Table of Contents

bitcoin

criptoBasic

general

basic

- how does bitcoin actually work?

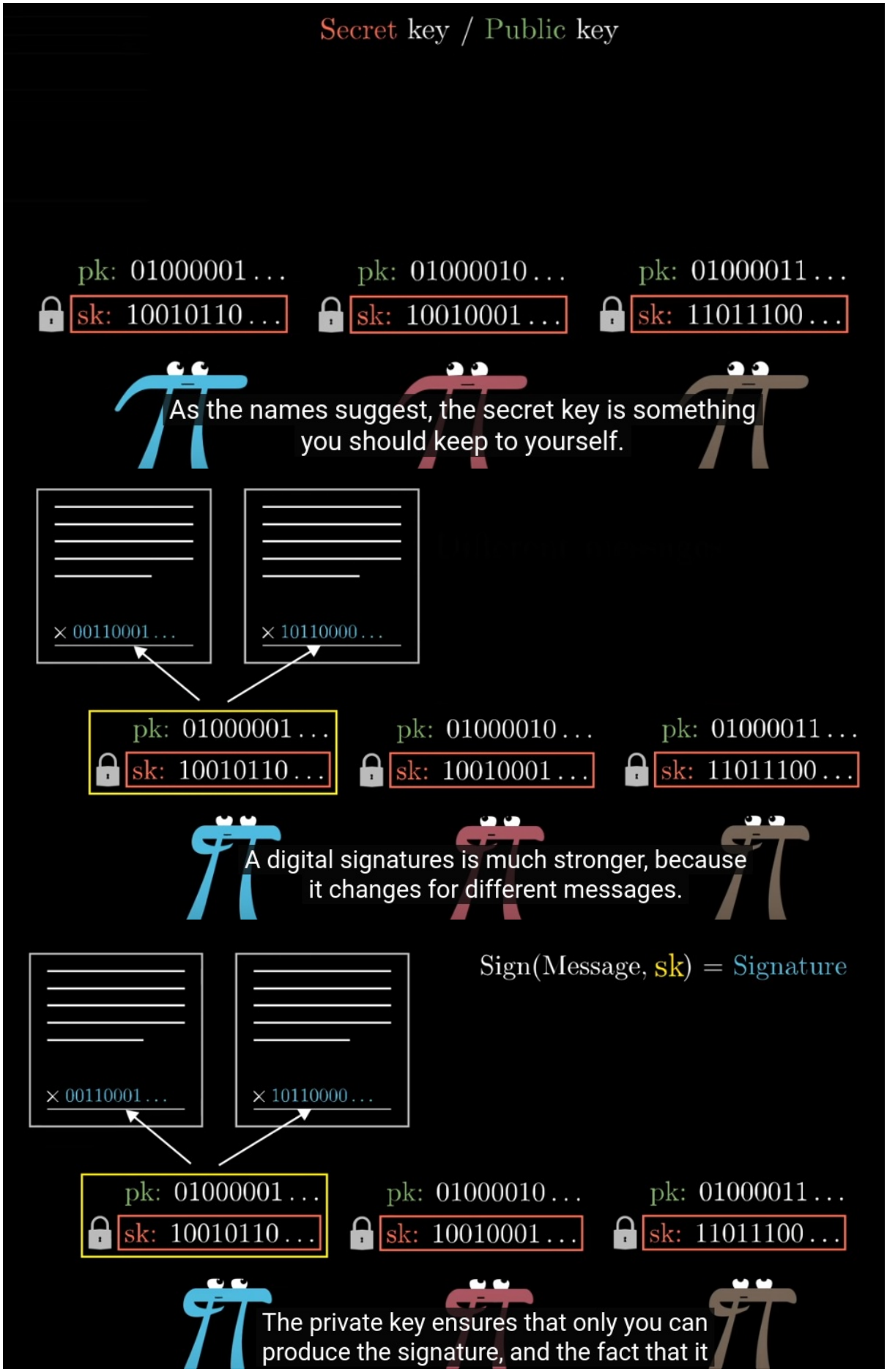
read

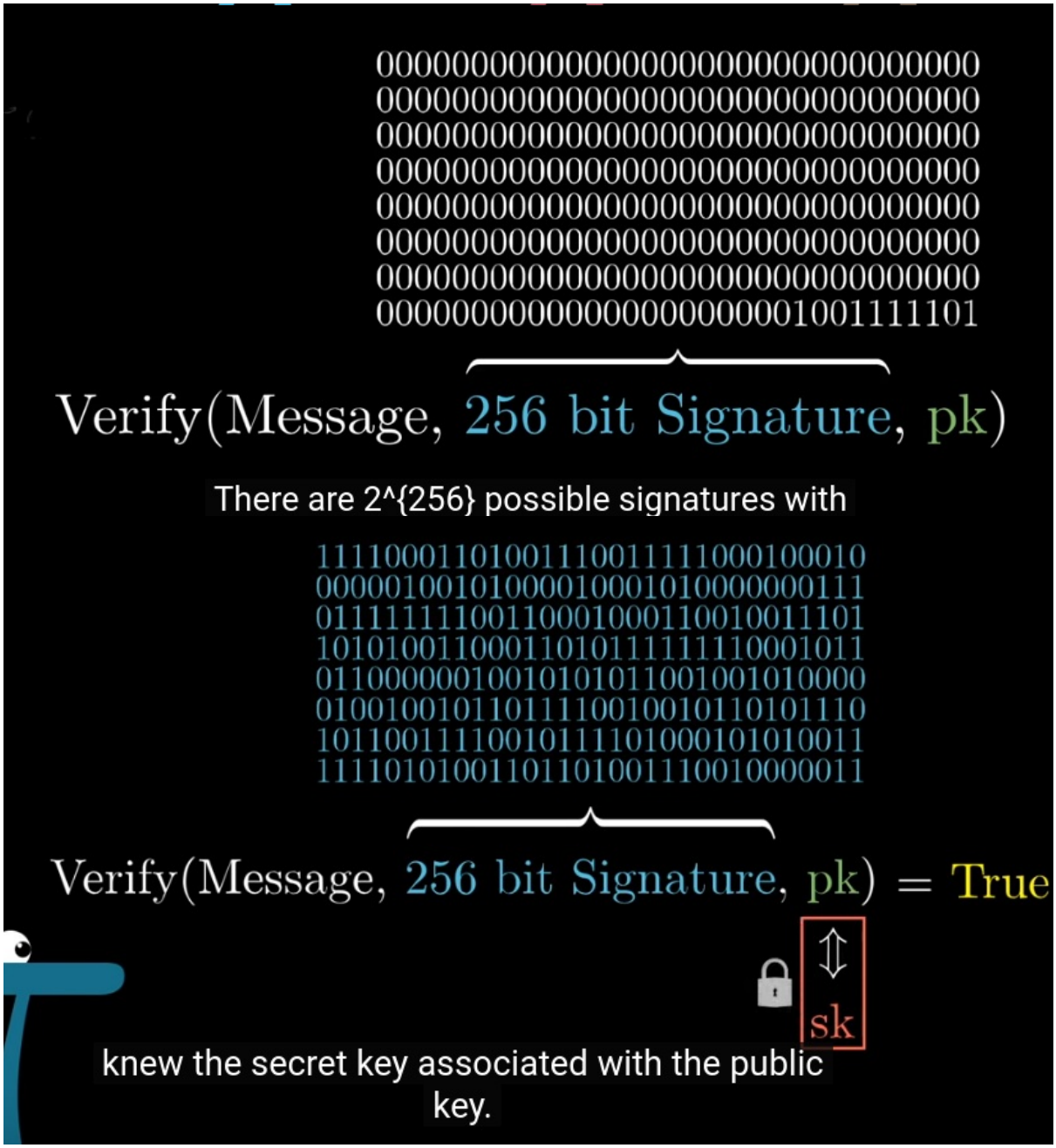
- read the whitePaper/bitcoin.pdf
- masteringBitcoin

#

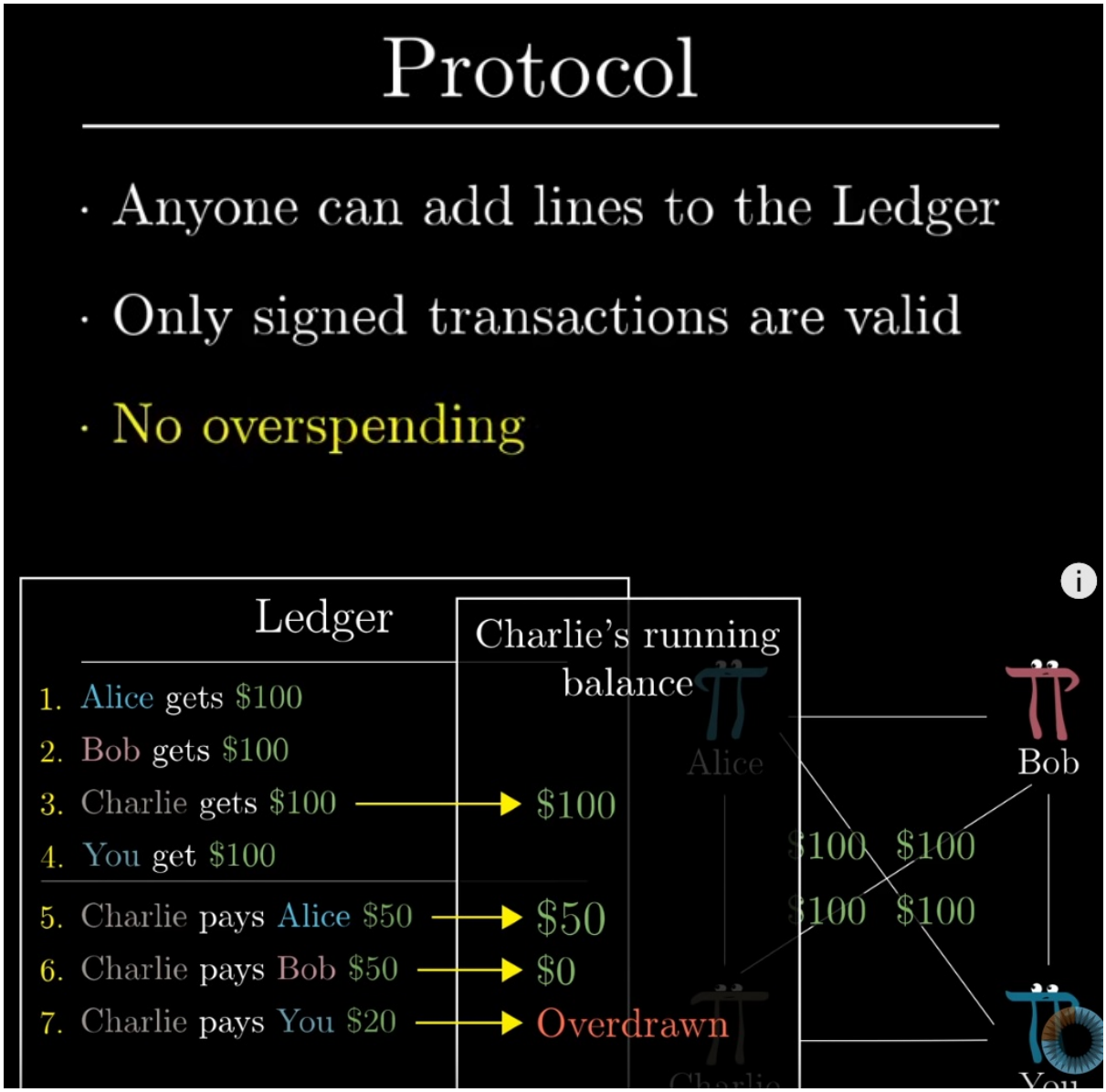
- But how does bitcoin actually work?
- https://www.youtube.com/watch?v=bBC-nXj3Ng4

signature

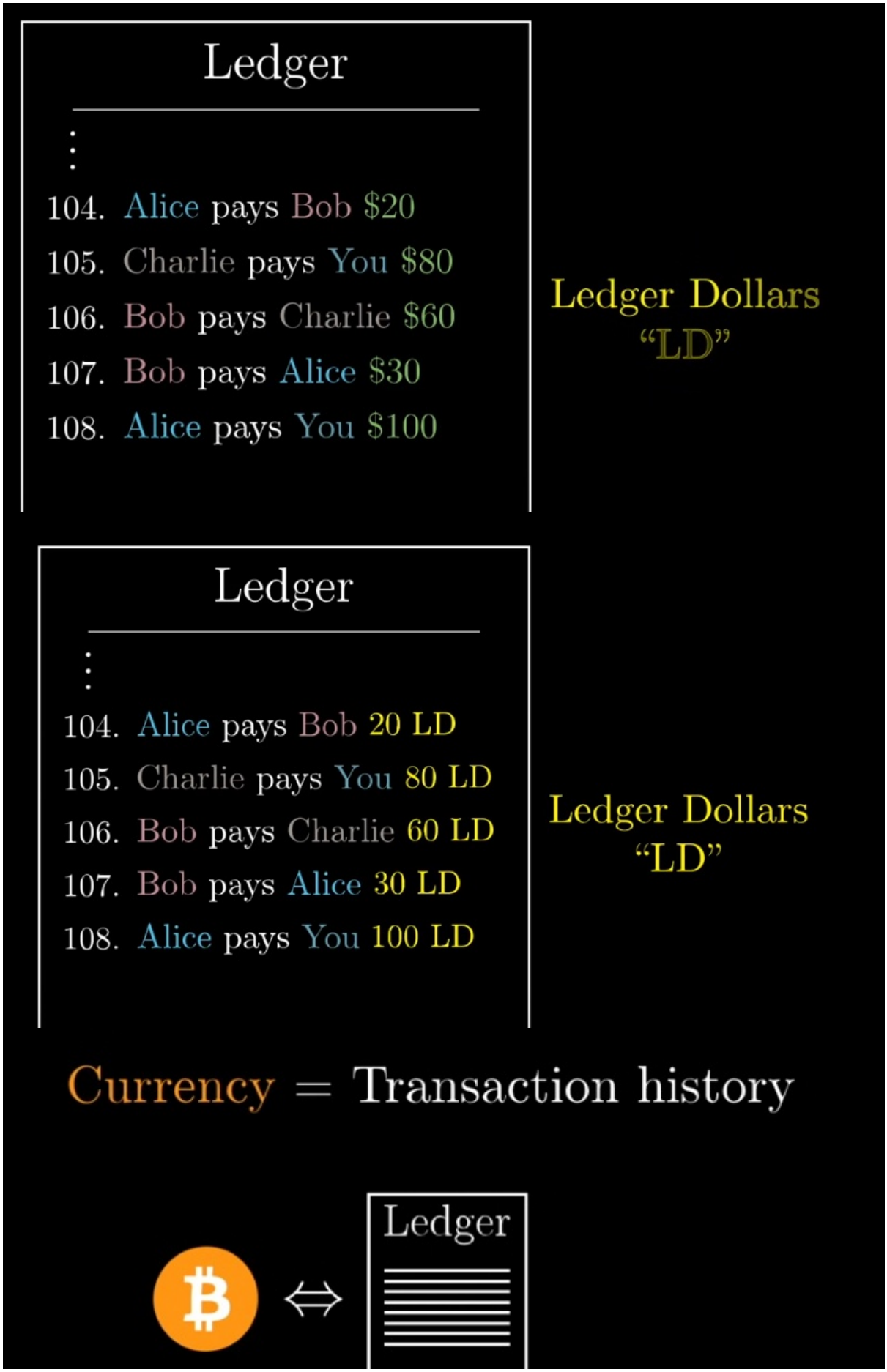

Secret key / Public key
pk: 01000001 . . .
sk: 10010110 . . .
pk: 01000010 . . .
sk: 10010001 . . .
pk: 01000011 . . .
sk: 11011100 . . .
As the names suggest, the secret key is something you should keep to yourself.
× 00110001 . . .
× 10110000 . . .
pk: 01000001 . . .
sk: 10010110 . . .
pk: 01000010 . . .
sk: 10010001 . . .
pk: 01000011 . . .
sk: 11011100 . . .
A digital signatures is much stronger, because it changes for different messages.
Sign(Message, sk) = Signature
× 00110001 . . .
× 10110000 . . .
pk: 01000001 . . .
sk: 10010110 . . .
pk: 01000010 . . .
sk: 10010001 . . .
pk: 01000011 . . .
sk: 11011100 . . .
The private key ensures that only you can produce the signature, and the fact that it



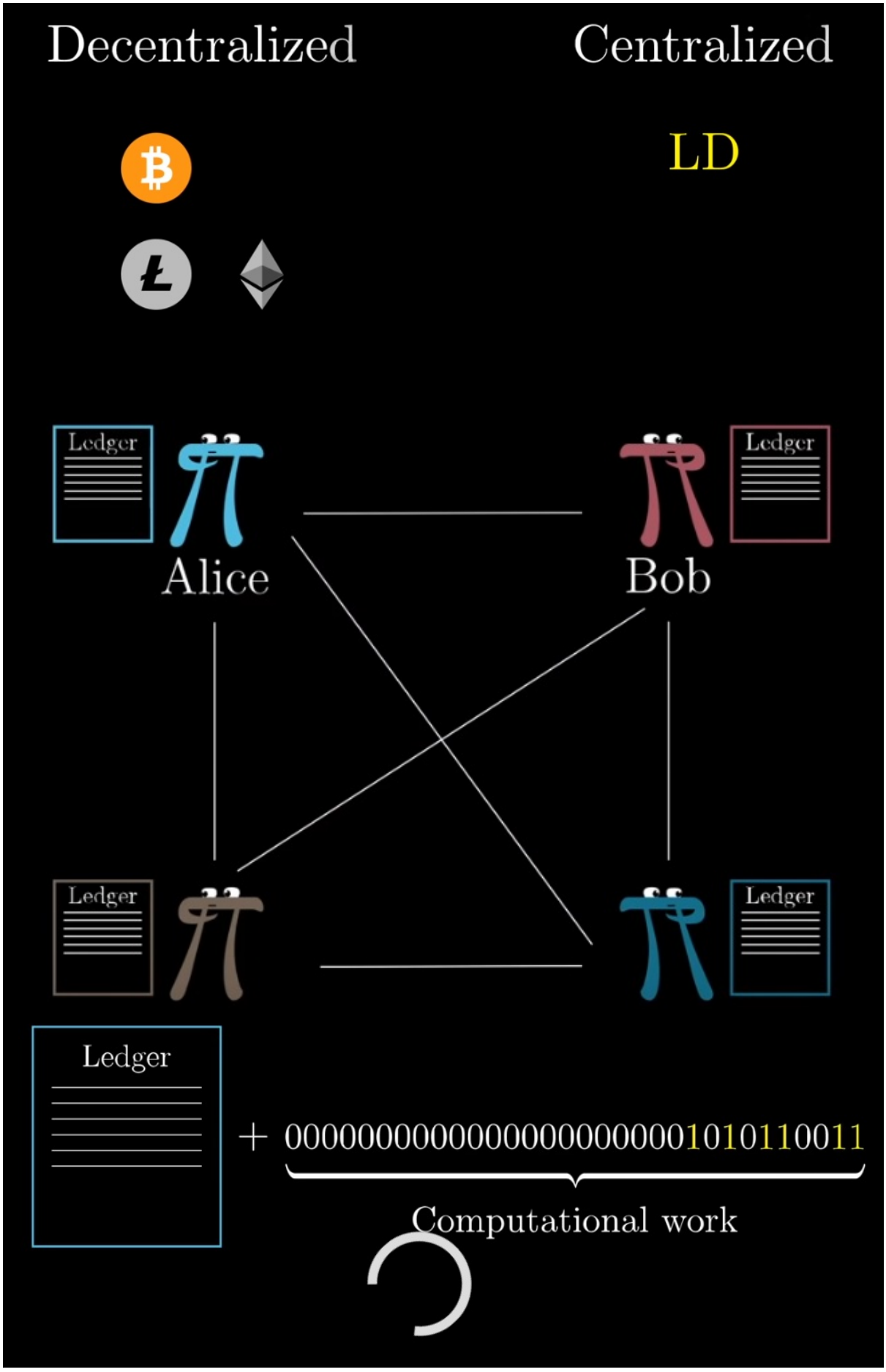
protocl: overspanding

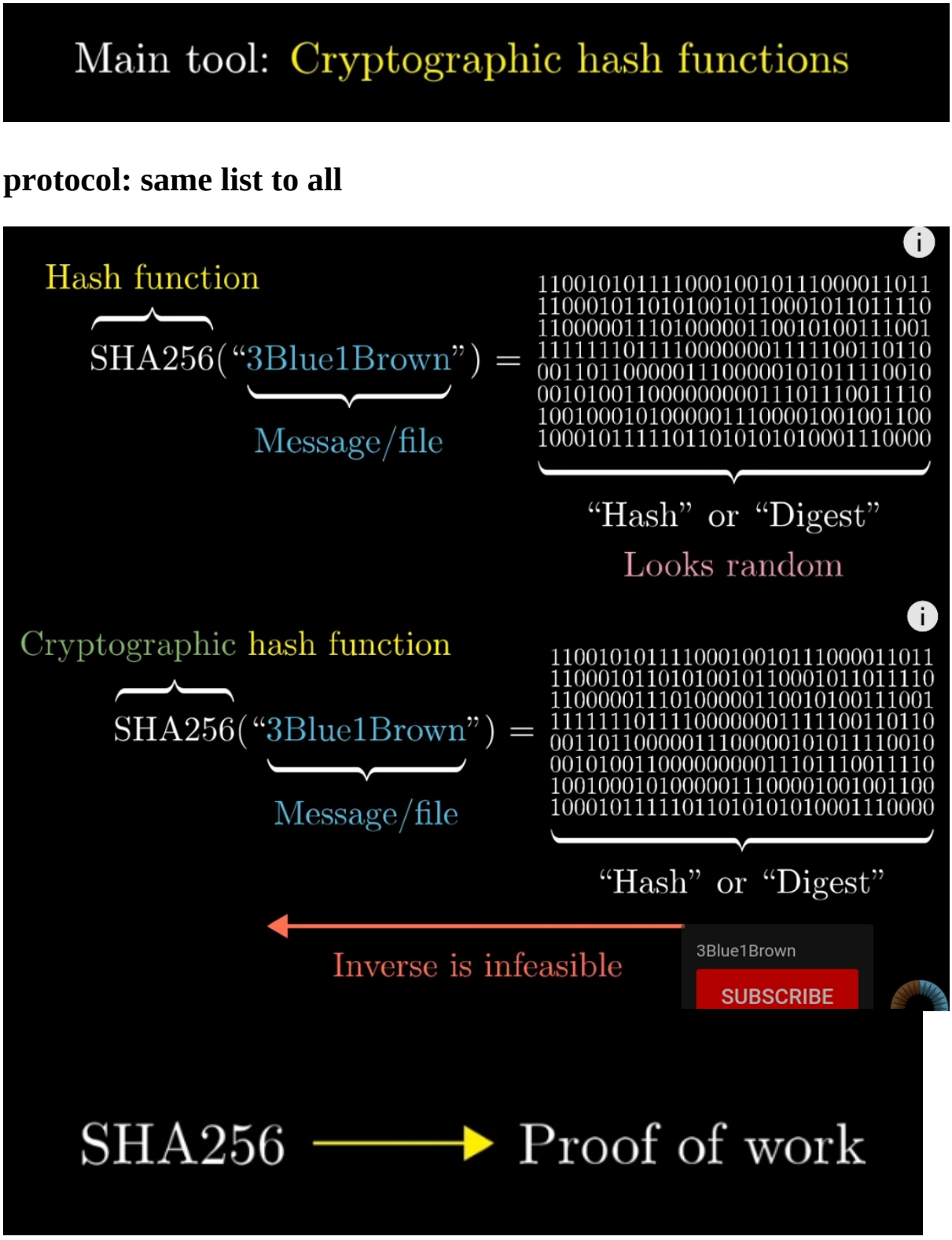


protocol: move to new currency

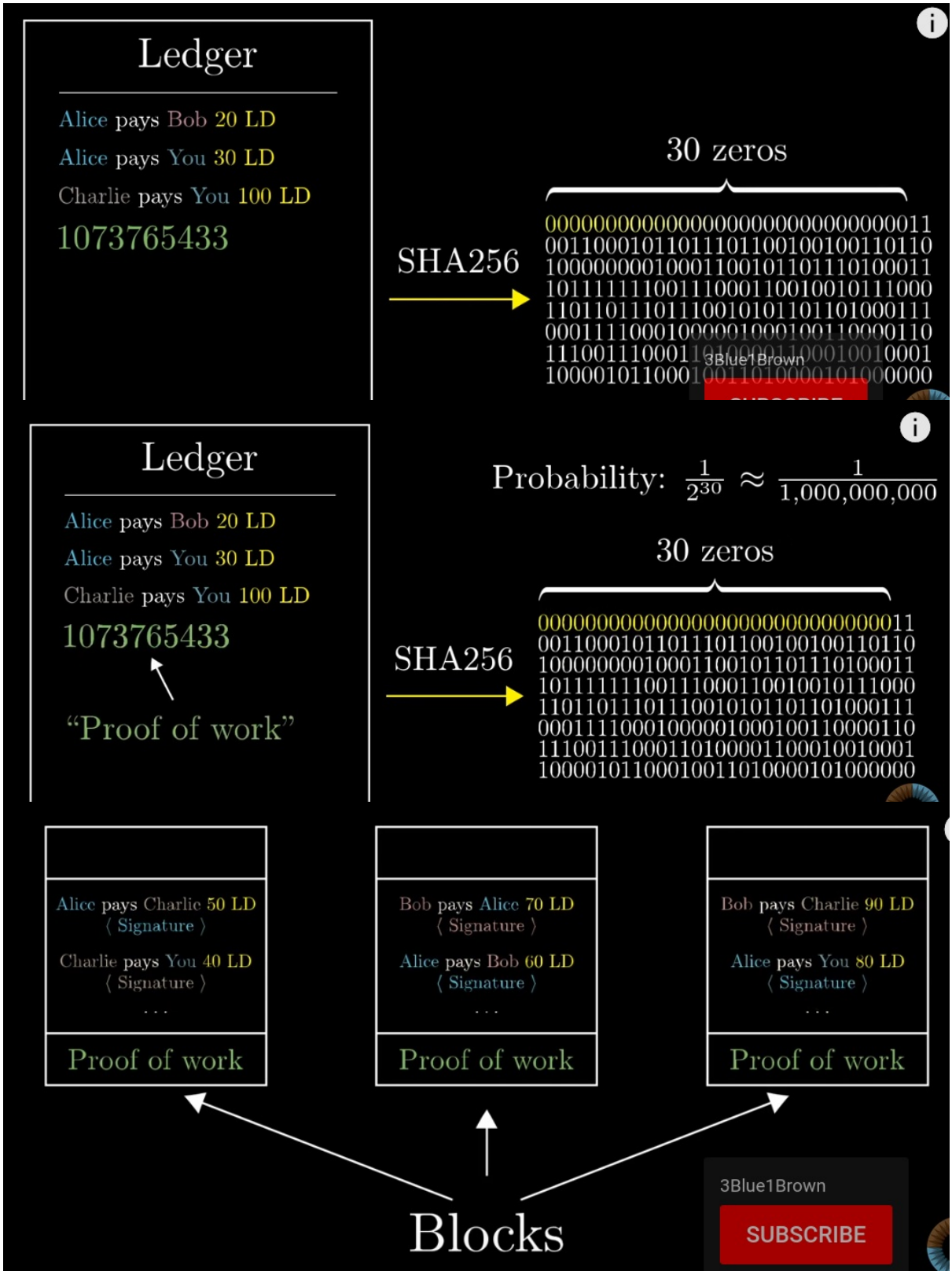

Ledger
104. Alice pays Bob $20
105. Charlie pays You $80
106. Bob pays Charlie $60
107. Bob pays Alice $30
108. Alice pays You $100
Ledger Dollars
"LD"
Ledger
104. Alice pays Bob 20 LD
105. Charlie pays You 80 LD
106. Bob pays Charlie 60 LD
107. Bob pays Alice 30 LD
108. Alice pays You 100 LD
Ledger Dollars
"LD"
Currency = Transaction history
Ledger

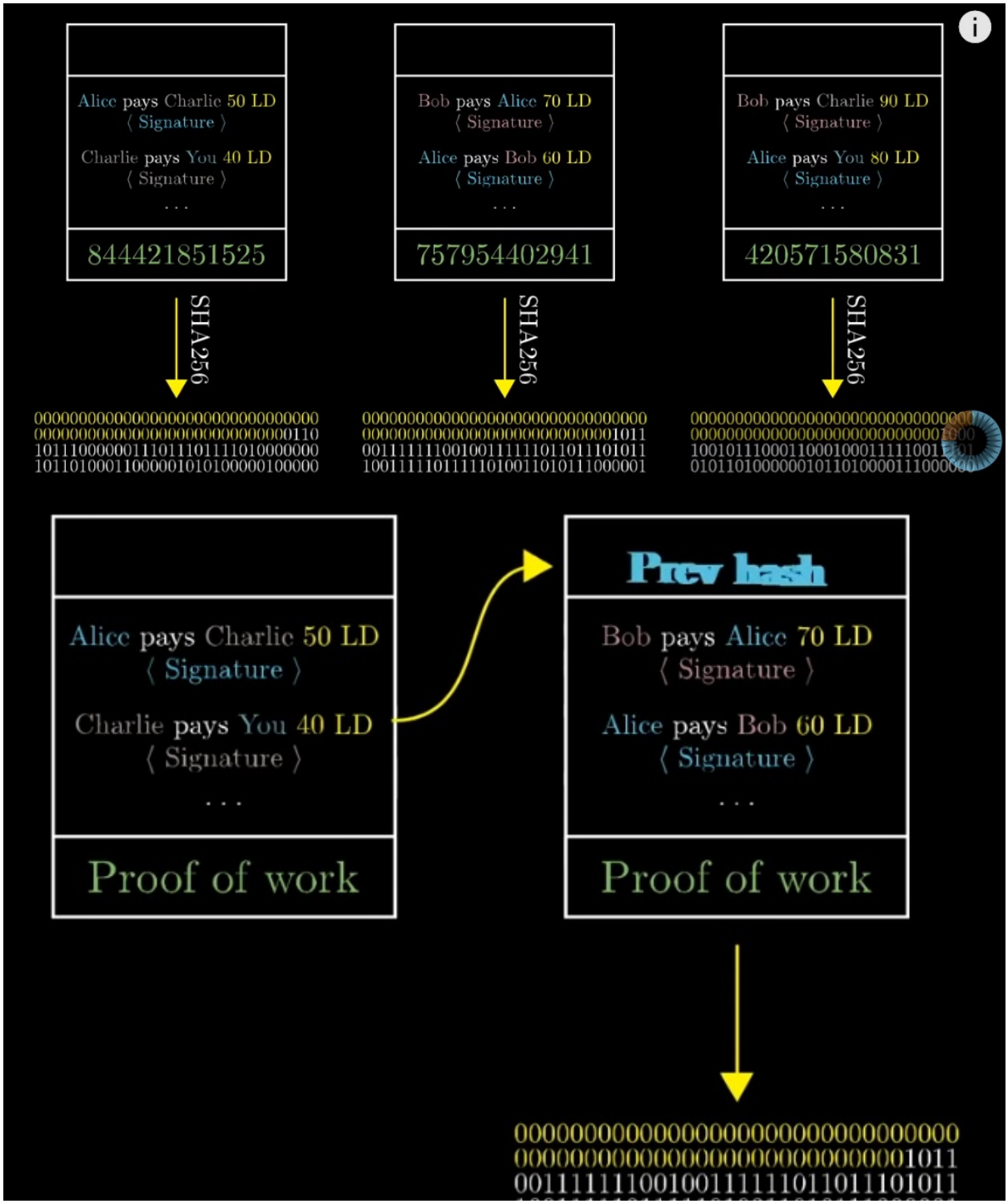
protocol: decentrailize

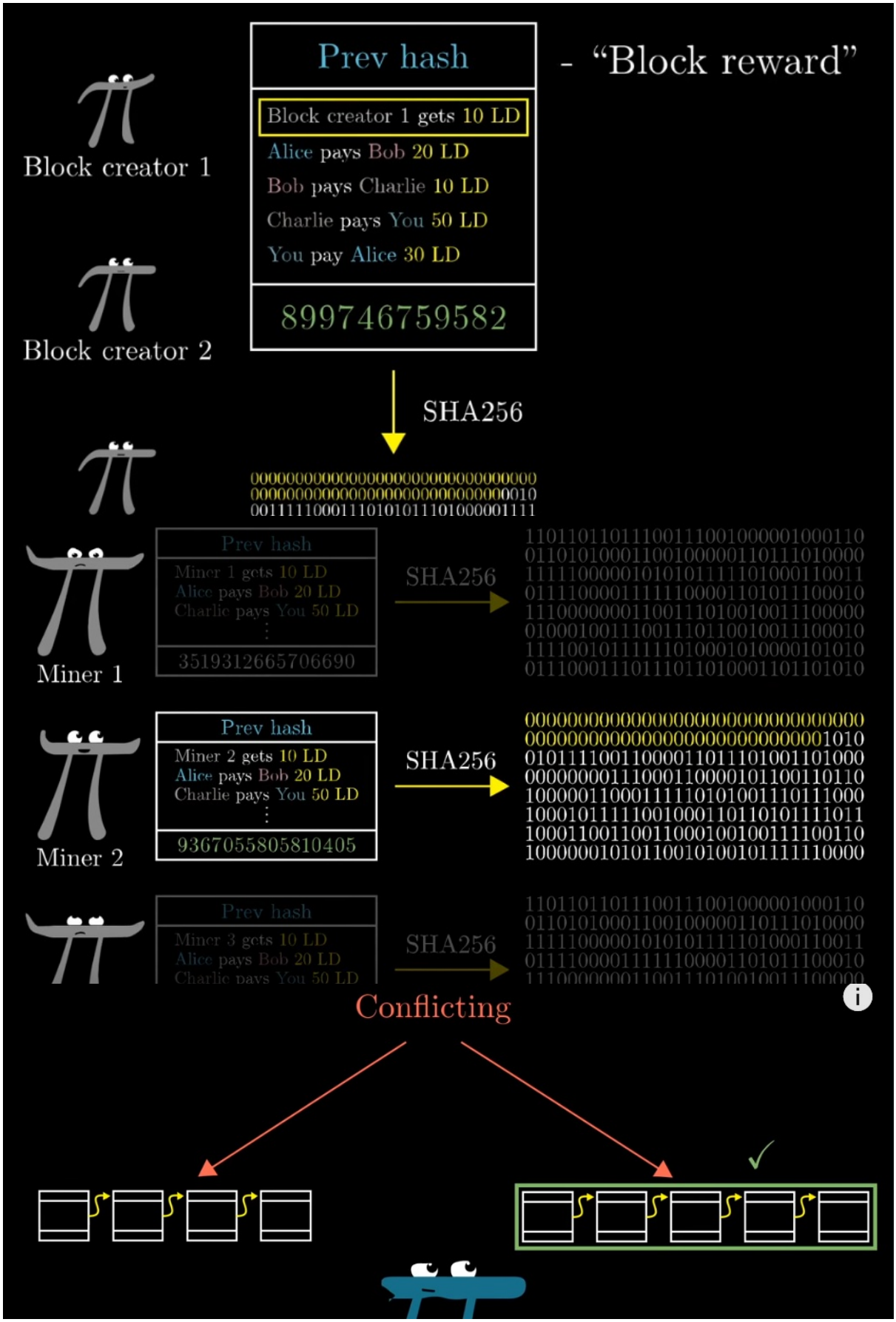

Decentralized
Centralized
LD
Ledger
Alice
Bob
Ledger
Ledger
Ledger
Ledger
Ledger
+ 00000000000000000000001010110011
Computational work

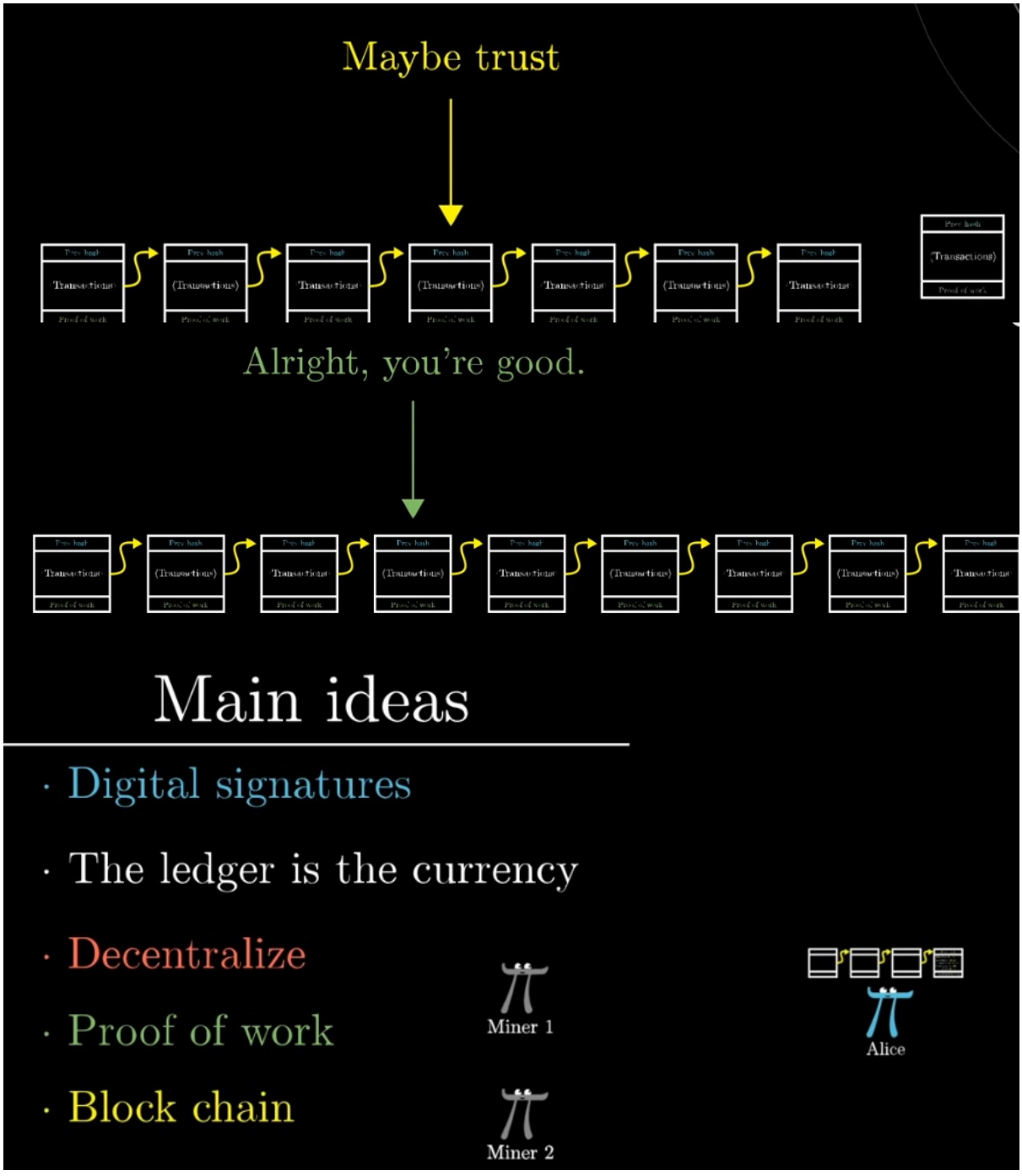


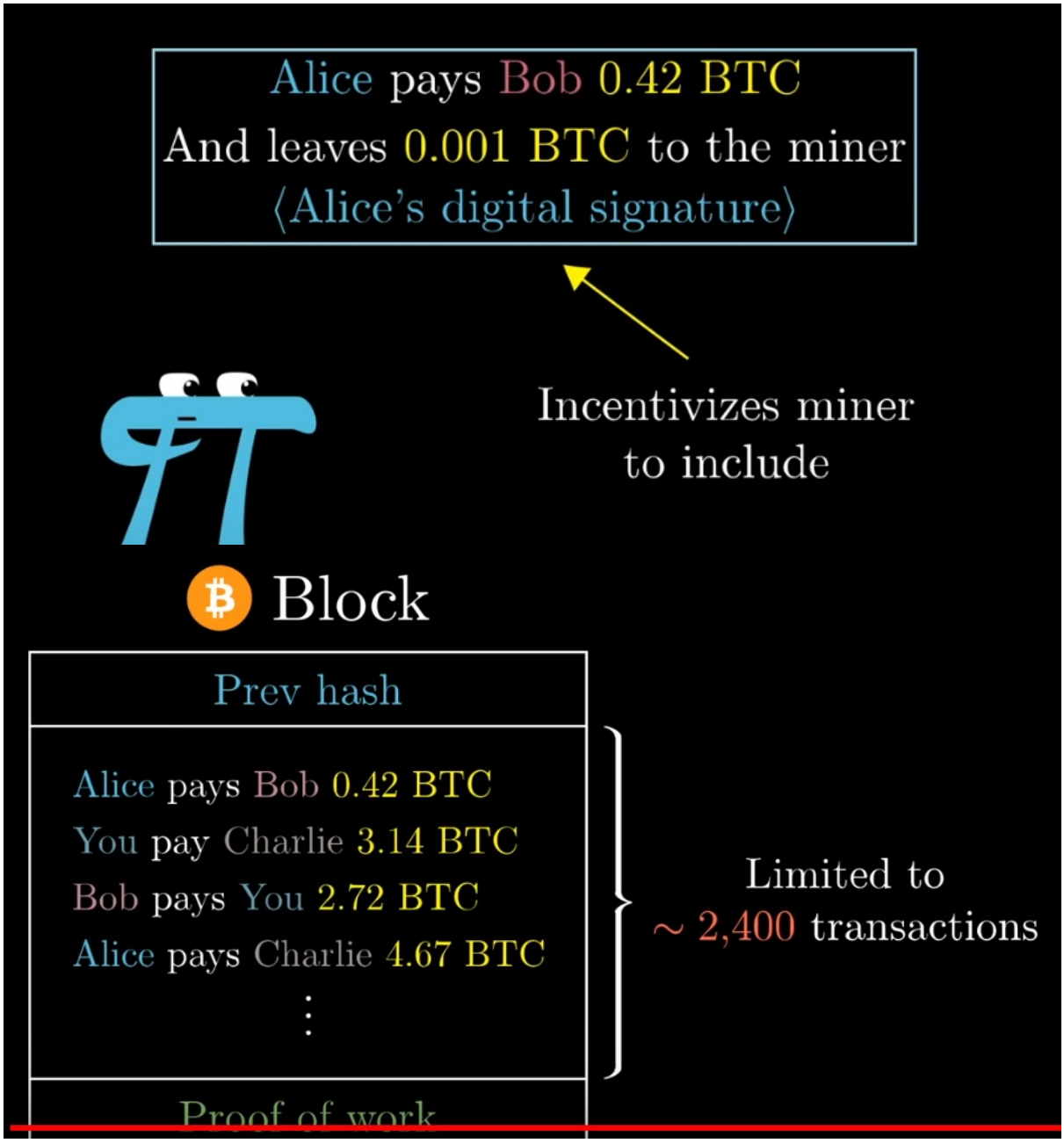
protocol: same list to all


Ledger
Alice pays Bob 20 LD
Alice pays You 30 LD
Charlie pays You 100 LD
1073765433
SHA256
30 zeros
00000000000000000000000000000011
00110001011011101100100100110110
10000000010001100101101110100011
10111111100111000110010010111000
11011011101110010101101101000111
00011110001000001000100110000110
11100111000110100001100010010001
10000101100010011010000101000000
3Blue1Brown
Ledger
Alice pays Bob 20 LD
Alice pays You 30 LD
Charlie pays You 100 LD
1073765433
"Proof of work"
Probability: $\frac{1}{2^{30}} \approx \frac{1}{1{,}000{,}000{,}000}$
SHA256
30 zeros
00000000000000000000000000000011
00110001011011101100100100110110
10000000010001100101101110100011
10111111100111000110010010111000
11011011101110010101101101000111
00011110001000001000100110000110
11100111000110100001100010010001
10000101100010011010000101000000
Alice pays Charlie 50 LD
⟨ Signature ⟩
Charlie pays You 40 LD
⟨ Signature ⟩
. . .
Proof of work
Bob pays Alice 70 LD
⟨ Signature ⟩
Alice pays Bob 60 LD
⟨ Signature ⟩
. . .
Proof of work
Bob pays Charlie 90 LD
⟨ Signature ⟩
Alice pays You 80 LD
⟨ Signature ⟩
. . .
Proof of work
Blocks
3Blue1Brown
SUBSCRIBE


Alice pays Charlie 50 LD
⟨ Signature ⟩
Charlie pays You 40 LD
⟨ Signature ⟩
. . .
844421851525
Bob pays Alice 70 LD
⟨ Signature ⟩
Alice pays Bob 60 LD
⟨ Signature ⟩
. . .
757954402941
Bob pays Charlie 90 LD
⟨ Signature ⟩
Alice pays You 80 LD
⟨ Signature ⟩
. . .
420571580831
SHA256
SHA256
SHA256
Prev hash
Alice pays Charlie 50 LD
⟨ Signature ⟩
Charlie pays You 40 LD
⟨ Signature ⟩
. . .
Proof of work
Bob pays Alice 70 LD
⟨ Signature ⟩
Alice pays Bob 60 LD
⟨ Signature ⟩
. . .
Proof of work


Prev hash
- "Block reward"
Block creator 1 gets 10 LD
Alice pays Bob 20 LD
Bob pays Charlie 10 LD
Charlie pays You 50 LD
You pay Alice 30 LD
899746759582
Block creator 1
Block creator 2
SHA256
Miner 1
Prev hash
Miner 1 gets 10 LD
Alice pays Bob 20 LD
Charlie pays You 50 LD
3519312665706690
SHA256
Miner 2
Prev hash
Miner 2 gets 10 LD
Alice pays Bob 20 LD
Charlie pays You 50 LD
9367055805810405
SHA256
Prev hash
Miner 3 gets 10 LD
Alice pays Bob 20 LD
SHA256
Conflicting


Maybe trust
Prev. hash
Transactions
Proof of work
(Transactions)
Alright, you're good.
Main ideas
· Digital signatures
· The ledger is the currency
· Decentralize
· Proof of work
· Block chain
Miner 1
Miner 2
Alice


Alice pays Bob 0.42 BTC
And leaves 0.001 BTC to the miner
⟨Alice's digital signature⟩
Incentivizes miner
to include
Block
Prev hash
Alice pays Bob 0.42 BTC
You pay Charlie 3.14 BTC
Bob pays You 2.72 BTC
Alice pays Charlie 4.67 BTC
Limited to
~ 2,400 transactions
Proof of work

#

- https://github.com/bitcoinbook/bitcoinbook
- https://www.amazon.com/-/he/dp-B09HJTFFFL/dp/B09HJTFFFL/ref=mt_other?_encoding=UTF8&me=&qid=