Join Our Telegram

https://t.me/ntublockchain

Lecture 1:

Bitcoin Overview & Cryptography Basics

Alex Xiong

BLOCKCHAIN
AT NTU

Who Are We

BLOCKCHAIN
AT NTU

What We Do

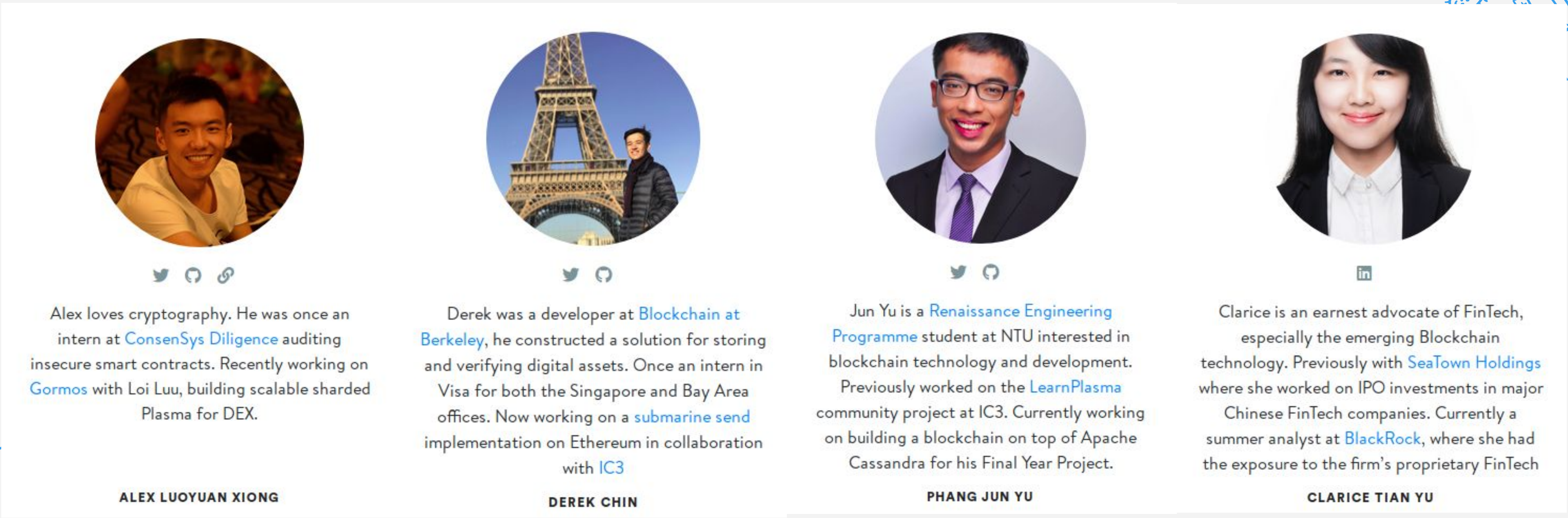
Education | R&D | Consulting

BLOCKCHAIN
AT NTU

Blockchain Fundamental Course

- □ Format
  - ↳ bi-weekly workshop ; 1.5 hr/session ; Monday
- □ Expectation
  - ↳ us: high level theories & low level details of blockchain fundamentals
  - ↳ you: dedication & participation & read like crazy & ASK QUESTIONS !
  - ↳ prerequisite: none
  - ↳ assignments: mostly reading materials, sometimes coding tasks (for dev)
  - ↳ deliverables: explain to 10-year-old
- □ Reference
  - ↳ <***Bitcoin and Cryptocurrency Technology***> [Andrew Miller, Arvind Narayanan, Edward Felten, Joseph Bonneau, and Steven Goldfeder]

Speakers



Alex loves cryptography. He was once an intern at ConsenSys Diligence auditing insecure smart contracts. Recently working on Gormos with Loi Luu, building scalable sharded Plasma for DEX.

ALEX LUOYUAN XIONG

Derek was a developer at Blockchain at Berkeley, he constructed a solution for storing and verifying digital assets. Once an intern in Visa for both the Singapore and Bay Area offices. Now working on a submarine send implementation on Ethereum in collaboration with IC3

DEREK CHIN

Jun Yu is a Renaissance Engineering Programme student at NTU interested in blockchain technology and development. Previously worked on the LearnPlasma community project at IC3. Currently working on building a blockchain on top of Apache Cassandra for his Final Year Project.

PHANG JUN YU

Clarice is an earnest advocate of FinTech, especially the emerging Blockchain technology. Previously with SeaTown Holdings where she worked on IPO investments in major Chinese FinTech companies. Currently a summer analyst at BlackRock, where she had the exposure to the firm's proprietary FinTech

CLARICE TIAN YU

https://t.me/ntublockchain

Woo...
finally admin stuff is done.

BLOCKCHAIN
AT NTU

Agenda

❑ **Motivation**: Pre-Bitcoin Area

❑ **Blockchain**: Data Structure for Secure Digital Ledger

❑ **Pseudonymity**: Identity on Bitcoin

❑ **Nakamoto Consensus**: Coming to Agreement

❑ **Bitcoin Protocol**: Putting All Together

Motivation

Let’s Start From Way Back...

Coordination Problem?

Cash

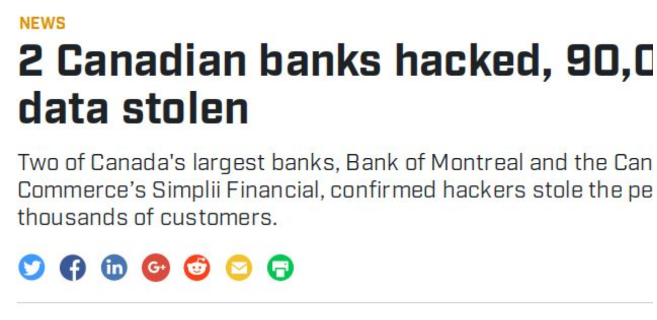
- Pros:
  - No default risk / No trust required / quick settlement
  - Offline, **no middle man**
  - Better **anonymity**
- Cons:
  - Possible counterfeits
  - ***Inconvenient**: Physical presence*

Digital Cash

AMERICAN EXPRESS
citi
DBS
fevo
Maybank
OCBC Bank
POSB
Standard Chartered
UOB

Digital Cash

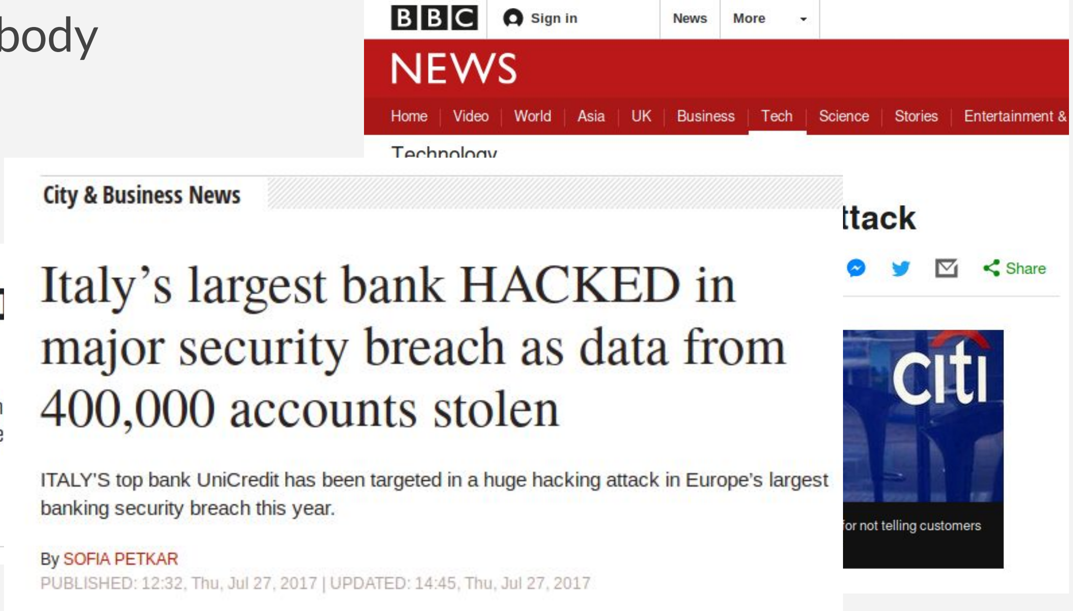
- ❑ Pros:
  - ↳ Convenient management + transaction
  - ↳ Scrutinized by regulatory body
- ❑ Cons:
  - ↳ Central point of failure



NEWS

2 Canadian banks hacked, 90,0
data stolen

Two of Canada's largest banks, Bank of Montreal and the Can
Commerce's Simplii Financial, confirmed hackers stole the pe
thousands of customers.



City & Business News

Italy's largest bank HACKED in major security breach as data from 400,000 accounts stolen

ITALY'S top bank UniCredit has been targeted in a huge hacking attack in Europe's largest banking security breach this year.

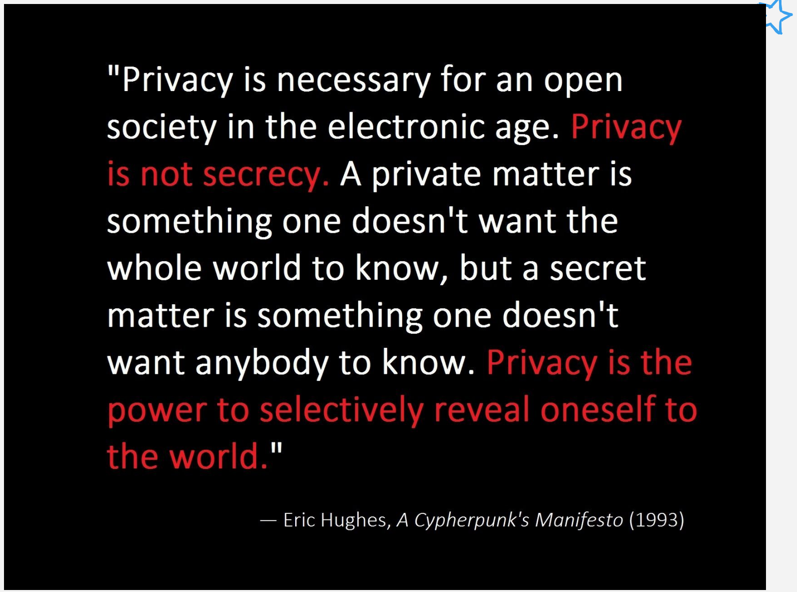
By SOFIA PETKAR
PUBLISHED: 12:32, Thu, Jul 27, 2017 | UPDATED: 14:45, Thu, Jul 27, 2017

Digital Cash

- ❑ Pros:
  - ↳ Convenient management + transaction
  - ↳ Scrutinized by regulatory body
- ❑ Cons:
  - ↳ Central point of failure
    - ◦ External hacks
    - ◦ Internal corruption
  - ↳ ***Strong trust (-worthy) assumption***

Cypherpunk Movement

- □ Cryptography & Privacy-enhancing tech for social and political change.
- □ Smaller government, don’t trust central authorities.
- □ Privacy ≠ Secrecy
  - ↳ <Why should we all have something to hide> by Moxie Marlinspike



"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

— Eric Hughes, *A Cypherpunk's Manifesto* (1993)

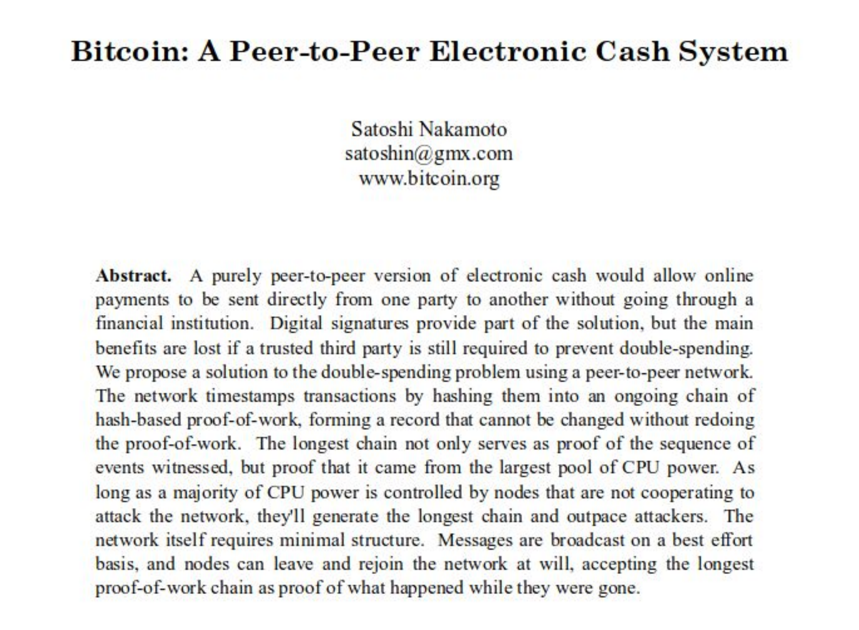
The Year 2008

Motivation:

Benefits of digital cash without trusted party.

Bitcoin Whitepaper

Satoshi Nakamoto ??



Bitcoin: A Peer-to-Peer Electronic Cash System

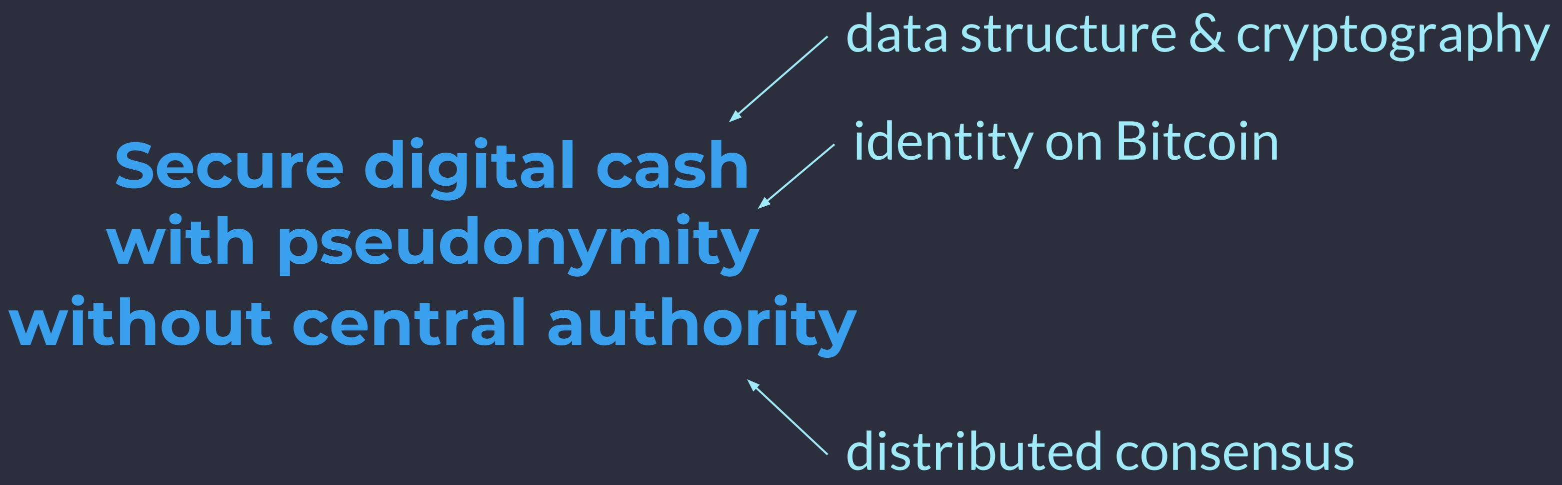
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

Goal:

Secure digital cash
with pseudonymity
without central authority

Goal:



Secure digital cash
with pseudonymity
without central authority

data structure & cryptography

identity on Bitcoin

distributed consensus

Agenda

- □ **Motivation**: Pre-Bitcoin Area
- □ **Blockchain**: Data Structure for Secure Digital Ledger
- □ **Pseudonymity**: Identity on Bitcoin
- □ **Nakamoto Consensus**: Coming to Agreement
- □ **Bitcoin Protocol**: Putting All Together

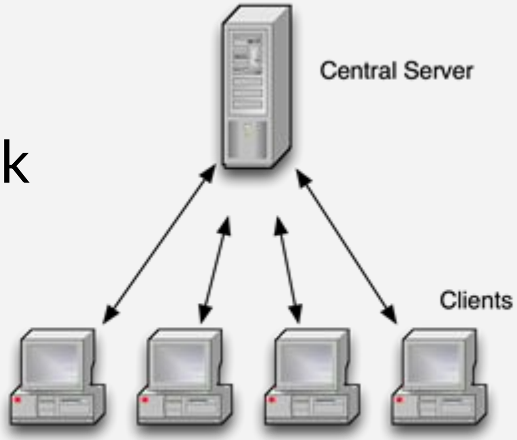
Block, chained

Mind the Gap

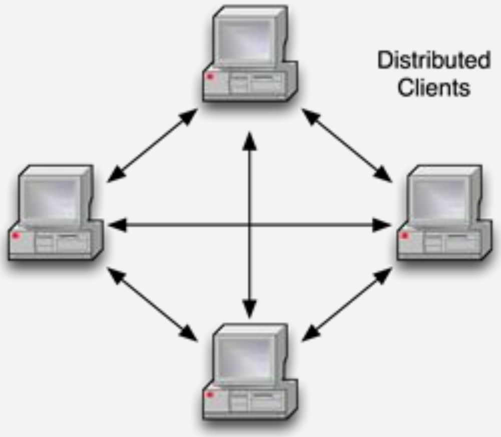
- ❑ Algorithm
- ❑ Data Structure
- ❑ Protocol
- ❑ Computer Network

Mind the Gap

- □ Algorithm
- □ Data Structure
- □ Protocol
- □ Computer Network



Client / Server



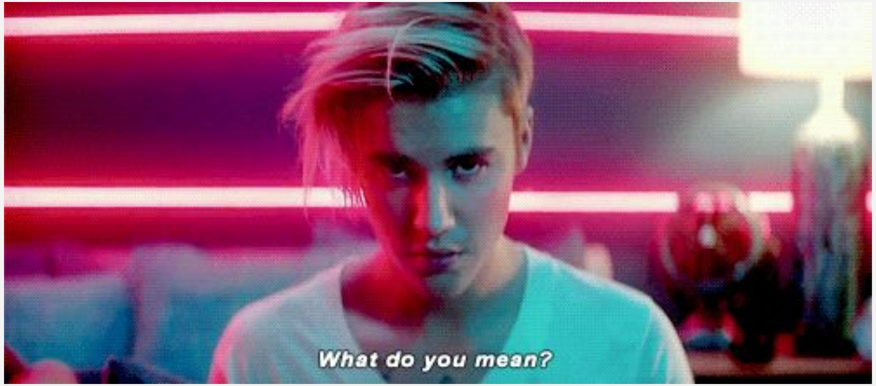
Peer to Peer

Goal:

Secure digital cash
with pseudonymity
without central authority

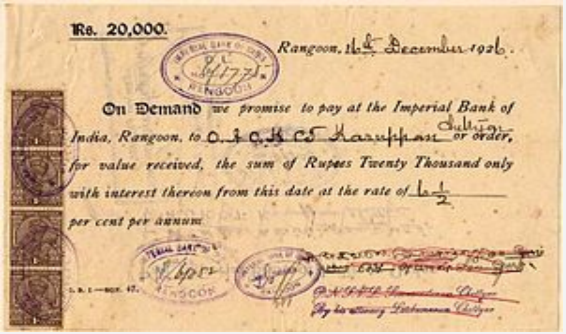
Secure ?! Digital Cash

- ❑ Proof of valid ownership on assets
  - ↳ Validity check about ownership
  - ↳ No one can “steal/spend” my coin
- ❑ No double-spending



Proof of Ownership

- ❑ “Unforgeable Stamp”
  - ↳ Detour to magical cryptography wonderland: *Digital Signature*



Rs. 20,000.

Rangoon, 16th December 1926.

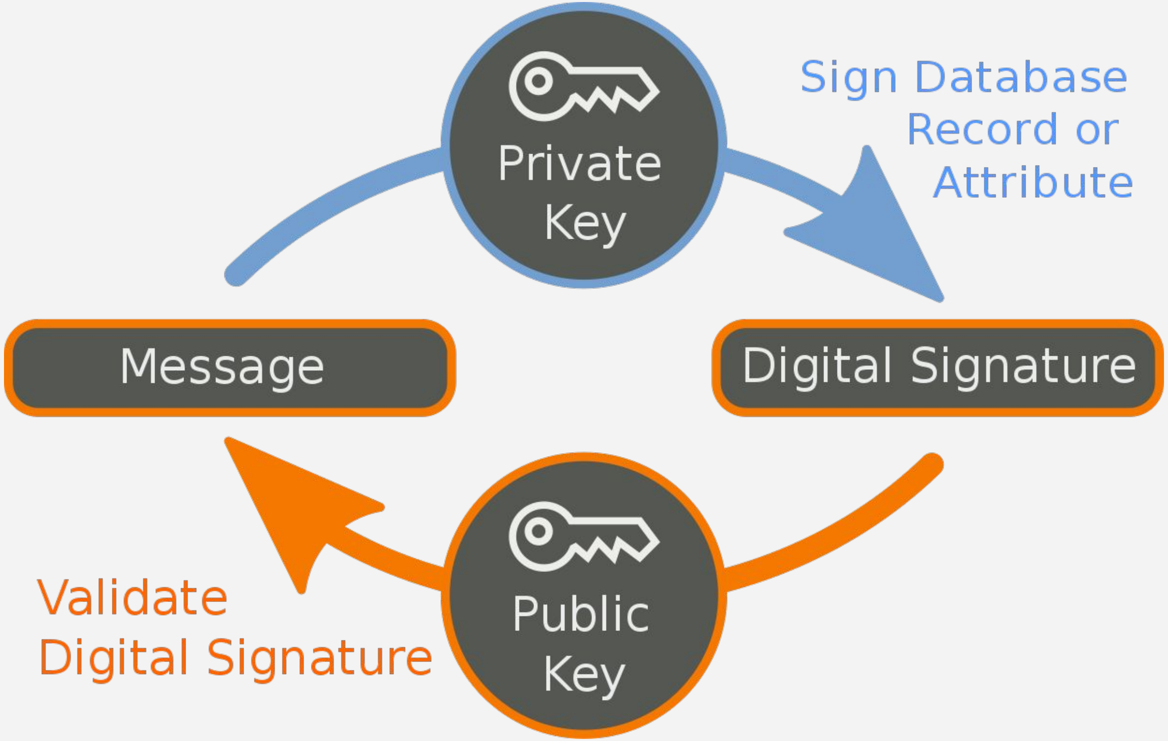
On Demand we promise to pay at the Imperial Bank of India, Rangoon, to O. A. O. K. C. Karuppan Chettyar or order, for value received, the sum of Rupees Twenty Thousand only with interest thereon from this date at the rate of 1½ per cent per annum

RANGOON

L. B. I.—NOV. 47.

By his attorney

Digital Signature Algorithm



Digital Signature Algorithm

❑ **Key Pair**: (*Public Key*, *Private Key*)

❑ **Sign** (priKey, message) => My digital signature

↳ Sign(random, message) => completely gibberish

↳ Sign(priKey, another message) => another digital signature

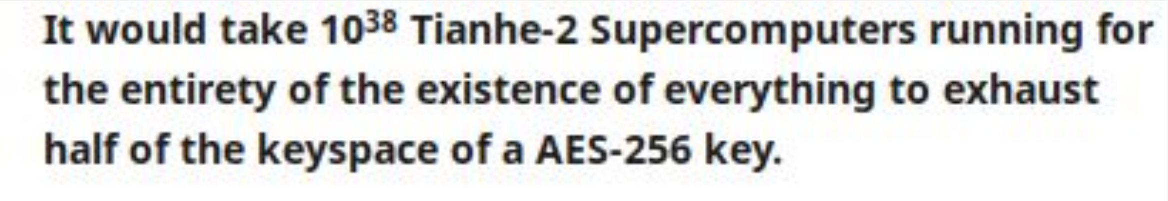
❑ **Verify** (pubKey, signature, message) => Yes/No

↳ Verify(pubKey, random, message) => No

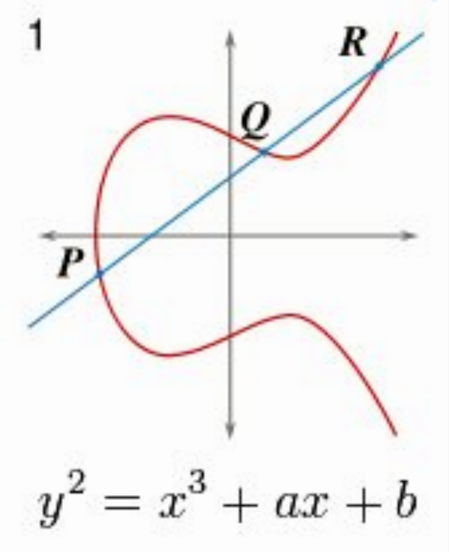
↳ Verify(pubKey, signature, random) => No

Elliptic Curve DSA (ECDSA)

- Key Generation
  - ↳ Randomly select a private key
  - ↳ Derive public key through ECDSA KeyGen Algorithm
  - ↳ Key length: 256 bits (brute force? luck? derive back?)

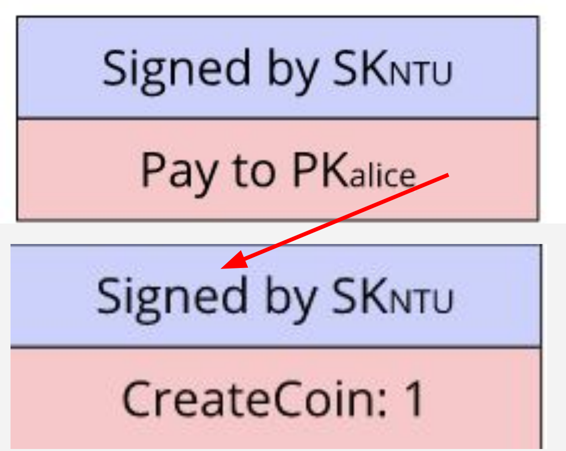


It would take 10^{38} Tianhe-2 Supercomputers running for the entirety of the existence of everything to exhaust half of the keyspace of a AES-256 key.



$$y^2 = x^3 + ax + b$$

Proof of Ownership

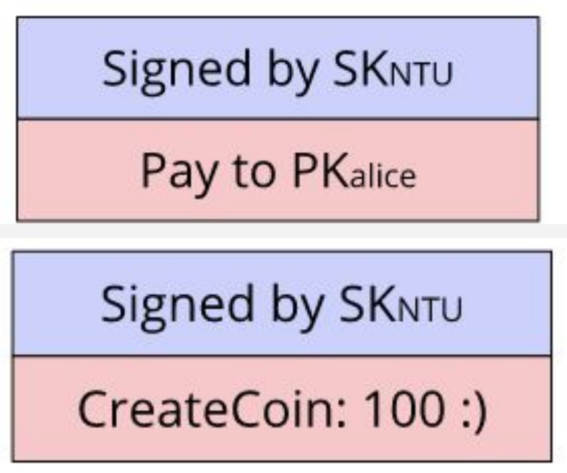


Signed by SK_{NTU}

Pay to PK_{alice}

Signed by SK_{NTU}

CreateCoin: 1



Signed by SK_{NTU}

Pay to PK_{alice}

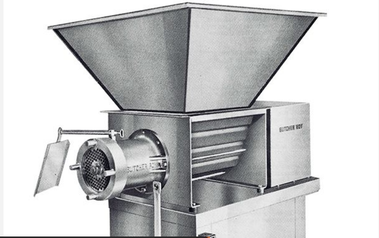
Signed by SK_{NTU}

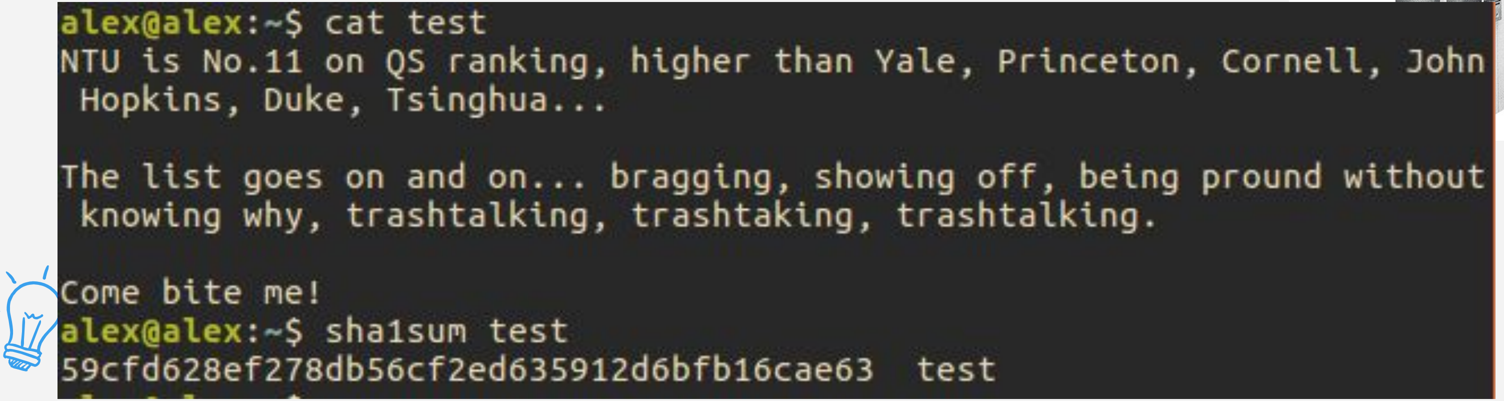
CreateCoin: 100 :)

How to bond two messages & signatures ??

Hash Function

- ❑ Message Digest
  - ↳ Long plaintext → short digest



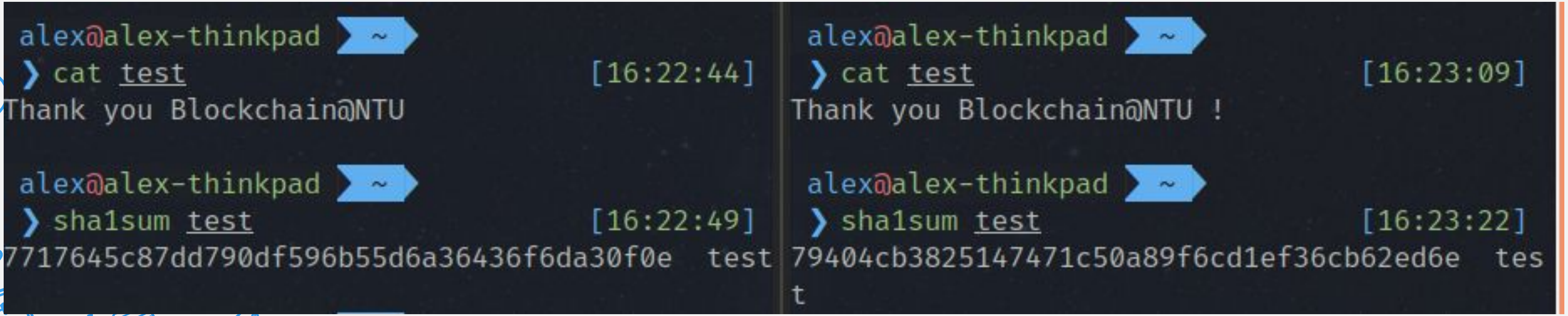


```
alex@alex:~$ cat test
NTU is No.11 on QS ranking, higher than Yale, Princeton, Cornell, John
 Hopkins, Duke, Tsinghua...

The list goes on and on... bragging, showing off, being pround without
 knowing why, trashtalking, trashtaking, trashtalking.

Come bite me!
alex@alex:~$ sha1sum test
59cfd628ef278db56cf2ed635912d6bfb16cae63  test
```

Hash Function

H(preimage) → hash digest

- ❑ Message Digest
  - ↳ Long plaintext → short digest
- ❑ One Way Function
  - ↳ Reverse calculation is HARD !
  - ↳ Small changes in preimage → entirely different digest



```
alex@alex-thinkpad  ~
❯ cat test                                  [16:22:44]
Thank you Blockchain@NTU

alex@alex-thinkpad  ~
❯ sha1sum test                              [16:22:49]
7717645c87dd790df596b55d6a36436f6da30f0e  test
```

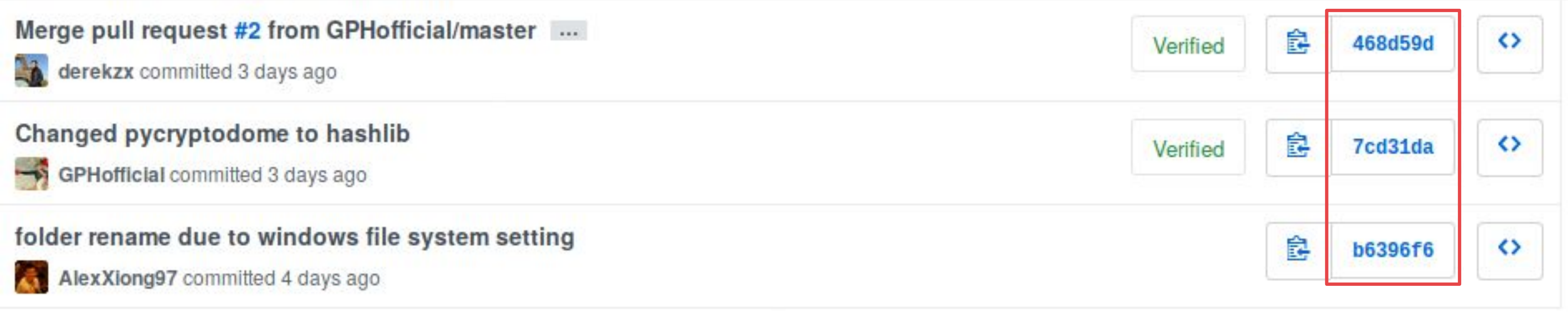
```
alex@alex-thinkpad  ~
❯ cat test                                  [16:23:09]
Thank you Blockchain@NTU !

alex@alex-thinkpad  ~
❯ sha1sum test                              [16:23:22]
79404cb3825147471c50a89f6cd1ef36cb62ed6e  tes
t
```

Hash Function

- □ Universal Hash Function (UHF)
  - ↳ Keyed hash
  - ↳ e.g. Carter-Wagman MAC
- □ Collision Resistant Hash
  - ↳ Keyless hash
  - ↳ e.g SHA1, MD5, **SHA256**, SHA3

Just so that you know

- ❑ SHA1
  - ↳ Collision found by Google (2017): SHAttered.io



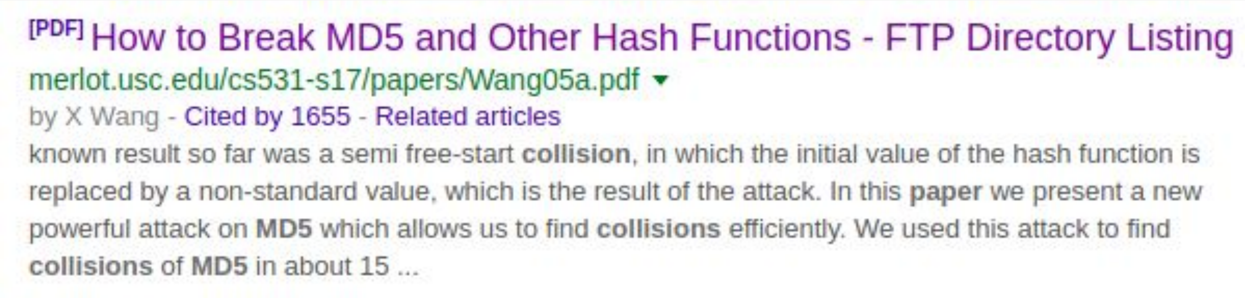
Merge pull request #2 from GPHofficial/master ...
derekzx committed 3 days ago
Verified 468d59d

Changed pycryptodome to hashlib
GPHofficial committed 3 days ago
Verified 7cd31da

folder rename due to windows file system setting
AlexXiong97 committed 4 days ago
b6396f6

Just so that you know

- ❑ MD5 : Microsoft unity file integrity check
  - ↳ Broken by Prof. Wang



[PDF] How to Break MD5 and Other Hash Functions - FTP Directory Listing

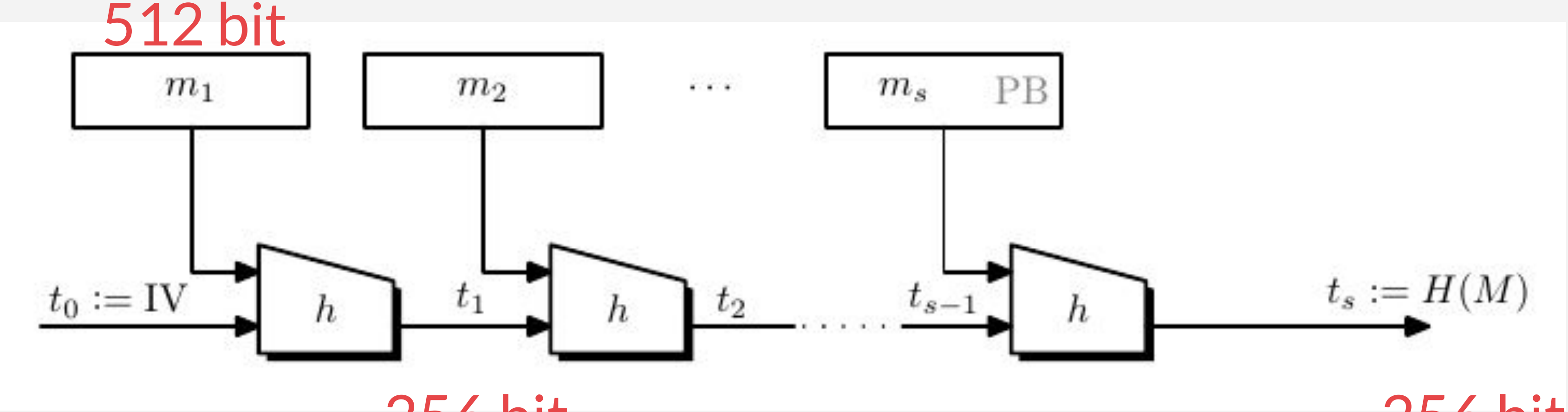
merlot.usc.edu/cs531-s17/papers/Wang05a.pdf ▾

by X Wang - Cited by 1655 - Related articles

known result so far was a semi free-start **collision**, in which the initial value of the hash function is replaced by a non-standard value, which is the result of the attack. In this **paper** we present a new powerful attack on **MD5** which allows us to find **collisions** efficiently. We used this attack to find **collisions** of **MD5** in about 15 ...

SHA256

512 bit

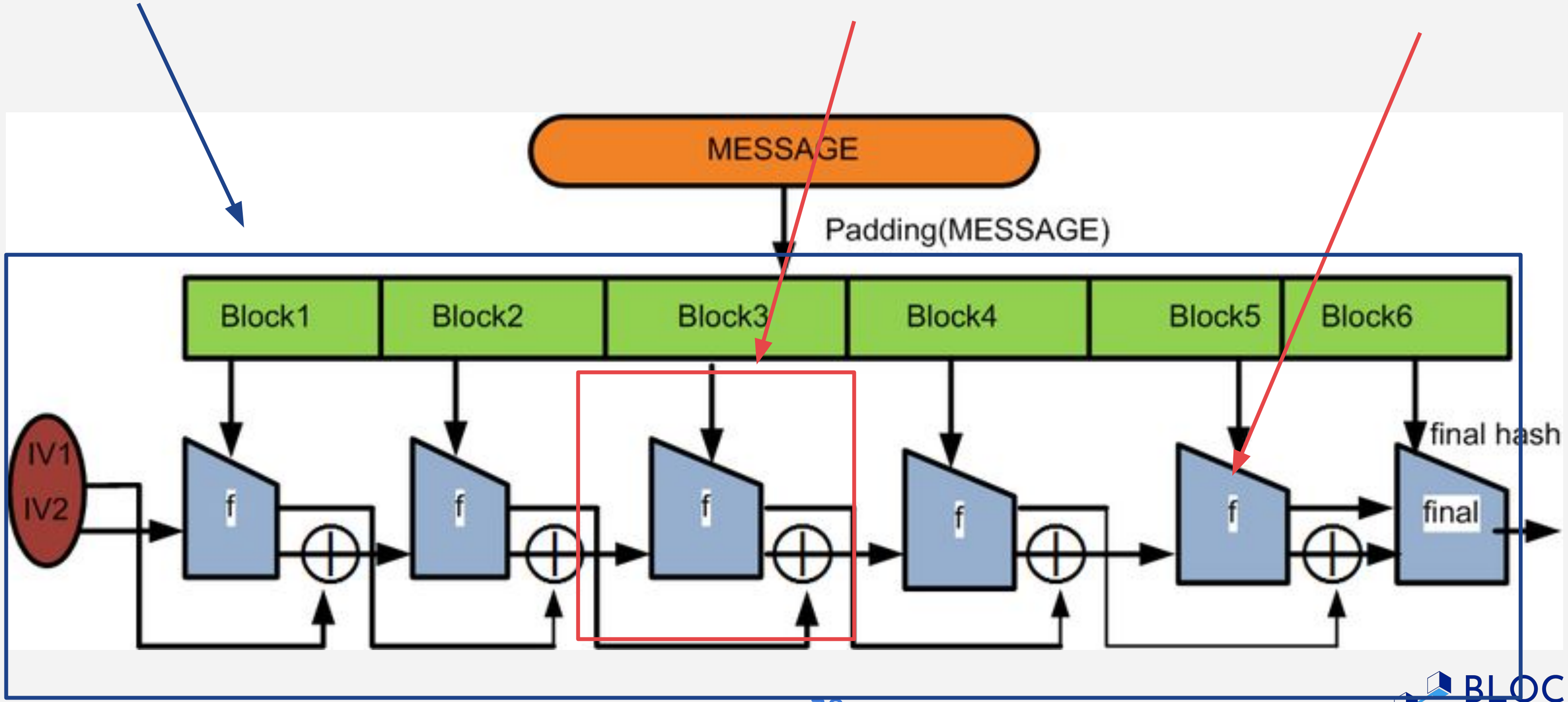


256 bit

256 bit

SHA256

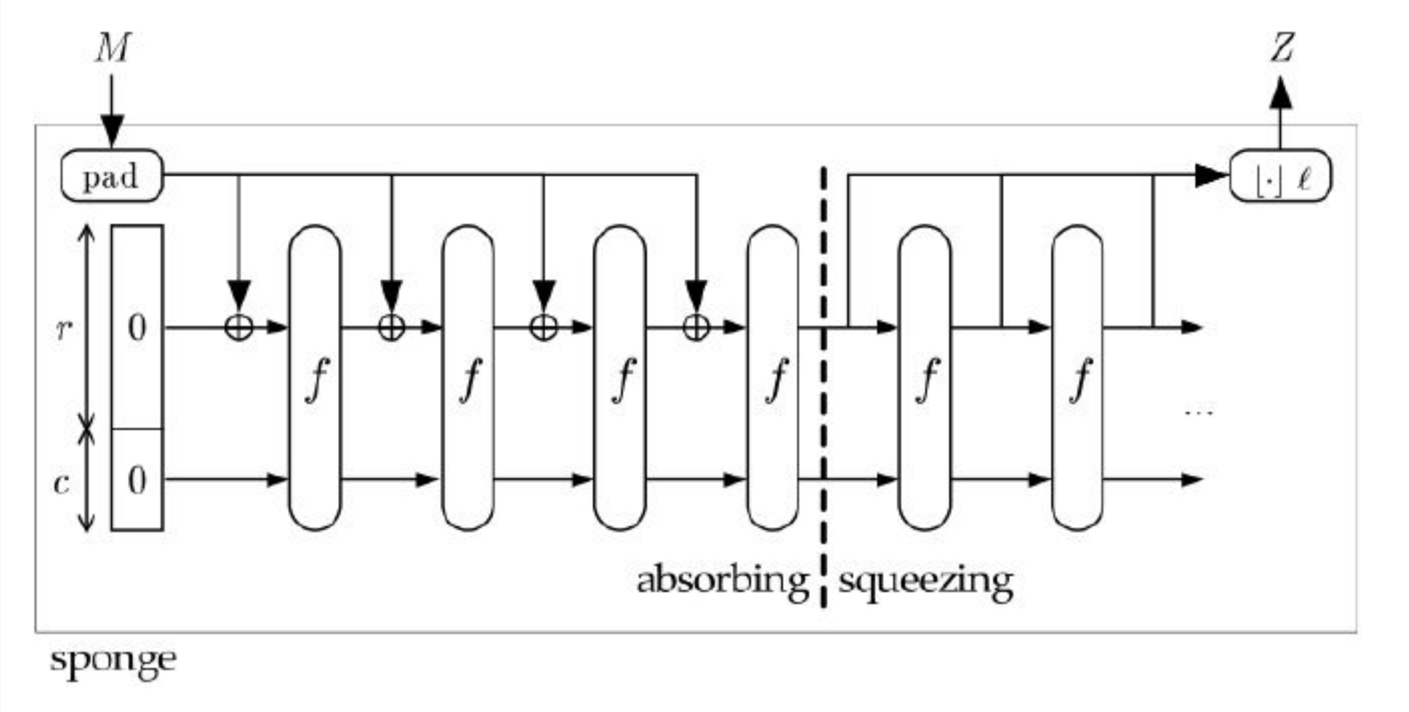
Merkle-Damgard + Davies-Mayer + SHACAL-2 block cipher

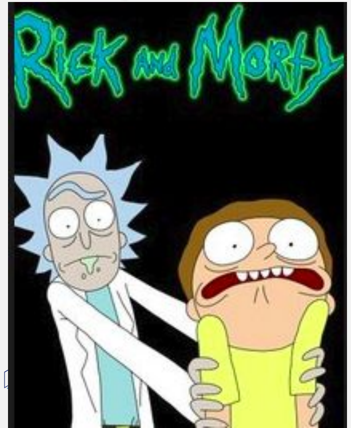


256 bit

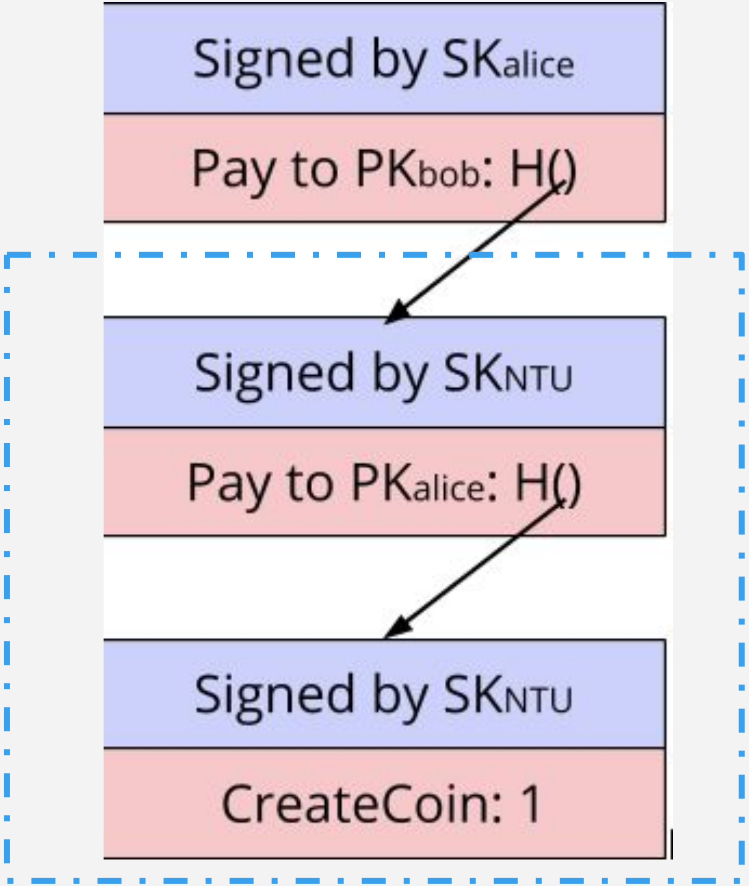
SHA3 using keccak256

Sponge Construction (keccak256 ≠ sha256 , sons from *different* families)





Proof of Ownership, God I’m Good!



Signed by SK_{alice}

Pay to PK_{bob}: H()

Signed by SK_{NTU}

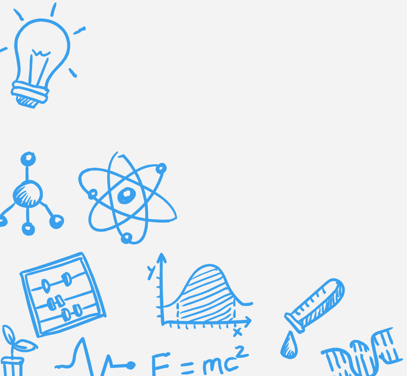
Pay to PK_{alice}: H()

Signed by SK_{NTU}

CreateCoin: 1

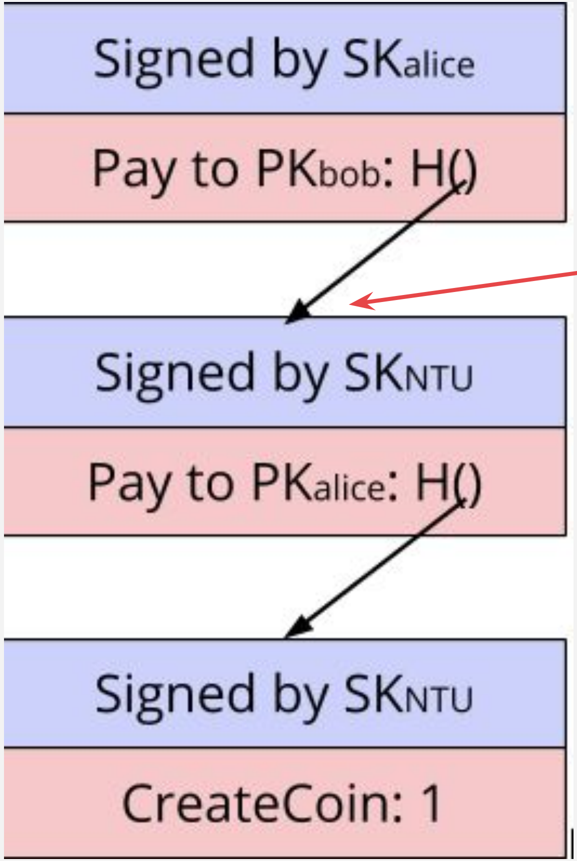
Secure ?! Digital Cash

- □ Proof of valid ownership on assets ✔
  - ↳ Validity check about ownership
  - ↳ No one can “steal/spend” my coin
- □ No double-spending



Cryptography is power in asymmetry

-- How I explain to my dad that I want to work on cryptography



Signed by SK_{alice}

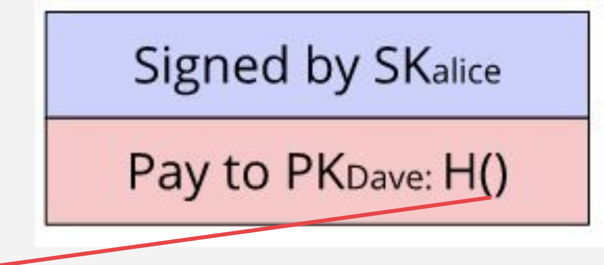
Pay to PK_{bob}: H()

Signed by SK_{NTU}

Pay to PK_{alice}: H()

Signed by SK_{NTU}

CreateCoin: 1



Signed by SK_{alice}

Pay to PK_{Dave}: H()

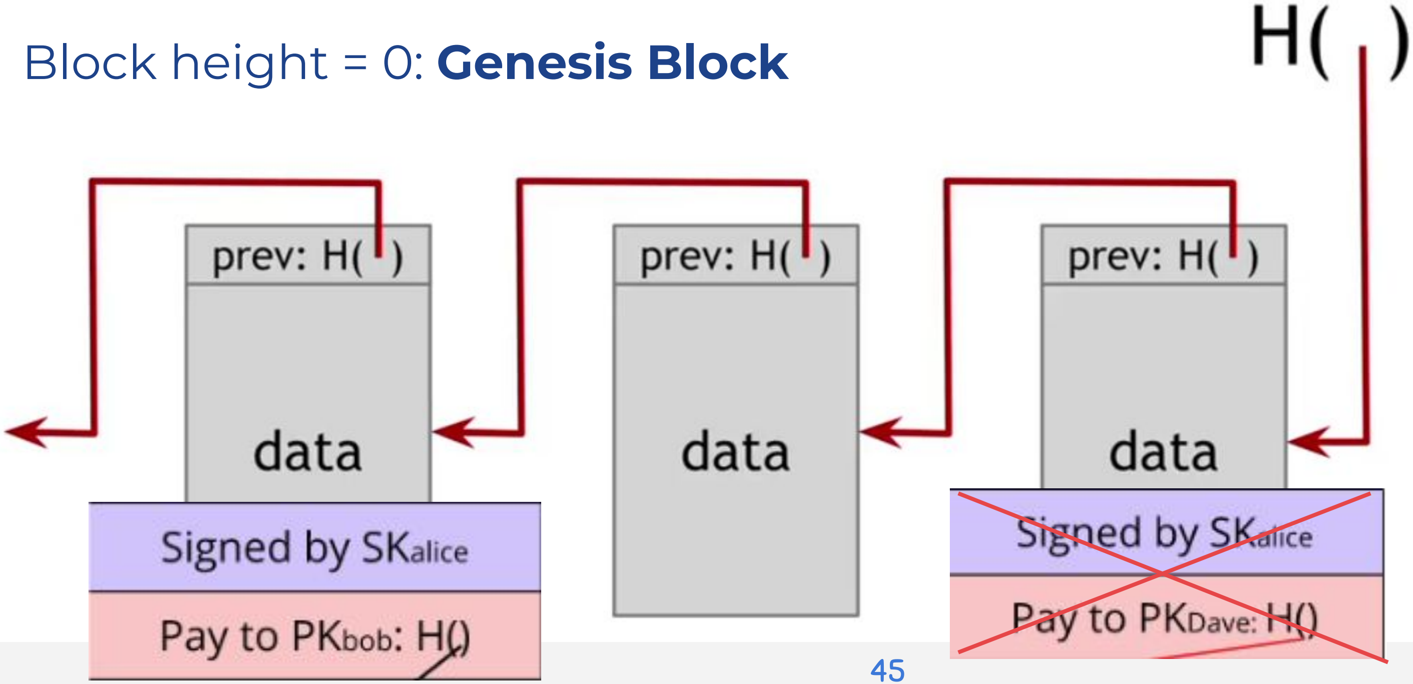
Whoops….

Double Spending

Hash Pointer (a.k.a. Blockchain)

use case: *tamper-evident log*

Block height = 0: **Genesis Block**



Secure !! Digital Cash

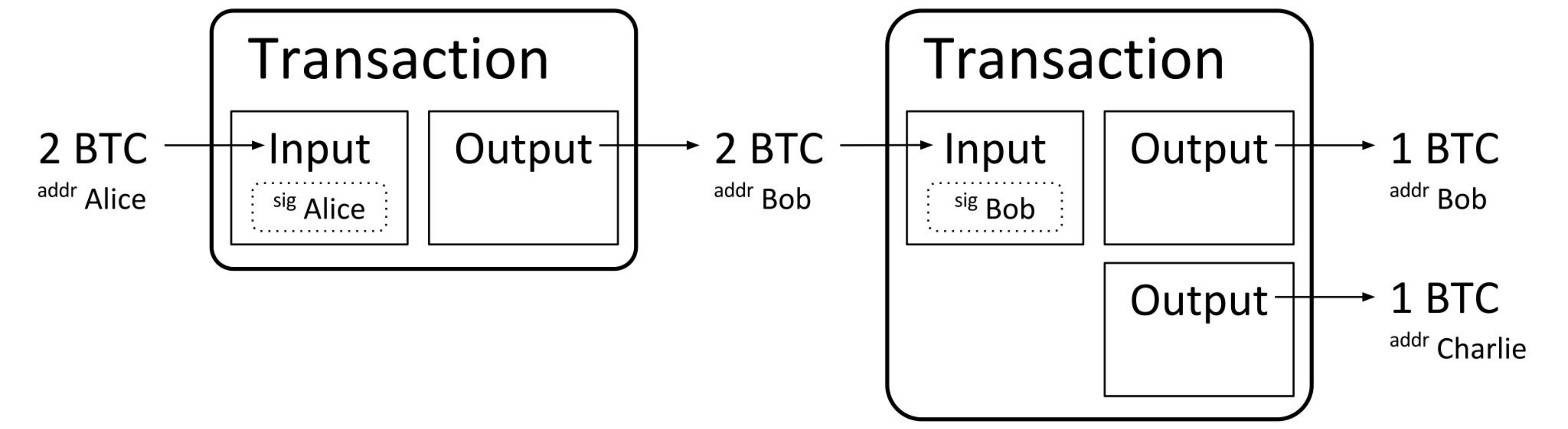
❑ Proof of valid ownership on assets ✔

  ↳ Validity check about ownership

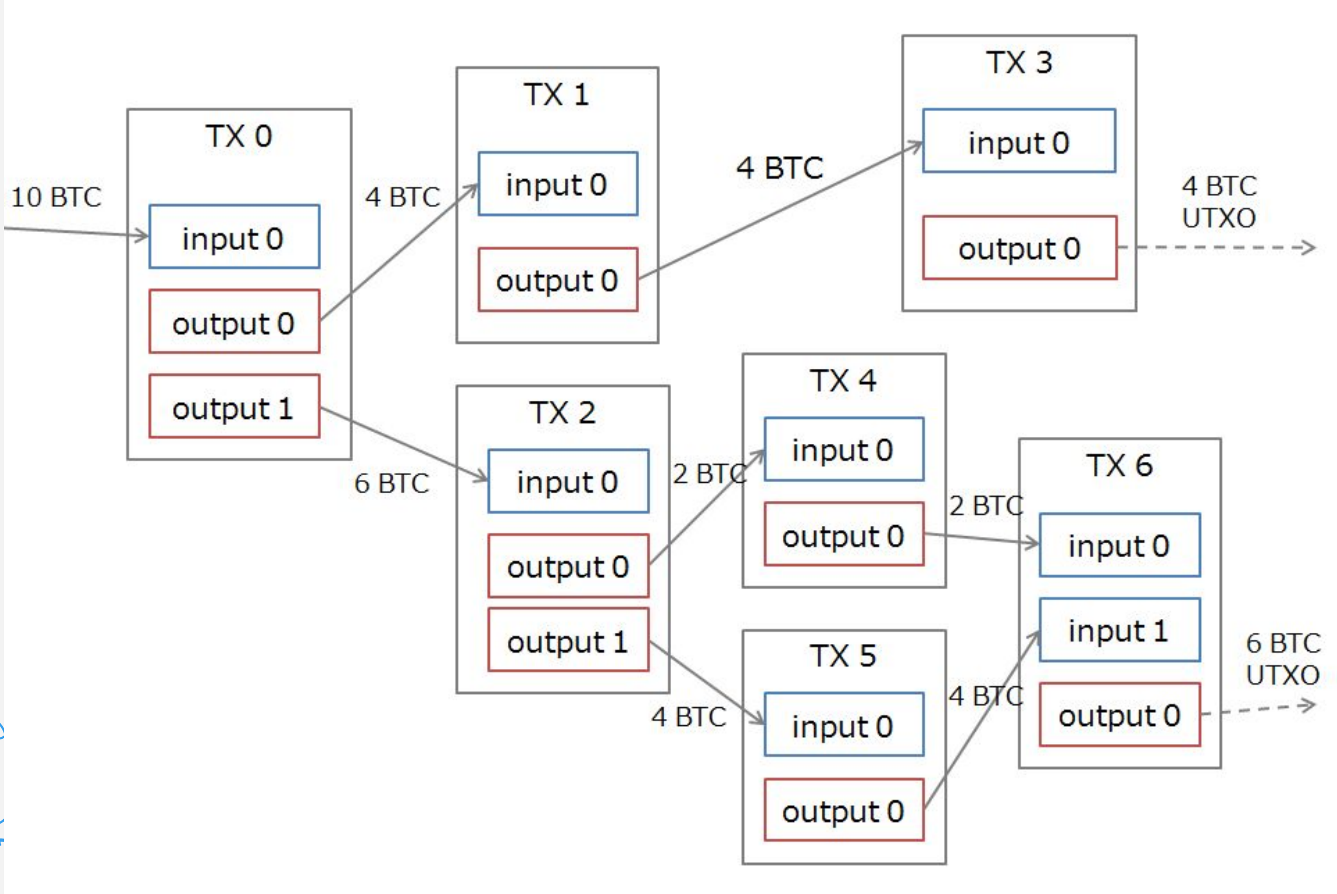
  ↳ No one can “steal/spend” my coin

❑ No double-spending ✔

Secure Digital Cash



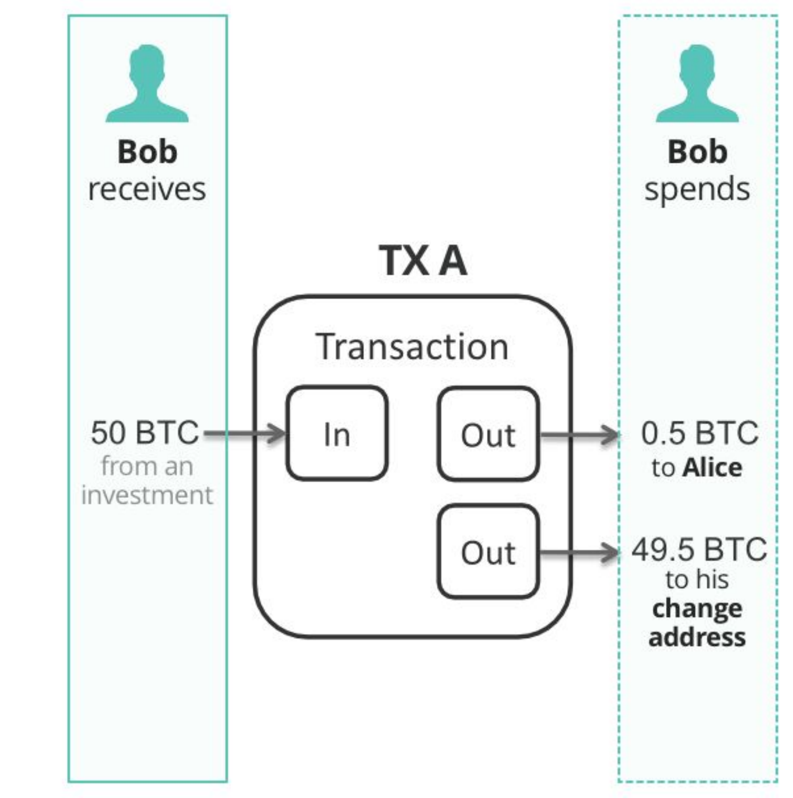
Unspent Transaction Output (UTXO)



UTXO: what about change?

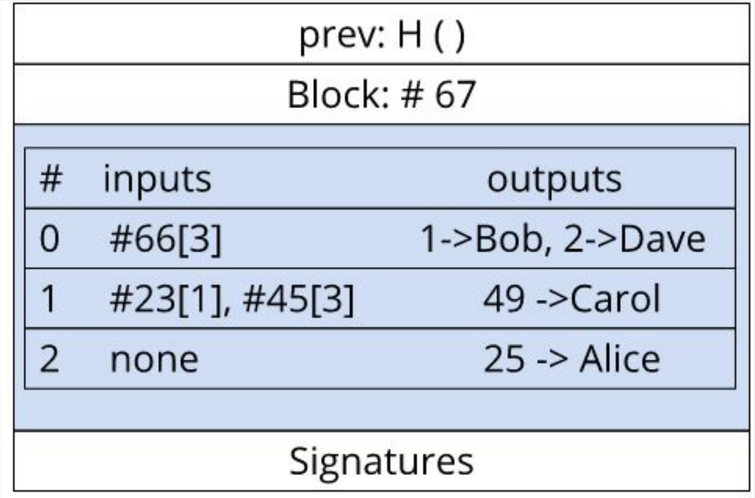
Keep the change!

Send it to yourself!



Putting all together

- ❑ Proof of ownership ✔
- ❑ No double-spending ✔
- ❑ UTXO model ledger ✔



prev: H ( )

Block: # 67

#	inputs	outputs
0	#66[3]	1->Bob, 2->Dave
1	#23[1], #45[3]	49 ->Carol
2	none	25 -> Alice

Signatures

Goal:

Secure digital cash
with pseudonymity
without central authority

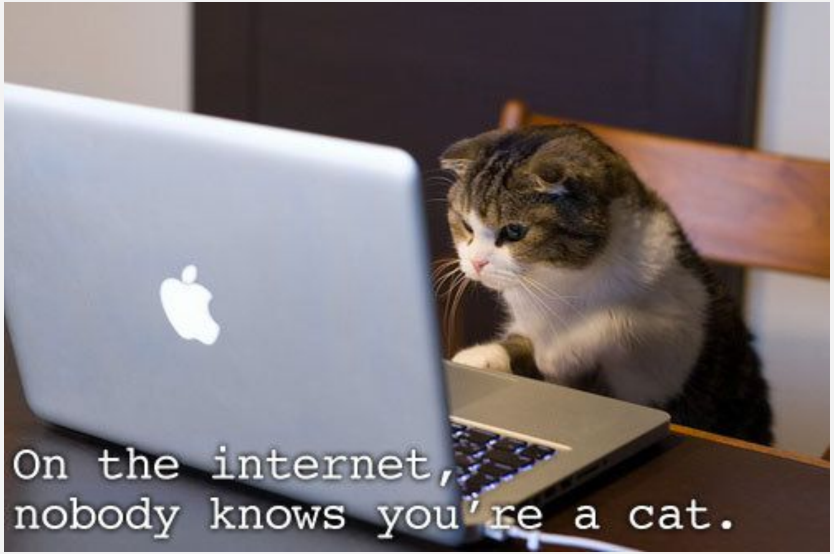
Goal:

Secure digital cash
with pseudonymity
without central authority

Pseudonymity

Pseudonymity

- ❑ Digital identity ⇐⇒ Real-life identity ?
- ❑ **H (PubKey)** as your identity !!
  - ↳ I can create as many private key, thus as many identities as I wish
  - ↳ Do I need to be a human?

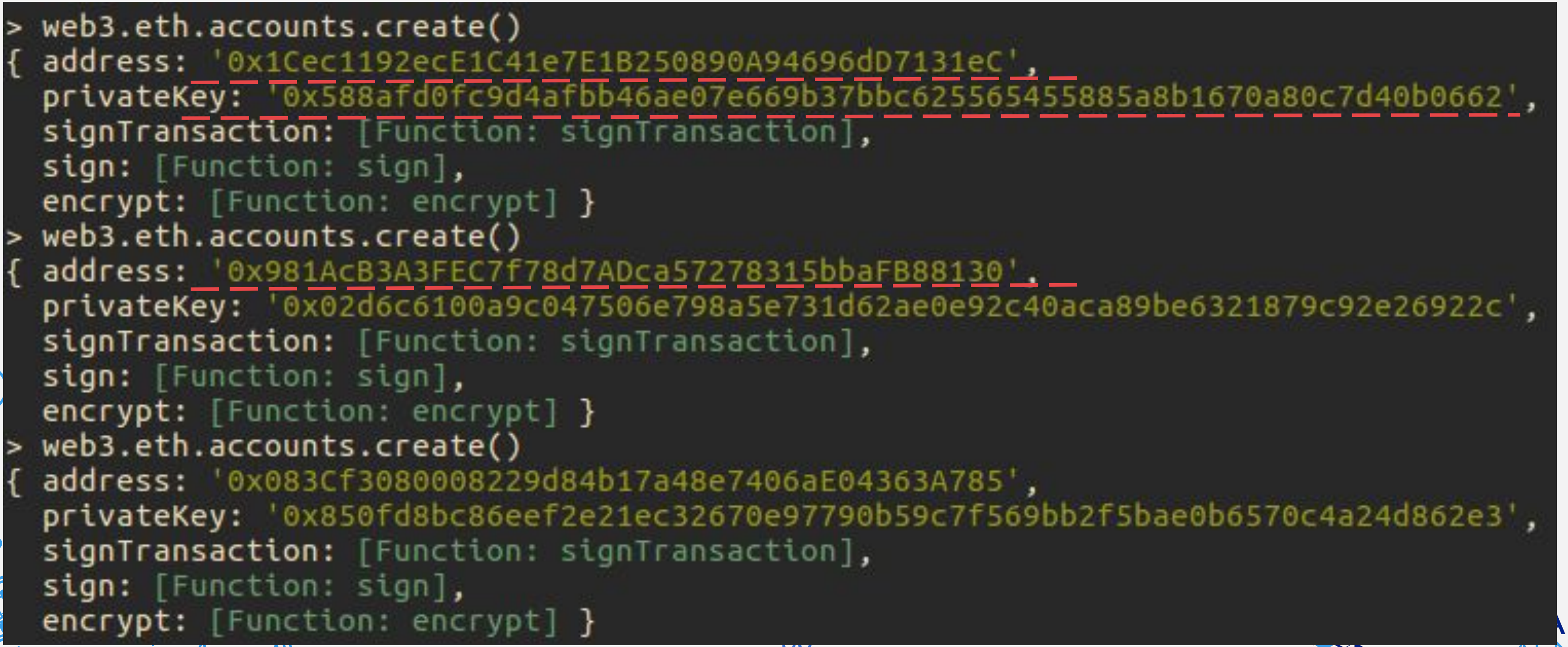


Pseudonymity

- ❑ Digital identity ⇐⇒ Real-life identity ?
- ❑ **H (PubKey)** as your identity !!
  - ↳ I can create as many private key, thus as many identities as I wish
  - ↳ Do I need to be a human?
  - ↳ Untraceable?
    - ◦ Network analysis, Bitcoin deanonymization
    - ◦ CoinJoin, Ring Signature

Identity on Blockchain

❑ Ethereum as example (Bitcoin is similar)

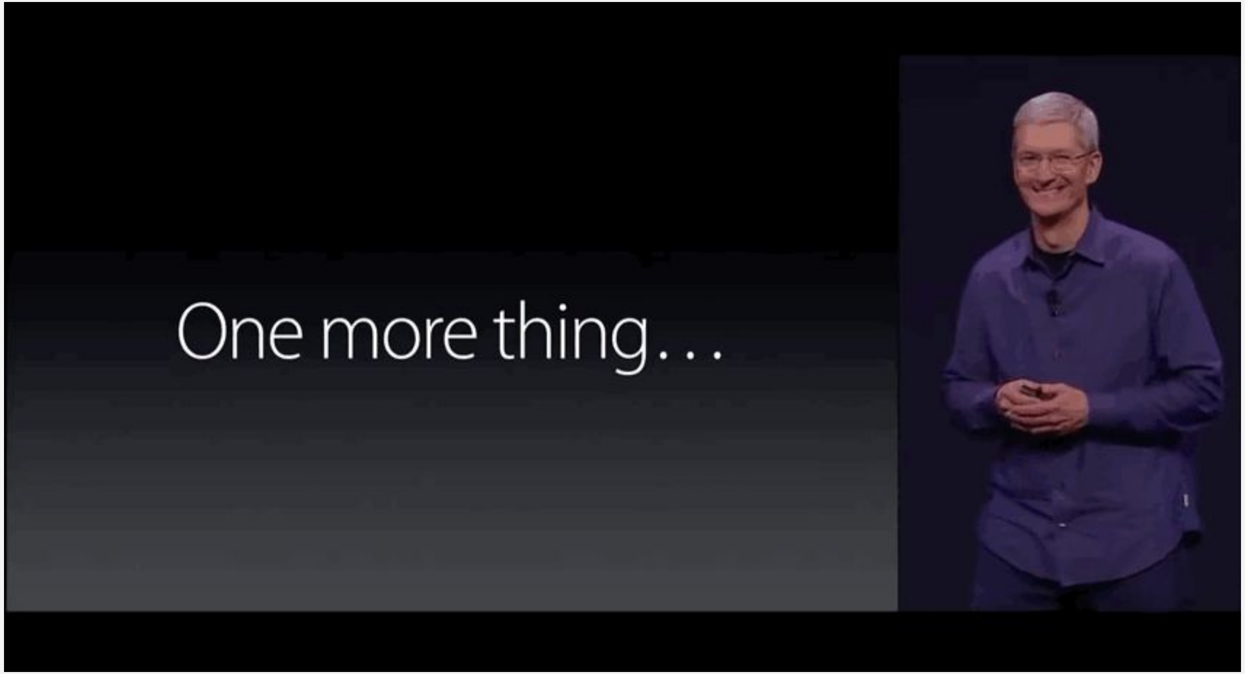


```
> web3.eth.accounts.create()
{ address: '0x1Cec1192ecE1C41e7E1B250890A94696dD7131eC',
  privateKey: '0x588afd0fc9d4afbb46ae07e669b37bbc625565455885a8b1670a80c7d40b0662',
  signTransaction: [Function: signTransaction],
  sign: [Function: sign],
  encrypt: [Function: encrypt] }
> web3.eth.accounts.create()
{ address: '0x981AcB3A3FEC7f78d7ADca57278315bbaFB88130',
  privateKey: '0x02d6c6100a9c047506e798a5e731d62ae0e92c40aca89be6321879c92e26922c',
  signTransaction: [Function: signTransaction],
  sign: [Function: sign],
  encrypt: [Function: encrypt] }
> web3.eth.accounts.create()
{ address: '0x083Cf3080008229d84b17a48e7406aE04363A785',
  privateKey: '0x850fd8bc86eef2e21ec32670e97790b59c7f569bb2f5bae0b6570c4a24d862e3',
  signTransaction: [Function: signTransaction],
  sign: [Function: sign],
  encrypt: [Function: encrypt] }
```

Goal:

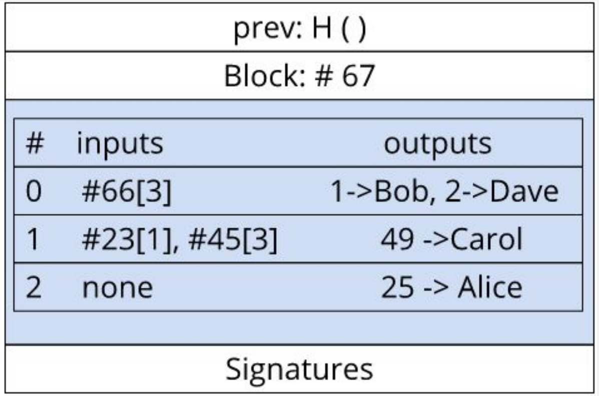
Secure digital cash
with pseudonymity
without central authority

Ah... One more thing



One more thing…

How to prove a tx is included?



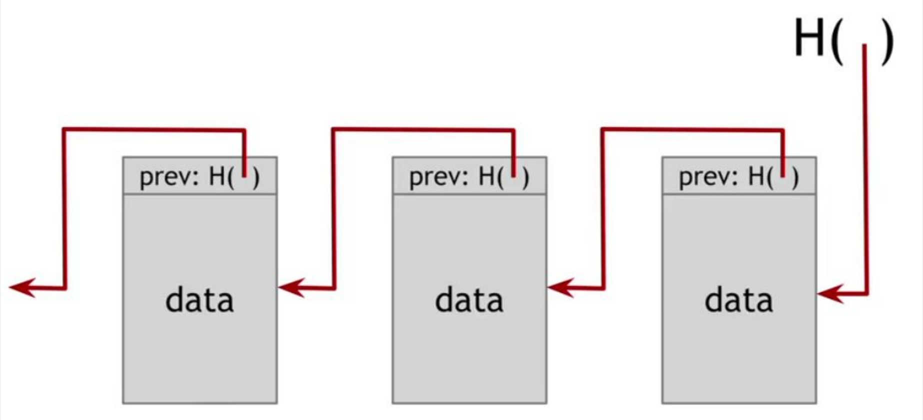
prev: H ( )

Block: # 67

#	inputs	outputs
0	#66[3]	1->Bob, 2->Dave
1	#23[1], #45[3]	49 ->Carol
2	none	25 -> Alice

Signatures

+



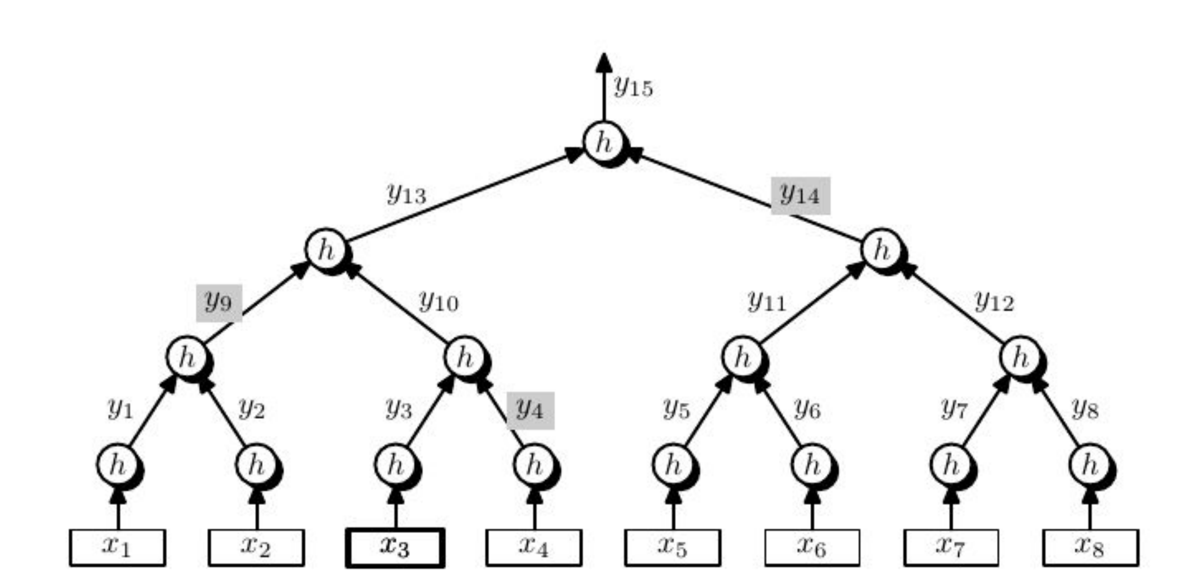
Merkle Tree

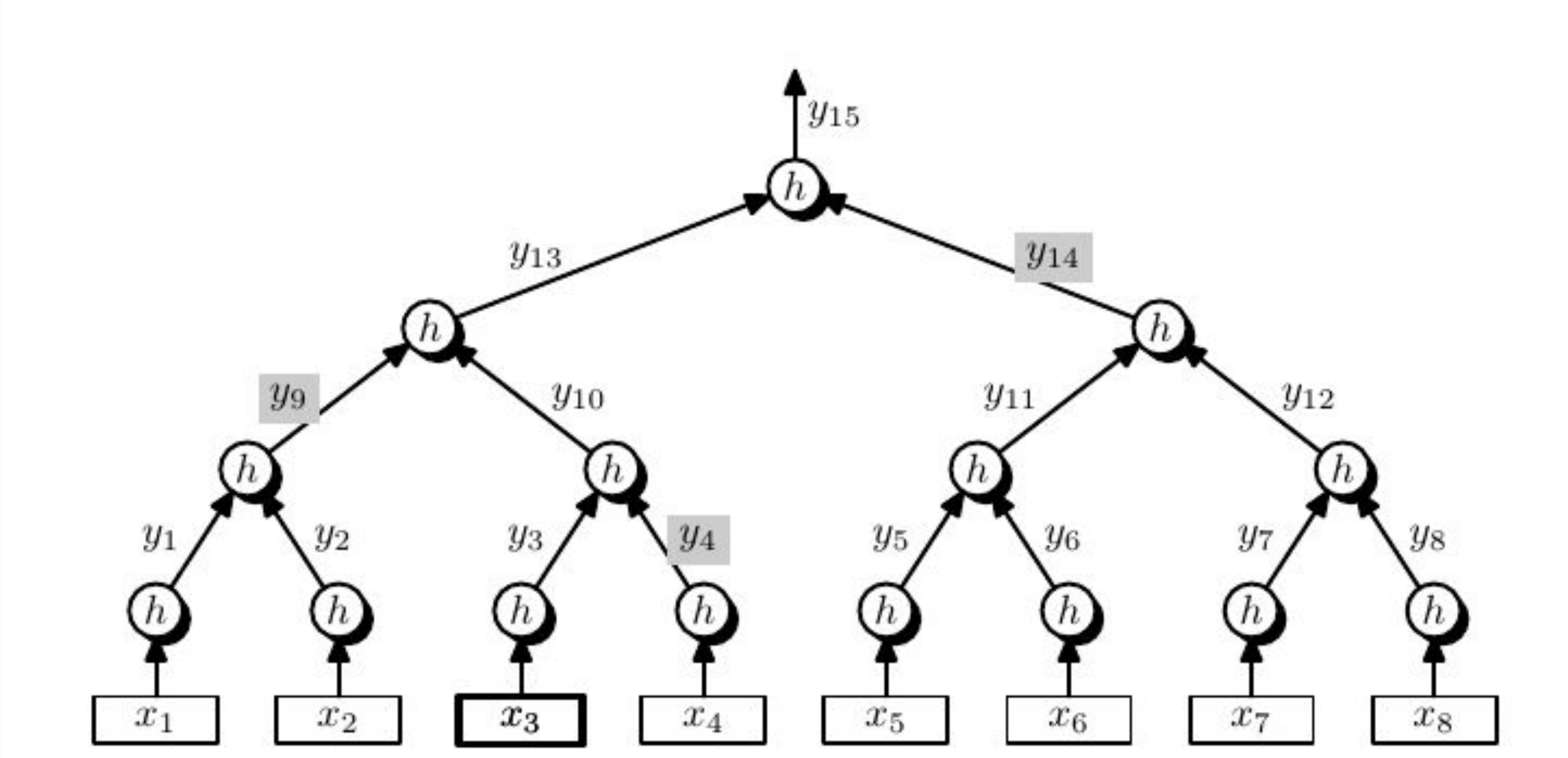
“Ralph Merkle saves our life”

-- all blockchain researchers

yeah, this smiley dude right here

Proof of Membership



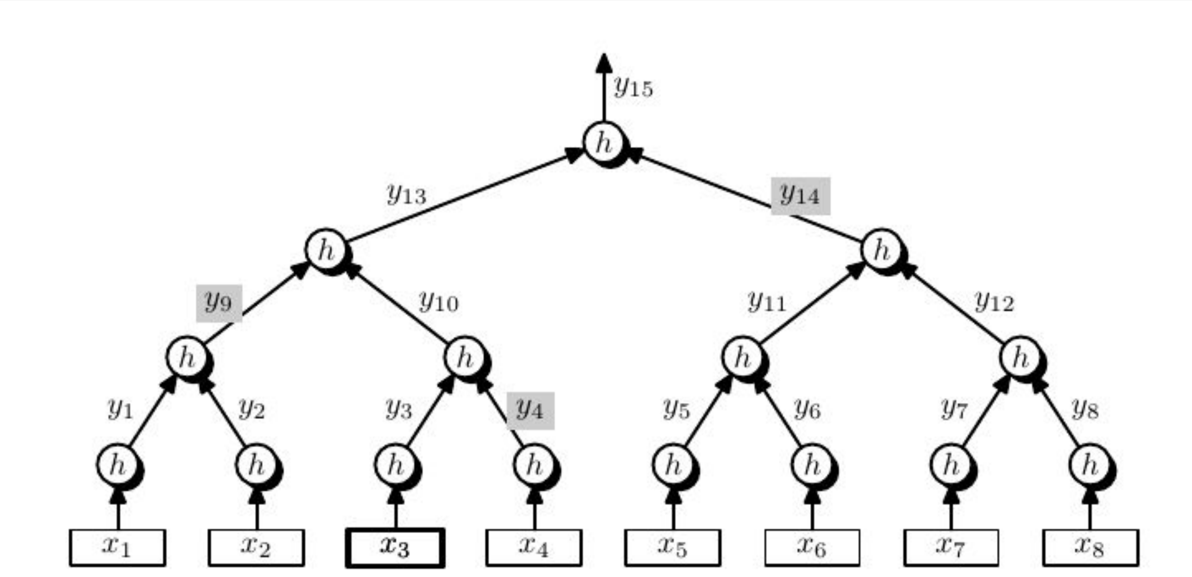


inputs	outputs
#66[3]	1->Bob, 2->Dave

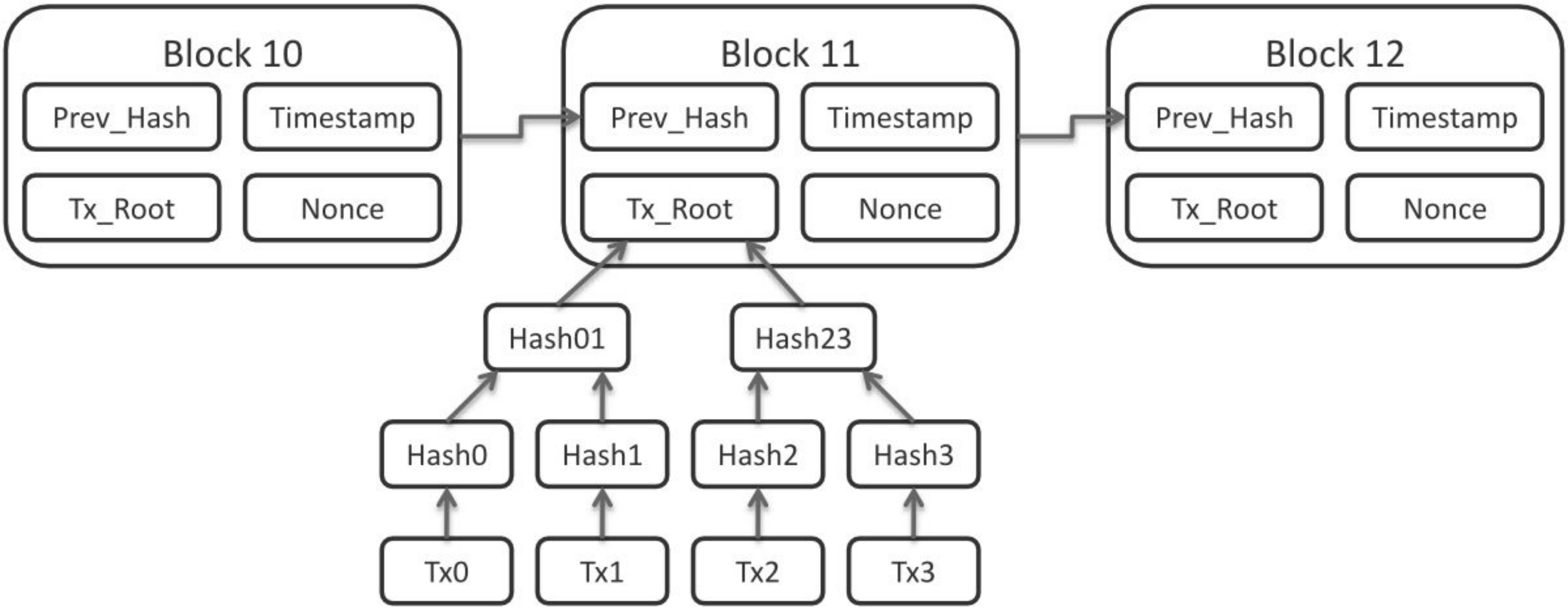
inputs	outputs
#23[1], #45[3]	49 ->Carol

Proof of Membership

Question: How to do ***Proof of Non-membership*** ?



The Most Important Picture !



Conclusion

- □ **Motivation**: Pre-Bitcoin Area
- □ **Blockchain**: Data Structure for Secure Digital Ledger
- □ **Pseudonymity**: Identity on Bitcoin
- □ **Nakamoto Consensus**: Coming to Agreement
- □ **Bitcoin Protocol**: Putting All Together

Assignment !!

- ❑ Easy: **draw** out “**the most important picture**” and explain along each components
  - ↳ What are they?
  - ↳ Why are they used?
- ❑ Medium: **read** the following
  - ↳ <How does blockchain works> first half.
  - ↳ NBFMG Textbook Intro & Chapter 1
- ❑ Hard:
  - ↳ **Research** on how to do “proof of non-membership”

Thank you!

🔨 with 💙 by

👷 Alex Xiong

💬 https://t.me/ntublockchain