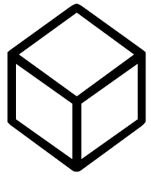
TIBA

Introduction to Ethereum

Spring 2020

Péter Garamvölgyi

TIBA



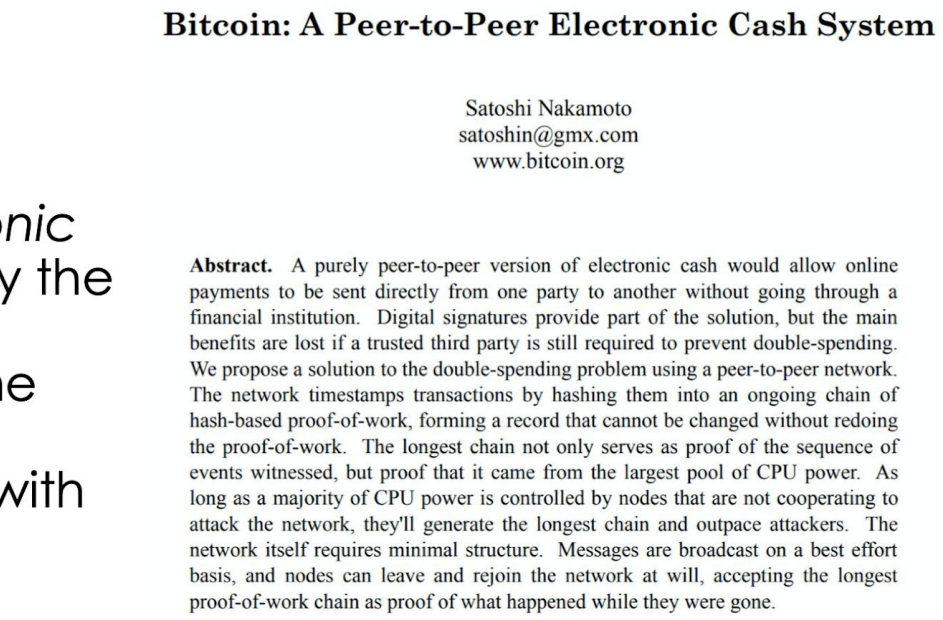
Previously on TIBA
Intro to Blockchain

TIBA

Lesson 1 -- History of Bitcoin

Blockchain History – Bitcoin

- **August 2008**, domain name bitcoin.org was registered
- **October 2008**, a paper titled "*Bitcoin: A Peer-to-Peer Electronic Cash System*" was published by the name **Satoshi Nakamoto**
- **January 2009**, Satoshi mined the genesis block of the bitcoin blockchain (block number 0), with a reward of 50 bitcoins



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

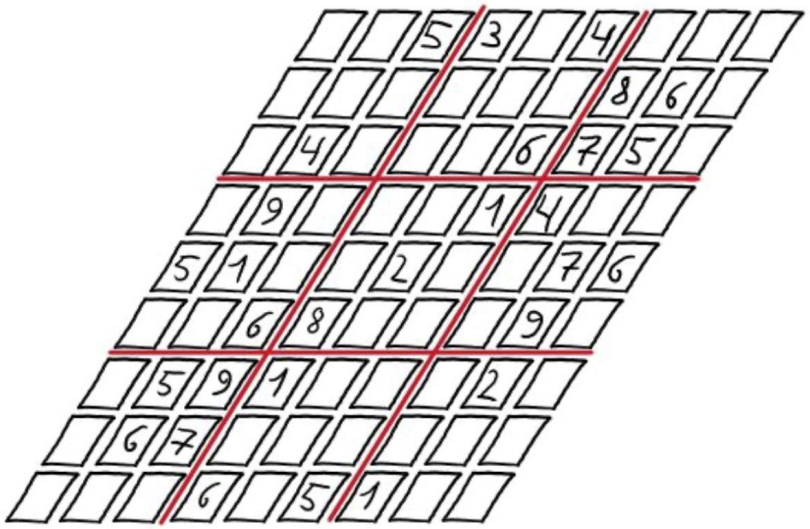
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Lesson 2 -- Cryptography

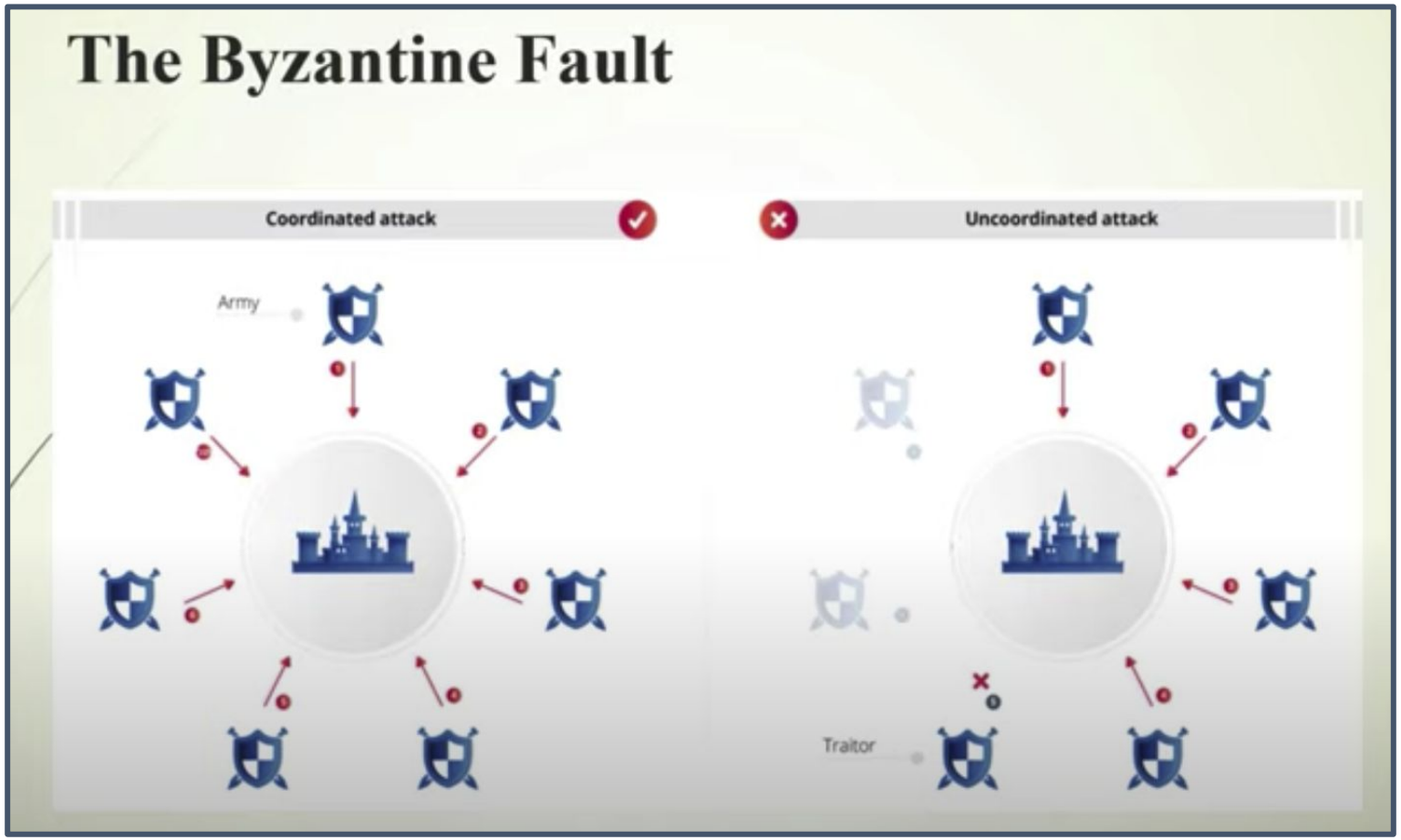
Introduction to Zero-Knowledge Proof

Commit

- First, I put 81 pieces of paper on the table, each with a number 1-9. The place of each piece is the same as the solution. And the Numbers in the question face up and the blanks face down.
- You can not turn up the pieces of paper to see the answer !



Lesson 3 -- Consensus



Lesson 4 -- Bitcoin & Blockchain

Bitcoin Transaction

UTXO Pool

- A memory pool of all current UTXOs
  - used by miners to verify transactions (by checking the money you're spending belongs to you)

UTXO pool

TIBA

What is Ethereum?
What are decentralized apps?

TIBA

Contents

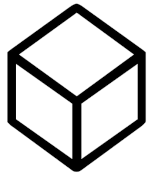
- What is Ethereum?
- Brief history of Ethereum
- What are dapps?
- How do dapps work?
- Who controls Ethereum?

TIBA

Contents

- **What is Ethereum?**
- Brief history of Ethereum
- What are dapps?
- How do dapps work?
- Who controls Ethereum?

TIBA



What is Ethereum?

TIBA

Ethereum　以太坊　イーサリアム　이더리움　इथीरियम

Ethereum is a global, open-source platform for decentralized applications.

On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world.

https://ethereum.org

TIBA

Cryptocurrencies ▾ | Exchanges | Watchlist | Filters | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$170,597,780,761	$9,279.44	$27,637,975,954	18,384,487 BTC	1.10%	
2	Ethereum	$23,338,028,821	$210.14	$10,592,755,236	111,057,819 ETH	1.49%	
3	Tether	$8,810,446,215	$1.00	$33,476,318,826	8,798,069,379 USDT *	0.00%	
4	XRP	$8,809,346,599	$0.199700	$1,345,544,652	44,112,853,111 XRP *	0.30%	
5	Bitcoin Cash	$4,356,582,852	$236.57	$2,305,773,957	18,415,838 BCH	1.09%	
6	Bitcoin SV	$3,582,023,713	$194.52	$1,025,831,849	18,414,333 BSV	0.48%	
7	Litecoin	$2,869,971,757	$44.29	$2,533,657,103	64,799,781 LTC	0.74%	

https://coinmarketcap.com

TIBA

"Ethereum is the foundation for a new era of the internet:

1. *An internet where money and payments are built in.*
2. *An internet where users can own their data, and your apps don't spy and steal from you.*
3. *An internet where everyone has access to an open financial system.*
4. *An internet built on neutral, open-access infrastructure, controlled by no company or person.*

Ethereum is programmable, which means that developers can use it to build new kinds of applications."

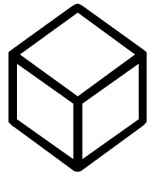
https://ethereum.org

TIBA

Contents

- What is Ethereum?
- **Brief history of Ethereum**
- What are dapps?
- How do dapps works?
- Who controls Ethereum?

TIBA



A brief history of Ethereum

2008-2013

- As Bitcoin gained popularity, people started to use it for more than just a cryptocurrency.
- Some people started building more complex applications on top of Bitcoin using Bitcoin Script
- Others started a new, competing blockchain systems with different characteristics (altcoins)

TIBA

Bitcoin Script

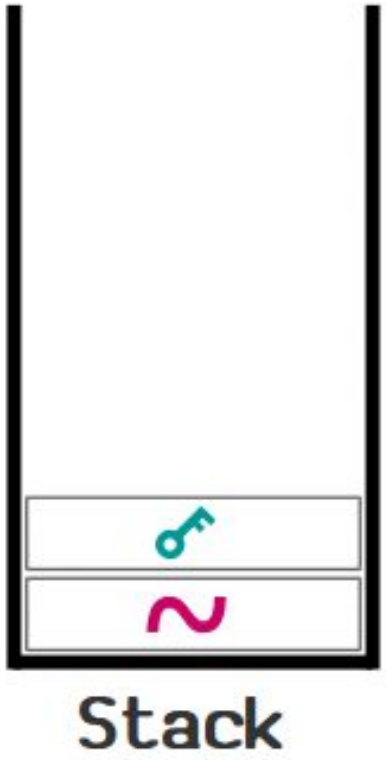
"A script is essentially a list of instructions recorded with each transaction that describe how the next person wanting to spend the Bitcoins being transferred can gain access to them."

- pay-to-pubkey-hash
- pay-to-multisig
- time lock
- puzzle

Bitcoin script is intentionally weak!

https://en.bitcoin.it/wiki/Script

Bitcoin Script



https://learnmeabitcoin.com/guide/script

TIBA

Altcoins

- All crypto that is not Bitcoin
- According to Wikipedia, there were already 20+ altcoins before Ethereum
- Some systems are substantially different (e.g. zCash, Monero). Others are use-case specific (Namecoin). Yet others are quite similar to existing systems (e.g. Litecoin, Dogecoin)

https://en.wikipedia.org/wiki/List_of_cryptocurrencies

Release	Currency	Symbol	Founder(s)	Hash algorithm	Programming language of implementation	Cryptocurrency blockchain (PoS, PoW, or other)	Notes
2009	Bitcoin	BTC,[2] XBT, ₿	Satoshi Nakamoto[nt 1]	SHA-256d[3][4]	C++[5]	PoW[4][6]	The first and most widely used decentralized ledger currency,[7] with the highest market capitalization.[8]
2011	Litecoin	LTC, Ł	Charlie Lee	Scrypt	C++[9]	PoW	One of the first cryptocurrencies to use Scrypt as a hashing algorithm.
2011	Namecoin	NMC	Vincent Durham[10][11]	SHA-256d	C++[12]	PoW	Also acts as an alternative, decentralized DNS.
2012	Peercoin	PPC	Sunny King (pseudonym) [citation needed]	SHA-256d[citation needed]	C++[13]	PoW & PoS	The first cryptocurrency to use POW and POS functions.
2013	Dogecoin	DOGE, XDG, Đ	Jackson Palmer & Billy Markus[14]	Scrypt[15]	C++[16]	PoW	Based on the Doge internet meme.
2013[citation needed]	Gridcoin	GRC	Rob Hälford[citation needed]	Scrypt	C++[17]	Decentralized PoS	Linked to citizen science through the Berkeley Open Infrastructure for Network Computing[18]

https://en.wikipedia.org/wiki/List_of_cryptocurrencies

Altcoins

- *"Introduced as a "joke currency" on 6 December 2013, Dogecoin quickly developed its own online community and reached a capitalization of US$60 million in January 2014."*

https://en.wikipedia.org/wiki/Dogecoin

Altcoins

- Many independent systems lead to fragmentation
  - Fragmentation of the ecosystem: Each chain needs different tools (wallets, node, dev tools, …). These need to be developed, maintained, installed.
  - Fragmentation of the mining power: For PoW chains, more mining power means better security.

TIBA

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$166.65 B	SHA-256	98,362 PH/s	*$335,741*	0%
Ethereum	ETH	$22.82 B	Ethash	171 TH/s	*$119,794*	4%
BitcoinCashABC	BCH	$4.21 B	SHA-256	3,025 PH/s	*$10,325*	12%
BitcoinSV	BSV	$3.50 B	SHA-256	2,276 PH/s	*$7,769*	15%
Litecoin	LTC	$2.81 B	Scrypt	215 TH/s	*$15,542*	5%
EthereumClassic	ETC	$765.21 M	Ethash	9 TH/s	*$6,310*	76%
Dash	DASH	$695.77 M	X11	4 PH/s	*$1,664*	7%
Zcash	ZEC	$427.17 M	Equihash	6 GH/s	*$11,511*	4%
BitcoinGold	BTG	$154.00 M	Zhash	1 MH/s	*$310*	42%

https://www.crypto51.app

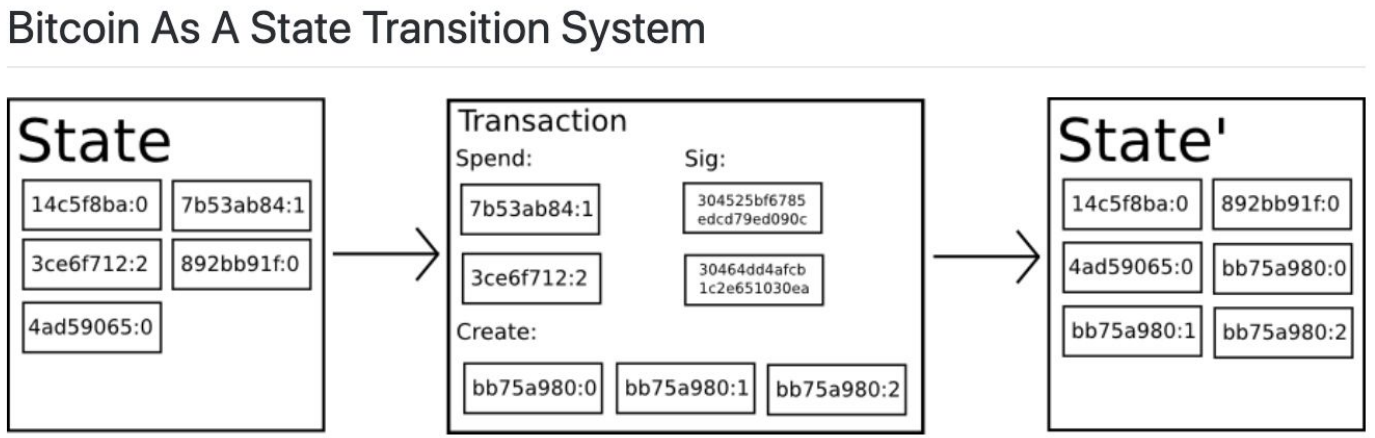
2013: Vitalik Buterin proposes Ethereum

- Ethereum was initially described in a white paper by **Vitalik Buterin**, a programmer and co-founder of Bitcoin Magazine, in late 2013 with a goal of building decentralized applications.

White Paper

Chris Chinchilla edited this page on 17 Jun 2019 · 176 revisions

A Next-Generation Smart Contract and Decentralized Application Platform



https://en.wikipedia.org/wiki/Ethereum
https://github.com/ethereum/wiki/wiki/White-Paper

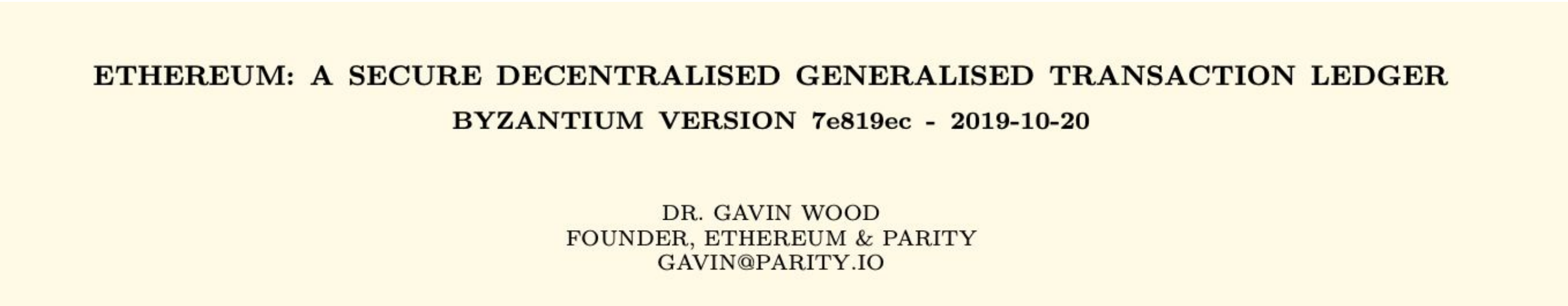
Vitalik Buterin

- Vitalik Buterin, a programmer from Toronto, first grew interested in Bitcoin in 2011.
- He co-founded the online news website Bitcoin Magazine in the same year, writing hundreds of articles on the cryptocurrency world.

https://www.coindesk.com/learn/ethereum-101/who-created-ethereum

A brief history of Ethereum - Yellow paper

- Gavin Wood, co-founder of Ethereum and Parity, wrote the Ethereum Yellow Paper that specified the Ethereum Virtual Machine



ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

BYZANTIUM VERSION 7e819ec - 2019-10-20

DR. GAVIN WOOD
FOUNDER, ETHEREUM & PARITY
GAVIN@PARITY.IO

https://ethereum.github.io/yellowpaper/paper.pdf

A brief history of Ethereum

- Subsequently, a Swiss non-profit foundation, the Ethereum Foundation (Stiftung Ethereum), was created as well

https://en.wikipedia.org/wiki/Ethereum

TIBA

A brief history of Ethereum - Crowdsale

- Development was funded by an online crowdsale that took place between July and August 2014.
- The system then went live on 30 July 2015, with 72 million coins minted.
- *"Slightly more than a half day after the sale began, 7.4 million ETH had already been presold, which at current prices works out to just more than 3,700 BTC. In fiat terms, that's about US$2.3 million. In Bugatti terms, that's about 1.2 Veyrons."*

https://en.wikipedia.org/wiki/Ethereum
https://cointelegraph.com/news/ethereum-raises-3700-btc-in-first-12-hours-of-ether-presale

TIBA

A brief history of Ethereum - the DAO

- In 2016, a major application (though not Ethereum itself!) was hacked by exploiting a bug in its source code. This is known as the DAO hack.
- The community collectively decided to change the history and undo the hack.
- Ethereum split into two independent chains: Ethereum (ETH) and Ethereum Classic (ETC)

A brief history of Ethereum - EEA

- In March 2017, various blockchain start-ups, research groups, and Fortune 500 companies announced the creation of the Enterprise Ethereum Alliance (EEA) with 30 founding members

TIBA

Ethereum 2.0

- Long-awaited new protocol using sharding and Proof-of-Stake to improve performance
- Rollout might begin this year

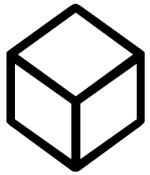
https://www.coindesk.com/vitalik-buterin-says-much-delayed-ethereum-2-0-still-on-track-for-july-launch

TIBA

Contents

- What is Ethereum?
- Brief history of Ethereum
- **What are dapps?**
- How do dapps work?
- Who controls Ethereum?

TIBA



What are **dapps** anyway?

TIBA

Traditional apps

- Today's apps work as **data silos** and **black boxes**.
- Company: "*Give me your data and I'll provide services in exchange.*"
- This is a decent model but it is prone to *accidental* and *intentional* misuse.
- With technical terms, this is often implemented as the client-server model.

Decentralized apps (dapps)

"[Dapps] are reliable and predictable, meaning that once they are "uploaded" to Ethereum, they will always run as programmed. They can control digital assets in order to create new kinds of financial applications. They can be decentralized, meaning that no single entity or person controls them."

→ *This can be implemented on a peer-to-peer basis.*

https://ethereum.org

TIBA

Decentralized apps (dapps)

Applications built on Ethereum (dapps) can do things regular apps can't:

- ✓ Create new kinds of money and digital assets
- ✓ Web apps that are unstoppable and uncensorable
- ✓ Build decentralized organizations, property, or virtual worlds that are governed collectively

https://ethereum.org/dapps

TIBA

Decentralized apps (dapps)

+ verifiable correctness
+ transparency
+ democratic governance
+ censorship resistance
+ transfer of value built-in
+ true ownership

- higher price
- lower speed
- privacy is challenging

TIBA

Dapp examples

- Financial applications: raise capital (**ICO**), borrow, invest, ...
- Markets, exchanges
- Governance (DAO)
- Collectibles (CryptoKitties) and games (Decentraland)
- Supply chain, identity, stablecoins, social networks

TIBA

Dapp example: ICO & STO

- ICO (Initial Coin Offering): create a new kind of coin (token) and use it to raise capital
  - 2017 was the ICO craze with many scams
- STO (Security Token Offering): a more regulated way of raising capital through token issuance
- Both are ways of crowdfunding
- Utility token vs security token distinction

learn more: https://99bitcoins.com/security-token-sto

TIBA

Dapp example: DAO

- Decentralized Autonomous Organizations are organizations governed by transparent rules expressed in code
- Rules are expressed in a smart contract
- Shareholder can vote on proposals
- You could govern many things like this: organizations, open-source projects, student associations, ...

learn more: https://cointelegraph.com/ethereum-for-beginners/what-is-dao

Dapp example: CryptoKitties

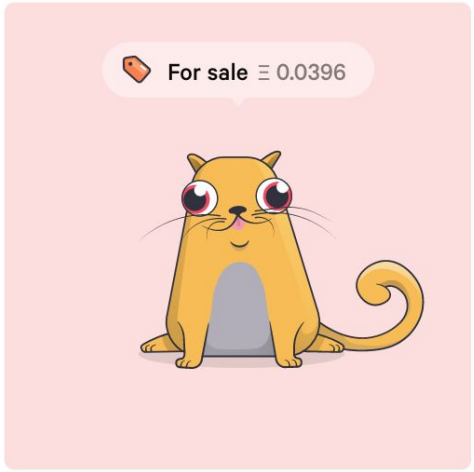
- Blockchain enables true unique ownership of digital data through NFTs (Non-Fungible Tokens) as collectibles.

What is CryptoKitties?

CryptoKitties is a game centered around breedable, collectible, and oh-so-adorable creatures we call CryptoKitties! Each cat is one-of-a-kind and 100% owned by you; it cannot be replicated, taken away,

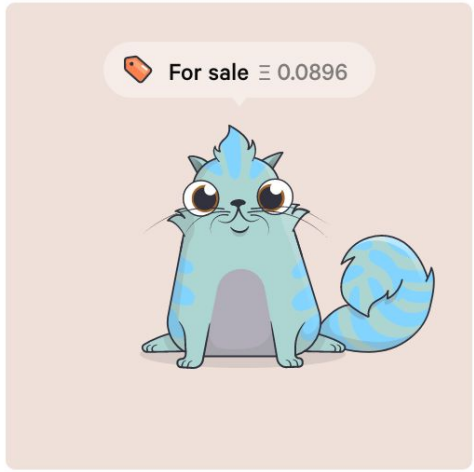
https://www.cryptokitties.co

TIBA



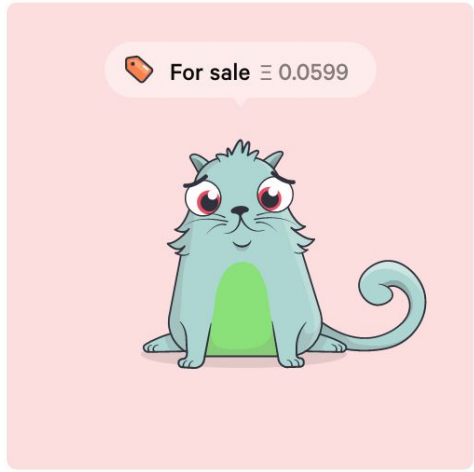
Kitty 240616 · Gen 8

Snappy



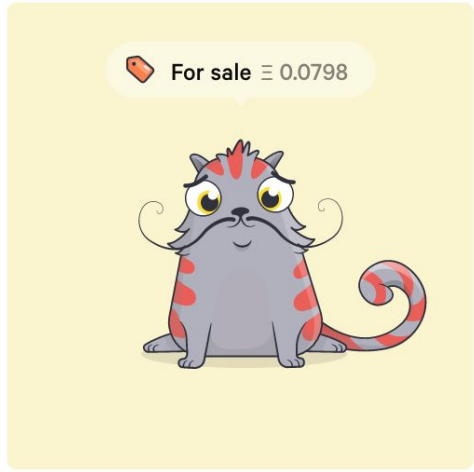
Kitty 240611 · Gen 4

Swift



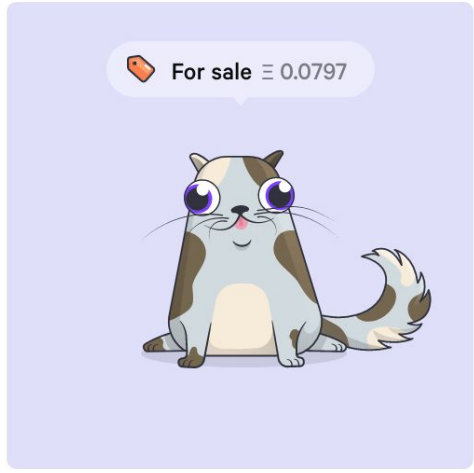
Kitty 240609 · Gen 7

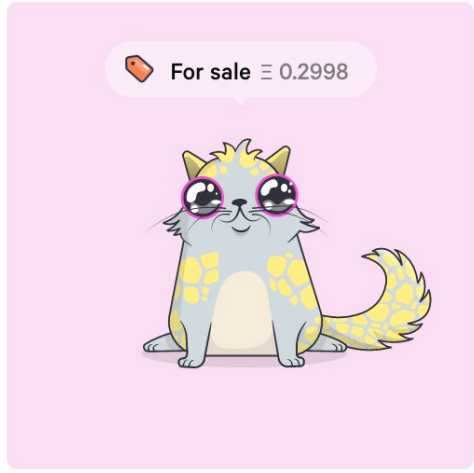
Snappy



Kitty 240603 · Gen 7

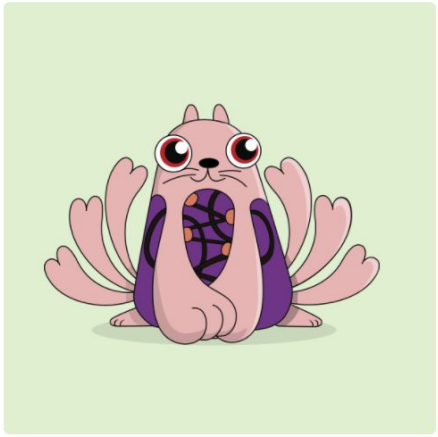
Snappy





TIBA

Kitiovanni
Fancy
4d 3h 57m 47s left



Find a Kitiovanni

Hunter
Fancy
1137 total

Find a Hunter

Vince
Fancy
1420 total

Find a Vince

Zelig
Fancy
504 total

Find a Zelig

Billie
Fancy
1259 total

Find a Billie

Bodhi
Fancy
612 total

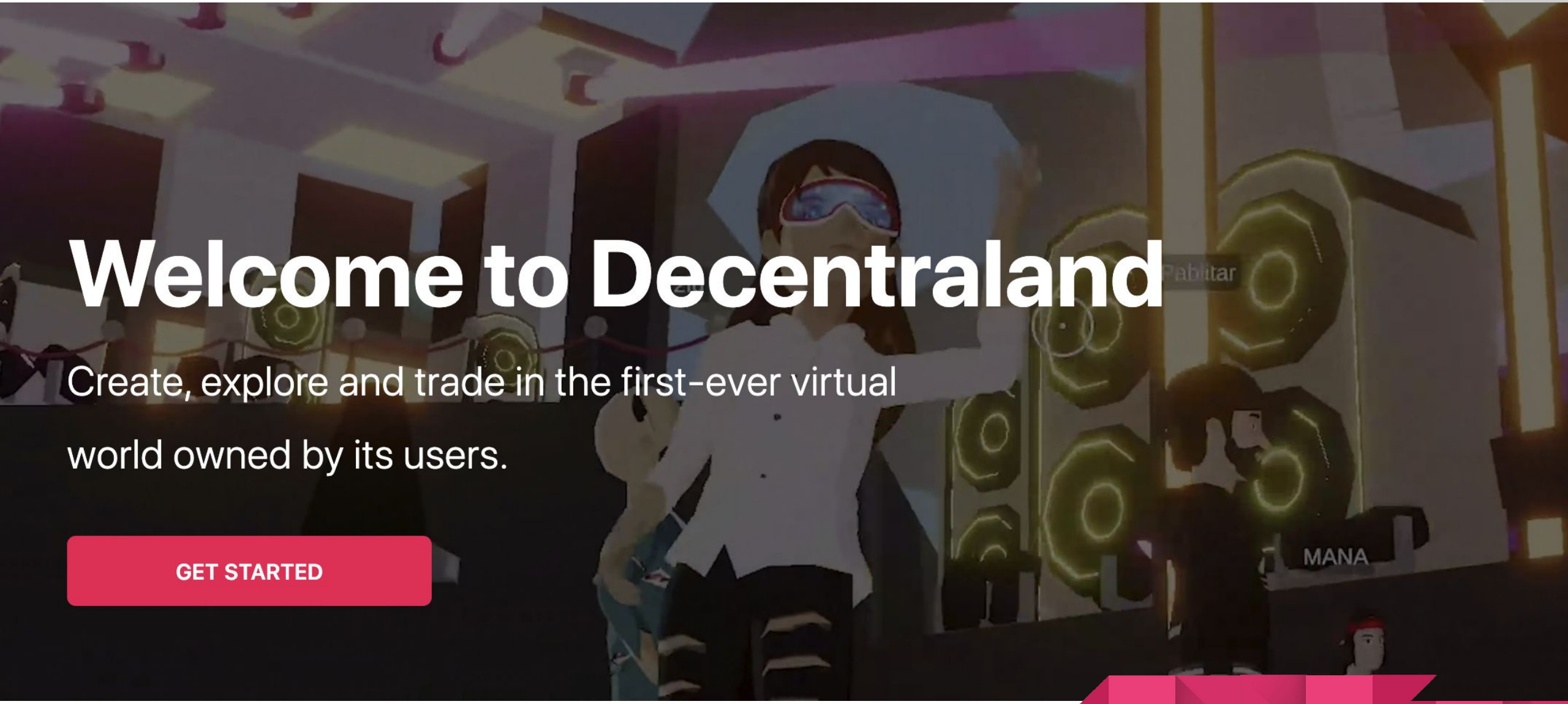
TIBA

Dapp example: Decentraland

- Decentraland is a virtual world owned by its users
- *"The finite, traversable, 3D virtual space within Decentraland is called LAND, a non-fungible digital asset maintained in an Ethereum smart contract. Land is divided into parcels that are identified by cartesian coordinates (x,y). These parcels are permanently owned by members of the community and are purchased using MANA, Decentraland's cryptocurrency token. This gives users full control over the environments and applications that they create, which can range from anything like static 3D scenes to more interactive applications or games."*

https://docs.decentraland.org/decentraland/introduction

TIBA

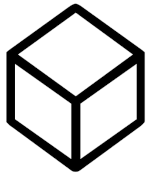

Welcome to Decentraland
Create, explore and trade in the first-ever virtual world owned by its users.
GET STARTED
MANA

TIBA

Contents

- What is Ethereum?
- Brief history of Ethereum
- What are dapps?
- **How do dapps work?**
- Who controls Ethereum?

TIBA



How do dapps work?

TIBA

Smart contracts

In the 1990s, cryptographer Nick Szabo coined the term and defined it as "a set of promises, specified in digital form, including protocols within which the parties perform on the other promises." In the context of Ethereum, the term is actually a bit of a misnomer, given that Ethereum smart contracts are neither smart nor legal contracts, but the term has stuck.

TIBA

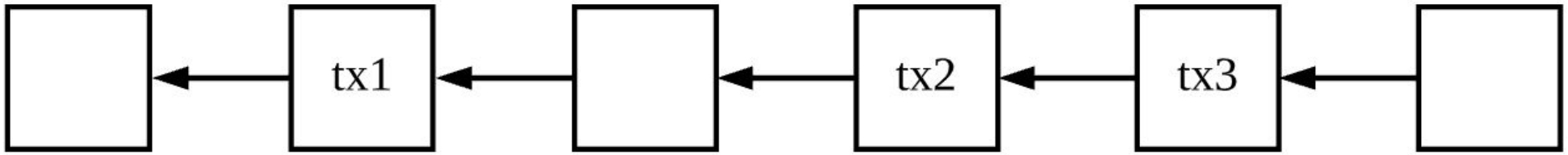
Smart contracts

While the word "contract" brings to mind legal agreements; in Ethereum "smart contracts" are just pieces of code that run on the blockchain and are guaranteed to produce the same result for everyone who runs them.

Smart contracts are not legal contracts

https://docs.ethhub.io/ethereum-basics/what-is-ethereum/#what-are-smart-contracts-and-decentralized-applications

Transactions in Bitcoin

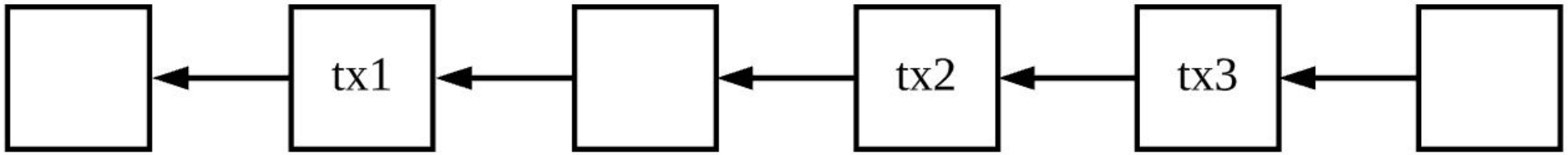


tx1: Send 2 BTC from Bob to Alice.

tx2: Send 1.22 BTC from Alice to Claire.

tx3: Send 4 BTC to Bob if both Alice and Claire agree.

Transactions in Ethereum



tx1: Send 2 ETH from Bob to Alice.

tx2: Send CryptoKittie #5315 from Alice to Claire.

tx3: Register domain name thu-tiba.org for IP address ...

TIBA

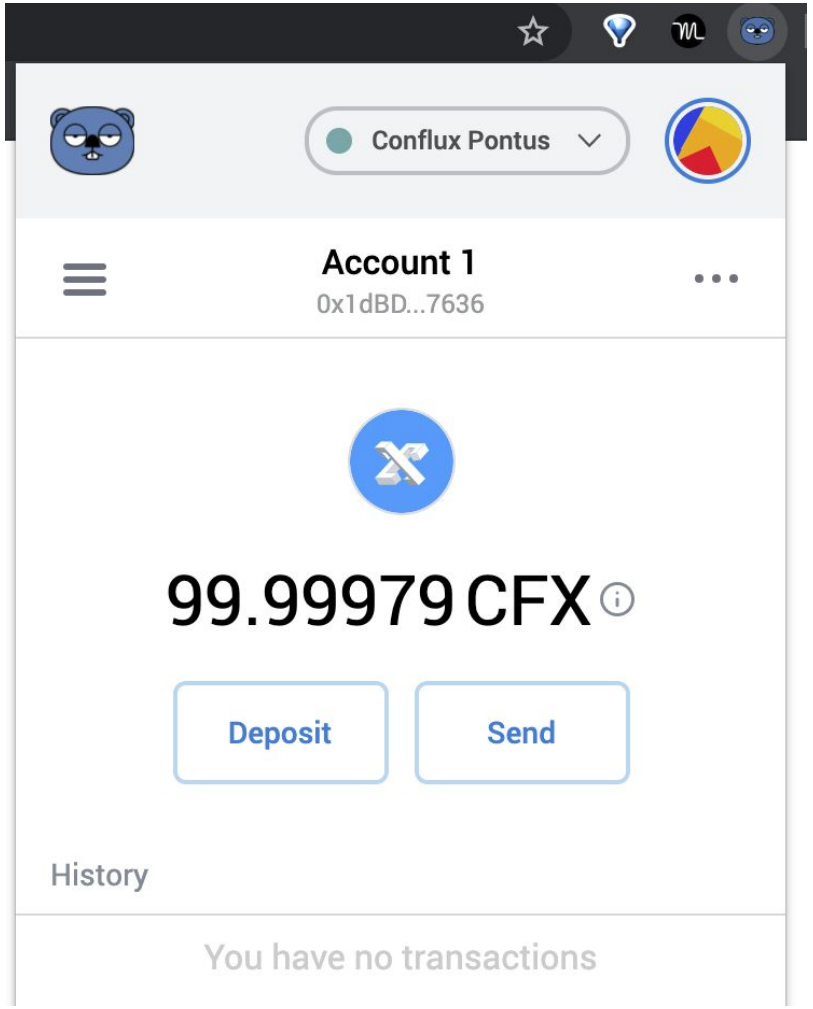
How to interact with dapps?

- The app frontend (which can be a normal website) creates a transactions and asks your wallet to sign it.
- Your wallet (e.g. MetaMask) signs the transaction and submits it to the network.
- The dapp state is updated accordingly.

No one can make changes on your behalf. You are the only person who can sign with your identity.

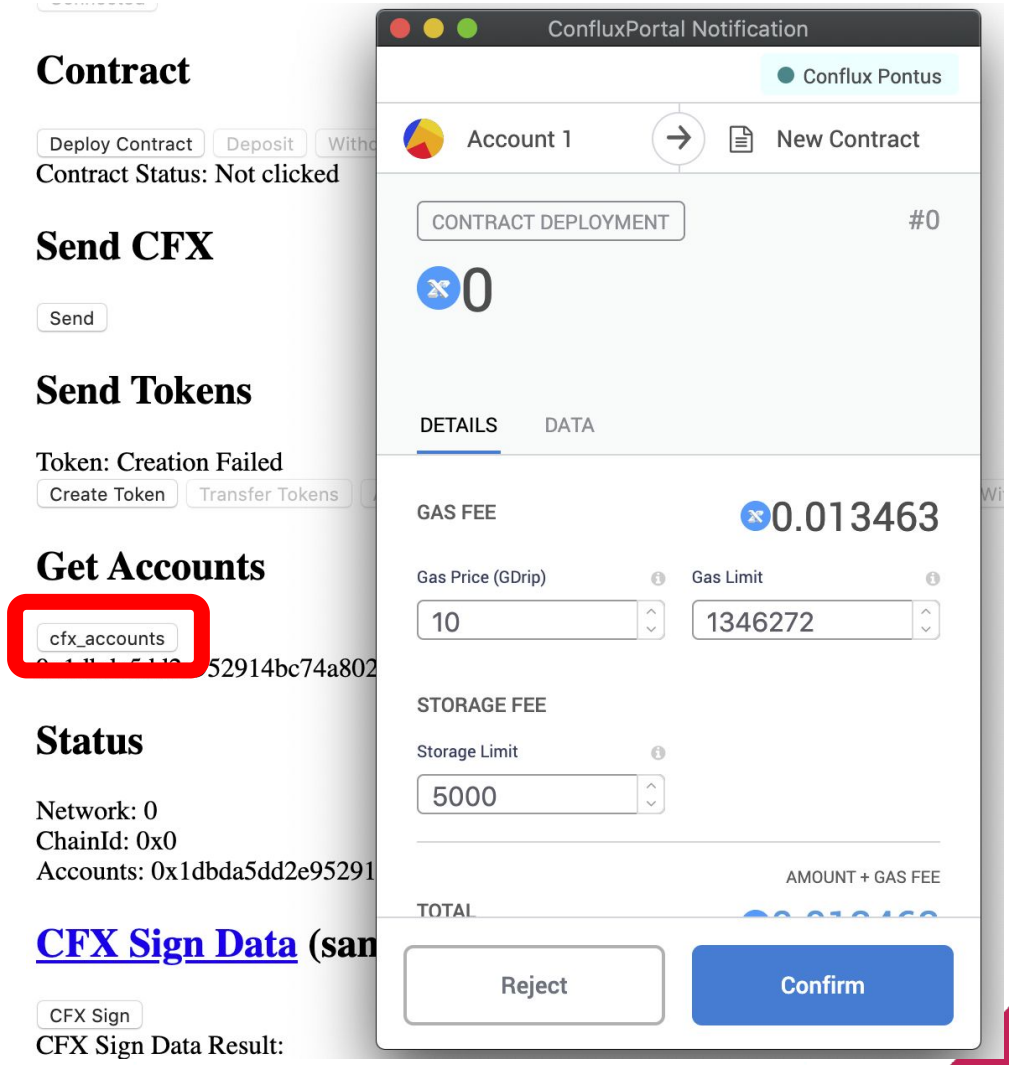
TIBA

How to interact with dapps?



TIBA

How to interact with dapps?

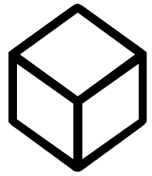


TIBA

Contents

- What is Ethereum?
- Brief history of Ethereum
- What are dapps?
- How do dapps work?
- **Who controls Ethereum?**

TIBA

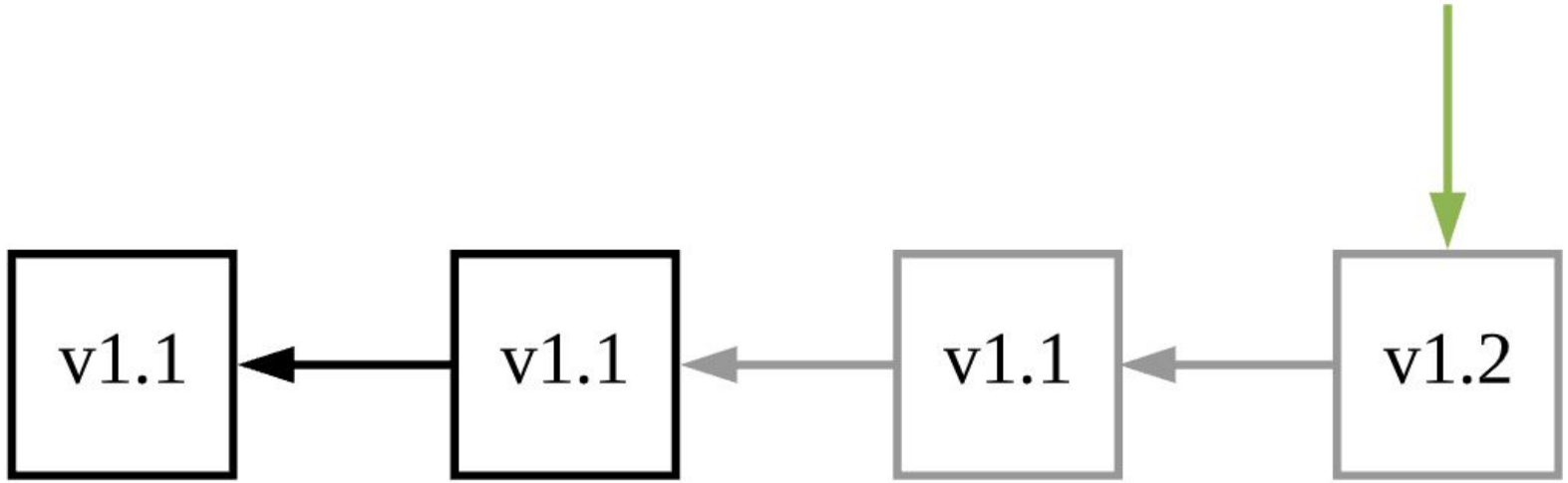


Who controls Ethereum?

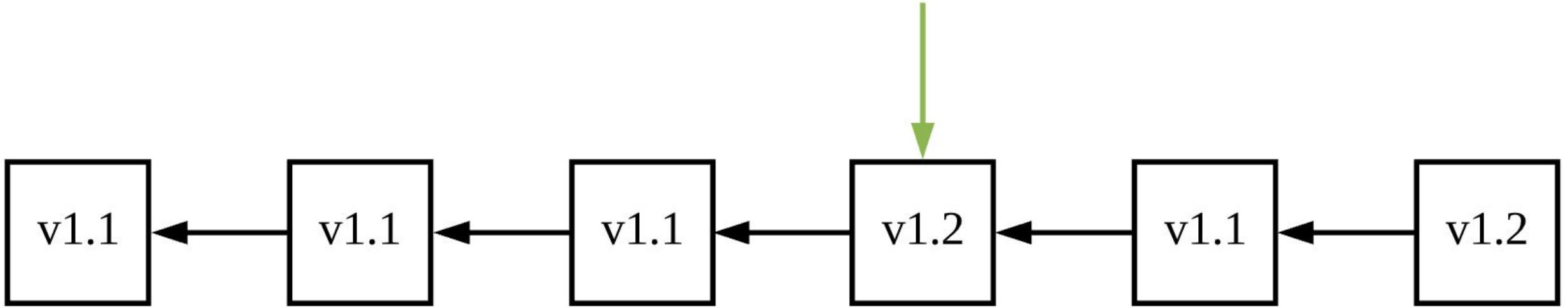
Blockchain governance

- Just like Bitcoin, Ethereum is updated using soft and hard forks.
- Soft forks can be bugfixes and minor updates that do not change the protocol.
- Hard forks are major protocol changes.
  - Change mining difficulty
  - Change block size
  - Change token issuance

Blockchain governance - soft forks

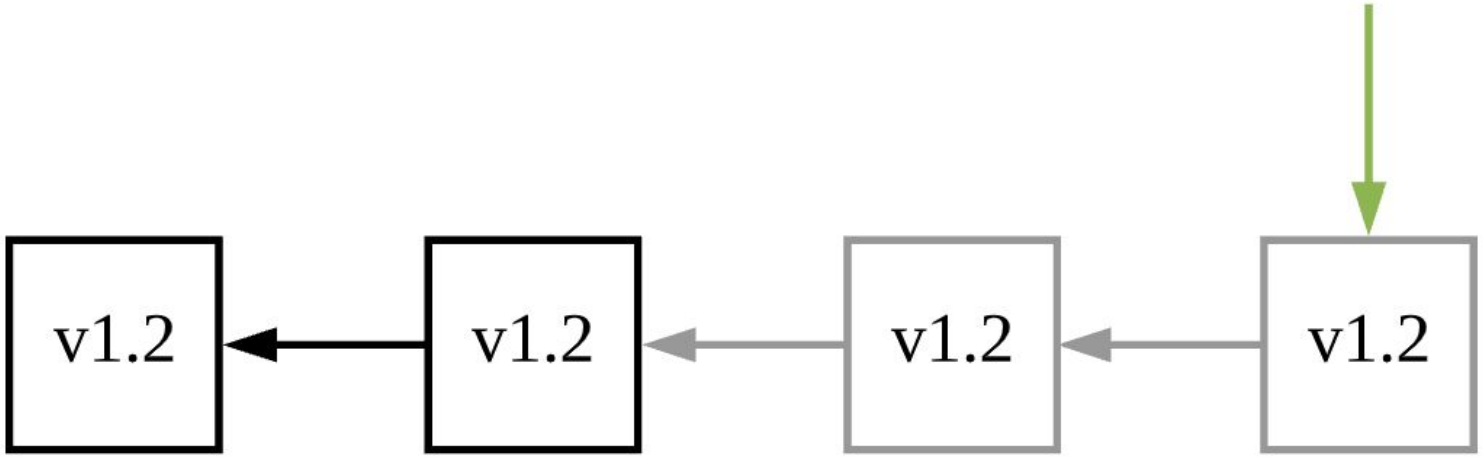


Blockchain governance - soft forks

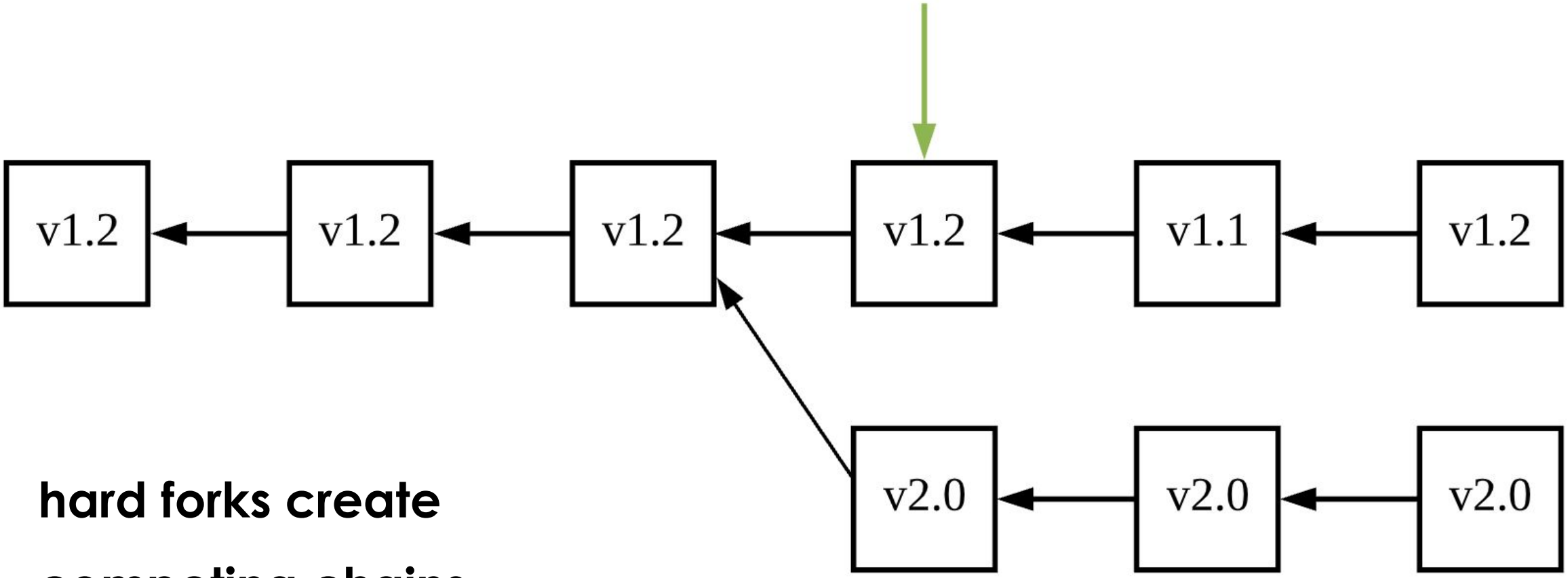


with soft forks, different node versions can mine on the same chain

Blockchain governance - hard forks

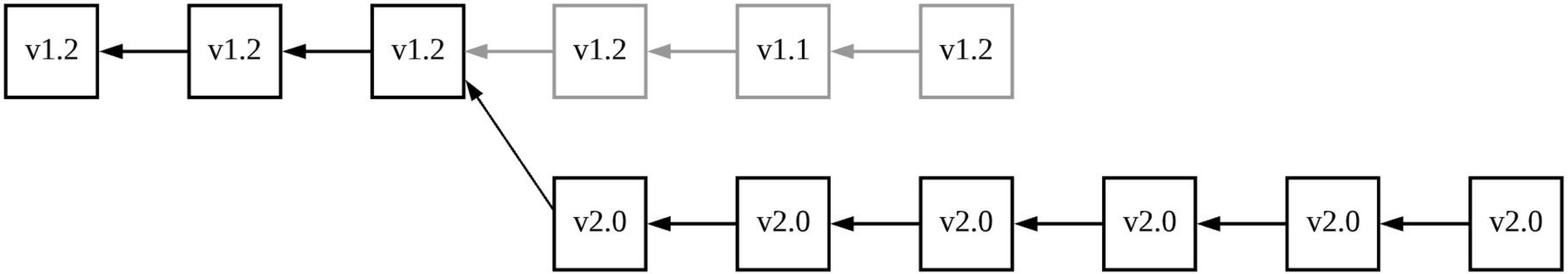


Blockchain governance - hard forks



hard forks create competing chains

Blockchain governance - hard forks



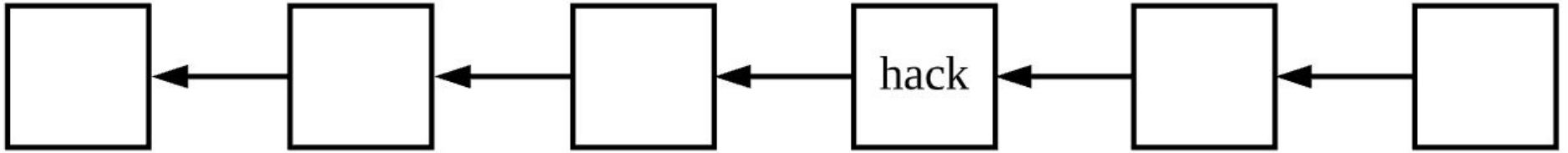
usually, one of the competing forks stays and the other one is abandoned

The DAO attack

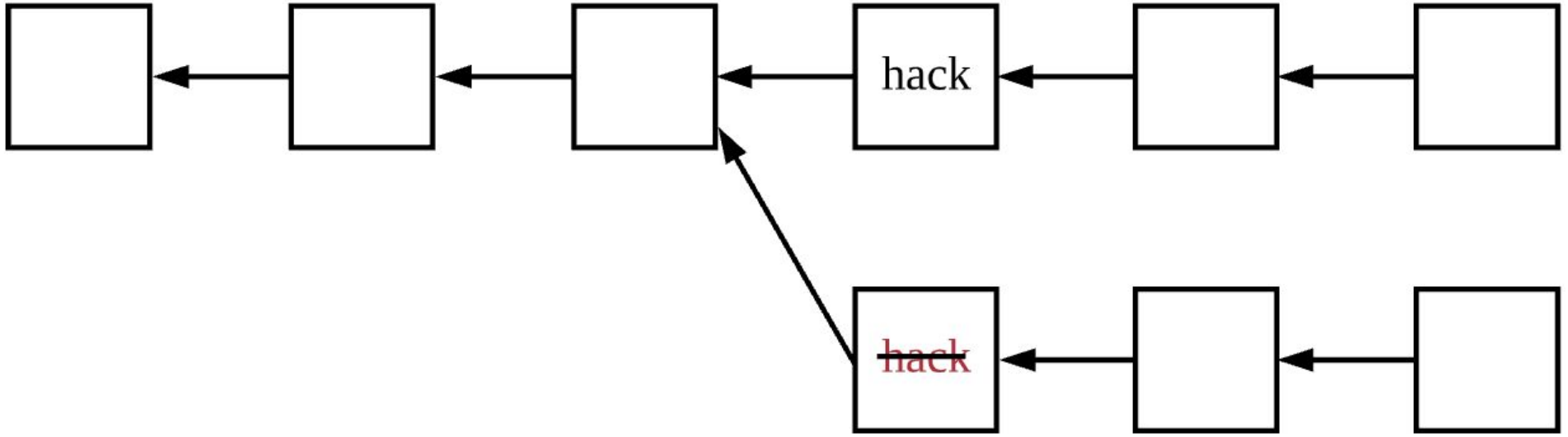
- *"... by the end of the funding period, The DAO was the largest crowdfunding in history, having raised over $150m from more than 11,000 enthusiastic members."*
- *"By Saturday, 18th June, the attacker managed to drain more than 3.6m ether into a "child DAO" that has the same structure as The DAO. The price of ether dropped from over $20 to under $13."*

https://www.coindesk.com/understanding-dao-hack-journalists

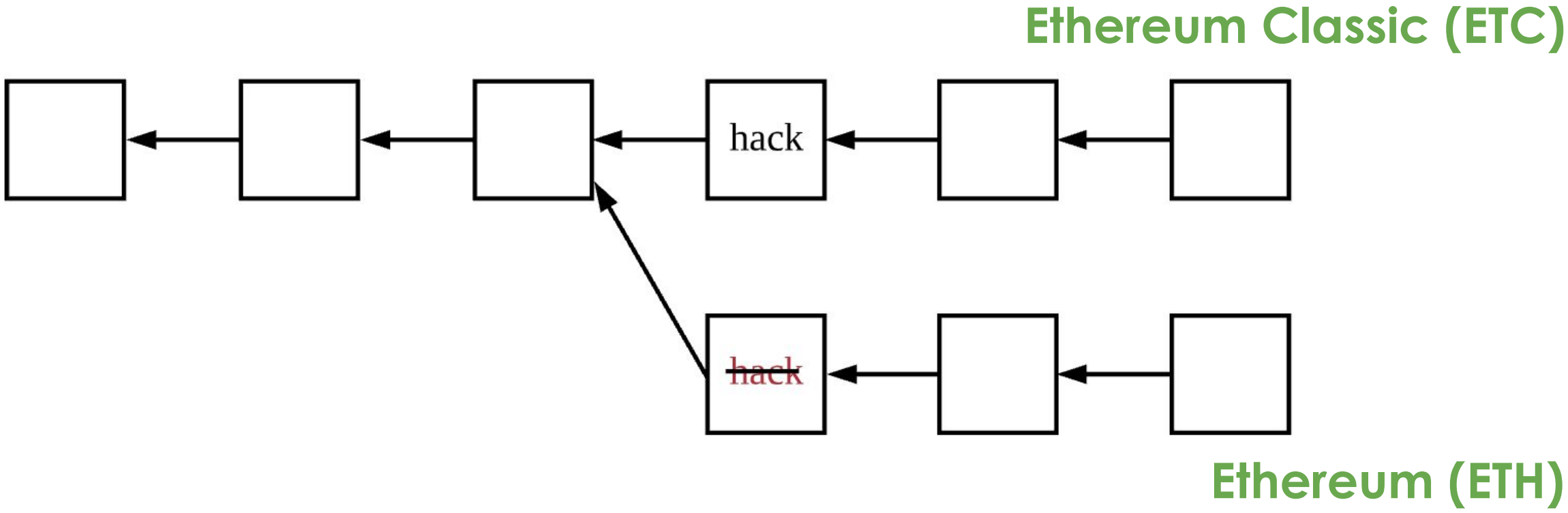
The DAO attack



The DAO attack



The DAO attack



TIBA

Questions?