Course 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

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 or contentious (ETC)

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

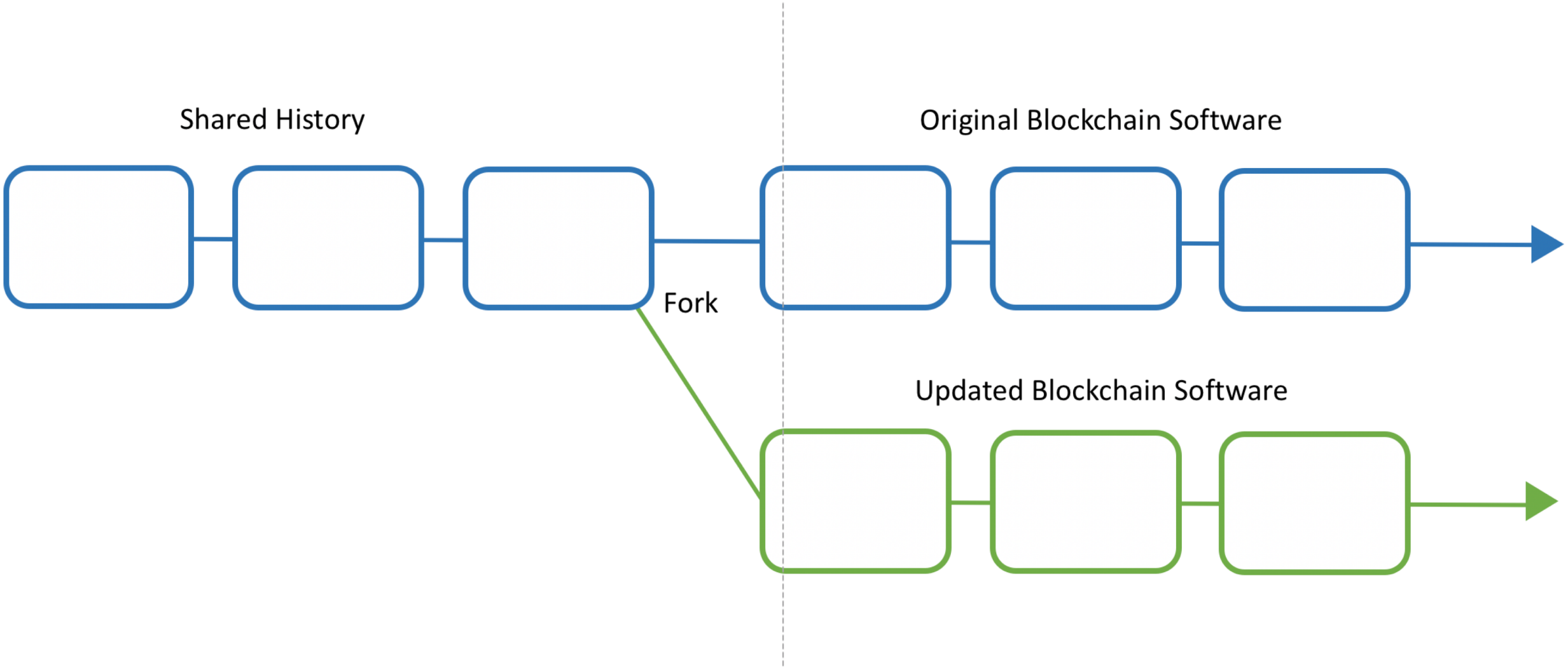
Risks: Smart contract risk

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



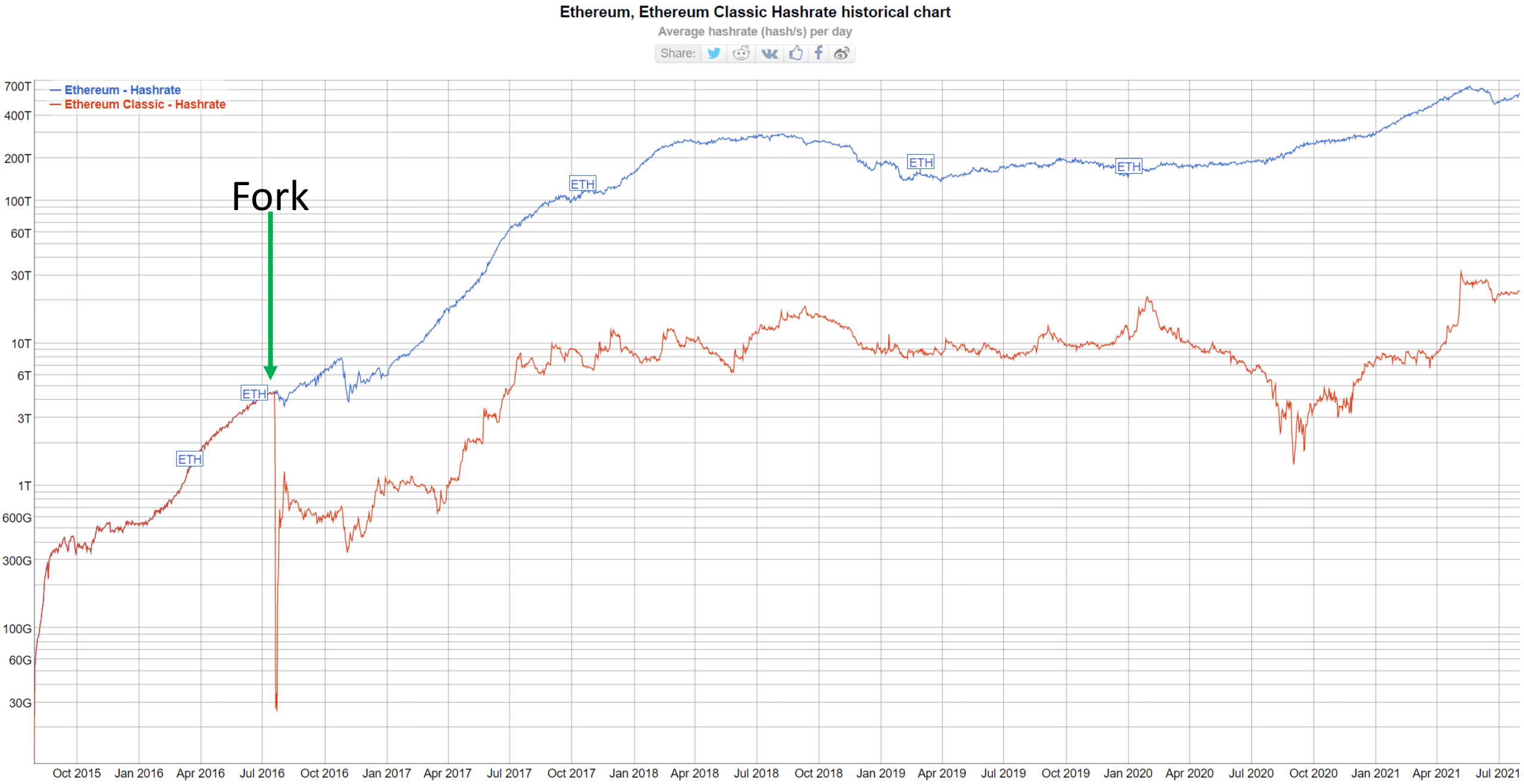
Risks: Smart contract risk

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/