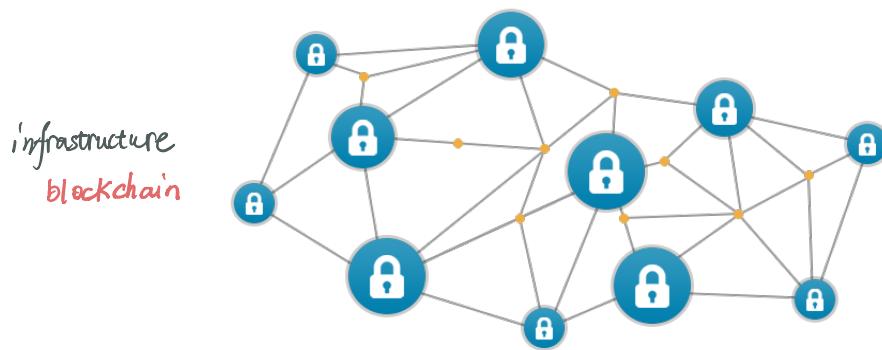


# ~~Blockchain~~ unchained

## Bitcoin

If you can't explain it simply, you don't understand it well.

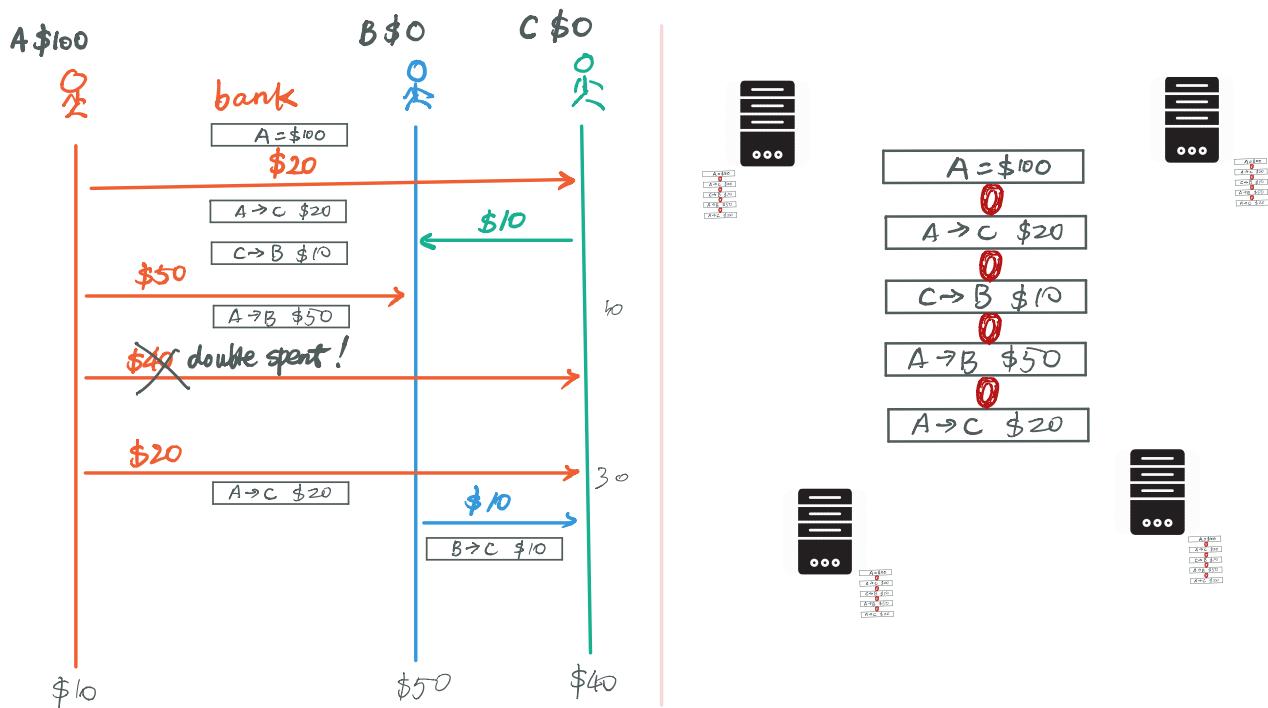


# Money Transfer

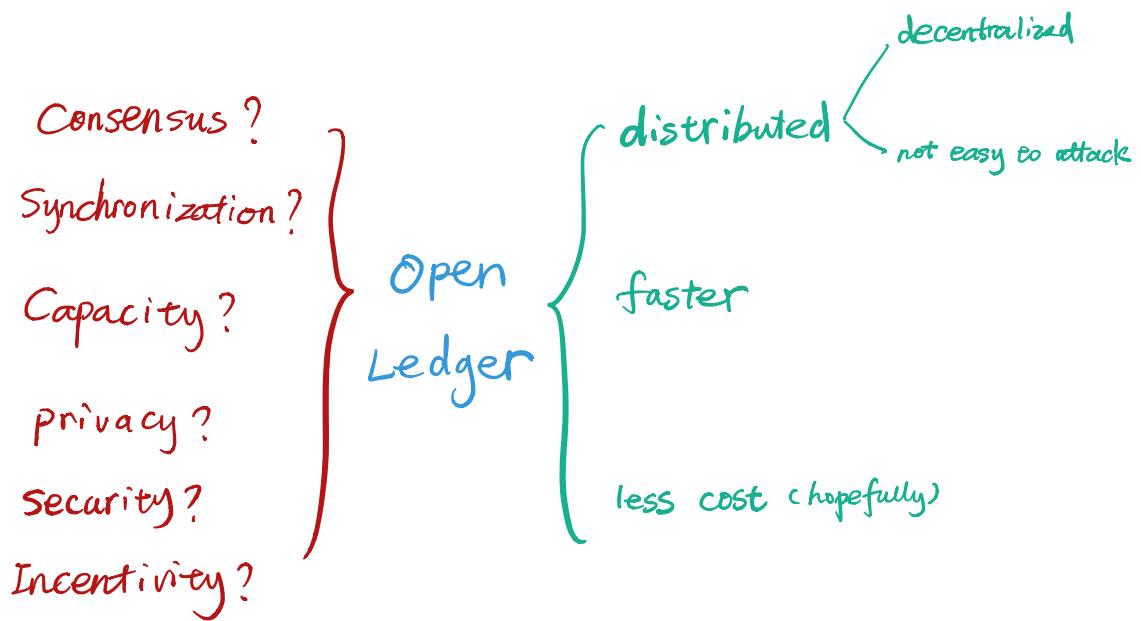


- ① takes too long
- ② fee too high

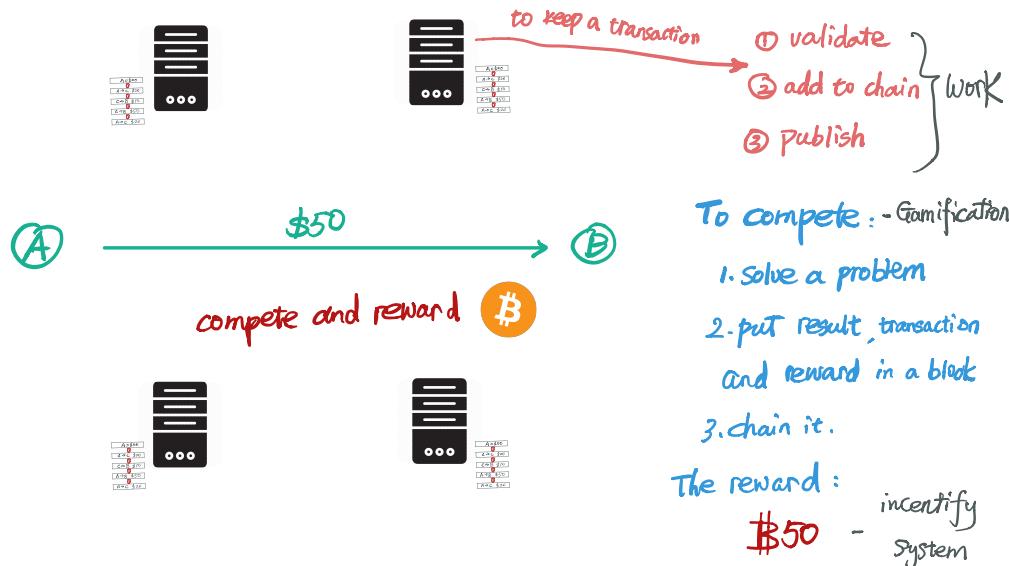
# Ledger



The history of the transaction is Currency.

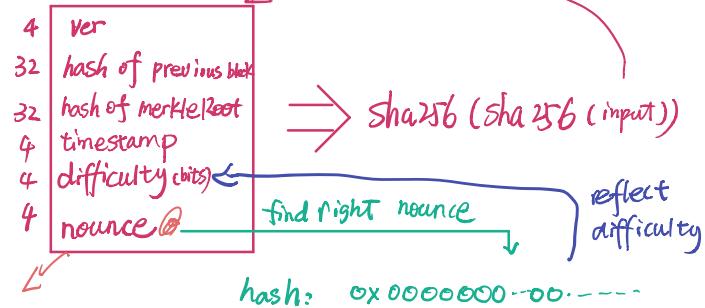


Why other people in the network wants  
to keep your transaction?



bytes	
4	magic : 0xd9b4bef9
4	length
4	ver 0x1
32	sha256 ( previous block )
32	merkleRoot
4	timestamp : creation time of the block
4	difficulty : 3,007,383,866,459,732
4	nounce: the problem to solve
	transaction count
	transactions

## Game (PoW):



what we learned:

1. to find a "nounce" is hard (random)
2. by tuning difficulty, the system can limit the generation of a block to close to 10min.
3. merkle tree + bloomfilter made wallet applicable.
4. chaining + PoW greatly reduced the chance of "do evil thing".
5. "incentive" encourage nodes to be good.

## What is a block?

- a data structure contains transactions
- linked with previous work
- blocks in longest chain excel

# Genesis Block

## Block #1

Summary	
Number Of Transactions	1
Height	1 (Mainchain)
Block Reward	50 BTC
Timestamp	Jan 8, 2009 6:54:29 PM
Mined by	
Merkle Root	<a href="#">0e3e2357e800b6cdff7fb54c3a3a17b5714ee1f9e68bebba44274bf64512098</a>
Previous Block	<a href="#">0</a>
Transactions	
0 Inputs (Newly Generated Coin)	 <a href="#">mined Jan 8, 2009 6:54:29 PM</a>
No Inputs (Previously Spent)	 <a href="#">12zDSU14qJp4Q2uXkxerL5mMBrzjJX</a> <a href="#">50 BTC [0]</a>
Type	pubkeyhash
scriptPubKey	<a href="#">4e0933be85119c726a59fe1fec1600ea139081621629f8be9749be352a9...</a> 
<a href="#">516273 CONFIRMATIONS</a>	
<a href="#">50 BTC</a>	

# Recent Block

Block #510266

<b>Summary</b>	
<b>Number Of Transactions</b>	563
<b>Height</b>	510266 (MainChain)
<b>Block Reward</b>	12.5 BTC
<b>Timestamp</b>	Feb 21, 2018 05:06 AM
<b>Mined by</b>	BTC Pool
<b>Merkle Root</b>	38967c70d63105a9e39498f111...
<b>Previous Block</b>	\$10265
<b>Difficulty</b>	300738666429.731
<b>Bits</b>	1756971
<b>Size (bytes)</b>	99231
<b>Version</b>	53687091
<b>Nonce</b>	2366357714
<b>Next Block</b>	\$1026
<b>Transactions</b>	
60e192ee04d95a74699161babcb5175f097545b2d1bb96961995de9f80c6e6	mined Feb 21, 2018 B5:46 AM
No Inputs (New Generated Coins)	
13TE7tNwKtP9KAHvAuorQzHmWdJf3jgHe	12c63481448 BTC (0)
Unsigned address [0]	0 BTC (0)
	8 CONFIRMATIONS
6a1eb02a5f15f19386c0373a3ff61719db4b2cc39ff92e9eab2d26f79709	mined Feb 21, 2018 B5:46 AM
17KgYoYnqAglghfmh0mGdLQD4ewfTlUenrVf7	0.03619554 BTC (0)
12Vt7z5i1Tp0swuWfWtAenGK6XmrsyU	0.03619554 BTC (0)
FEE: 0 BTC	8 CONFIRMATIONS
5af40470654d7611701b8c262ca759ed4757aded4ad5843e6151523ae9707	mined Feb 21, 2018 B5:46 AM
1H7nK2d4RheBuwODgFrnnm0nRTf8G9H	29.73215027 BTC
14pQZmxGPNhABhOnGJqpi05gBywv	29.73024227 BTC (0)
17DyJ2zsuA5hKw254HrmHsAsPUkx09	0.04 BTC (0)
FEE: 0.001808 BTC	8 CONFIRMATIONS
	27.7354272 BTC
14f3f6d1c14bd0a949a7a17931f1c1c61C09140396705b57364c6f457	mined Feb 21, 2018 B5:46 AM

A Tx

## Transaction

## Summary

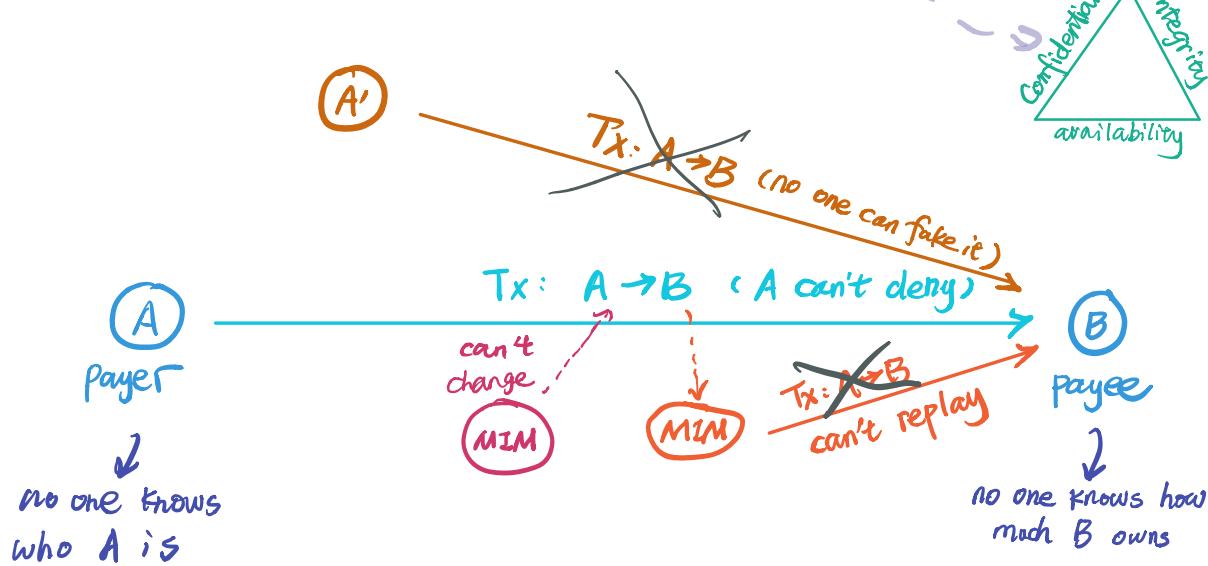
<b>Size</b>	226 (bytes)
<b>Fee Rate</b>	0.00058999999999999999 BTC per kB
<b>Received Time</b>	Feb 21, 2018 10:03:44 AM
<b>Mined Time</b>	N/A
<b>Included in Block</b>	Unconfirmed

## Details

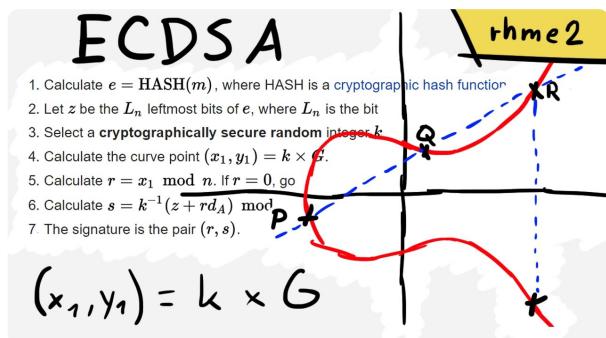
cb671e761a9ede0550af141c01d06b4f1475a8816ae60906f5064c2972d8c86c	
14dKmeMV4HmpbbSbkeeYG524nNuEFP6M5Q	4.43931125 BTC
18La8SWywMxm5lbVpzgWDVYkGwSj1HPPAi	0.03584102 BTC (U)
FEE: 0.00013334 BTC	
UNCONFIRMED TRANSACTION!	
4.43917791 BTC	

$$\text{fee} = \text{input}(s) - \text{output}(s)$$

How about { Security | Privacy } in OL?



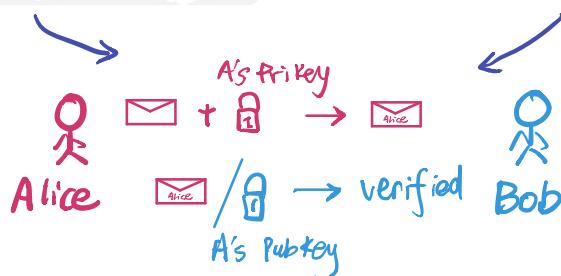
What do we have?



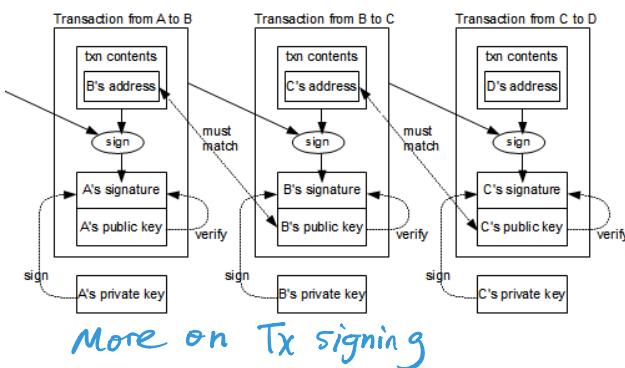
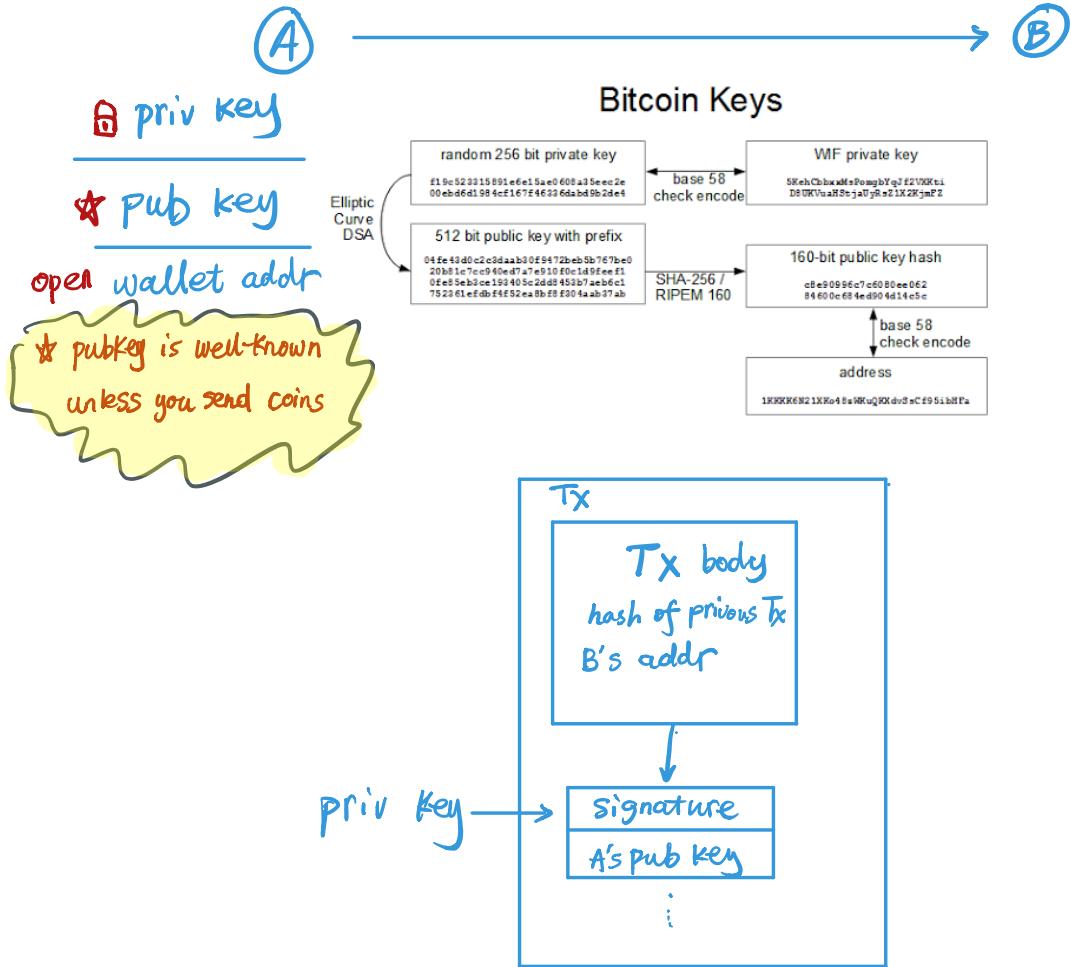
- Select two large prime numbers  $p, q$
- Compute  $n = p \times q$   
 $v = (p-1) \times (q-1)$
- Select small odd integer  $k$  relatively prime to  $v$   
 $\gcd(k, v) = 1$
- Compute  $d$  such that  $(d \times k) \% v = (k \times d) \% v = 1$
- Public key is  $(k, n)$
- Private key is  $(d, n)$

- example
 

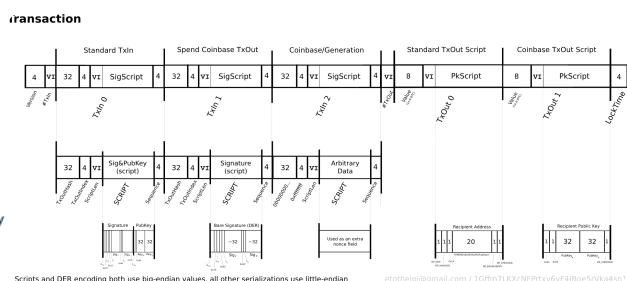
$p = 11$
$q = 29$
$n = 319$
$v = 280$
$k = 3$
$d = 187$
- public key  $(3, 319)$
- private key  $(187, 319)$



# What does bitcoin do?



## More on Tx signing



more on Tx structure

It's a VM

What about security of ecosystem?

- bad nodes
- bad nodes > 51% of computing power
- SPV ← • chain is too big to fit a commodity node  
Simplified Payment Verification  
availability)
- Threat from Quantum computing

Shor's algo

Grover's algo

basics of RSA

$$454243391453 \\ (299721) \times 349493$$

given  $[a, b, \dots]$

$$x? \rightarrow f(x) \rightarrow Y$$

$$O(2^{k/2}) \rightarrow O(k^3)$$

$$O(N) \rightarrow O(\sqrt{N})$$

could be  
used in ECDSA

Any problem

Crack 256 bit priv key : classic 340 T T T (T=Trillion)

a few hundred Million

18 million T

hash of pub key is important!

How about capacity?

- 1 M block  
added 2010
  - 10 Min a block  
 $(6 \times 24 \times 365 \times 9 = 474336)$  latest: 510438
  - Wallet just need  
headers and related Merkle Tree path

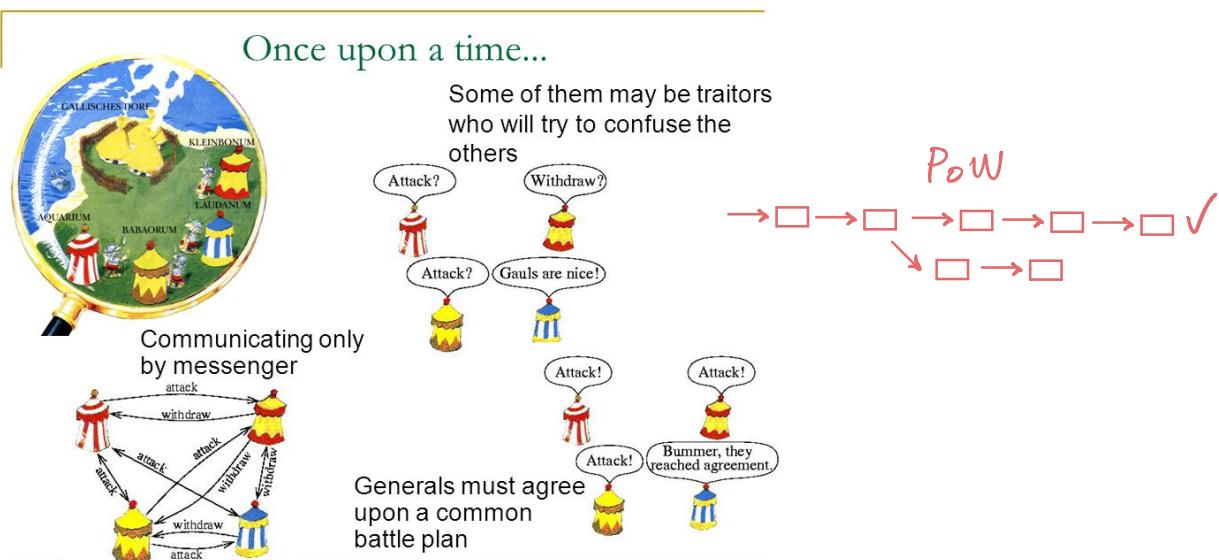


why not bigger?

$$1MB \times 8\text{bit} \times 7\text{peers} / 30\text{sec} = 1.86\text{Mb/s}$$
$$8MB \times 8\text{bit} \times 7\text{peers} / 30\text{sec} = 15\text{Mb/s}$$

upload speed

How { Sync  
Consensus } work?



The pictures are taken from: R. Goscinny and A. Uderzo, Asterix and Latraviata.

How miner work ?  
(TBD)

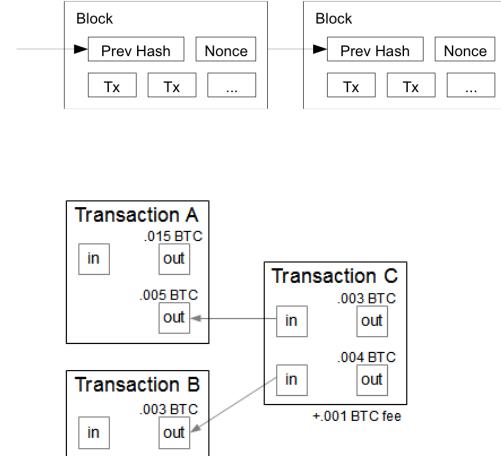
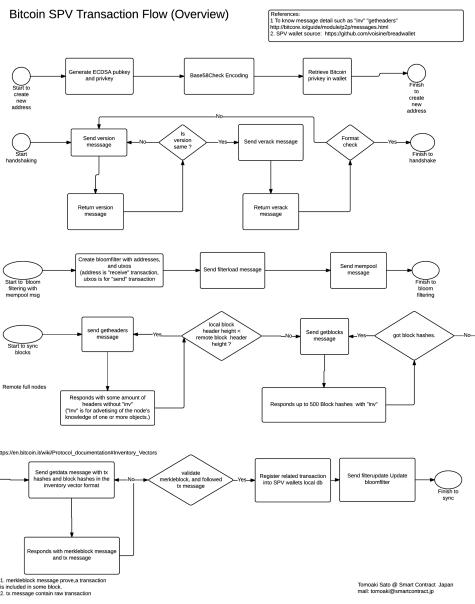
# Genius Design

- Chained ledger
- Proof-of-Work
- incentivization
- Merkle-Tree supported SPV
- Hashed public key (hide the flaw of ECDSA)
- 21,000,000 total coins
  - "  
2.1 quadrillion satoshis  $\approx 2^{50.9} < 2^{53}$
- base58 - why why why!
  - ↳ human readable (0, O, I, l striped)

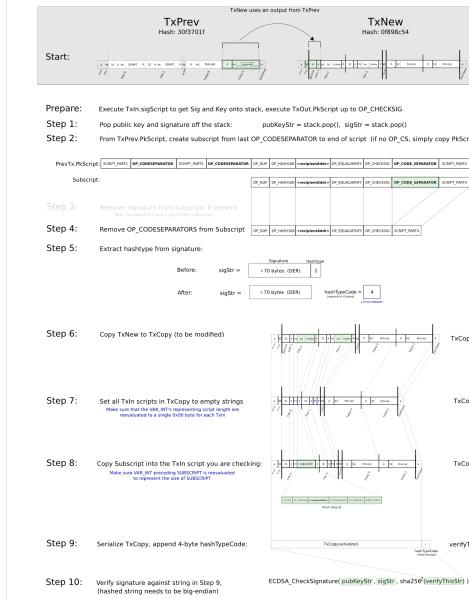
What can we learn for sw design?

- ask questions
- ask great questions
- ask great questions that future oriented
- Think it through and connect the dots

# Unused



## Transaction Verification Steps: OP\_CHECKSIG (SIGHASH\_ALL only)



etotheipi@gmail.com / 1ArmoryXcfq7TnCSuZa9fOjRYwJ4bkRKfv