# Demystifying Blockchain Series

Blockchain@NTU Facebook Page

Slack Channel (Slides, materials)

BLOCKCHAIN @ NTU SINGAPORE

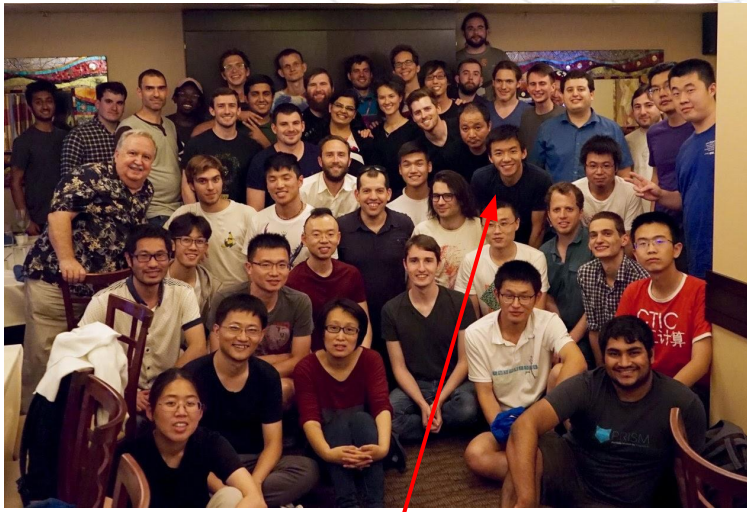
# Demystifying Blockchain

The Absolute Minimum You Should Know About Blockchain, No Excuse. (Part1)

BLOCKCHAIN
@ NTU SINGAPORE

# > $ whoami

- **Alex -- NTU electrical engineering student**
- **Started in late 2016, interested in applied cryptography, distributed system.**
- **Worked at ConsenSys Diligence team in New York ( Summer 2017 )**
  - Smart contract development
  - Whitehat + Code auditing (0x Project)
  - Found bug in memory management in Solidity Compiler (v0.4.12)
- **Built**
  - Bytecode verifier (command line tool)
  - TEE chain prototype (with Ittay, Odded from Cornell and Aparna from Berkeley)
  - Authview decentralized review system (with Zhiyao)
- **Research:**
  - Practical **cross-chain exchanges using trusted hardware and state channel** ( with Loi Luu from Kyber Network)



Me and my teeth

# Blockchain @ NTU Singapore

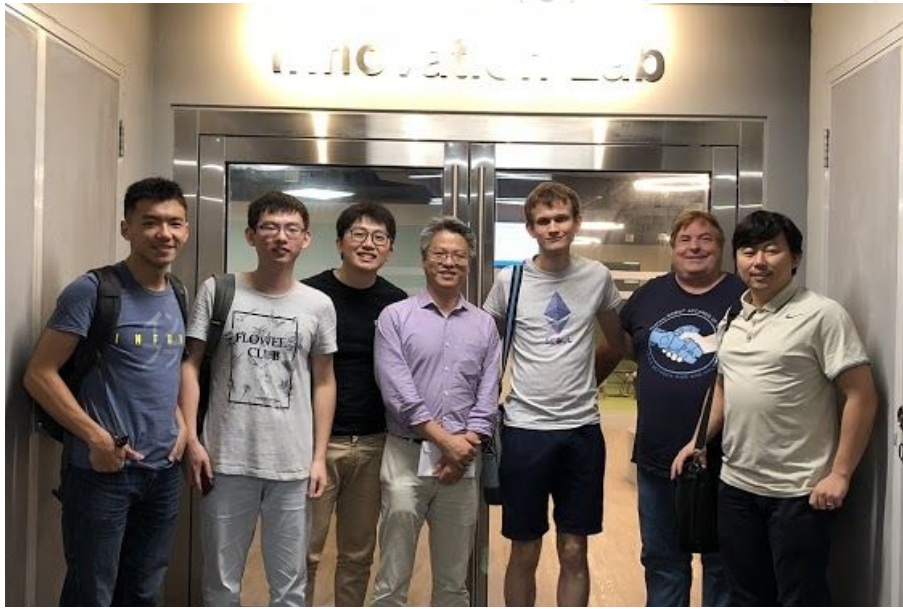
- Research, develop and educate
- Academic research +

  dApp projects +

  Weekly sharing +

  Industrial networking
- Advisor: Prof. Wen (SCSE) and

  Vitalik (Ethereum Foundation)



Penn blockchain

BLOCKCHAIN AT BERKELEY

BLOCKCHAIN @ NTU SINGAPORE

# Motivation



CNBC HOME INTL NEWS MARKETS INVESTING TECH MAKE IT

## Google and Goldman Sachs are two of the most active investors in blockchain firms: Report

- Google and Goldman Sachs are two of the most active corporate investors in blockchain companies
- In 2017, there have been 42 equity investment deals by corporates, totaling $327 million


BLOCKCHAIN @ NTU SINGAPORE

# Motivation

Distributed

PSEUDONYMOUS

DECENTRALIZED


Distributed Ledger Technology

BLOCKCHAIN @ NTU SINGAPORE

# About Workshop: How

- Mathematical, logical, technical reasoning
- Buzzword free, self-contained
- For dev: we code, test and repeat
- Guided bootstrap your self-learning

- “10-year old test”

# About Workshop: What

## Week 1 (Yes! Wake up! ):

history →cryptography basics →peer-to-peer network

+ proof of work →Bitcoin design →mining, storing,

using Bitcoin →attacking Bitcoin →applications

→from Bitcoin to Altcoin to Ethereum

# About Workshop: What

## Week 2 (ride the wave, baby):

Ethereum crash course →smart contract maniac → decentralized application → token fever →private chain and case study →Blockchain@NTU →existing bottleneck, solution, research frontier →reading list

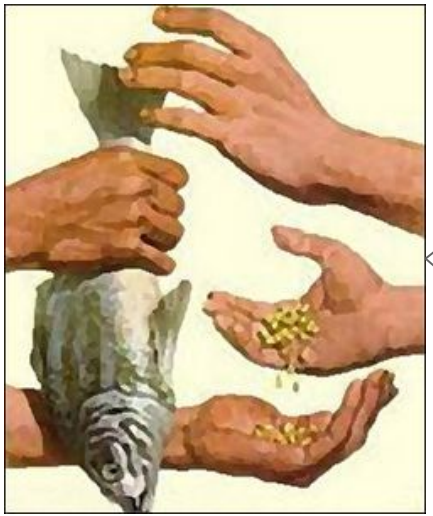
# About Workshop: What

## Week 3 (code, debug, repeat):

"Hello,World!" smart contract →Solidity basics →inter-contract interactions →Truffle framework + testrpc →writing test scripts →web3 library →ERC20 standard →commit-reveal paradigm →advanced topic (exploiting vulnerable contracts etc.)

# Blank Page Alert

# Let's start from the beginning…

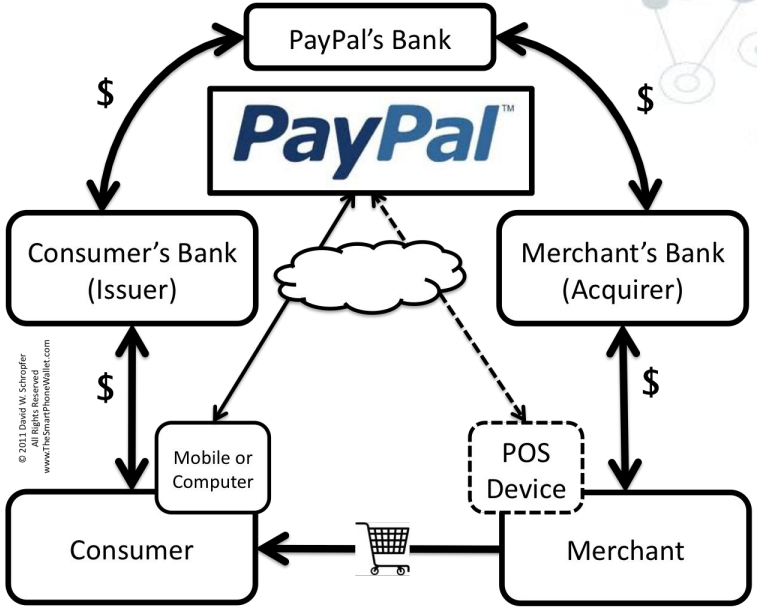


Coordination Problem?

CREDIT

# Credit Card…

- **Intermediary Model: Paypal, Amazon**
  - give credit card details
  - Paypal approves and notify sellers
  - Settle at the end of the day



# ...and problems

- Upside:
  - don't have to give identity to merchant
- Downside:
  - must have the same intermediary
  - trust Paypal (grant your credit card info)


It's 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach

Tuesday, October 03, 2017 Swati Khandelwal

# Cash / Fungible

- No default on debt
- Better anonymity
- Offline, no third party required

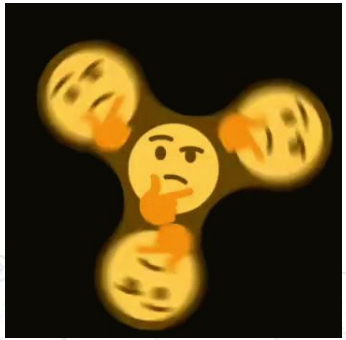
# One Trillion Dollar Question

Best of the both worlds?

**Secure digital cash**

**with pseudonymity**

**without central authority**



# DigiCash : Chaum magic

- **“redeemable note” →digital signature**
- **Oh, no, “double spending”!**
  - I pick a serial number?
  - YOU pick a serial number and cover it→”Blind Signature”
  - random subset decoding [Chaum, Fiat, Naor]

# B-Money: Wei Dai cypherpunk

- use computation puzzle (Hashcash) + linked timestamping
- cited by Satoshi
- smallest unit/denomination in Ethereum

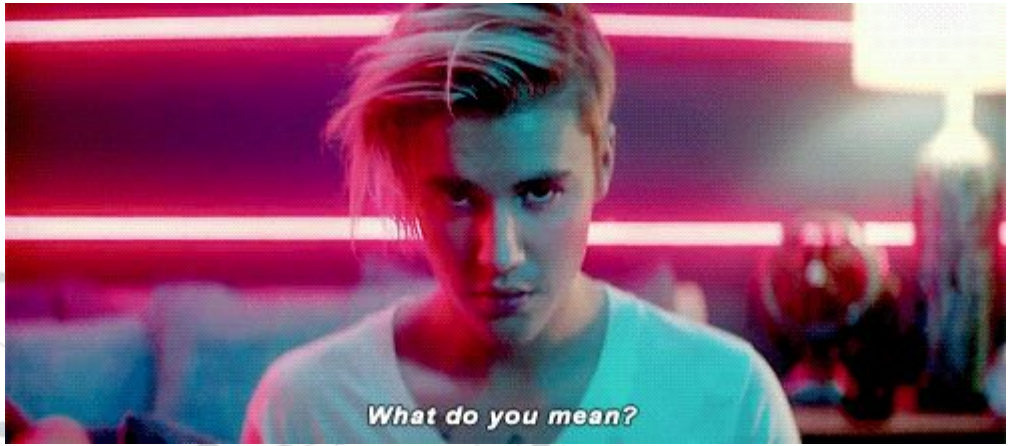
# Enough history, let's talk money

# What do I mean?

**Secure digital cash**

**with pseudonymity**

**without central authority**



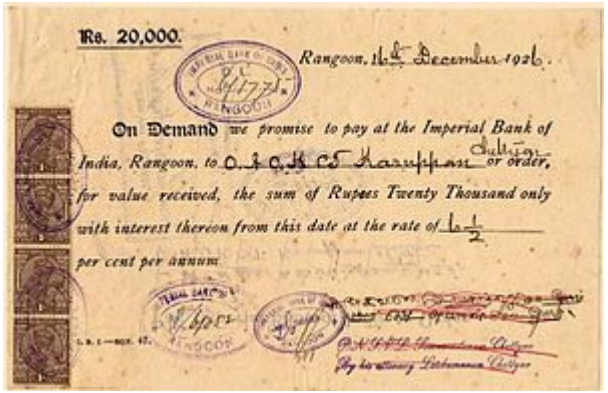
# Secure Digital Cash

- **Digital Cash**
  - Ledger with “State” and “State Update”
- **Secure**
  - Validity
  - No double spending

# Secure Digital Cash: validity

- Unforgeable stamp

  →detour to Digital Signature

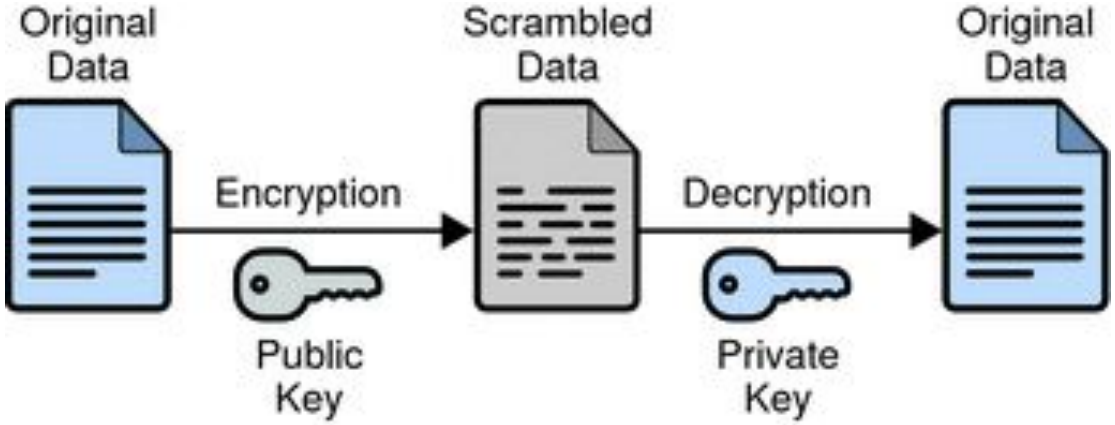
# Digital Signature in a Nutshell

- Sign on “messages” using a secret known only by myself: secret key

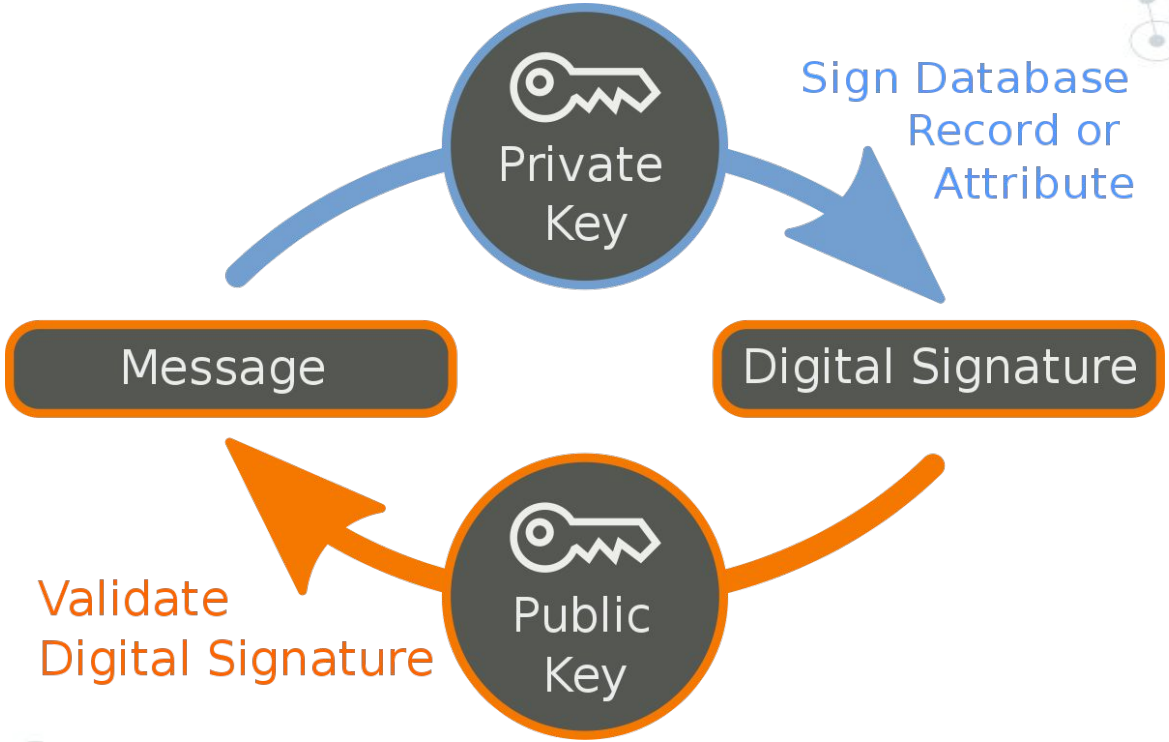
- Verifiable by anyone via public key, yet unforgeable

# Public Key Encryption

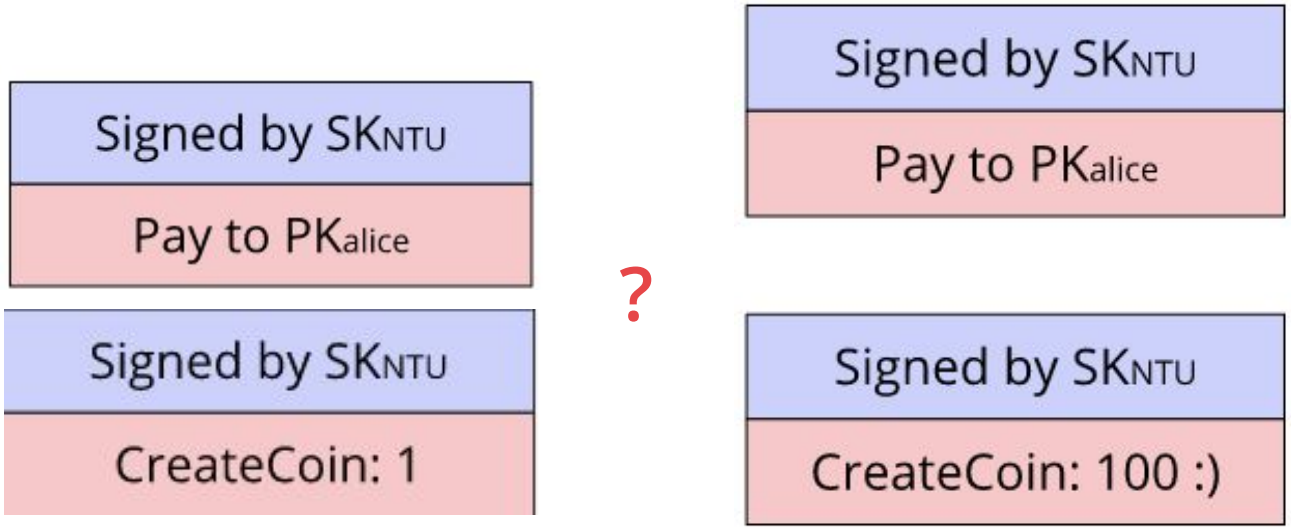
- a.k.a. asymmetric encryption
- idea: key pair (public key, private key)



# Digital Signature in a Nutshell



# Spending Coin



# Hash Function

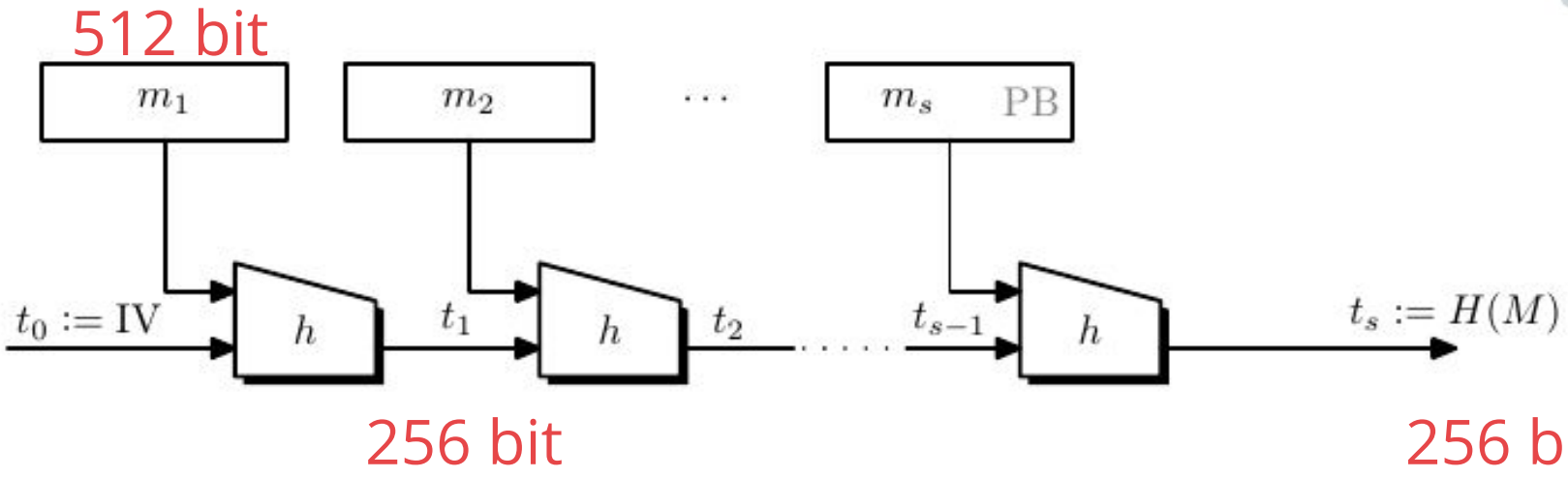
- a.k.a Message Digest
- One-way Function
  - “Meat Machine”
- Long plaintext →short digest

```
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
```

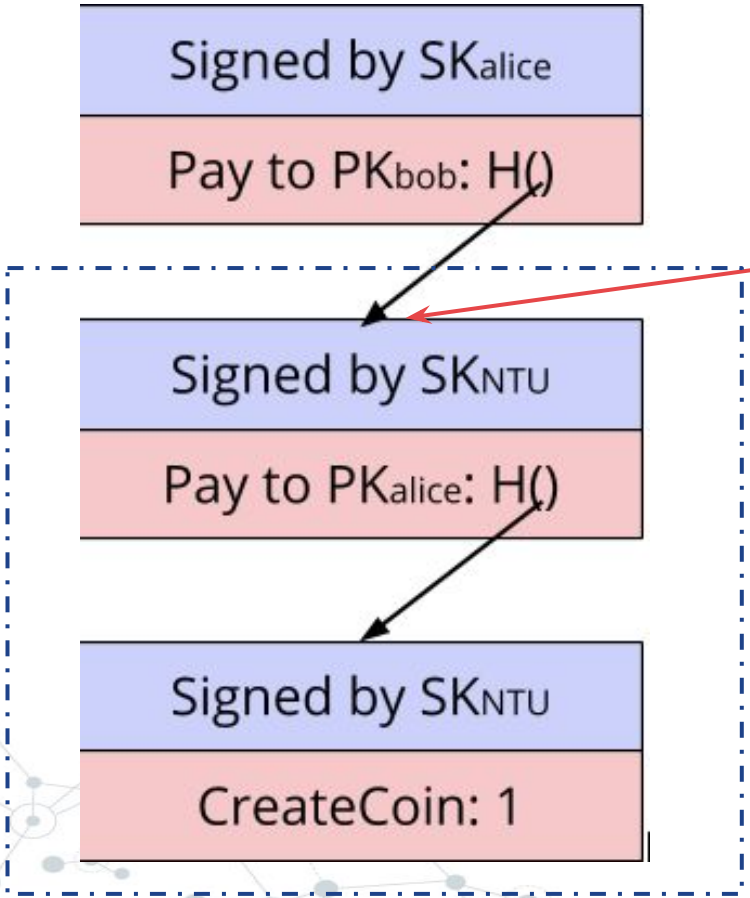
# Hash Function

- **Universal Hash Function (UHF)**
  - Keyed hash
  - e.g. Carter-Wegman MAC uses UHF + PRF
- **Collision Resistant Hash**
  - Keyless hash
  - e.g. SHA1, MD5, **SHA256**, **SHA3** etc.

# SHA256


512 bit
$m_1$
$m_2$
$\cdots$
$m_s$ PB
$t_0 := \mathrm{IV}$
$h$
$t_1$
$h$
$t_2$
$t_{s-1}$
$h$
$t_s := H(M)$
256 bit
256 bit

# Spending coin the right way…?



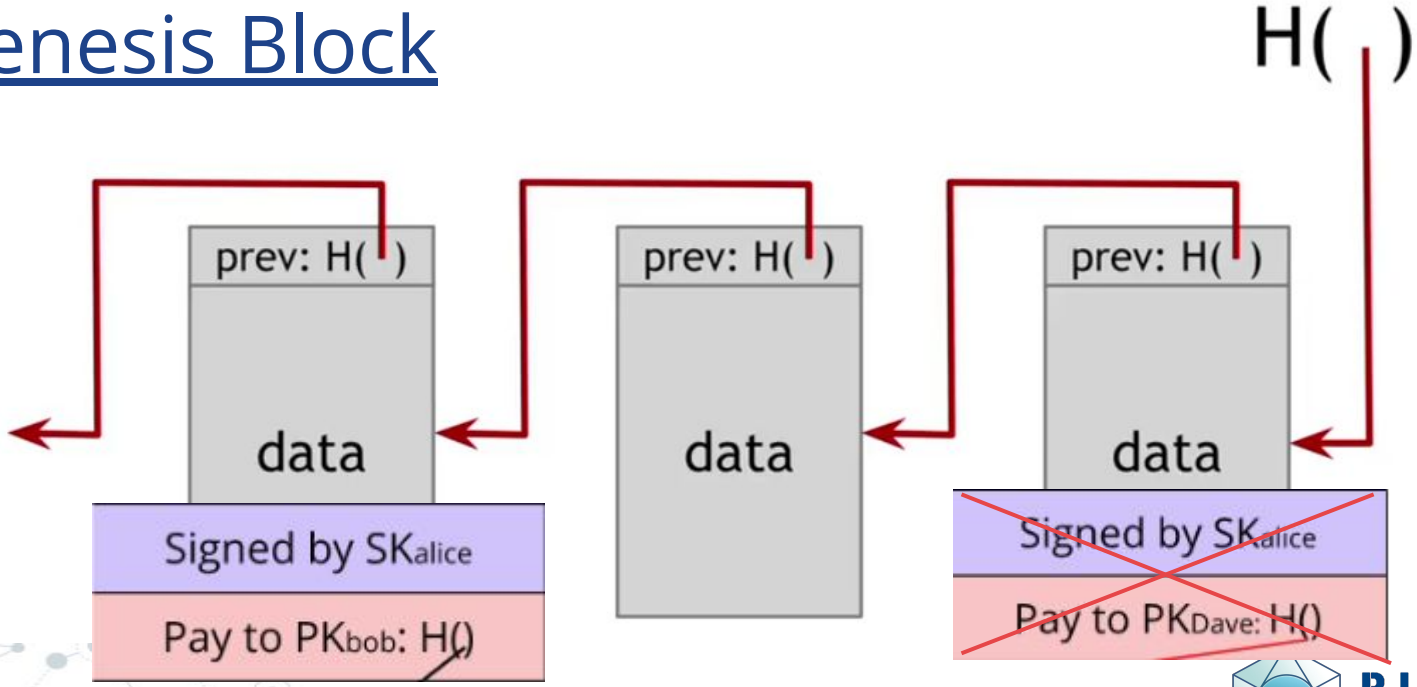

Whoops….

Double Spending

# Hash Pointer (a.k.a. Block Chain)

use case: *tamper-evident log*

[Genesis Block]

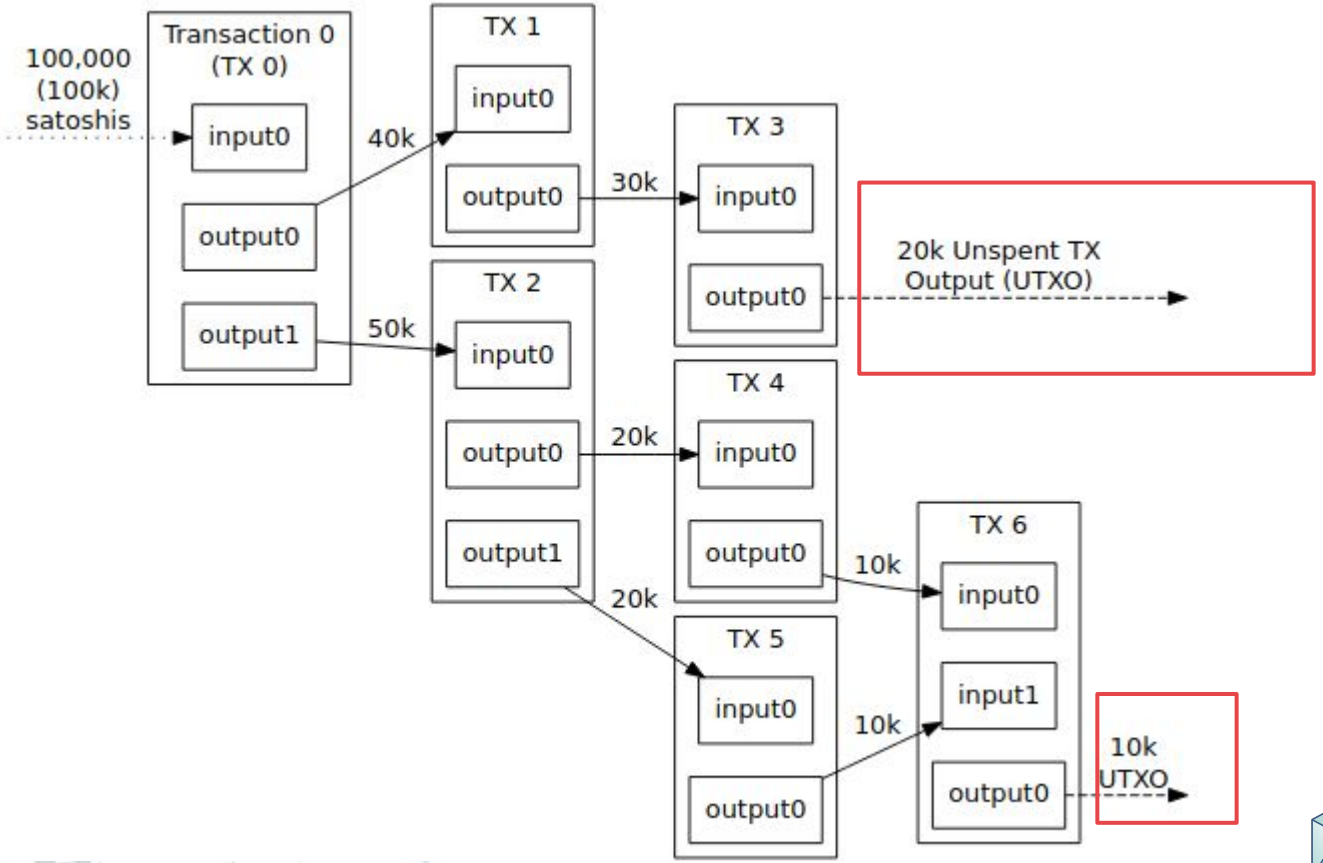


# Putting them together

- No double-spending
- Multiple inputs, outputs
- Immutable

| 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 | | |

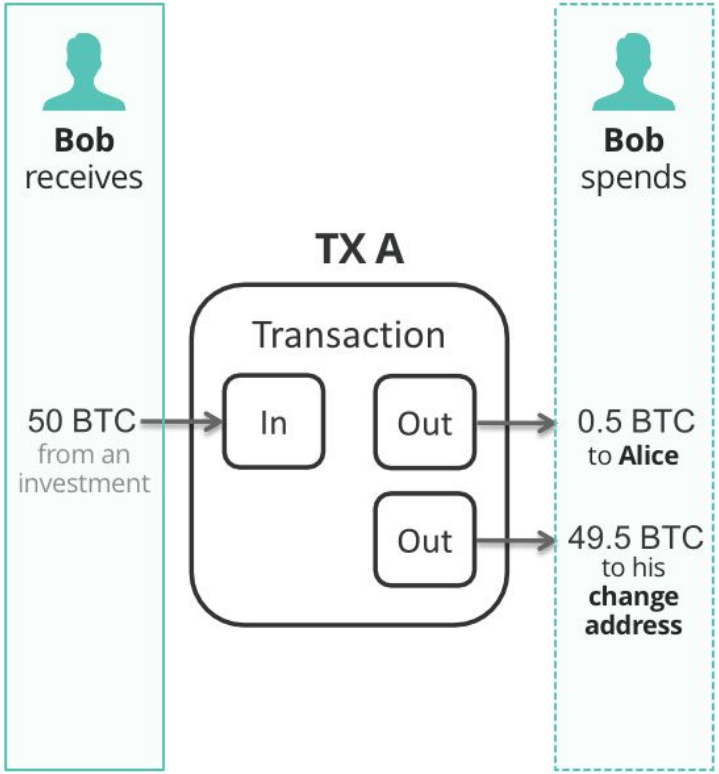
# UTXO: Unspent Transaction Output



# UTXO

Keep the change?

Send to yourself !

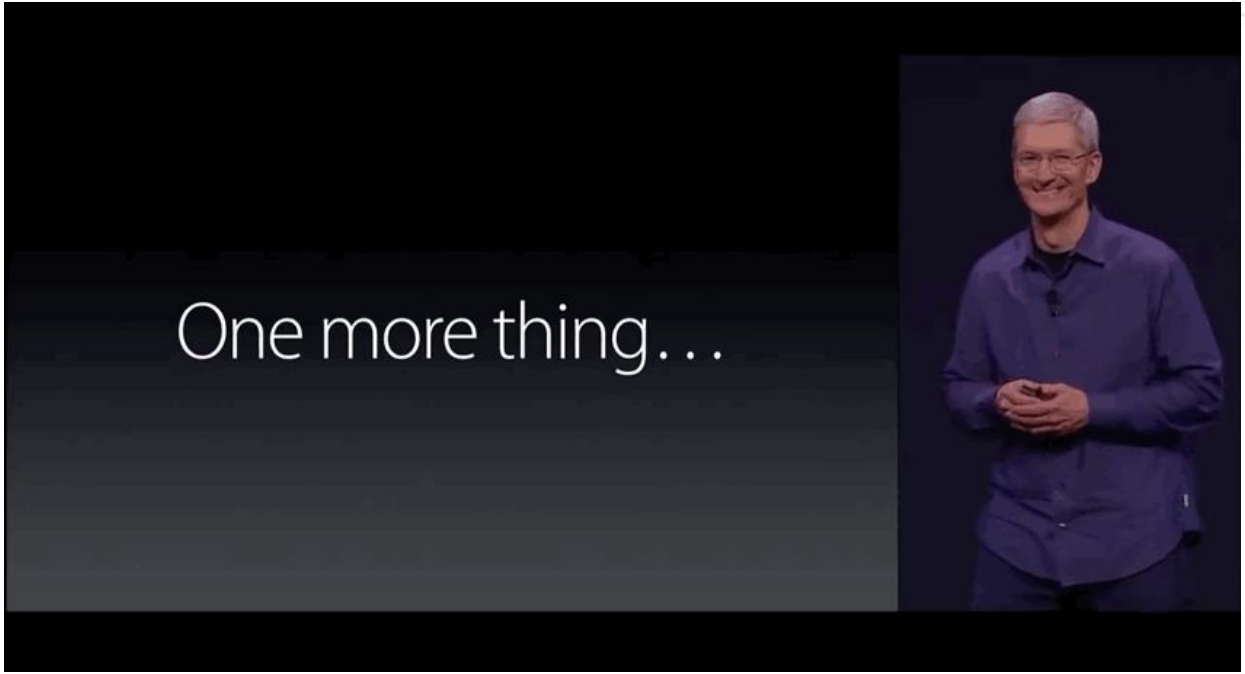


# Putting them together

- No double-spending
- Multiple inputs, outputs
- Immutable

| 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 | | |

# Oh, one more thing…



# Merkle Tree

**“Ralph Merkle saves our life”**

-- all blockchain researchers

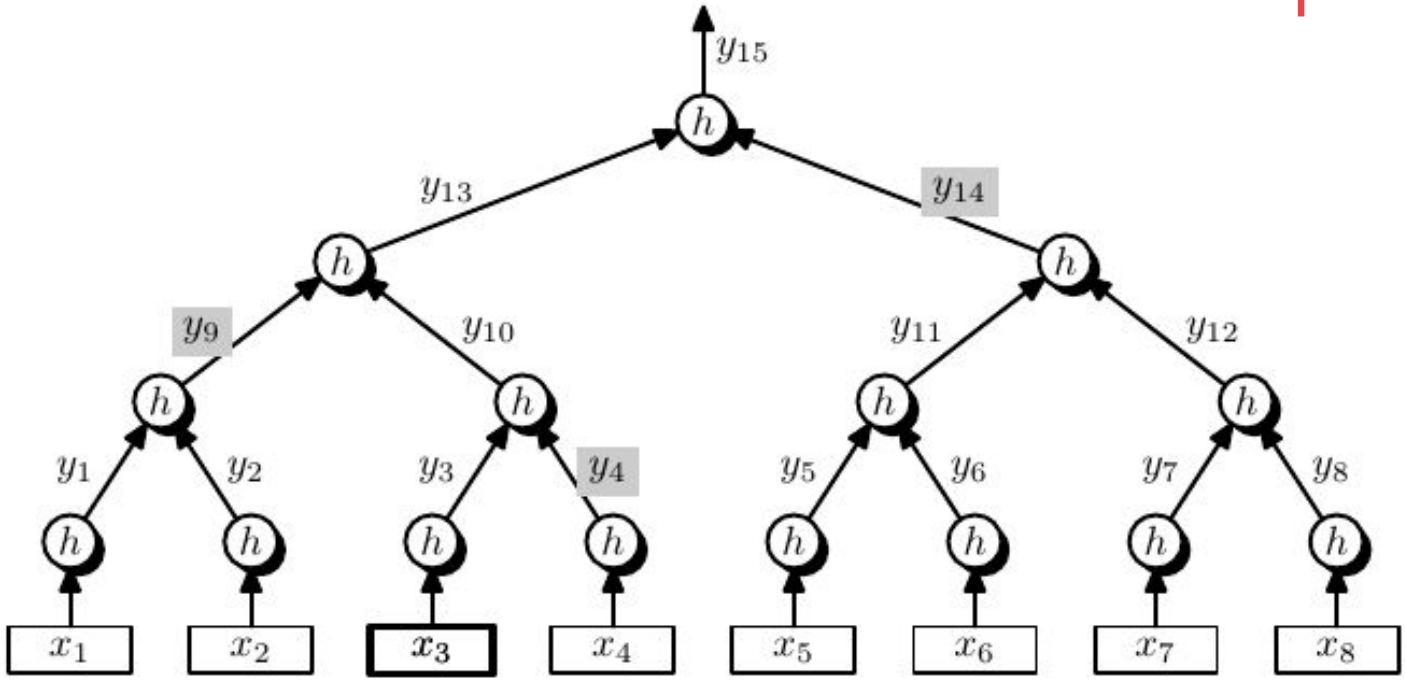
**“We all should thank this guy”**

-- Vitalik Buterin

yeah, this smiley dude right here

# Merkle Tree: proof of membership

Homework: Proof of non-membership



# What do I mean?

Secure digital cash

**with pseudonymity**

without central authority

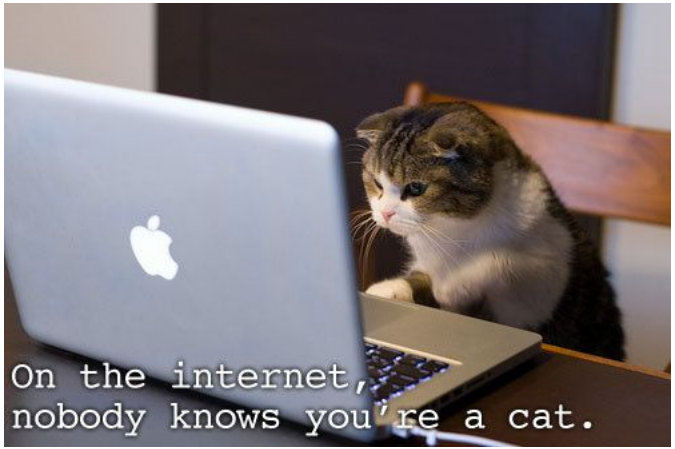
# Identity on Blockchain

- Public key is your identity !!
- Address: last 20 bytes of sha3( public key )

```
> 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] }
```

# Pseudonymity

- Create as many accounts as you want
- Doesn't directly associate with your real-life identity
  - Really? (mixing, differential cryptanalysis, ring signature)



# What do I mean?

**Secure digital cash**

**with pseudonymity**

**without central authority**

# Client-server v.s. Peer-to-Peer Mesh

- Who include new TXs?
- Who verify others TXs?
- Who maintain and update the ledger?
- Who create the coins?


# Distributed Consensus

- Geo-scattered i18n friends deciding a holiday plan
- Someone needs to draft a “proposal” (witness, transaction, statement…)
- And he/she needs to “broadcast” to connected friends
- There are time-zone difference, message delay…
- People need to “vote” or re-propose
- Certain threshold of votes constitute an agreement

# 2 Goals

- **Safety property**: **consistent** on the agreed value
  - either “haven’t agree yet”
  - or  agree on the same value
- **Liveness property**: **will eventually terminate and make progress**

# Consensus is hard!

- **nodes might crash or outright malicious**
  - Byzantine failure, Crash failure
- **network delay, latency**
  - FLP impossibility result [Fischer, Lynch, Paterson]
- **nodes connectivity**
- **"Sybil Attack" in open, pseudonymous network**

# Consensus in Bitcoin

1. New transactions are broadcast to all nodes (gradually)
2. Each node collects new TX they hear into a block
3. Each round, one random node gets to broadcast its block
4. Other nodes accept the block if all transactions inside this block is valid (unspent, signatures)
5. Nodes express their acceptance by including its hash in the next block they create.

# Proof of Work (PoW)

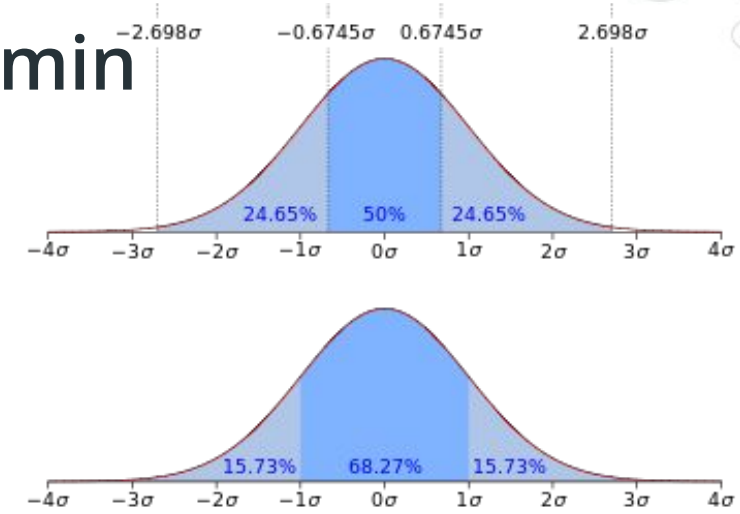
- "Non-monopolizable" resource: **computational power**
- Hash puzzle:

H(*nonce* || *prev_hash* || *tx*... ||*block reward tx*) < target

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

# Proof of Work (PoW)

- Difficult to compute (not “guessable”)
- Trivial to verify
- Adjustable overtime ≈ 10 min

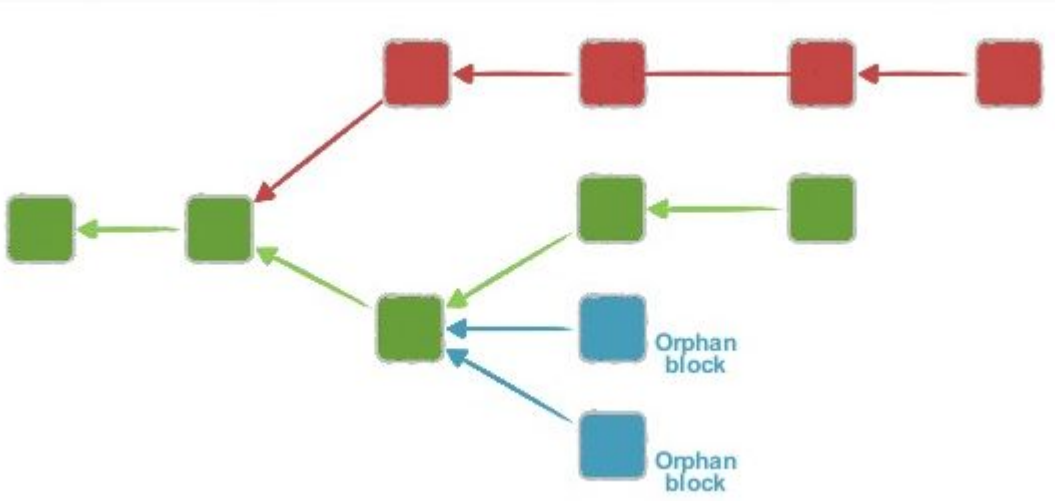

BLOCKCHAIN @ NTU SINGAPORE

# Incentive in Bitcoin

- **Block Reward**
  - 12.5 BTC/block, halves every 210,000 blocks
  - total supply: 21 million BTC (Year 2040)
- **Transaction Fee**

# Nakamoto Consensus (all together)

1. Cryptoeconomics (using incentive)
2. Randomness (block interval)
3. Computational Puzzles
4. Longest chain wins (a.k.a. canonical chain)
   - Orphan blocks
   - Stale blocks



# Fist bump, balalala

**Secure digital cash**

**with pseudonymity**

**without central authority**

# Bitcoin Design: recap + beyond

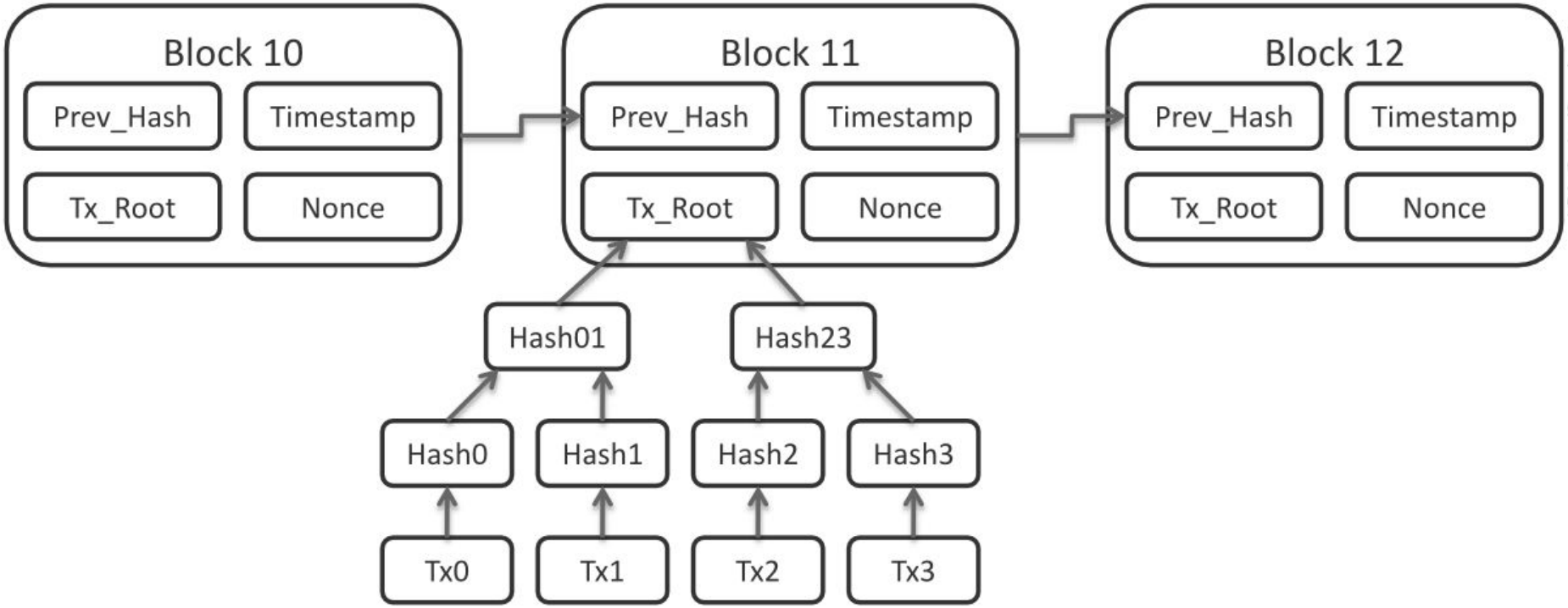
Nakamoto Consensus +

UTXO (Unspent Transaction Outputs) +

Blockchain on Merkle Tree +

Bitcoin Script

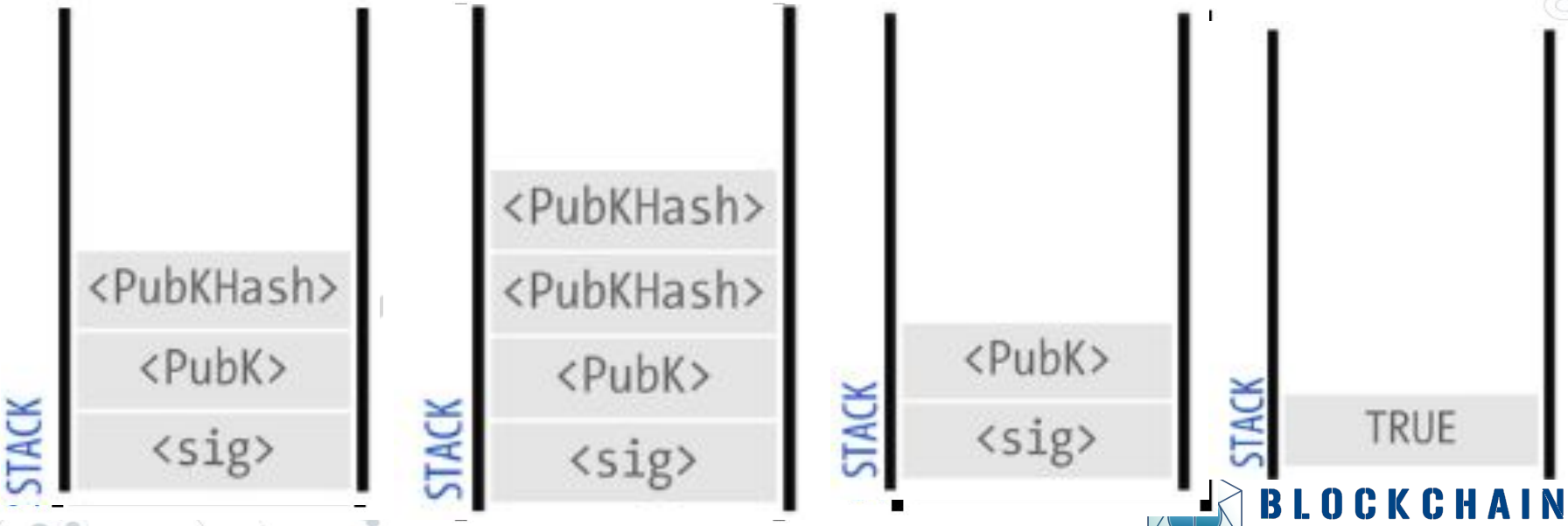
# Bitcoin Design



# Bitcoin Design: Bitcoin Script

## Output to script !

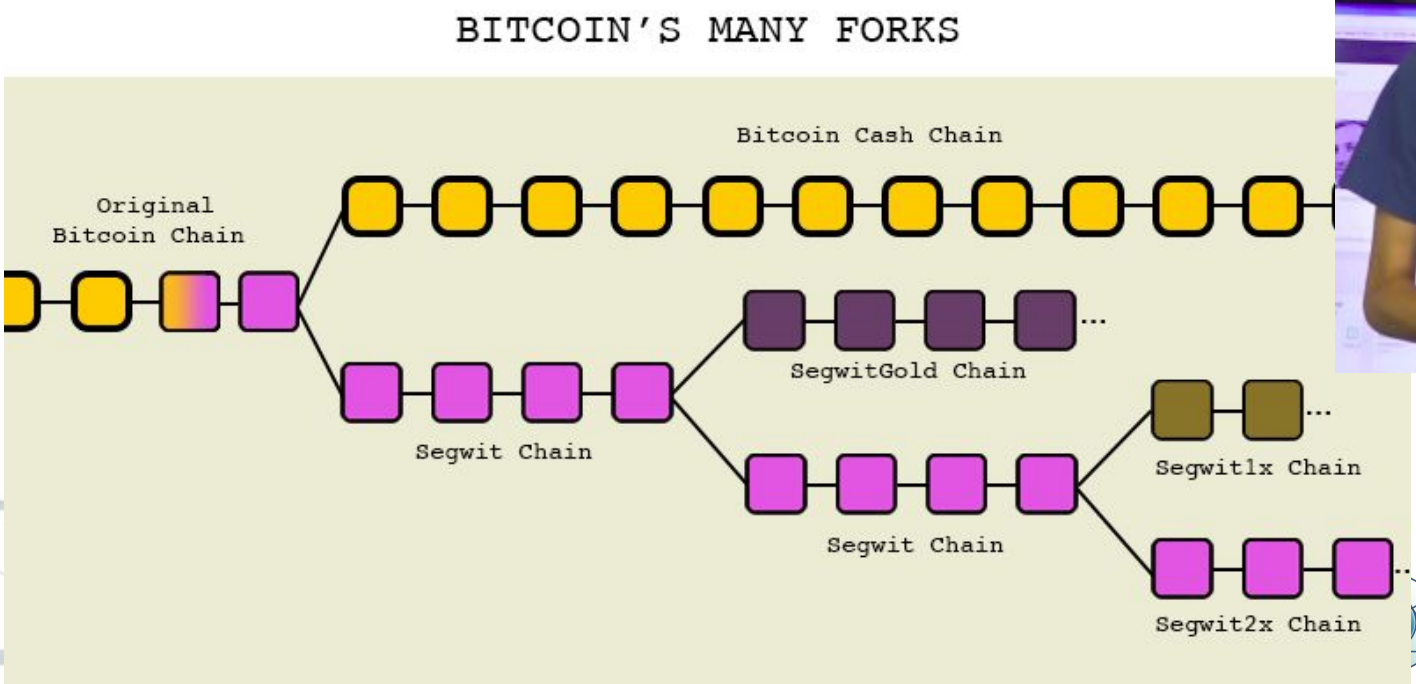
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG



# Bitcoin Design: block confirmation

6 block confirmation ≈ 1 hr

Softfork and Hardfork

# Bitcoin Design: FAQ

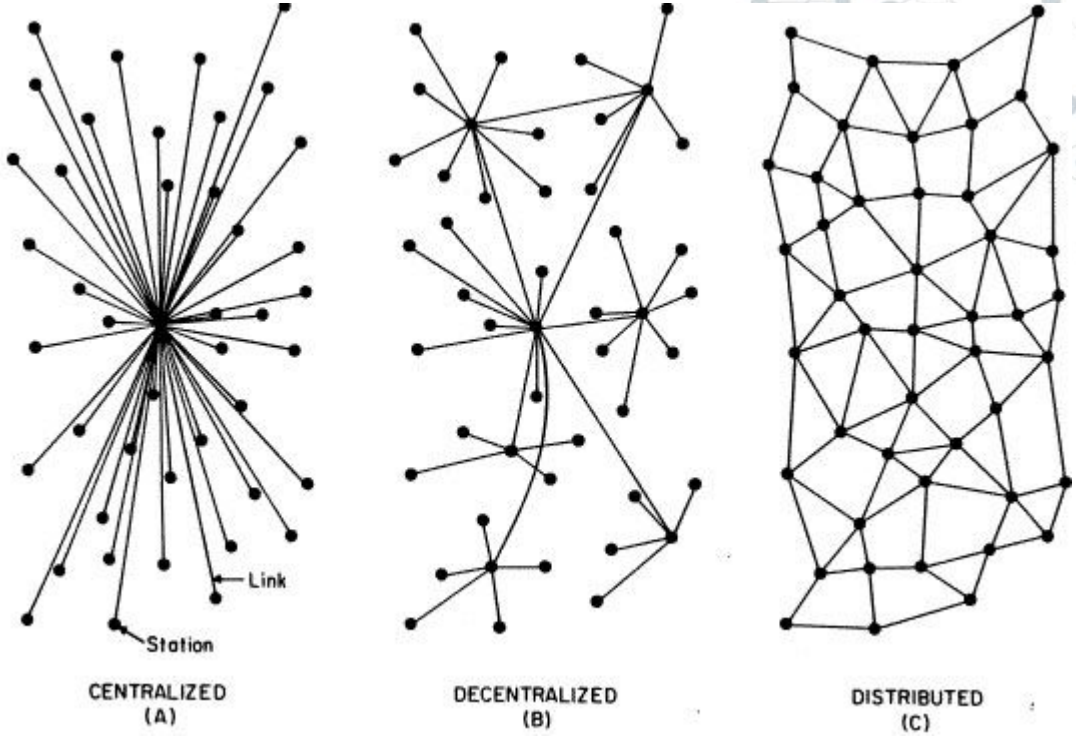
- Censorship Possible?
- Stealing money?
- Can NSA destroy Bitcoin Network?
- No more block reward after 2040?
- Wasting energy?

# Decentralization v.s. “Walled Garden”

It’s not binary!

nor

all-or-nothing!

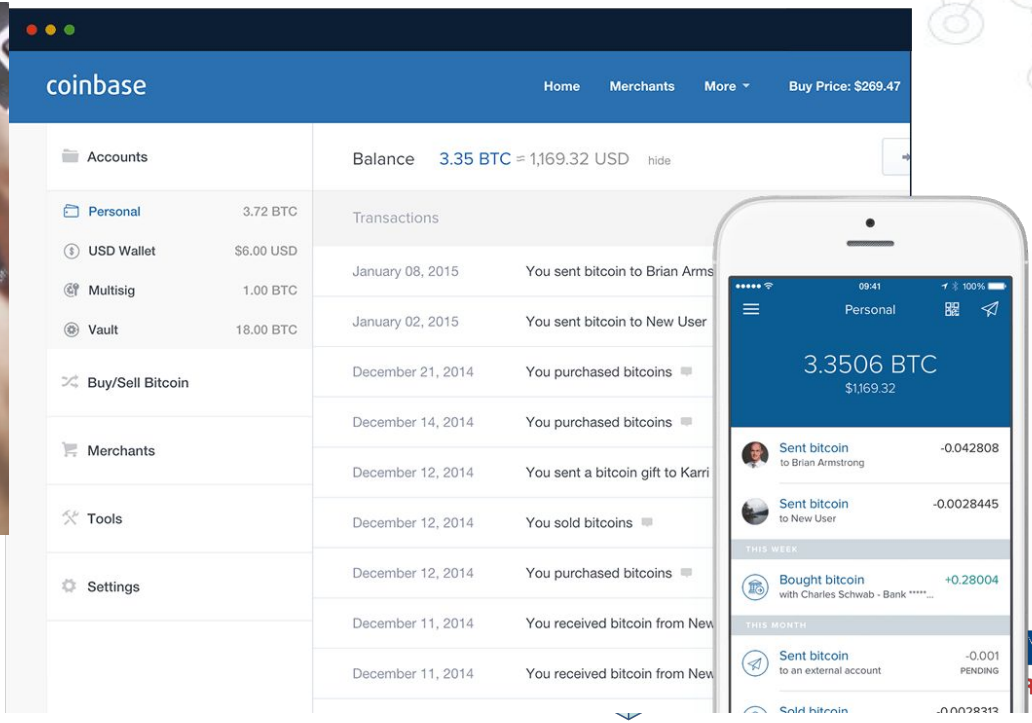


# Decentralization Polygraph

- Who maintains the ledger?
- Who decide which transactions to include?
- Who prints new cash / creates new coins?
- Who changes the rule of the system?

# Storing, buying Bitcoin

- Wallet (hot, cold, online, physical)



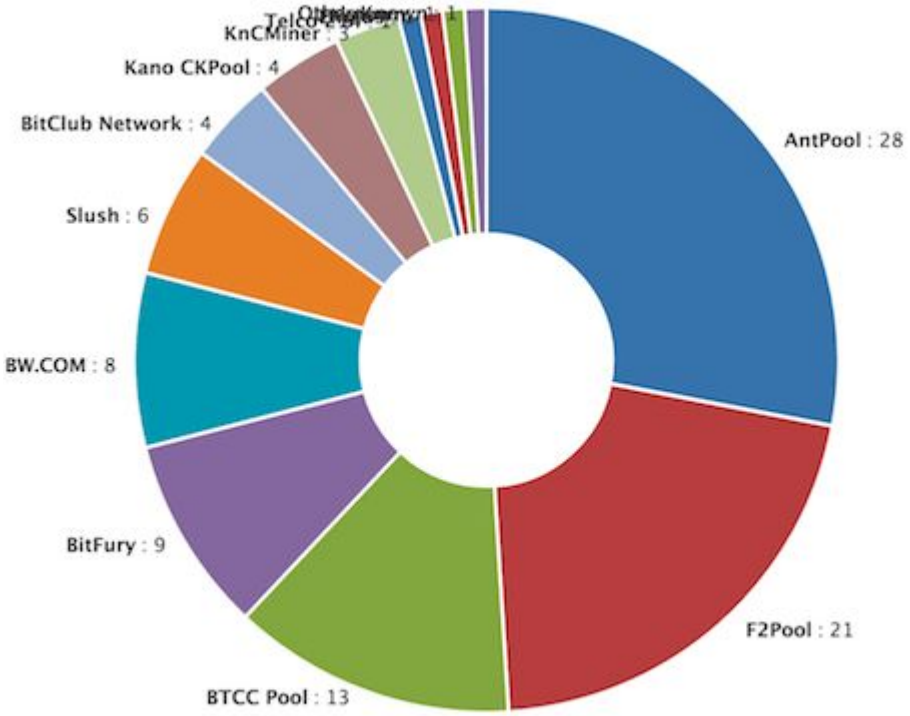
# Storing, buying Bitcoin

- Exchanges


bitbank
BITFINEX
bitonic
BITSO
BITSTAMP
bitsquare
bitt
BITTREX
BTCC
比特币中国 BTCCHINA.COM
Coincheck
coinfloor
kraken
QUADRIGACX
ripio
ShapeShift
THEROCK TRADING LTD.
Zaif

# Bitcoin Mining

- Mining Pool
- Mining Farm
- Special Hardware
  - GPU mining
  - ASIC mining
  - FPGA mining

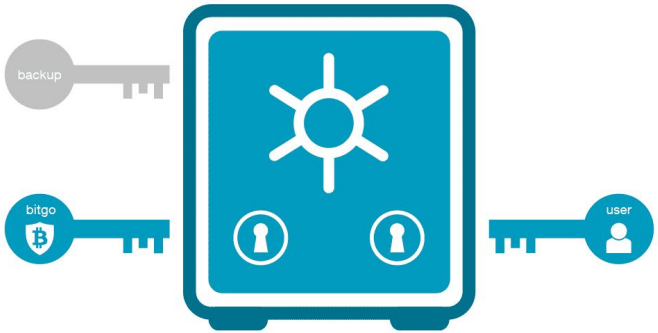


# Attacking Bitcoin

- 51% Attack
- Front-running Attack
- Selfish Mining (block withholding attack): 33%
  - Stubborn mining, feather forking, punitive forking attack (next time)

# Applications on Bitcoin Blockchain

- Smart Assets: “colored coins”
- Voting: multi-sig wallet
- Domain Name Registry



# Altcoin

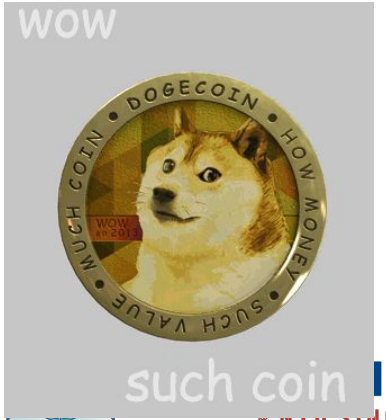
- Different puzzles?
- Different difficulty/block interval?
- Different consensus algorithm?
- Different scripting language?
- Different inflation rate?

# Altcoin

- Namecoin : decentralized DNS
- Litecoin: memory-hard hashing, scrypt
- Peercoin: Proof of Stake mining
- Dogecoin: why is everybody so serious?

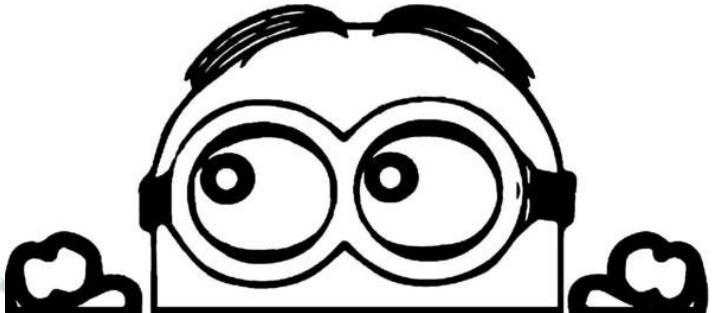
namecoin

peercoin



# Coming up next....

- Most famous Altcoin: Ethereum
- Smart Contract
- Private chain v.s. Public chain
- Bottleneck + research frontier
- Resources + reading list



# Coming up next next…

## Week 3 (code, debug, repeat):

"Hello,World!" smart contract →Solidity basics →inter-contract interactions →Truffle framework + testrpc →writing test scripts →web3 library →ERC20 standard →commit-reveal paradigm →advanced topic (exploiting vulnerable contracts etc.)

# Assignment + Reading

- Think about “proof of non-membership”

- Read:
  - Satoshi Nakamoto: Bitcoin Whitepaper
  - Vitalik Buterin: Ethereum Whitepaper

# Thank you so much!!

Blockchain@NTU Facebook Page

Slack Channel (Slides, materials)

BLOCKCHAIN @ NTU SINGAPORE

# Detour: black magic blows my mind !!

# Cryptography

- Mathematical techniques + computational theory

Hide a secret →encryption ; Reveal a secret →decryption;

Verify a statement' integrity →MAC;

Verify a statement from someone →digital signature;

Verify a statement from 1 out of N authors →ring signature;

Verify the validity of a statement without any other details about the statement → zero knowledge proof;

Calculate on encrypted data →homomorphic encryption…

“

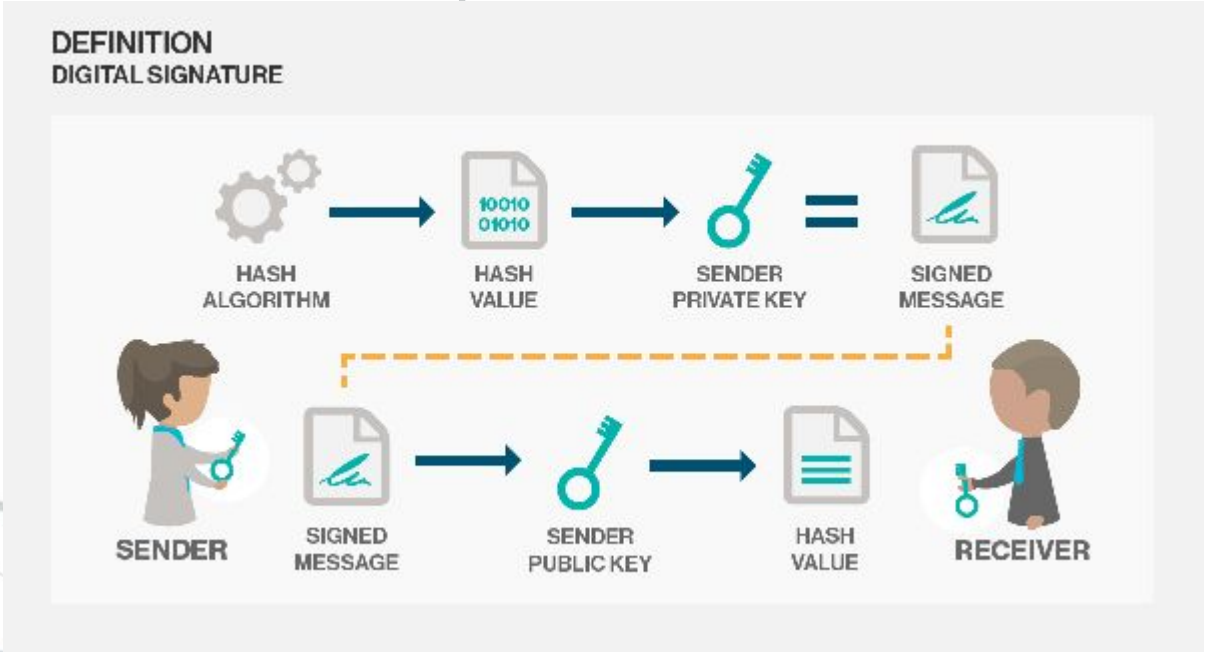
*Cryptography is power in asymmetry*

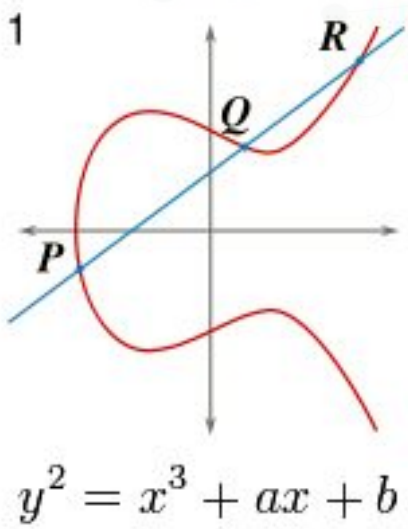
# Heuristic for Cryptographic primitive

- **Confusion : Gibberish transformation**
  - Key Addition, substitution
- **Diffusion : spread out, statistically uniformed**
  - mix-col in AES
- **Hard Problem in Math (number theory etc.)**
  - DLP, Factorization, Elliptic Curve, Shortest Vector Problem

# Digital Signature Algorithm (DSA)

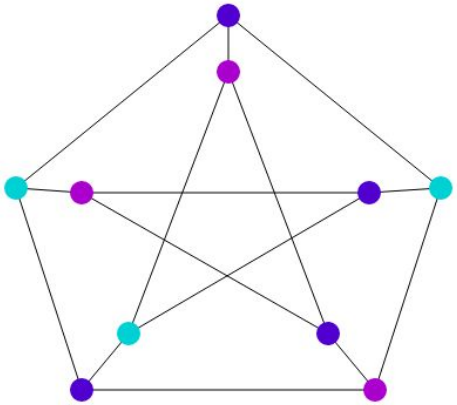
- Could based on various *hard problems*
- In Bitcoin, Ethereum: **ECDSA**

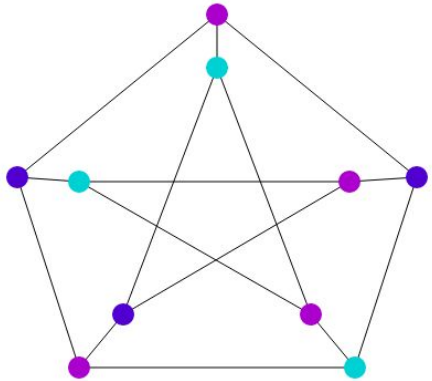


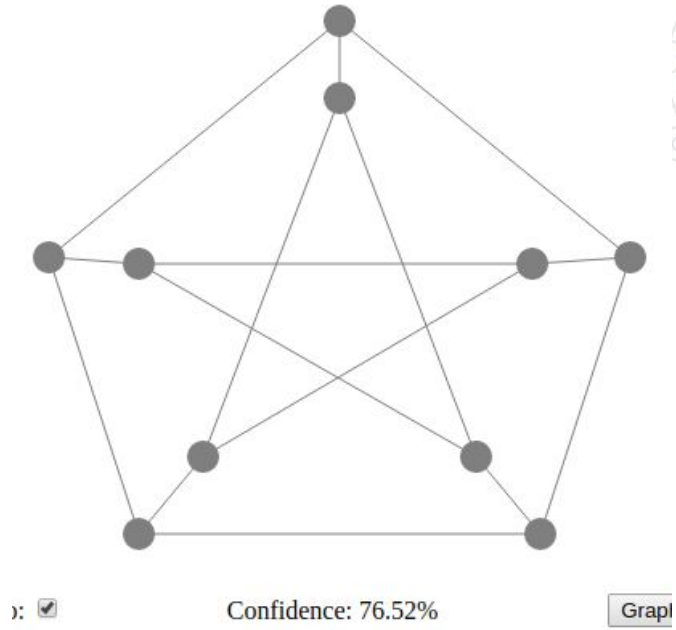



# Black magic : ZKP (3-color problem)

- **Singtel builds 1,000 signal towers**
  - 3 frequency ranges
  - no interference
  - outsource to public







# Just that you know

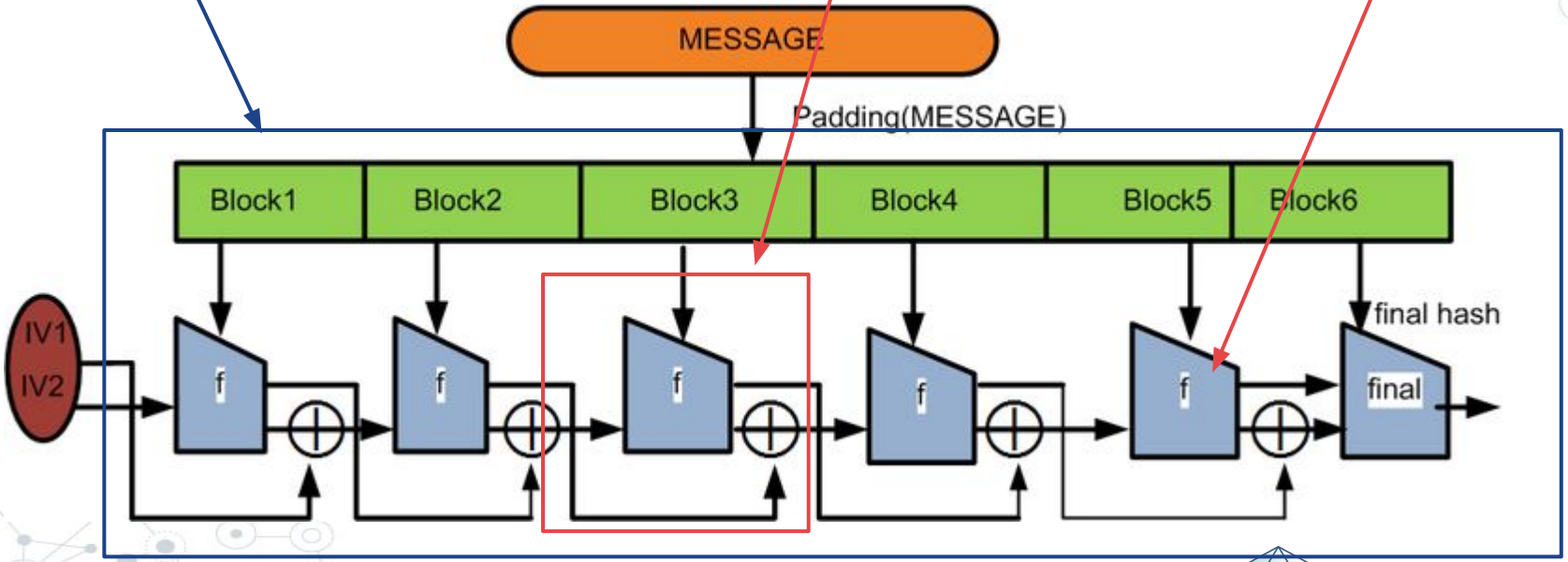
- SHA1: Github -- collision found by Google (2017)


- MD5: many Microsoft Utility -- broken by 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

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



# SHA3 using Keccak256

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