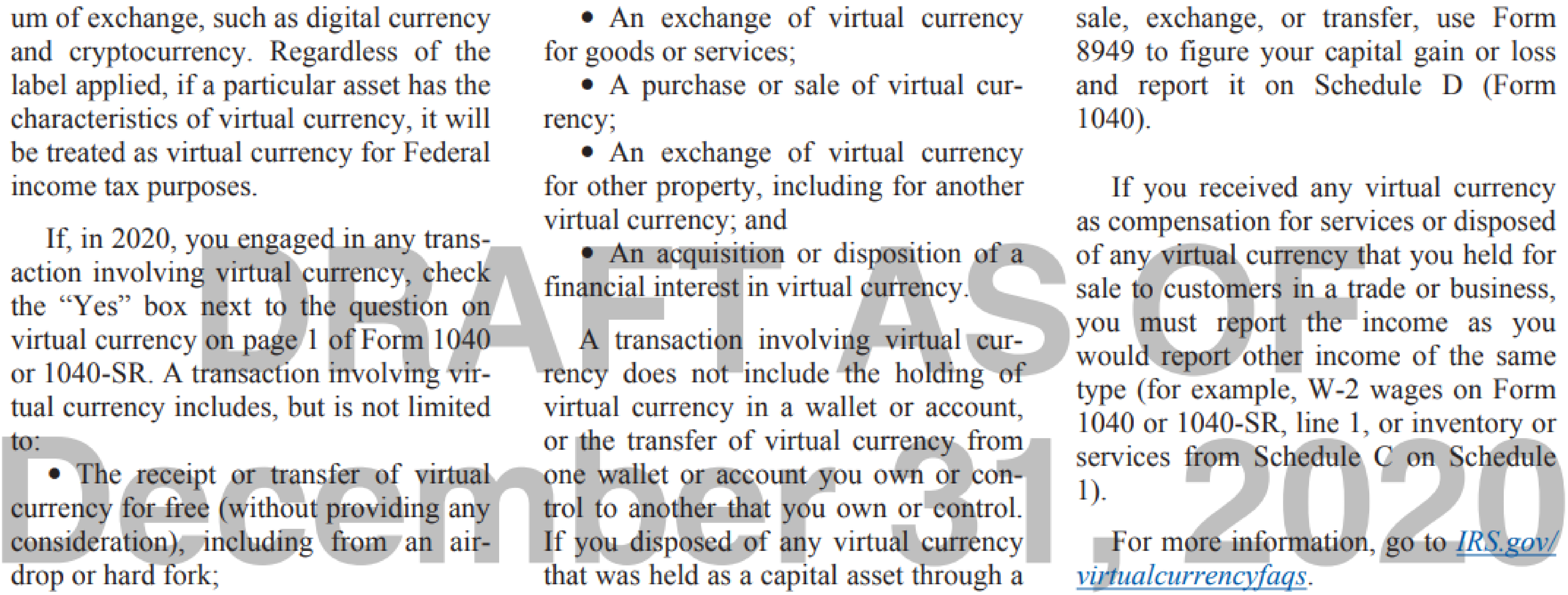
- Many major market-cap cryptocurrencies have been ruled commodities by the CFTC, exempting them from money-transmitter laws.
- Individual states, such as New York, however, have regulation that targets brokerages facilitating the transfer and exchange of cryptocurrencies.
- As DeFi continues to grow and the total number of issued assets continues to expand, we expect to see increasingly specific and nuanced regulation aimed at DeFi protocols and their users.

Risks: Regulatory risk

Tax

- Cryptocurrency taxation has yet to be fully developed from a regulatory standpoint, and accounting software/on-chain monitoring is just starting to reach mainstream retail audiences.
- IRS proposal draft:

Risks: Regulatory risk



um of exchange, such as digital currency and cryptocurrency. Regardless of the label applied, if a particular asset has the characteristics of virtual currency, it will be treated as virtual currency for Federal income tax purposes.

If, in 2020, you engaged in any transaction involving virtual currency, check the "Yes" box next to the question on virtual currency on page 1 of Form 1040 or 1040-SR. A transaction involving virtual currency includes, but is not limited to:

- The receipt or transfer of virtual currency for free (without providing any consideration), including from an airdrop or hard fork;
- An exchange of virtual currency for goods or services;
- A purchase or sale of virtual currency;
- An exchange of virtual currency for other property, including for another virtual currency; and
- An acquisition or disposition of a financial interest in virtual currency.

A transaction involving virtual currency does not include the holding of virtual currency in a wallet or account, or the transfer of virtual currency from one wallet or account you own or control to another that you own or control. If you disposed of any virtual currency that was held as a capital asset through a sale, exchange, or transfer, use Form 8949 to figure your capital gain or loss and report it on Schedule D (Form 1040).

If you received any virtual currency as compensation for services or disposed of any virtual currency that you held for sale to customers in a trade or business, you must report the income as you would report other income of the same type (for example, W-2 wages on Form 1040 or 1040-SR, line 1, or inventory or services from Schedule C on Schedule 1).

For more information, go to *IRS.gov/virtualcurrencyfaqs*.

https://www.irs.gov/pub/irs-dft/i1040gi--dft.pdf

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