Part IV:

DeFi Risks and Opportunities

Campbell R. Harvey
Duke University and NBER

Learning Experience Outline

Four courses in **DeFi and the Future of Finance:**

I. DeFi Infrastructure

II. DeFi Primitives

III. DeFi Deep Dive

IV. DeFi Risks and Opportunities

1. Smart Contract Risk
2. Governance, DNS, Oracle, DEX Risk, and Custodial Risks
3. Scaling Risk
4. Regulatory Risk and Environmental Risk
5. The Future Winners and Losers

Overview

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.

Part IV:

DeFi Risks and Opportunities

1. Smart Contract Risk

(i) Types of Exploits

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 sell heavily on the oracle exchange to manipulate the price, then proceed to purchase far more on the primary exchange 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

Key features of flash loans

- No collateral
- No duration
- No counterparty risk
- No interest rate

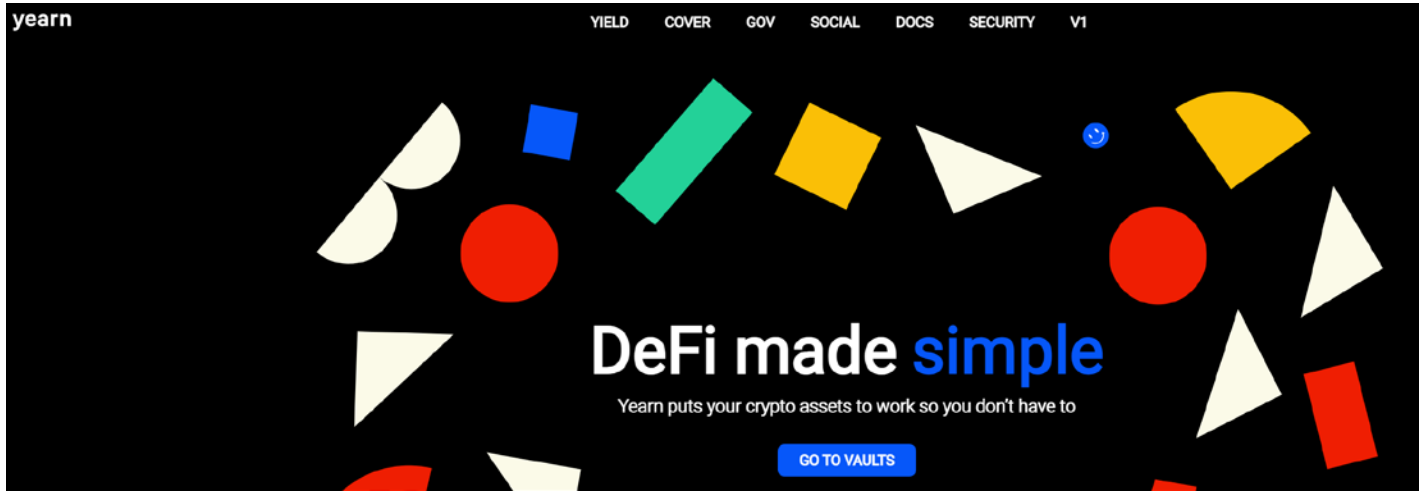
How is this possible?

- Atomicity of Ethereum transactions

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

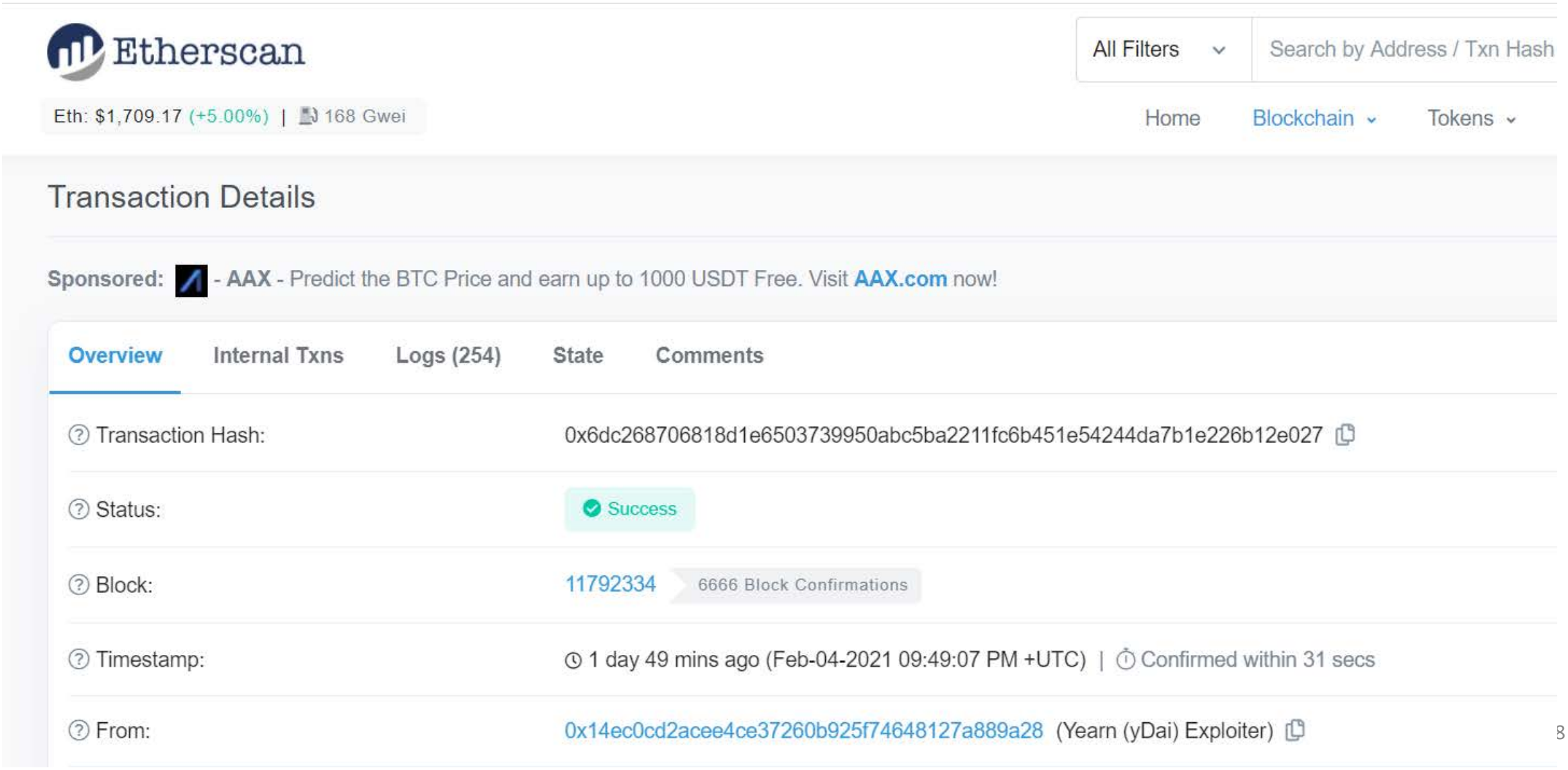
by Michael McSweeney

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

February 3, 2021

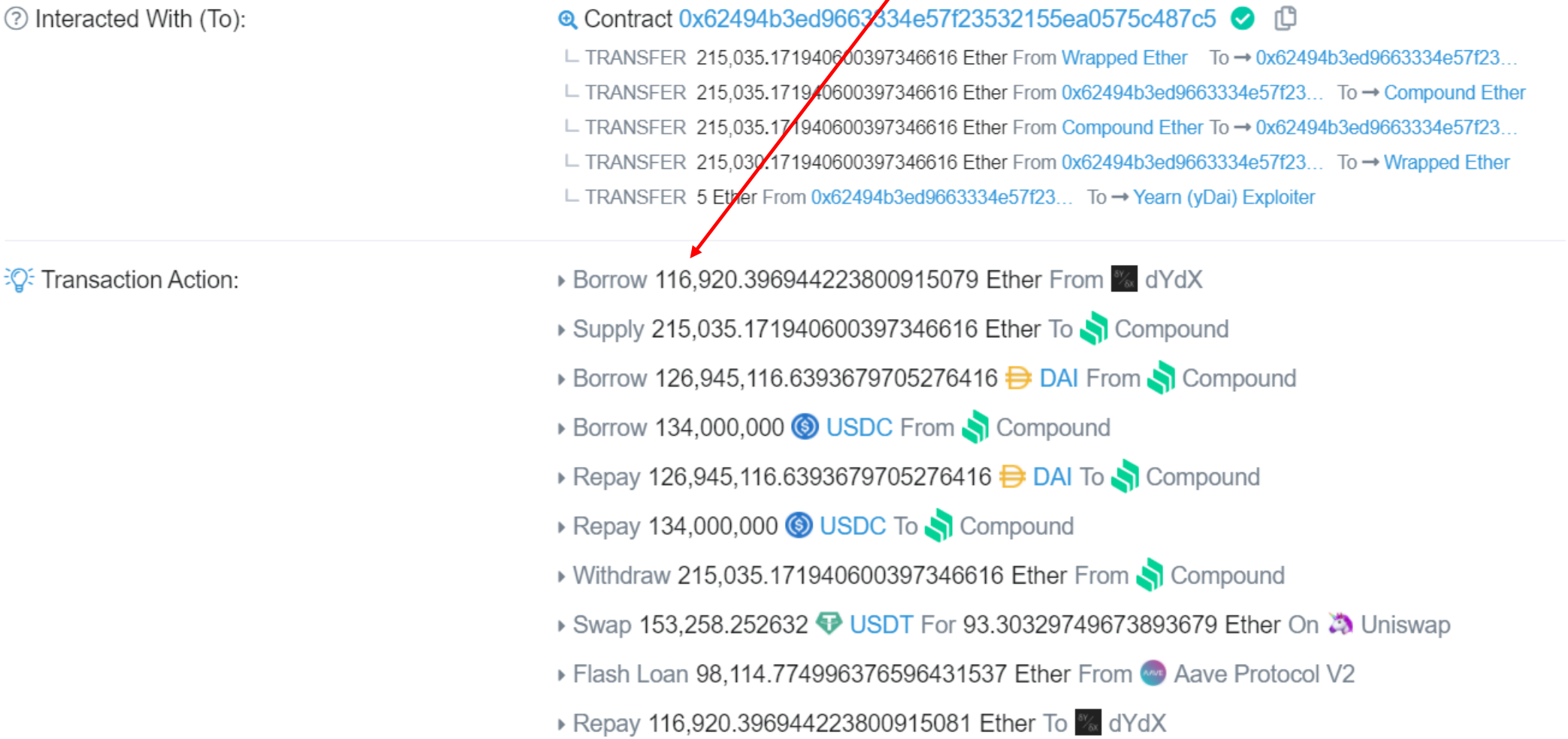
https://www.theblockcrypto.com/linked/93818/yearn-finance-dai-pool-defi-exploit-attack

Risks: Smart contract risk



Risks: Smart contract risk

$200m Flash loan – with no collateral



Risks: Smart contract risk

161 token transfers. Just displaying the first 10.

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

Flash attack

C.R.E.A.M. v1

- $130m exploit
- Complex exploit involved 68 assets

Bloomberg

Cryptocurrencies

DeFi Protocol Cream Finance Loses $130 Million in Latest Crypto Hack

By Emily Graffeo +Follow

October 27, 2021, 1:34 PM EDT

- Cream suffers another major flash loan attack in 2021
- Ethereum-based lending protocol is looking into incident

October 27, 2021

Cream Finance @CreamdotFinance · 2h

Our Ethereum C.R.E.A.M. v1 lending markets were exploited and liquidity was removed on October 27, 1354 UTC. The attacker removed a total of ~$130m USD worth of tokens from these markets, using this address: etherscan.io/address/0x2435...

No other markets were impacted.

etherscan.io

Address 0x24354d31bc9d90f62fe5f2454709c32...

The Address 0x24354d31bc9d90f62fe5f2454709c32049cf86...

https://www.bloomberg.com/news/articles/2021-10-27/defi-protocol-cream-finance-loses-130-million-in-latest-hack

Flash attack

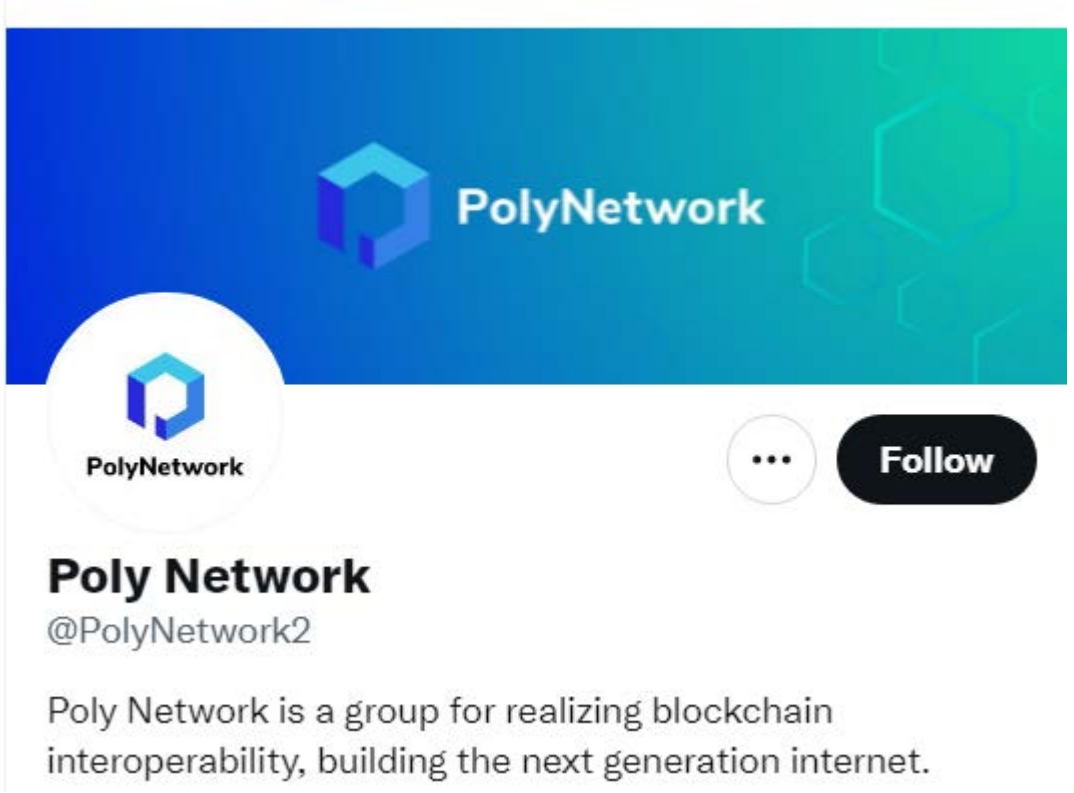
$2.1b Flash loan – with no collateral

https://etherscan.io/tx/0x0fe2542079644e107cbf13690eb9c2c65963ccb79089ff96bfaf8dced2331c92

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

Part IV:

DeFi Risks and Opportunities

1. Smart Contract Risk

(ii) The DAO

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

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

Etherscan

All Filters | Search by Address

Eth: $267.20 (-2.49%)

Home | Blockchain | Toke

Block #1428757

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

Overview | Comments

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

All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

#	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

All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

#	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 ETH to the original investors

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 or contentious (ETC)

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

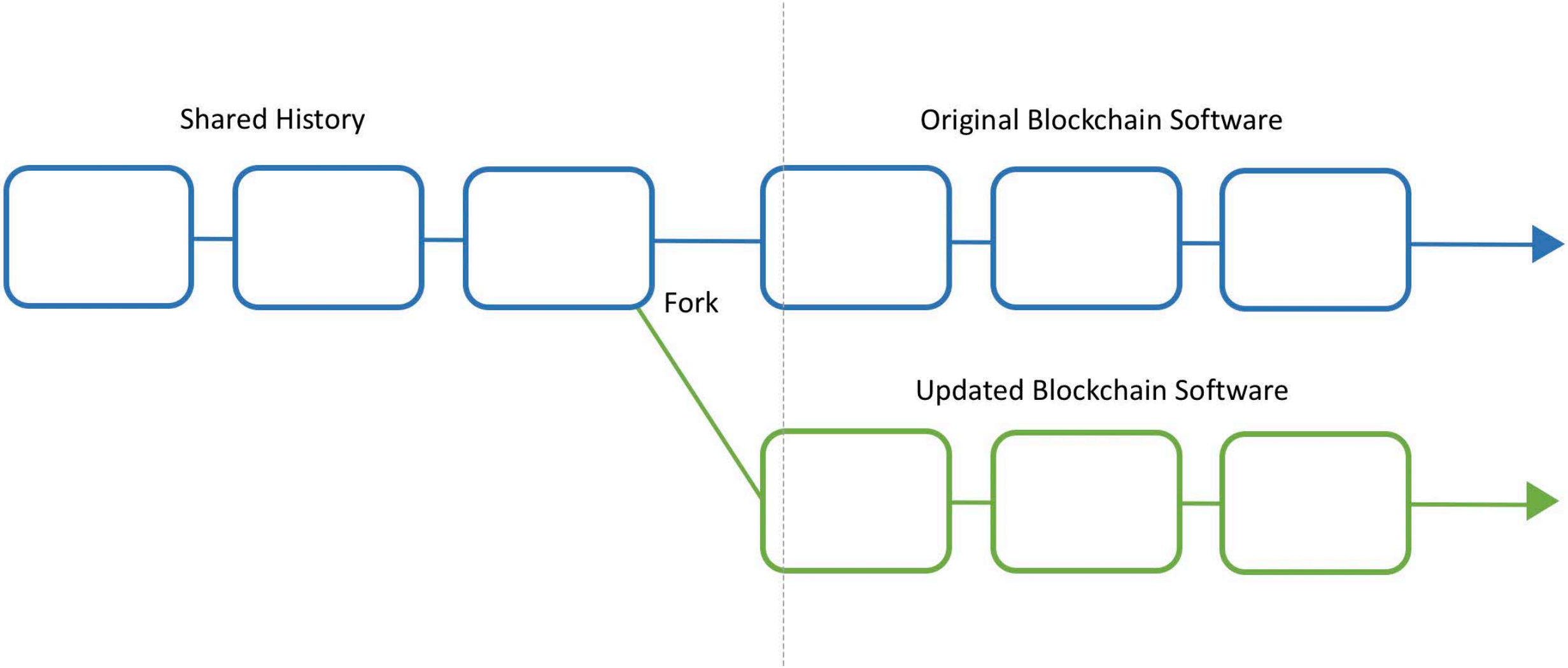
Risks: Smart contract risk

Hard forks examples

- Consensus change: PoW to PoS
- Block size
- Mining algorithm (SHA-256 to alternative)

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

Risks: Smart contract risk



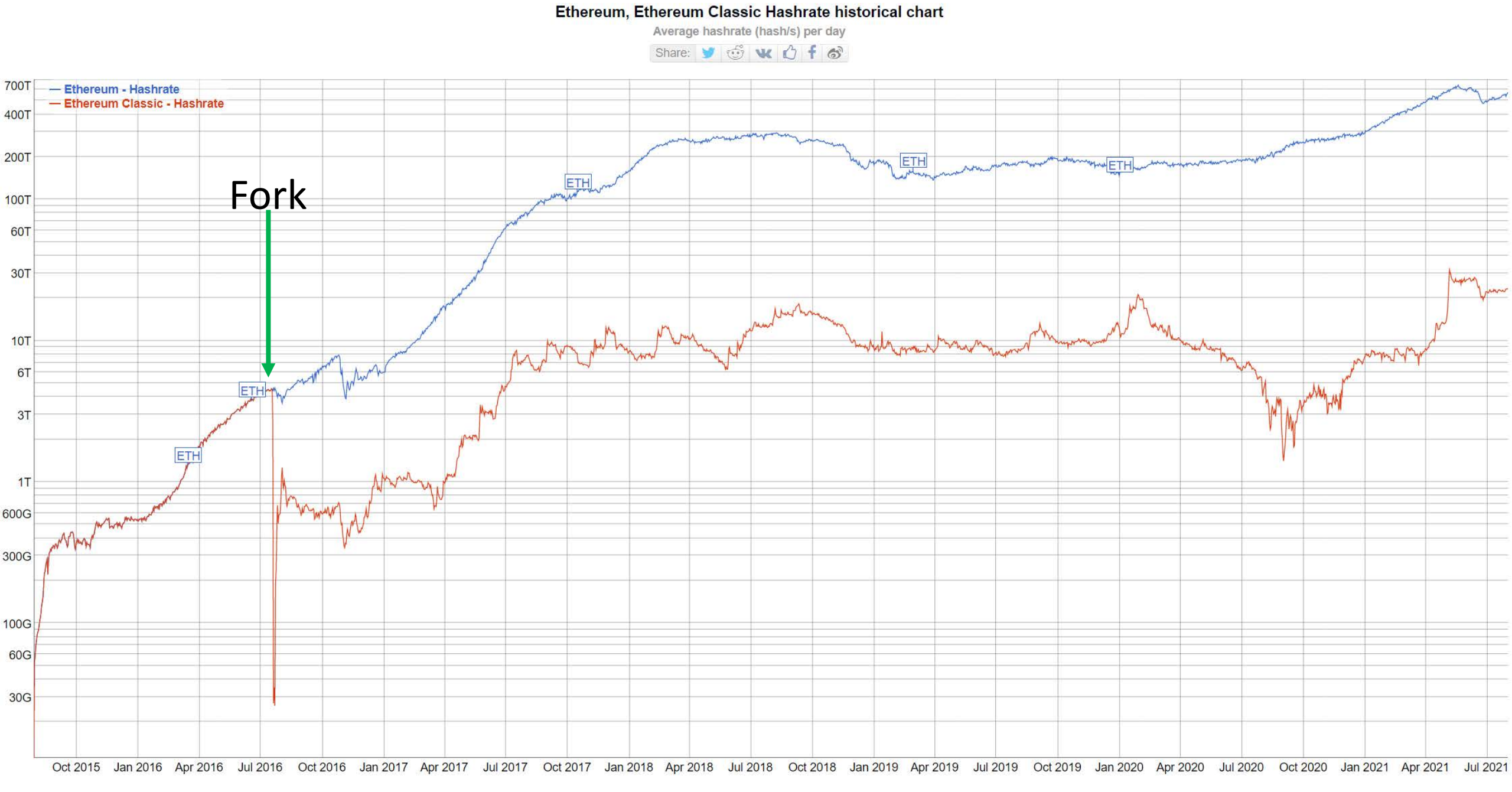
Risks: Smart contract risk

ETC was contentious hard fork

- If you owned 10 ETH at the time of the fork, your new balance would be 10 ETH (on forked new Ethereum) and 10 ETC (on ETC original blockchain).

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
2	Ethereum ETH Buy	$2,522.48	3.94%	9.80%	$294,943,910,915	$22,799,464,332 9,041,075 ETH	116,959,333 ETH
19	Ethereum Classic ETC	$49.59	4.03%	1.08%	$6,401,688,583	$2,065,923,030 41,544,558 ETC	128,734,382 ETC

ETH hash rate 22x ETC



Risks: Smart contract risk

Hard forks examples

- EIP-1159 “London” upgrade proposed by Vitalik Buterin
- Scheduled for August 4 or 5, 2021
- Key innovation is to simplify fees.
  - Users pay a “base fee” which is automatically calculated by the wallet
  - Base fee does not go the miner – it is burned (so reduces ETH inflation)
  - Users can add a “tip” which does go to the miner to speed up transactions
- EIP-1559 is not Ethereum 2.0 which is an even bigger change

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

Risks: Smart contract risk: Other: Rug pull

Mechanics

- A new token, TKN, is launched on a DEX
- It comes with a very high reward for offering liquidity (high interest rate)
- Retail investors are attracted and offer liquidity (contribute ETH and TKN to the liquidity pool)
- Once the pool is large enough, the original developers (who hold a lot of TKN, sell everything on the DEX causing price of TKN to drop to near zero). That is a rug pull.

Risks: Smart contract risk: Other: Rug pull

The SQUID cryptocurrency peaked at a price of $2,861 before plummeting to $0 around 5:40 a.m. ET., according to the website CoinMarketCap. This kind of theft, commonly called a “rug pull” by crypto investors, happens when the creators of the crypto quickly cash out their coins for real money, draining the liquidity pool from the exchange.

https://gizmodo.com/squid-game-cryptocurrency-scammers-make-off-with-2-1-m-1847972824

November 1, 2021

GIZMODO

HOME LATEST REVIEWS TECH IO9 EARTHER SCIENCE FIELD GUIDE

NEWS

Squid Game Cryptocurrency Scammers Make Off With $3.3 Million

The SQUID coin scam was covered uncritically by mainstream news outlets.

By Matt Novak

Yesterday 7:10AM | Comments (102) | Alerts

Image: Netflix

The anonymous hucksters behind a *Squid Game* cryptocurrency have officially pulled the rug on the project, making off with an estimated $3.38 million.

Risks: Smart contract risk: Other: Rug pull

Risks: Smart contract risk: Other: Rug pull

Red flags

- Illiterate white paper with unfounded claims
- Promoted with fake Elon Musk tweets
- Telegram set up to disallow comments
- Not approved for trading on Coinbase or Binance
- “The “schedule” for the crypto’s rollout is also filled with red flags, including a claim that there will be “hiring for Asia and Europe Market.” What does that mean? You guess is as good as ours, but it’s almost certainly bullshit.”

https://gizmodo.com/new-squid-game-cryptocurrency-launches-as-obvious-scam-1847961584

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

https://hacken.io/researches-and-investigations/biggest-defi-hacks-of-2020-report/
https://www.cybavo.com/blog/defi-hacks-2021/