What's a Blockchain?
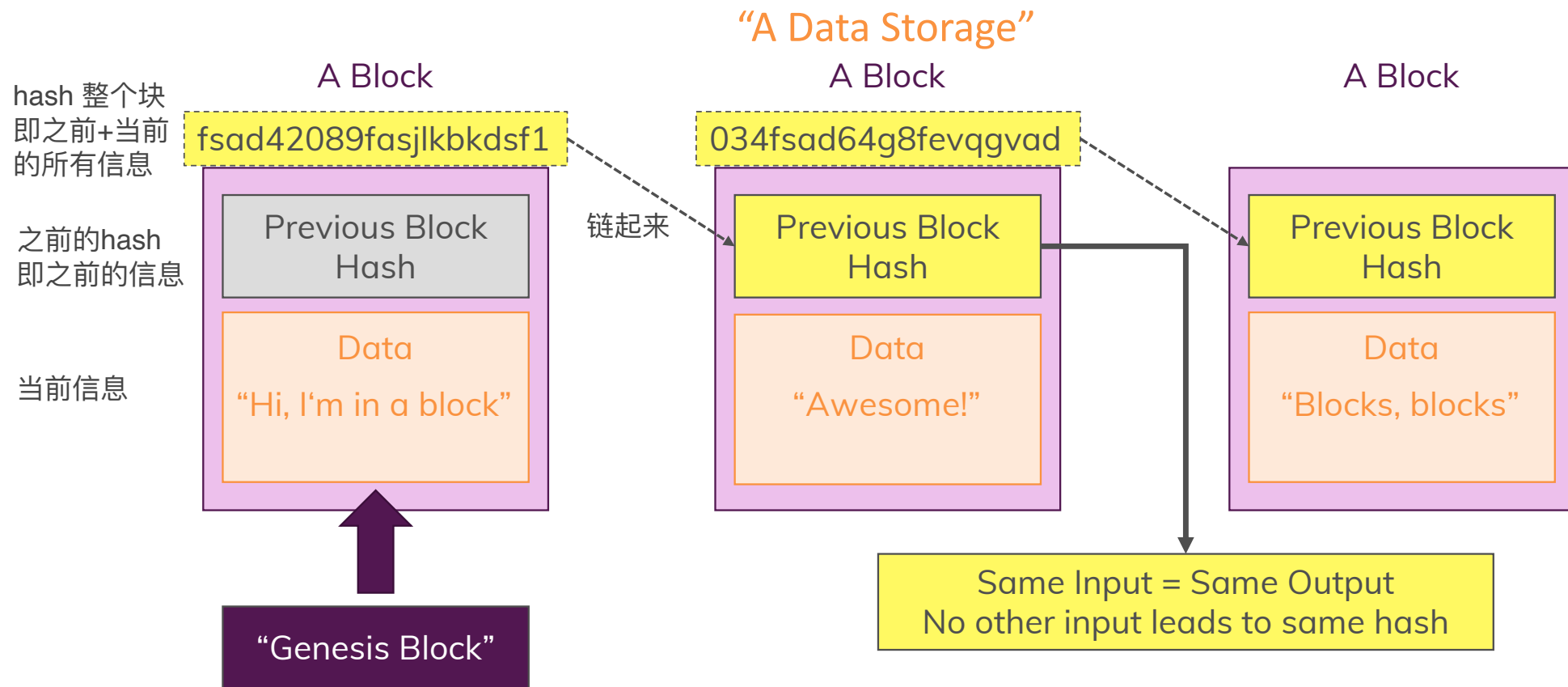
A distributed data storage consisting of containers (blocks) which are connected.

What is a Blockchain?

"A Data Storage"

hash 整个块
即之前+当前
的所有信息

之前的hash
即之前的信息

当前信息

A Block

fsad42089fasjlkbkdsf1

Previous Block Hash

Data
"Hi, I'm in a block"

链起来

"Genesis Block"

A Block

034fsad64g8fevqgvad

Previous Block Hash

Data
"Awesome!"

A Block

Previous Block Hash

Data
"Blocks, blocks"

Same Input = Same Output
No other input leads to same hash
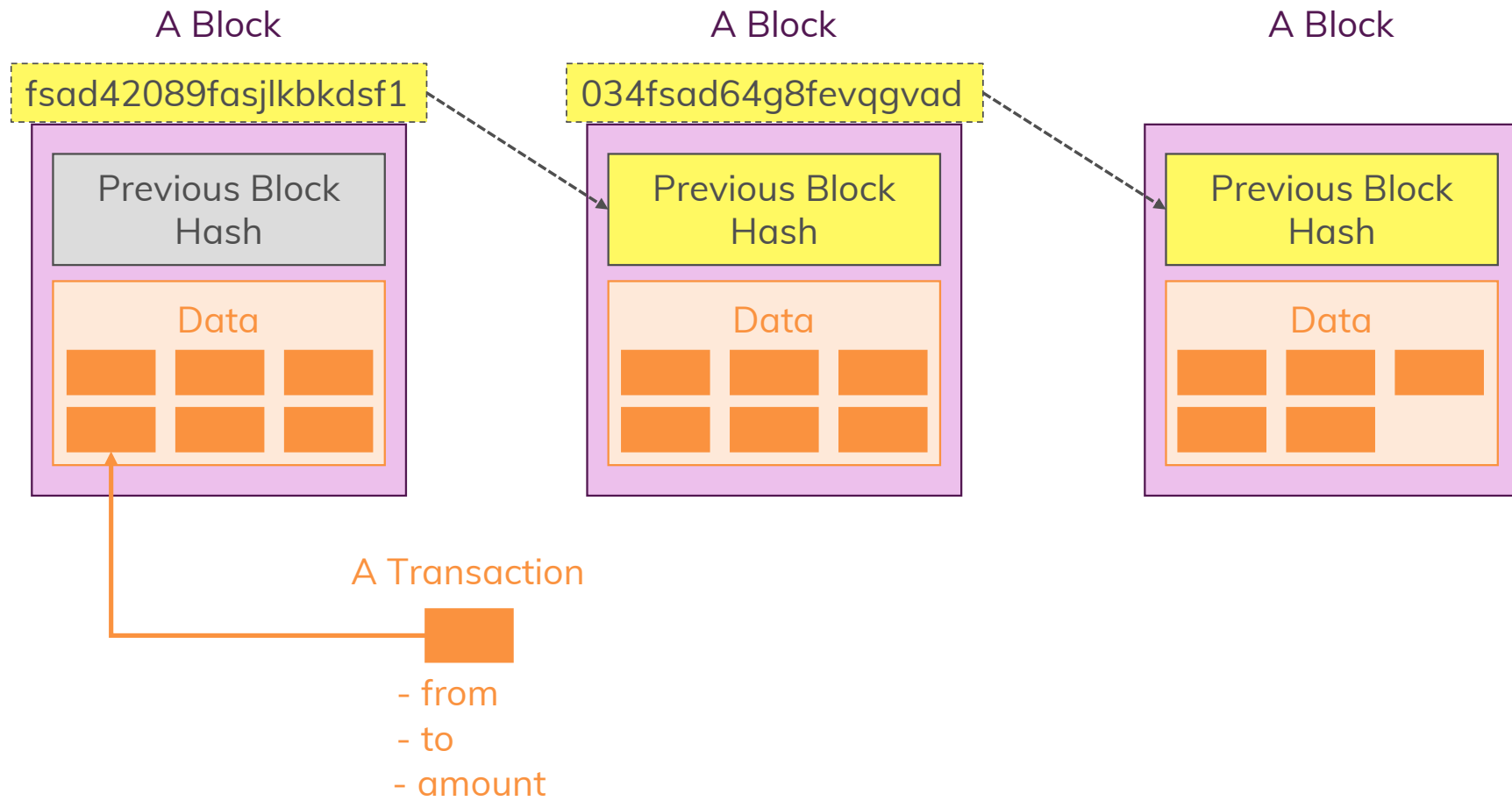
Security mechanism:
Each block knows the hashes before it.
If we change one block, the block behind will find that the recalculated hash doesn't match with what was already stored.

篡改信息
之后全对不上
轻松暴露

If the data you store in a block is a list of transactions, the coins transferred in the transactions form your cryptocurrency.
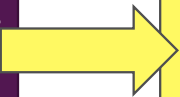
Storing Transactions

A Block

fsad42089fasjlkbkdsf1

Previous Block Hash
Data

A Block

034fsad64g8fevqgvad

Previous Block Hash
Data

A Block

Previous Block Hash
Data

A Transaction

- from
- to
- amount

Where are the Coins?

Coins are transferred with Transactions

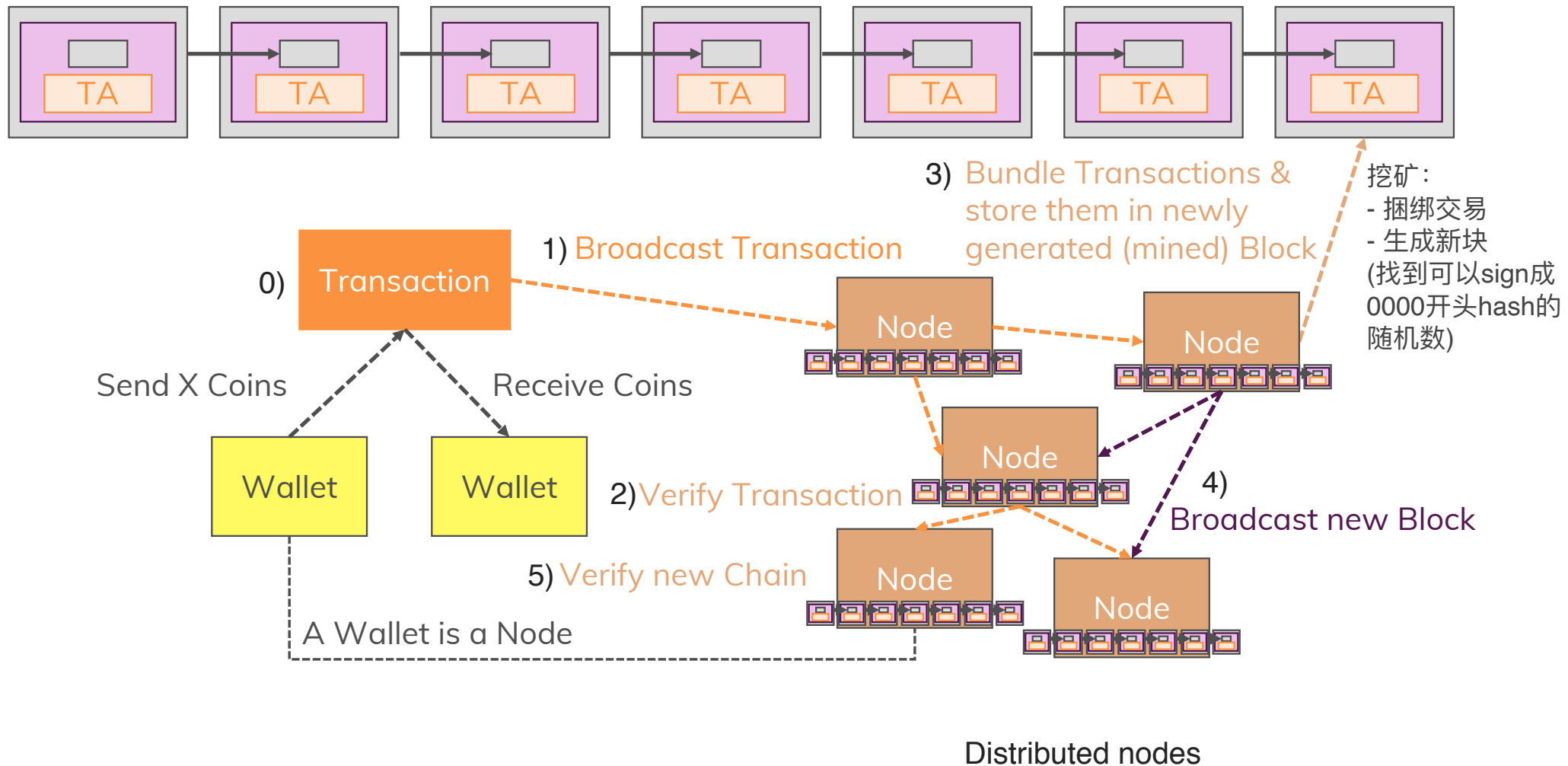Changing them into other currencies is not possible inside the Blockchain

The value of a coin is determined by the value the participants of the blockchain network assign to it (i.e. what you're willing to pay in "real" currencies).

Coins are created via Mining (as a reward for the effort)

distributed, secured data storage

Blockchain Big Picture

Blockchain diagram showing a chain of blocks (each labeled TA) connected in sequence.

0) Transaction
Send X Coins
Receive Coins
Wallet
Wallet
A Wallet is a Node

1) Broadcast Transaction

2) Verify Transaction

3) Bundle Transactions & store them in newly generated (mined) Block

4) Broadcast new Block

5) Verify new Chain

挖矿：
- 捆绑交易
- 生成新块
(找到可以sign成0000开头hash的随机数)

Node
Node
Node
Node
Node

Distributed nodes

https://anders.com/blockchain/block.html

Blockchain Demo   Hash   **Block**   Blockchain   D

Block

Block:	#	1

Nonce: 59396   初始的随机数

Data:
```
付款方：张澎
收款方：Mike
金额：￥100.00
日期：20190316
```

Hash: 6e197600cda40a36fad4281902882646b0f8d5b5cffc7b37721c4b4582cf6a38

Mine

Block

Block: # 1

Nonce: 29645

Data:
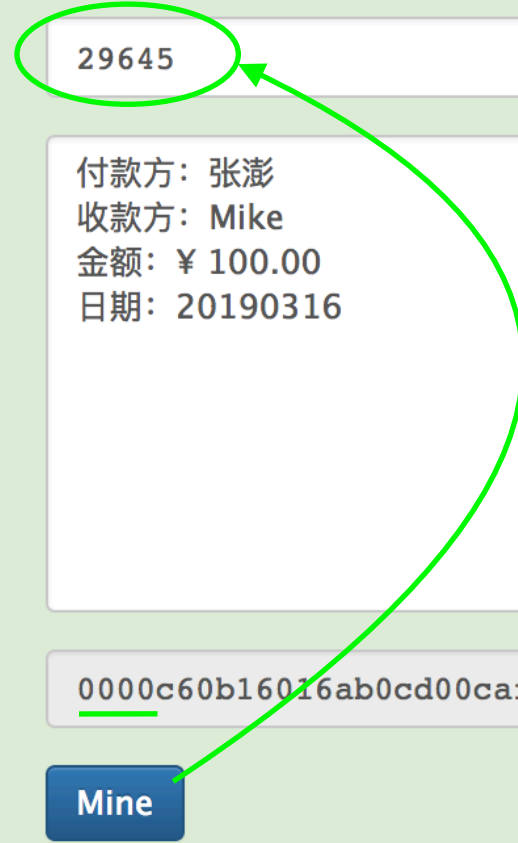付款方：张澎
收款方：Mike
金额：¥ 100.00
日期：20190316

挖矿而改变

Hash: 0000c60b16016ab0cd00caf5566734ee87d457fd65837f356f1823a0396764b6

Mine

Blockchain Demo   Hash Block **Blockchain** Distributed Tokens Coinbase

Blockchain

Block:	#	1

Nonce: 114433

Data:
付款方：张澎
收款方：Mike
金额：￥100.00
日期：20190316

付款方：张澎
收款方：Mike
金额：￥300.00
日期：20190317

Prev: 0000000000000000000000000000000000000000000000000000000000000000

Hash: 0000d03d00d789ae7e7c527b075869884f5b52286818aebfb3

Mine

Block:	#	2

Nonce: 57649

Data:
付款方：Mike
收款方：张澎
金额：￥100.00
日期：20190318

付款方：Mike
收款方：张澎
金额：￥300.00
日期：20190317

Prev: 0000d03d00d789ae7e7c527b075869884f5b52286818aebfb3

Hash: 0000613b98f1ec386a2a37b25aa0240d2ac9b8d94a1028425f

Mine

Block:	#	3

Nonce: 12937

Data:

Prev: 0000613b98f1ec386a2a37b25aa0240

Hash: f444f653d543a9900c00ce20a6a0e0

Mine

已 signed（已挖出来）

还未挖（未 sign）

notes:
- hash: same input -> same output
- hash: same length
- 0000... hash: this block is signed
- mining the nonce: try numbers to make hash start with 0000
- tokens
- coinbase