CSCI-UA.9480
Introduction to Computer Security

Session 1.7

Cryptocurrencies, Blockchains, Smart Contracts

Prof. Nadim Kobeissi

Merkle Trees and Hash Chains

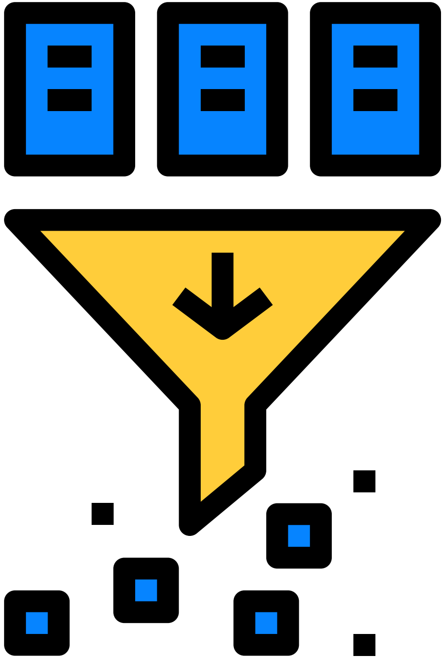
1.7a

Reminder: what's a hash function?

Simple!

- A hash function `H(x)` takes some input x which can be of any length...
- And produces some value y which is of a fixed length (usually 128, 256 , 384 or 512 bits.)

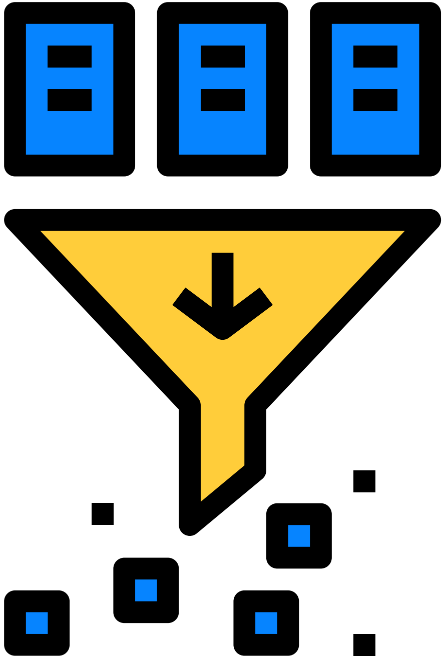
$$H(x) \rightarrow y$$



Reminder: what's a *secure* hash function?

A hash function, but…

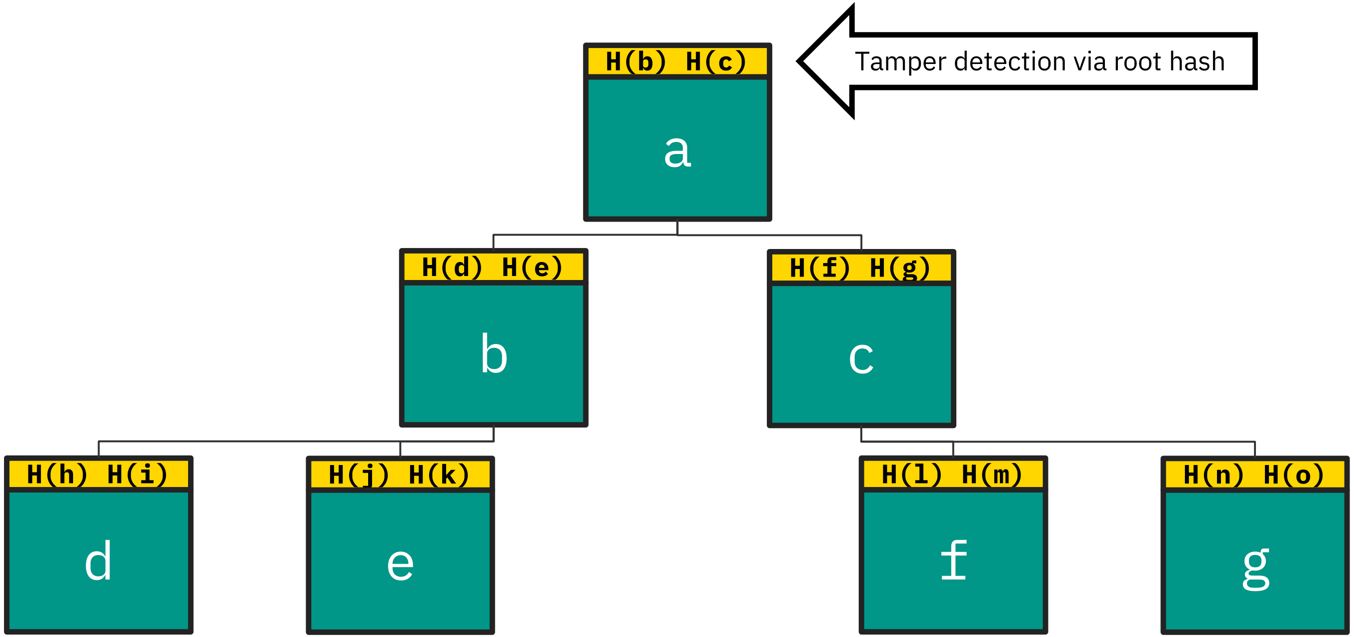
- Anyone with x can calculate y very easily…
- Going from y back to x is impossible.
- y reveals no information about x (pseudorandom, uniformly chosen.)
- Finding an x′ that also maps to y is extremely improbable.



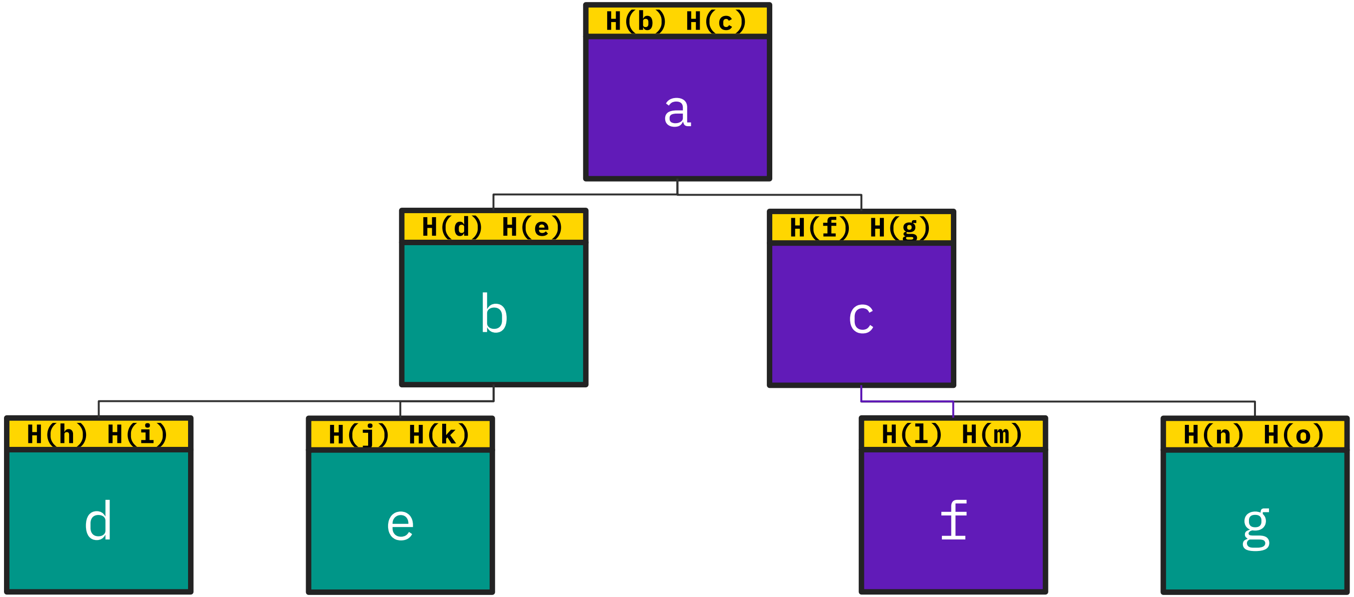
BLAKE2s(“tomat**o**”) =
5cc655abb6feebac1ba4c24d4b06461a

BLAKE2s(“tomat**e**”) =
75e6179a12dd9303ecdc877aeb6d50ab

Merkle Trees (1979.)



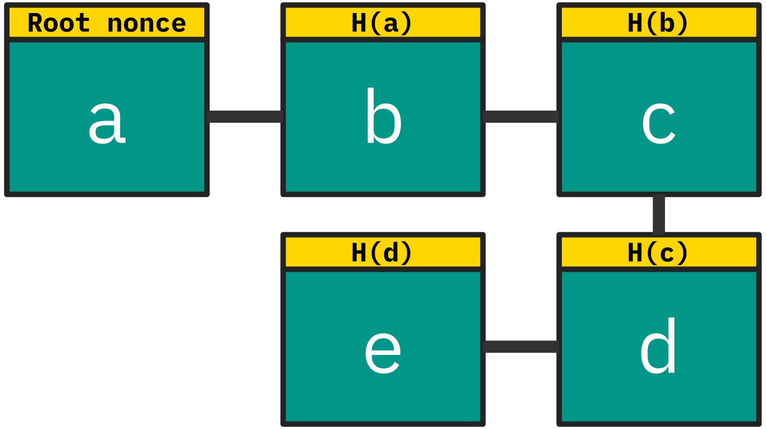
Proof of membership via Merkle trees.



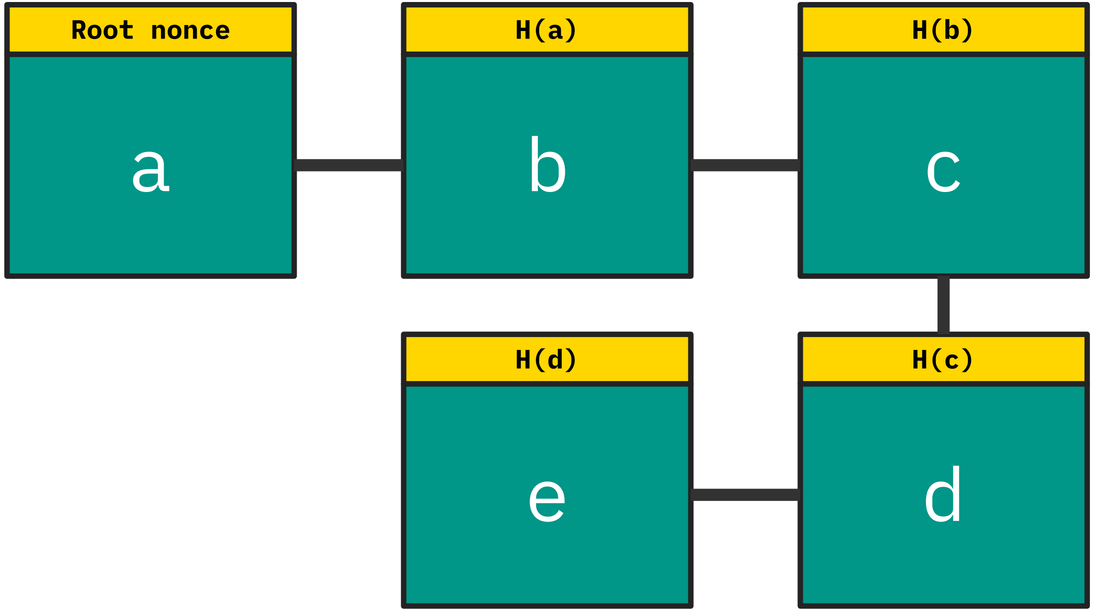
What’s a block chain?

A tamper-evident log.

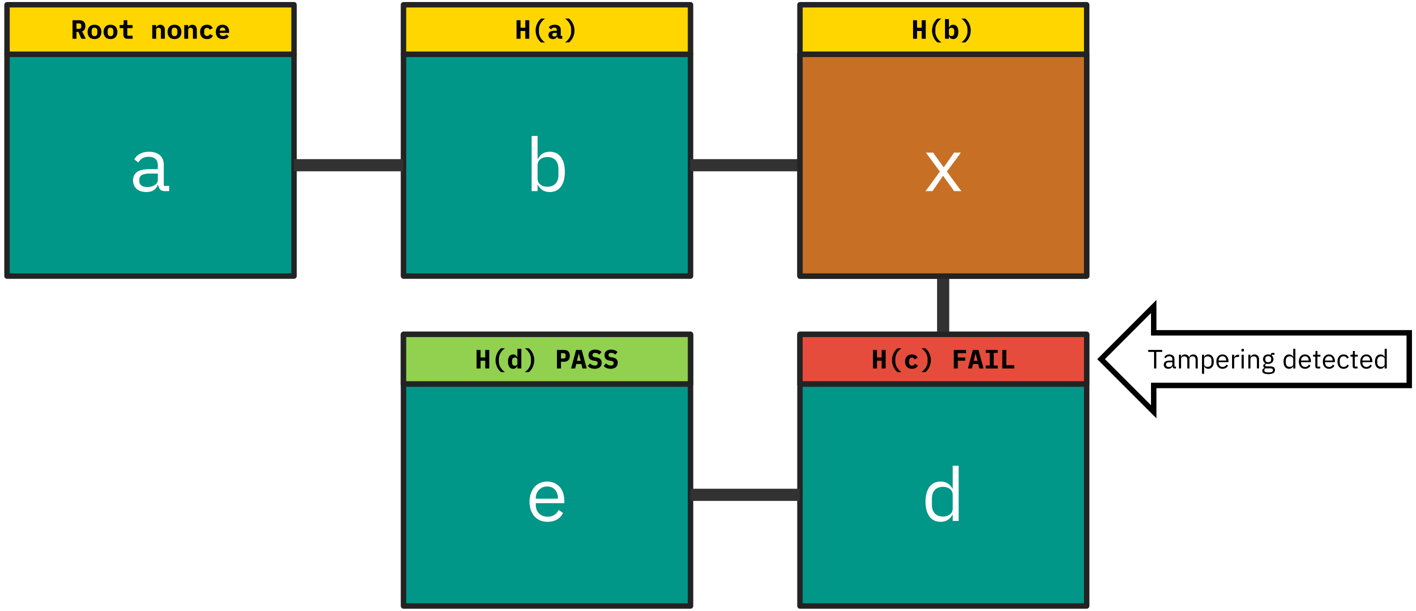
- A log data structure where we can append data to the end of the log…
- …but if someone alters data earlier in the log, we can detect it.



What’s a block chain?

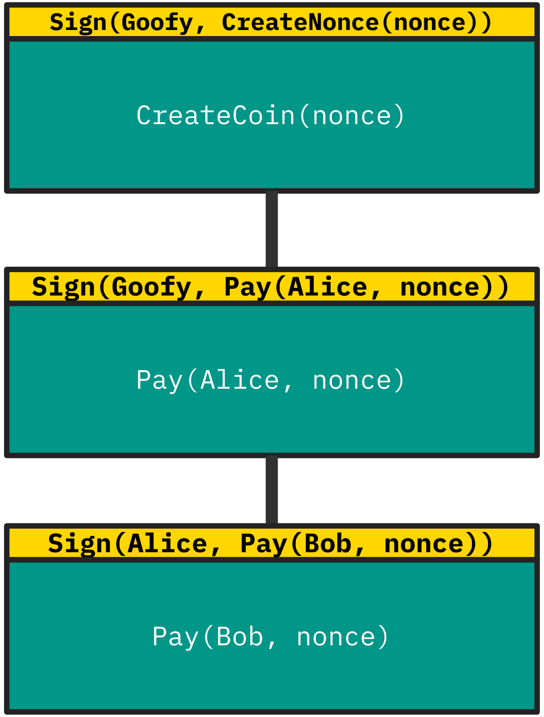


What’s a block chain?



Introducing GoofyCoin.

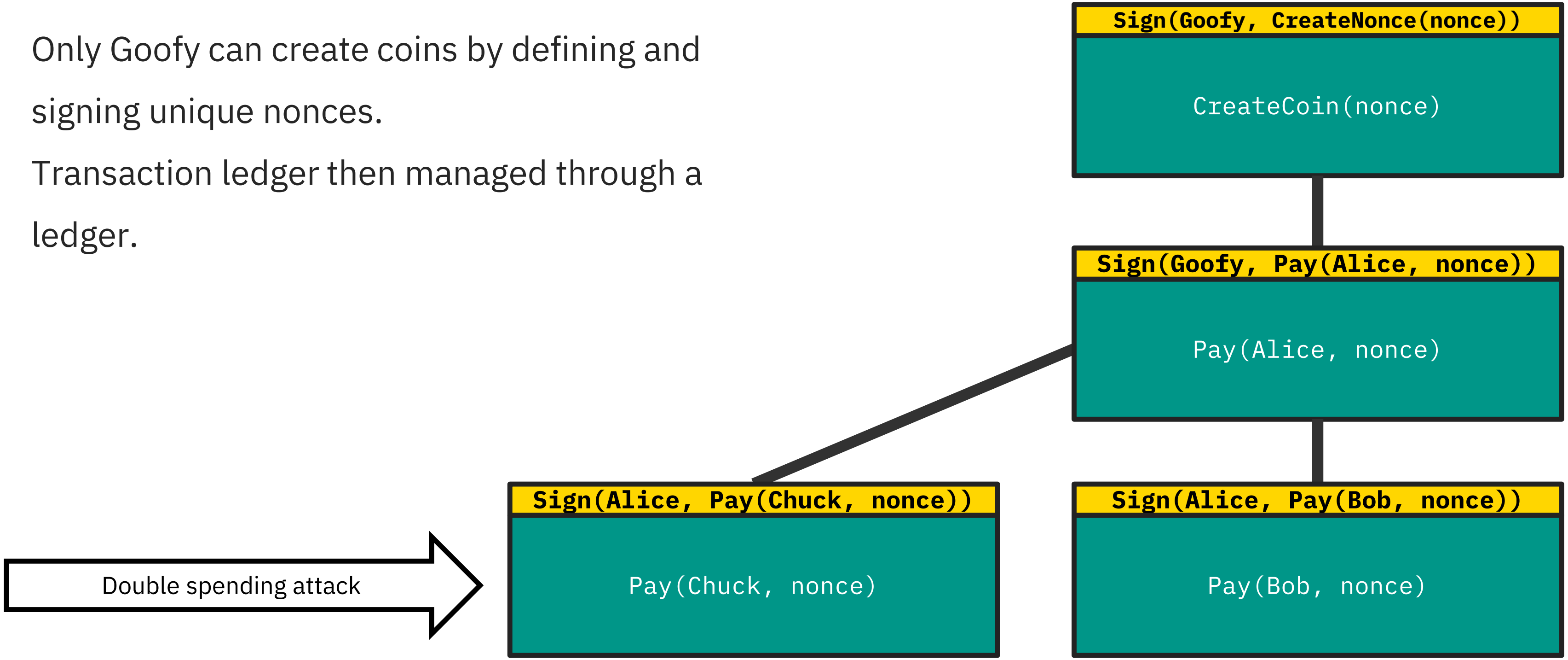
- Only Goofy can create coins by defining and signing unique nonces.
- Transaction ledger then managed through a ledger.



Sign(Goofy, CreateNonce(nonce))
CreateCoin(nonce)
Sign(Goofy, Pay(Alice, nonce))
Pay(Alice, nonce)
Sign(Alice, Pay(Bob, nonce))
Pay(Bob, nonce)

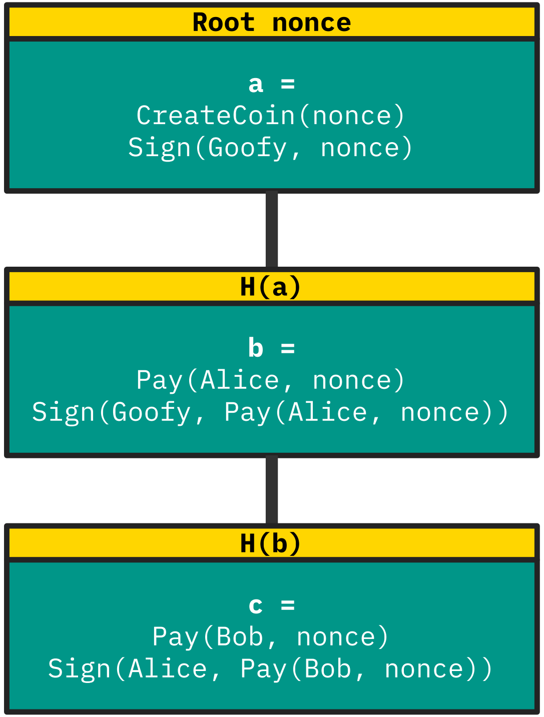
Introducing GoofyCoin.

- Only Goofy can create coins by defining and signing unique nonces.
- Transaction ledger then managed through a ledger.


Sign(Goofy, CreateNonce(nonce))
CreateCoin(nonce)
Sign(Goofy, Pay(Alice, nonce))
Pay(Alice, nonce)
Double spending attack
Sign(Alice, Pay(Chuck, nonce))
Pay(Chuck, nonce)
Sign(Alice, Pay(Bob, nonce))
Pay(Bob, nonce)

Fixing GoofyCoin.

- Only Goofy can create coins by defining and signing unique nonces.
- Transaction ledger then managed through a ~~ledger~~ block chain.
- We can verify ledger integrity by traversing the chain.



Bitcoin

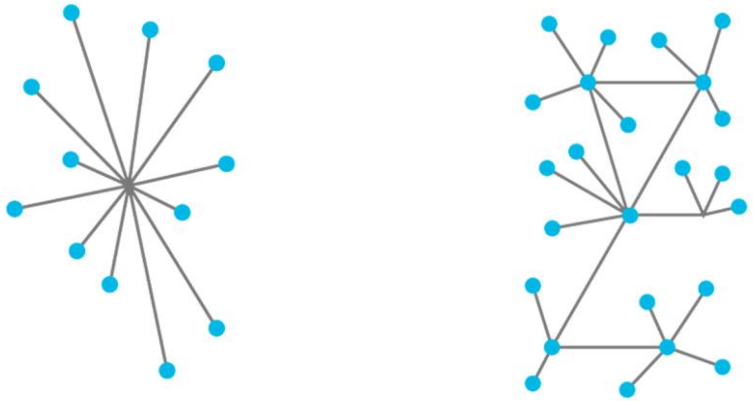
1.7b

Bitcoin: origins.

- Bitcoin paper published by Satoshi Nakamoto in October 2008, software in January 2009.
- Huge and unsuccessful media hunt to identify its creator.

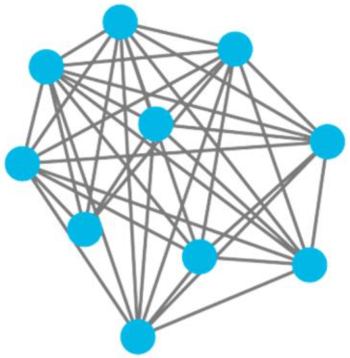
Looking at traditional banking...

- Banks are a centralized consensus model.
- International banking is, at best, decentralized consensus with some central nodes.



Bitcoin: decentralized consensus.

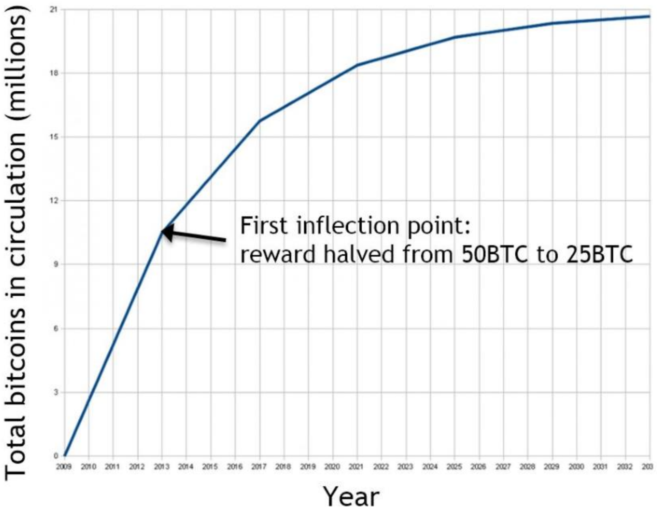
- Bitcoin's block chain ledger achieves *decentralized consensus*, allowing the currency's history and value to be determined even if some parties are dishonest.
- Identities can simply be a public key.



Bitcoin: incentives.

- *Block rewards:* “mining” a new block on the block chain grants you a number of Bitcoins as a reward (which decreases over time.)
- *Transaction fees:* a party sending a transaction can stipulate a reward for those who mine the block containing that transaction.

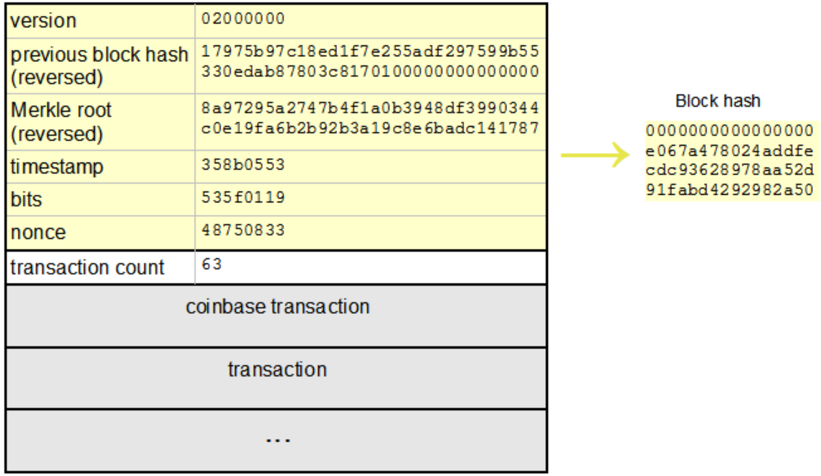
New blocks must achieve consensus for the reward to be claimed.



Bitcoin: proof of work.

Blocks are valuable because mining them is hard.

- Find a value such that the hash of your value, the previous hash, and the list of transactions in this block is below some target value.
- Since hash outputs are pseudorandom and unpredictable, getting that many zeroes is measurably hard.



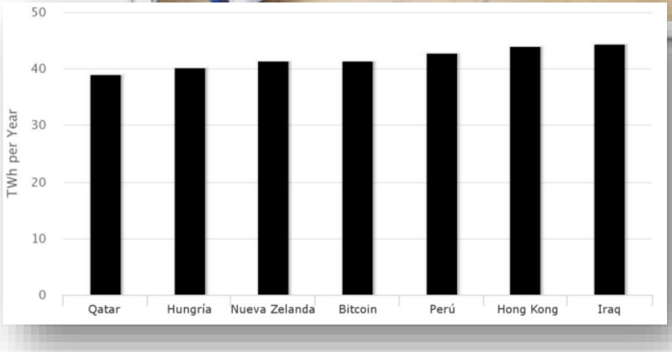
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50

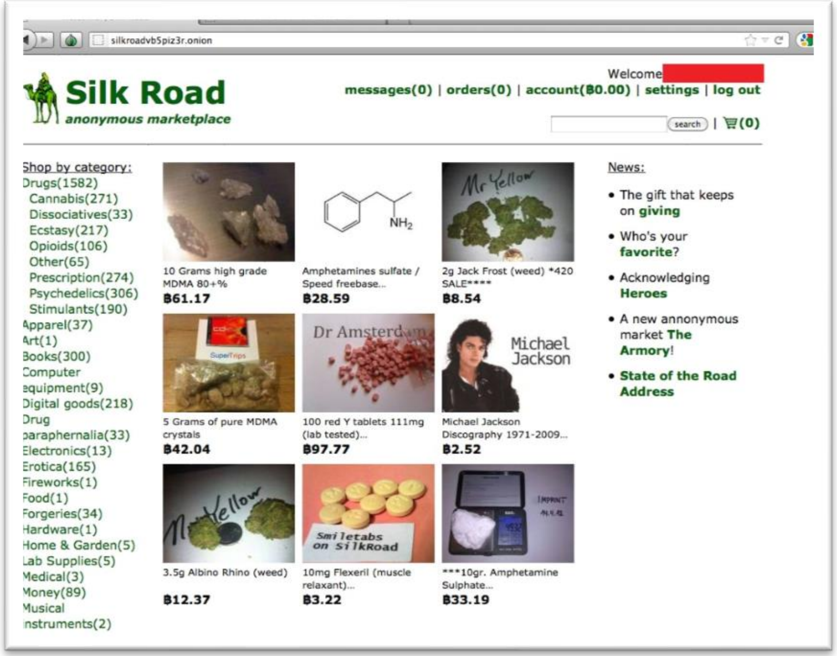
Bitcoin: energy consumption, mining power.

- Currently, Bitcoin consumes as much energy as all of Ireland.
- Mining power is centralized in gigantic “Bitcoin farms”, who use hundreds of GPUs to hash very quickly.
- Buying a GPU has become very expensive!😠



Bitcoin: an entire industry and economy.

- Many services, some highly usable (Coinbase) for managing your portfolio.
- Dedicated hardware, Bitcoin trading houses, exchanges, conferences...
- Increasing regulation.



silkroadvb5piz3r.onion

Silk Road

anonymous marketplace

Welcome [redacted]

messages(0) | orders(0) | account(฿0.00) | settings | log out

search | (0)

Shop by category:

Drugs(1582)
Cannabis(271)
Dissociatives(33)
Ecstasy(217)
Opioids(106)
Other(65)
Prescription(274)
Psychedelics(306)
Stimulants(190)
Apparel(37)
Art(1)
Books(300)
Computer equipment(9)
Digital goods(218)
Drug paraphernalia(33)
Electronics(13)
Erotica(165)
Fireworks(1)
Food(1)
Forgeries(34)
Hardware(1)
Home & Garden(5)
Lab Supplies(5)
Medical(3)
Money(89)
Musical instruments(2)

10 Grams high grade MDMA 80+%
฿61.17

Amphetamines sulfate / Speed freebase...
฿28.59

2g Jack Frost (weed) *420 SALE****
฿8.54

5 Grams of pure MDMA crystals
฿42.04

100 red Y tablets 111mg (lab tested)...
฿97.77

Michael Jackson Discography 1971-2009...
฿2.52

3.5g Albino Rhino (weed)
฿12.37

10mg Flexeril (muscle relaxant)...
฿3.22

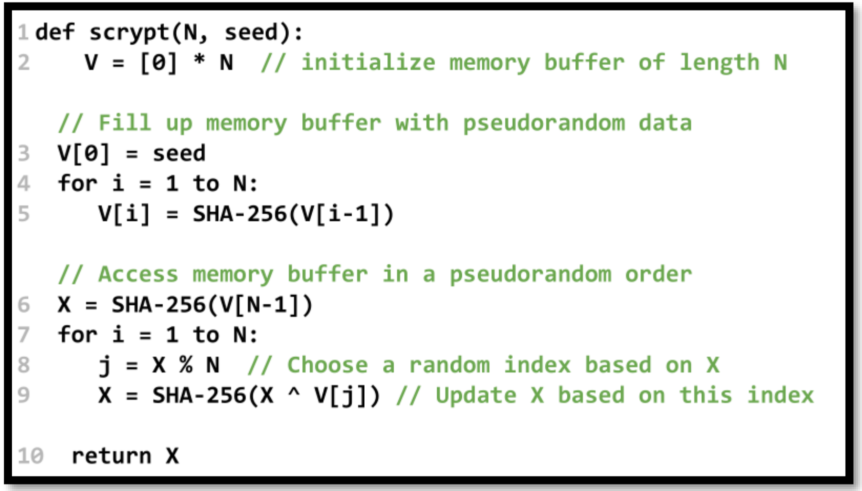
***10gr. Amphetamine Sulphate...
฿33.19

News:

- The gift that keeps on **giving**
- Who's your **favorite**?
- Acknowledging **Heroes**
- A new annonymous market **The Armory**!
- **State of the Road Address**

Bitcoin: alternative mining puzzles.

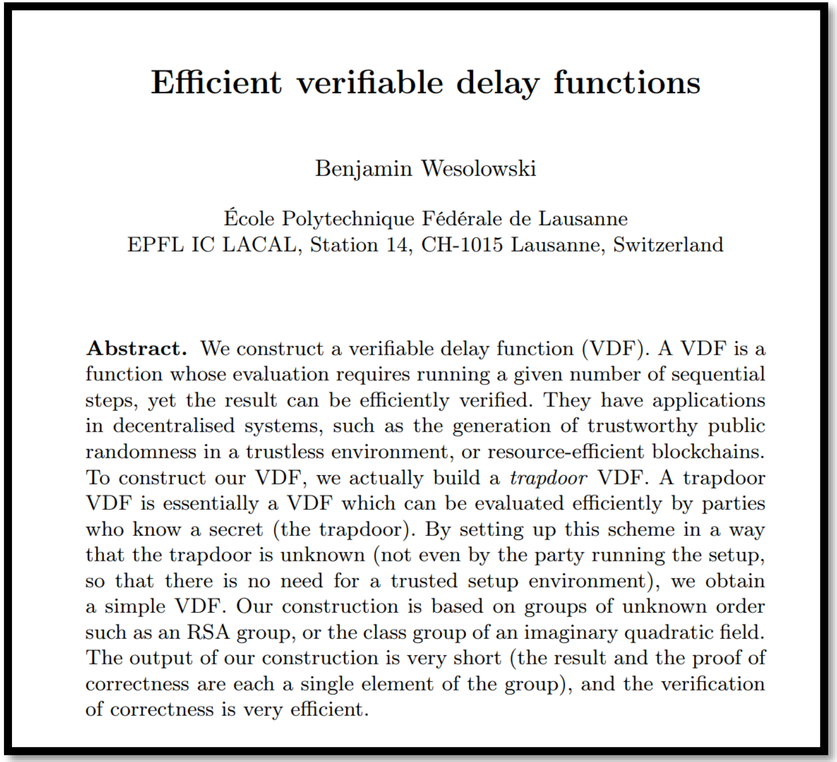
- GPU resistant, ASIC resistant, “memory-hard” (scrypt or Equihash.)



```
def scrypt(N, seed):
   V = [0] * N  // initialize memory buffer of length N

  // Fill up memory buffer with pseudorandom data
  V[0] = seed
  for i = 1 to N:
    V[i] = SHA-256(V[i-1])

  // Access memory buffer in a pseudorandom order
  X = SHA-256(V[N-1])
  for i = 1 to N:
    j = X % N  // Choose a random index based on X
    X = SHA-256(X ^ V[j]) // Update X based on this index

  return X
```

Bitcoin: VDFs, new alternative puzzle.

- *Verifiable Delay Functions*: evaluation requires sequential (non-parallelizable steps), but result can be efficiently verified.
  - Breakthrough research on efficient VDFs to be published at EUROCRYPT 2019.
- Difference with scrypt:
  - scrypt is difficult to compute, difficult to verify.
  - VDF is difficult to compute, easy to verify.



Efficient verifiable delay functions

Benjamin Wesolowski

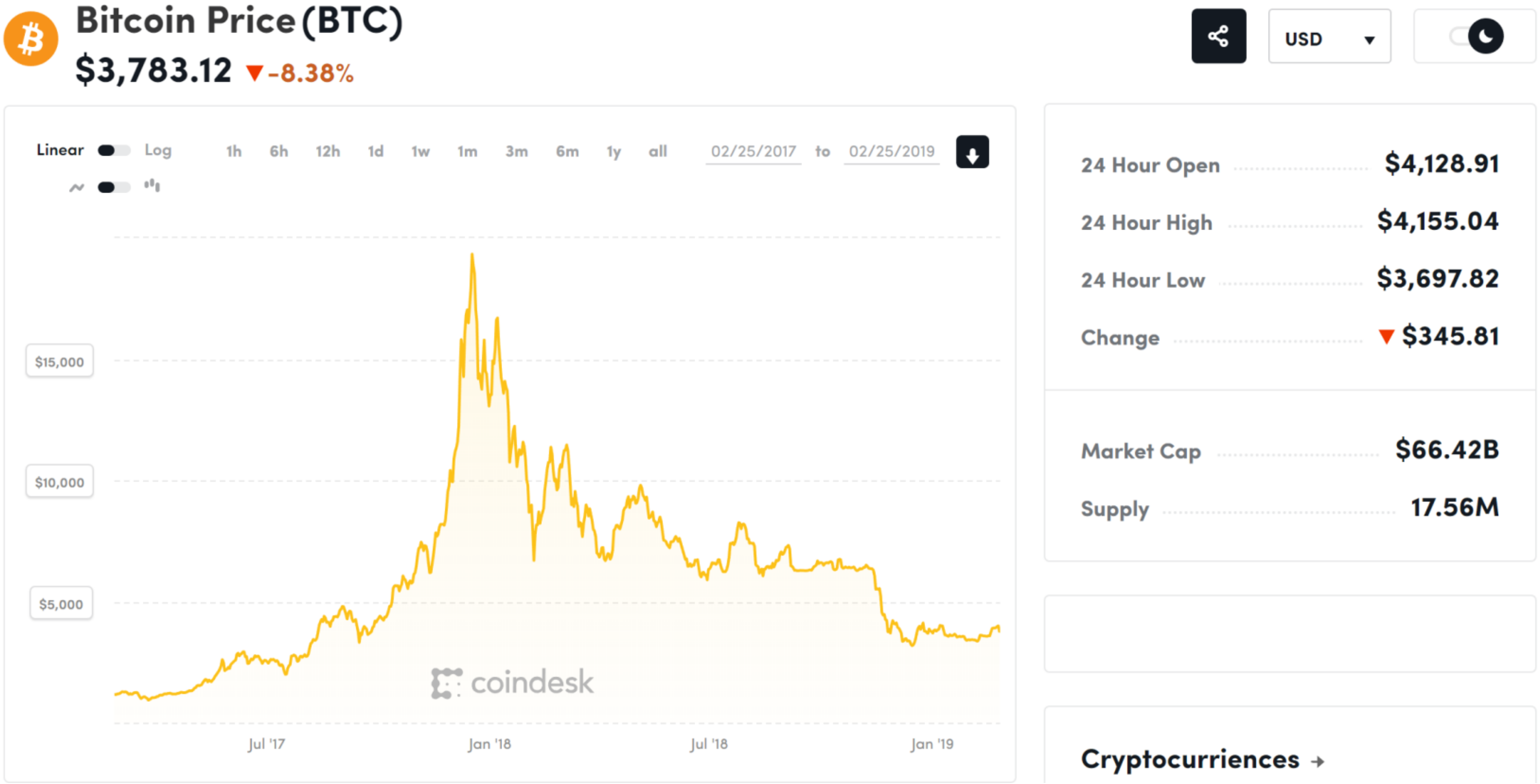
École Polytechnique Fédérale de Lausanne
EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland

Abstract. We construct a verifiable delay function (VDF). A VDF is a function whose evaluation requires running a given number of sequential steps, yet the result can be efficiently verified. They have applications in decentralised systems, such as the generation of trustworthy public randomness in a trustless environment, or resource-efficient blockchains. To construct our VDF, we actually build a *trapdoor* VDF. A trapdoor VDF is essentially a VDF which can be evaluated efficiently by parties who know a secret (the trapdoor). By setting up this scheme in a way that the trapdoor is unknown (not even by the party running the setup, so that there is no need for a trusted setup environment), we obtain a simple VDF. Our construction is based on groups of unknown order such as an RSA group, or the class group of an imaginary quadratic field. The output of our construction is very short (the result and the proof of correctness are each a single element of the group), and the verification of correctness is very efficient.

Bitcoin: usability and anonymity.

- Bitcoin is not anonymous: coins have a history, transactions can be linked…
- Still difficult to use for day-to-day transactions.
- More used as an investment asset like gold or steel.

Bitcoin to USD conversion rate.

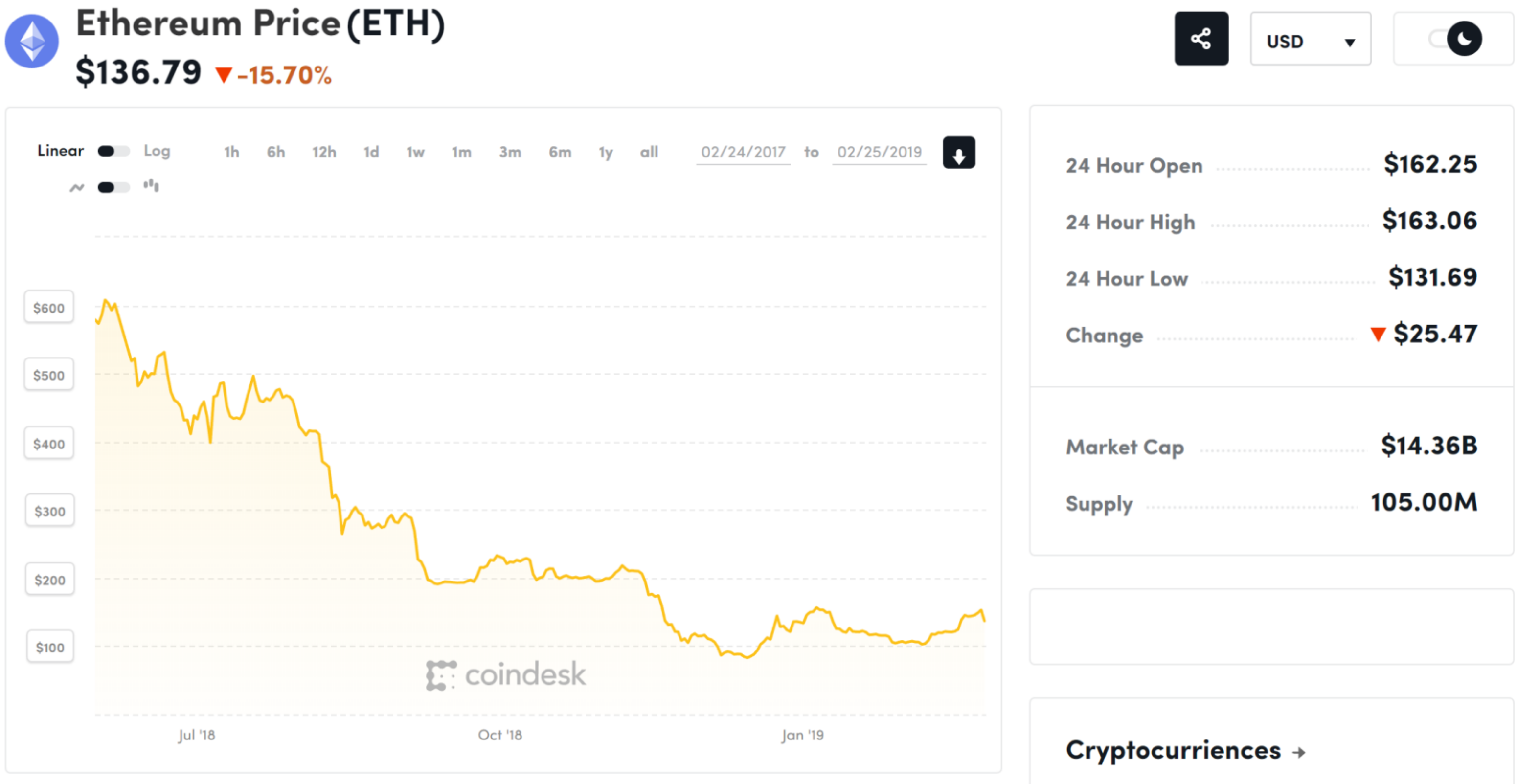


Bitcoin Price (BTC)

$3,783.12 ▼-8.38%

24 Hour Open	$4,128.91
24 Hour High	$4,155.04
24 Hour Low	$3,697.82
Change	▼ $345.81
Market Cap	$66.42B
Supply	17.56M

Ethereum to USD conversion rate.



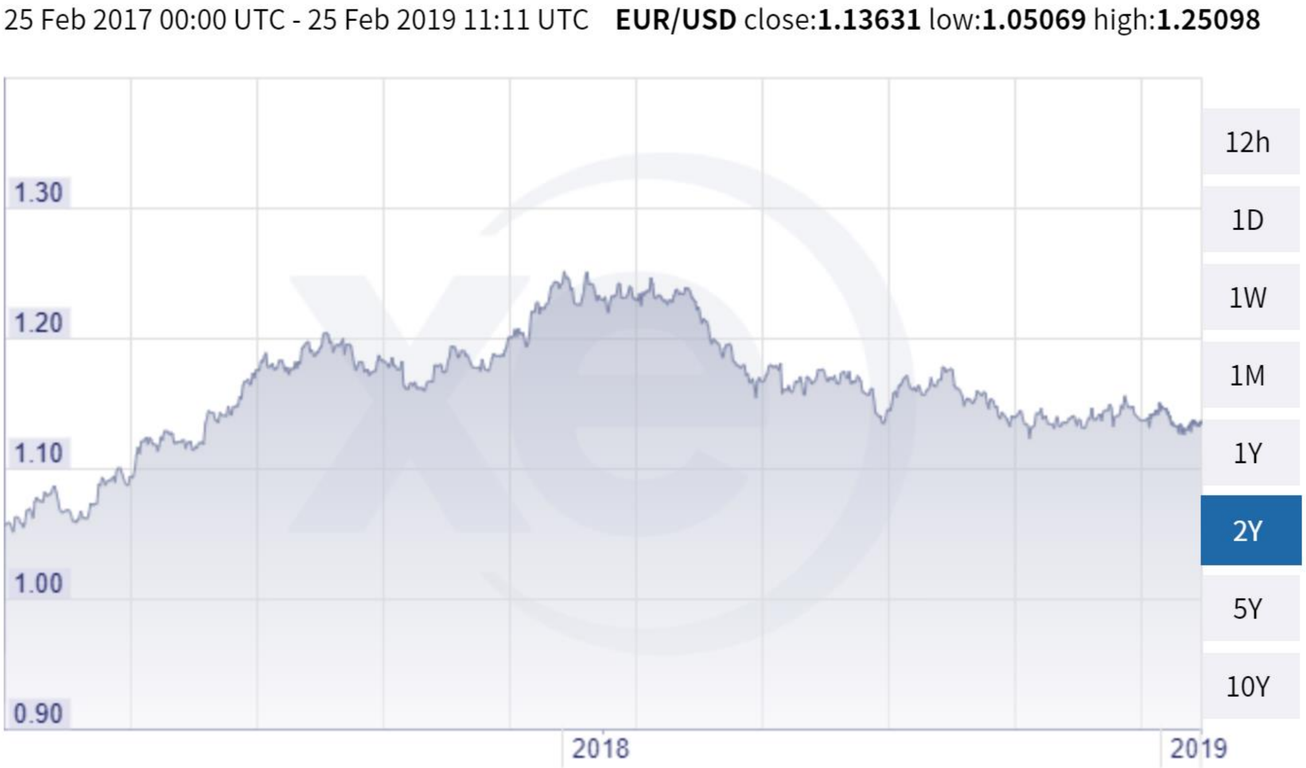
Ethereum Price (ETH)

$136.79 ▼-15.70%

02/24/2017 to 02/25/2019

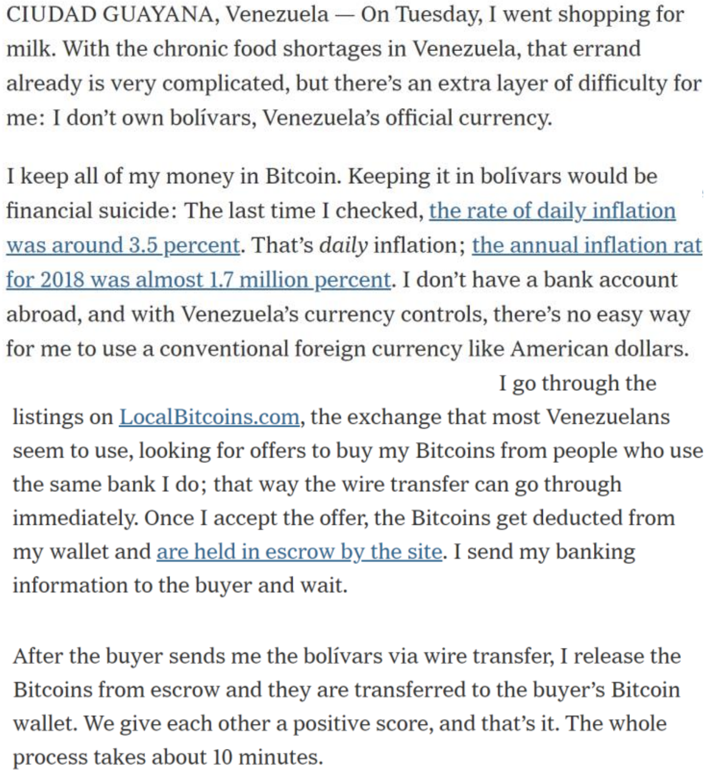
24 Hour Open	$162.25
24 Hour High	$163.06
24 Hour Low	$131.69
Change	▼ $25.47
Market Cap	$14.36B
Supply	105.00M

Euro to USD conversion rate.



25 Feb 2017 00:00 UTC - 25 Feb 2019 11:11 UTC **EUR/USD** close:**1.13631** low:**1.05069** high:**1.25098**

On the other hand…

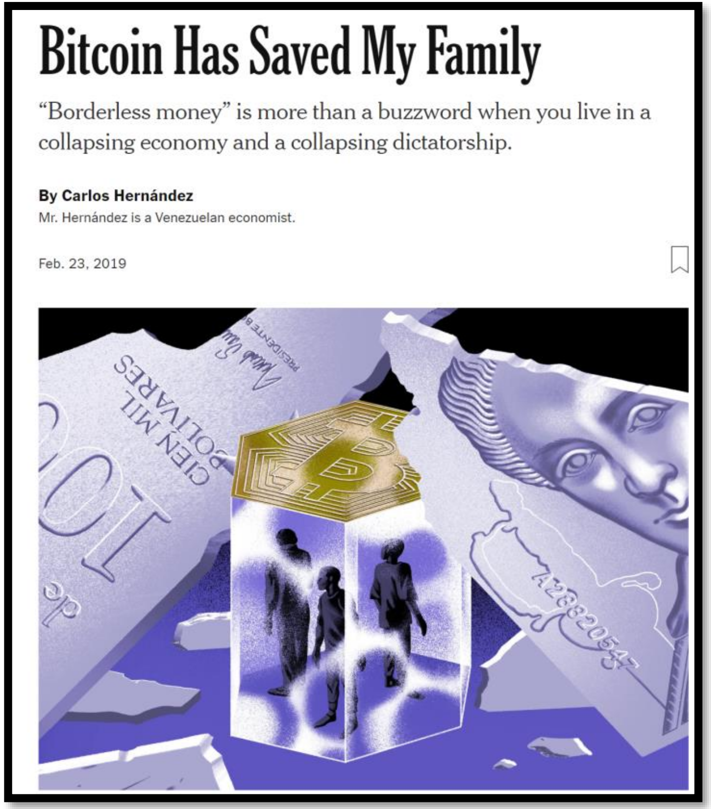


CIUDAD GUAYANA, Venezuela — On Tuesday, I went shopping for milk. With the chronic food shortages in Venezuela, that errand already is very complicated, but there's an extra layer of difficulty for me: I don't own bolívars, Venezuela's official currency.

I keep all of my money in Bitcoin. Keeping it in bolívars would be financial suicide: The last time I checked, the rate of daily inflation was around 3.5 percent. That's *daily* inflation; the annual inflation rat for 2018 was almost 1.7 million percent. I don't have a bank account abroad, and with Venezuela's currency controls, there's no easy way for me to use a conventional foreign currency like American dollars.

I go through the listings on LocalBitcoins.com, the exchange that most Venezuelans seem to use, looking for offers to buy my Bitcoins from people who use the same bank I do; that way the wire transfer can go through immediately. Once I accept the offer, the Bitcoins get deducted from my wallet and are held in escrow by the site. I send my banking information to the buyer and wait.

After the buyer sends me the bolívars via wire transfer, I release the Bitcoins from escrow and they are transferred to the buyer's Bitcoin wallet. We give each other a positive score, and that's it. The whole process takes about 10 minutes.



Bitcoin Has Saved My Family

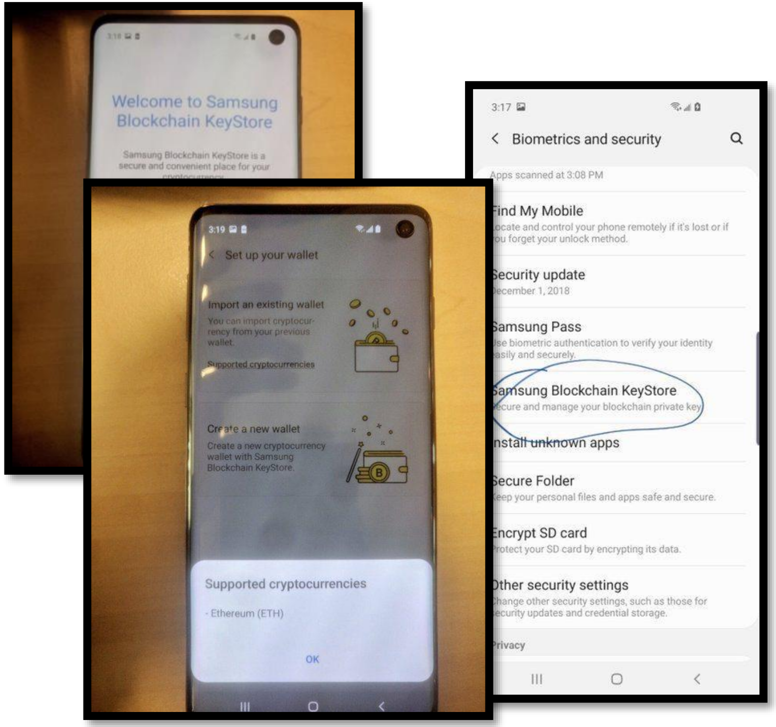
"Borderless money" is more than a buzzword when you live in a collapsing economy and a collapsing dictatorship.

By Carlos Hernández
Mr. Hernández is a Venezuelan economist.

Feb. 23, 2019

One central problem: daily usability.

- Hardware wallets are difficult to use for daily tasks.
- Software wallets are generally low in quality, depend on server-side wallets, and not interoperable.
- Potential commoditization of hardware wallets: include in smartphones.
    - ○ Example: Samsung Galaxy S10 includes secure Ethereum wallet.



3:18

Welcome to Samsung Blockchain KeyStore

Samsung Blockchain KeyStore is a secure and convenient place for your cryptocurrency

3:19

Set up your wallet

Import an existing wallet

You can import cryptocurrency from your previous wallet.

Supported cryptocurrencies

Create a new wallet

Create a new cryptocurrency wallet with Samsung Blockchain KeyStore.

Supported cryptocurrencies

- Ethereum (ETH)

OK

3:17

Biometrics and security

Apps scanned at 3:08 PM

Find My Mobile

ocate and control your phone remotely if it's lost or if ou forget your unlock method.

Security update

ecember 1, 2018

Samsung Pass

se biometric authentication to verify your identity asily and securely.

Samsung Blockchain KeyStore

ecure and manage your blockchain private key

nstall unknown apps

Secure Folder

eep your personal files and apps safe and secure.

Encrypt SD card

rotect your SD card by encrypting its data.

Other security settings

hange other security settings, such as those for ecurity updates and credential storage.

rivacy

Ethereum and Smart Contracts

1.7c

Ethereum: origins.

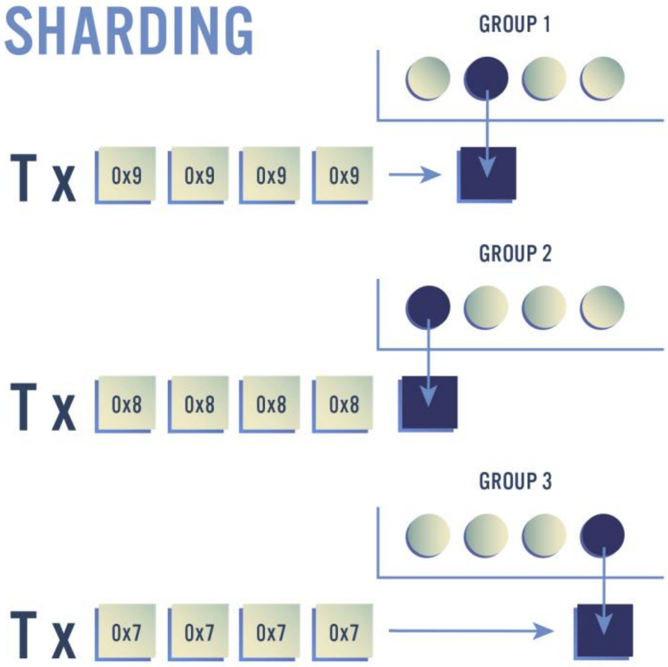
- We know who the authors are!
  - Vitalik Buterin, Gav Wood, Jeff Wilcke, Vlad Zamfir and Justin Drake.
- Active community members, Ethereum Foundation, make decisions, etc.

Ethereum vs. Bitcoin.

- Ethereum is fairly similar to Bitcoin: hash-based proof of work, block chain, etc.
- May switch to proof of stake: interest on how much assets you hold.
- Trying to solve problems like sharding.

Ethereum: sharding.

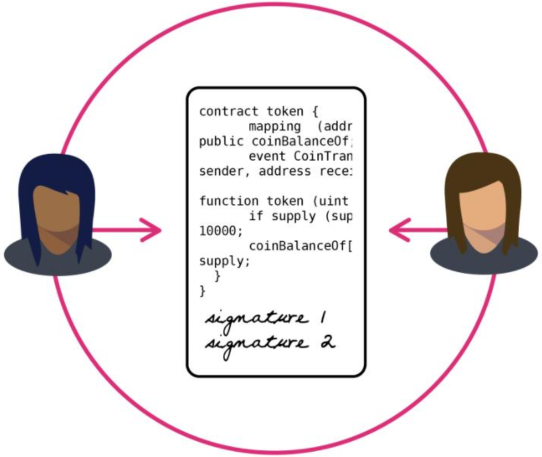
- Bitcoin can handle 3-7 transactions per second, Ethereum 12-30 transactions per second. *Worldwide*.
- Slow compared to Visa, etc.



Ethereum: the idea of smart contracts.

But the real difference in Ethereum is smart contracts.

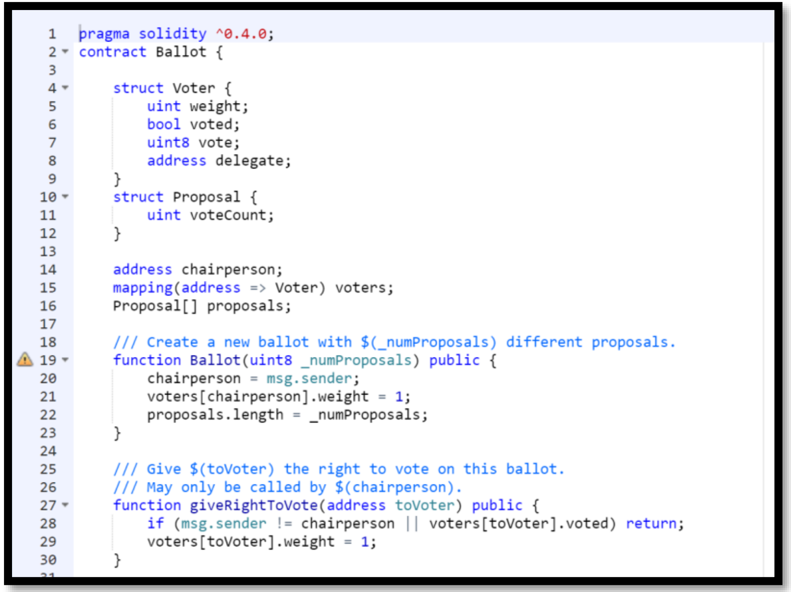
- Imagine a state machine running with the block chain as its operating system.
- State transitions for programs governed by decentralized consensus.
- Helpful example: verifiably fair casino.



```
contract token {
        mapping  (addr
public coinBalanceOf
        event CoinTran
sender, address rece

function token (uint
        if supply (sup
10000;
        coinBalanceOf[
supply;
  }
}
```

Ethereum: Solidity.

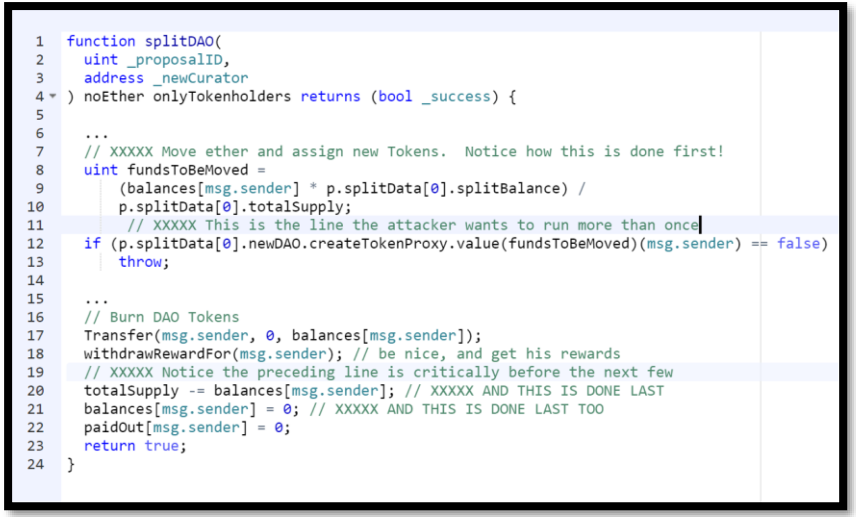
- Syntax and feel similar to JavaScript (to promote adoption.)
- Still under development.
- Allows for handling events, receiving ETH…
- Execution cost limited by “gas.”
- Other languages: Vyper, etc.



```
pragma solidity ^0.4.0;
contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        address delegate;
    }
    struct Proposal {
        uint voteCount;
    }

    address chairperson;
    mapping(address => Voter) voters;
    Proposal[] proposals;

    /// Create a new ballot with $(_numProposals) different proposals.
    function Ballot(uint8 _numProposals) public {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
        proposals.length = _numProposals;
    }

    /// Give $(toVoter) the right to vote on this ballot.
    /// May only be called by $(chairperson).
    function giveRightToVote(address toVoter) public {
        if (msg.sender != chairperson || voters[toVoter].voted) return;
        voters[toVoter].weight = 1;
    }
```

Ethereum: the DAO.

- Investor-directed venture capital fund running via smart contract.
- In June 2016, a programming error in the Solidity smart contract code allowed diverting $55 Million USD.
- Entire Ethereum blockchain was forked to revert this.



```
function splitDAO(
  uint _proposalID,
  address _newCurator
) noEther onlyTokenholders returns (bool _success) {

  ...
  // XXXXX Move ether and assign new Tokens.  Notice how this is done first!
  uint fundsToBeMoved =
      (balances[msg.sender] * p.splitData[0].splitBalance) /
      p.splitData[0].totalSupply;
       // XXXXX This is the line the attacker wants to run more than once
  if (p.splitData[0].newDAO.createTokenProxy.value(fundsToBeMoved)(msg.sender) == false)
      throw;

  ...
  // Burn DAO Tokens
  Transfer(msg.sender, 0, balances[msg.sender]);
  withdrawRewardFor(msg.sender); // be nice, and get his rewards
  // XXXXX Notice the preceding line is critically before the next few
  totalSupply -= balances[msg.sender]; // XXXXX AND THIS IS DONE LAST
  balances[msg.sender] = 0; // XXXXX AND THIS IS DONE LAST TOO
  paidOut[msg.sender] = 0;
  return true;
}
```

The Future of Blockchain Tech

1.7d

Did you know?

None of the concepts behind Bitcoin or Ethereum are new: Merkle trees (Merkle, 1976), decentralized consensus (Lamport, 1982), proof of work (Dwork & Naor, 1993), smart contracts (Szabo, 1997), Bitgold (Szabo, 1998)…

Forecast: uncertain.

- Blockchain and ICO hype is dying down (thankfully.)
- Scalability, efficiency, miner fairness remain serious problems.
- Usability in daily transactions is far from being a given.
- Smart contracts might radically diversity use cases.

Next time: E-Voting and Other Modern Uses of Cryptography

1.8