BLOCKCHAIN: THE GOLD OF NERDS

ALESSANDRO PANCONESI
DIPARTIMENTO DI INFORMATICA, SAPIENZA UNIVERSITÀ DI ROMA
CRYPTOCURRENCIES, WILL THEY CHANGE THE WORLD?
YAP
ISLAND OF STONE MONEY
YAP

ISLAND OF STONE MONEY
YAP
ISLAND OF STONE MONEY
450 km!!!
MONEY TRANSFER ON YAP
ISLAND OF STONE MONEY
TOWARD THE BLOCKCHAIN
TRISTAN DE CUNHA

REMOTEST ISLAND
TRISTAN DE CUNHA
REMOTEST ISLAND

2000 miles

1700 miles
TRISTAN DE CUNHA
THE REMOTEST ISLAND
The inhabitants of the most remote island install a blackboard in the main square...
A owns 1 2 ... 10
B owns 11 12 ... 20
C owns 21 22 ... 30
D owns 251 252 ... 260
Properties of the blackboard

- Anybody can write
- Board is permanent: it cannot be erased or modified
A owns \( \text{①} \text{②} \cdots \text{⑩} \)
B owns \( \text{⑪} \text{⑫} \cdots \text{⑴} \)
C owns \( \text{⑴} \text{⑵} \cdots \text{⑶} \)
Z owns \( \text{⑵} \text{⑶} \cdots \text{⑶} \)

A \overset{①②}{\rightarrow} B \quad \text{Mike Bob}
PUBLIC LEDGER

A owns 1 2 ... 10
B owns 11 12 ... 20
C owns 21 22 ... 30
E owns 251 252 ... 260

A 2 B Alice Bob
B 3 C Bob Alice
D 51 J David Jane

C 1 D Charlie David
D 1 A ?
A owns ① ② ... ⑩
B owns ⑪ ⑫ ... ⑲
C owns ⑳ ㉑ ... ㉐
Z owns ㉑ ㉒ ... ㉐

A → B Alice Bob
B → C Bob Charlie
D → J David James

C → D Charlie David
D → A David Mike
C owns new corn (261) ... (270)

Blackboard #2
AND SO ON SO FORTH…

C owns new cotax (261) ... (30)

Blackboard #2
1. A owns 10
B owns 20
C owns 30
D owns 40
E owns 50
A → B → E
B → C
D → J

2. A owns 10
B owns 20
C owns 30
D owns 40
E owns 50
A → B → E
B → C
D → J

3. A owns 10
B owns 20
C owns 30
D owns 40
E owns 50
A → B → E
B → C
D → J

4. C owns new coin 20
D → J

PUBLIC LEDGER: A CHAIN
BLOCKCHAIN
The blockchain is the **distributed implementation** of the system of blackboards.
Blockchain

Implementing the blockchain is a difficult problem:

- Digital signature: no problem, thanks to public-key cryptography

- Each participant must share the same copy of the ledger: this is a difficult and subtle problem
BYZANTINE AGREEMENT
A distributed system worth its salt must be fault-tolerant
Byzantine agreement

- Each general has an initial opinion: YES or NO
- Loyal generals must come to an agreement: either they all decide YES or they all decide NO
- They have reliable point-to-point communication channels
If more than a third of the generals are traitors, agreement is impossible.
Proof of work

- Roughly speaking, if more than half of the computer cycles is in honest hands, proof of work ensures agreement.
Proof of stake

- If more than half of the coins in the system are in honest hands, byzantine agreement is possible
SILVIO MICALI’S BRAINCHILD
Last but not least

Alice and Bob agree on the following:
If tomorrow is a sunny day
and
etc etc
Then
Alice will pay Bob two coins by Friday
Thanks