加密/数字货币

吴嘉婧

中山大学，软件工程学院

研究组网站： http://xplanet.site

Email: wujiajing@mail.sysu.edu.cn

提纲

(加密/数字)货币

- 导言：(加密/数字)货币
- 各种加密货币的介绍

Outline

1. 什么是 加密货币/数字货币

2. 典型 加密货币 有哪些

Intro: 数字货币

1. 电子货币

记账 中心化记账

储存 账号或磁卡

价值 = 法币

支付宝 ALIPAY

微信支付 Wechat Pay

PayPal

2. 虚拟货币

中心化记账

账号

企业决定

STEAM

3. 加密货币

区块链（匿名）

数字

△

市场

背后机制

背后机制

libra

4. 数字货币

区块链（匿名）

数字

△

中国互联网金融协会区块链工作组：

“数字货币必须具备法定地位、国家主权背书，明确发行责任主体。以比特币和以太币等为代表的货币没有国别，没有主权背书，没有合格发行主体，没有国家信用支撑，这些都不是数字货币。”

比特币

1. 去中心化：解决谁来记账的问题？PoW

挖矿的工具：hash算法

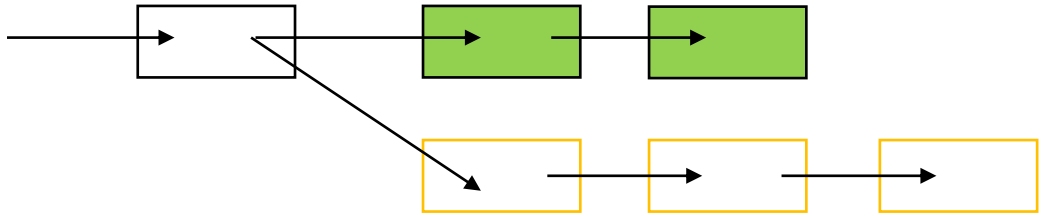
将任何一串数据输入到SHA256将得到一个256bit的hash值

计算SH265算法的数学难题

矿工：矿工 = 记账员

CPU -> GPU -> 专业矿机

2. 作弊：解决矿工虚假记账的问题？



历史：黄金矿场最赚钱的是卖工具的人（无风险收益），而不是淘金的人

矿机 → 比特大陆 → 蚂蚁矿机 → 矿场 → 矿池

詹克团

原比特大陆董事长

英文名/别名：暂无

所在领域：矿机

吴忌寒 比特大陆创始人兼董事

人称"一代矿霸"的吴忌寒又叫Jihad，北大毕业，理学和经济学双学...

比特币

①10min一个区块

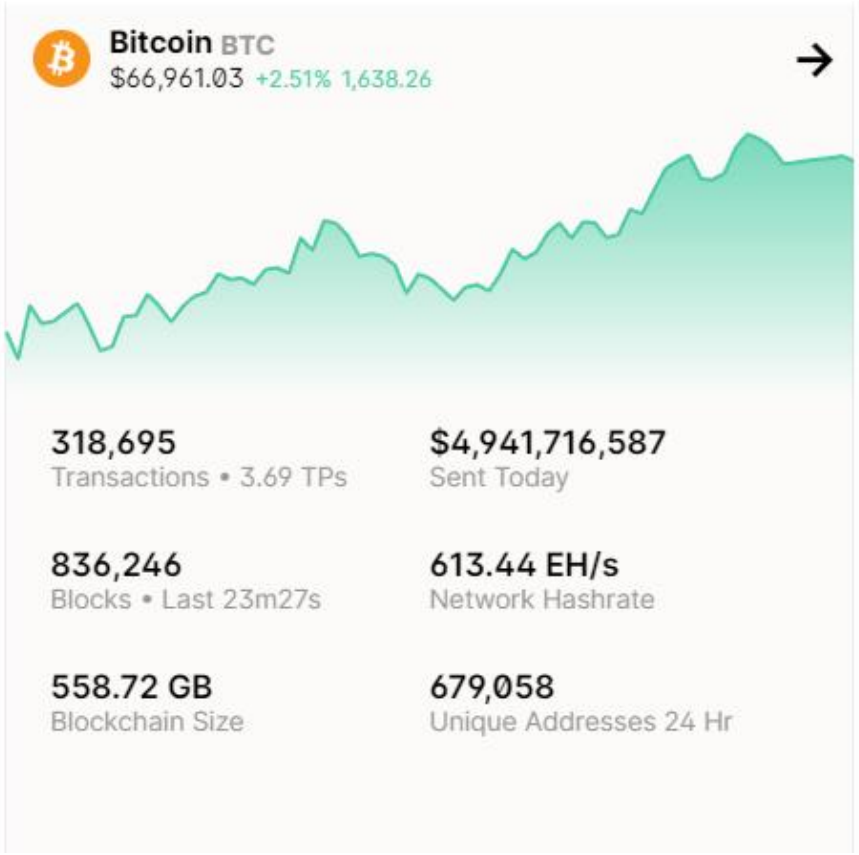
②一个区块1M

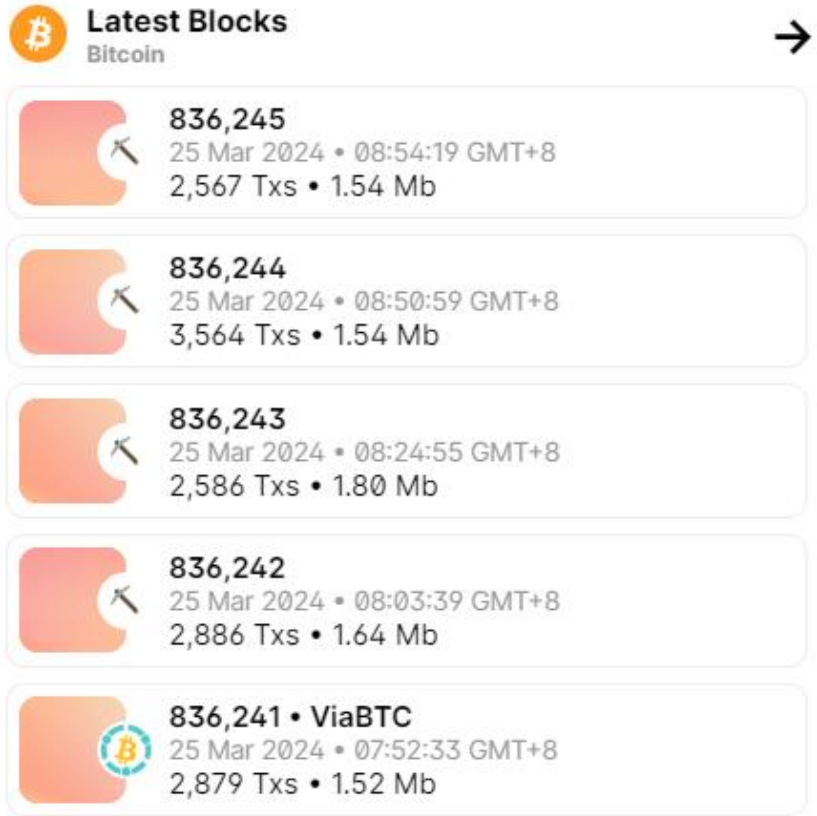
③每秒大概7笔交易

④SHA256算法

⑤总量2100万

⑥匿名





Bitcoin BTC

Bitcoin (BTC) is a decentralized currency that eliminates the need for central authorities such as banks or governments by using a peer-to-peer internet network to confirm transactions directly between users.

Price History

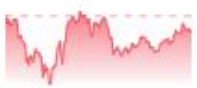
$66,598.30 • Mar 2024

Vol 25,489,933,246 BTC

1D 1W 1M 1Y **MAX** USD

Blockchain


Chart
Bitcoin 3.159%
Ethereum 4.289%
2023年3月31日
1Y
+180%
+160%
+140%
+120%
+100%
+80%
+60%
+40%
+20%
0%
2023年3月28日
2023年5月28日
2023年7月28日
2023年9月27日
2023年11月27日
2024年1月27日

Name	Price	1d	Market Cap	Volume(24h)	Circulating Supply	7d Chart	Trade
Bitcoin BTC	$67,080.00	+2.40%	$1,320,978,448,614	$27,614,228,217	19,664,037 BTC		Trade
Ethereum ETH	$3,450.40	+1.69%	$414,606,619,279	$13,925,314,501	120,074,261 ETH		Trade
Tether USDT	$1.00	+0.16%	$104,110,500,940	$53,153,477,689	104.01B USDT		Trade
BNB BNB	$577.83	+3.04%	$89,057,616,203	$1,851,001,013	153,856,150 BNB		Trade
Solana SOL	$187.36	+6.52%	$83,239,528,476	$3,923,933,754	444,186,772 SOL		Trade
XRP XRP	$0.63	+0.29%	$34,581,436,787	$1,313,194,713	54.88B XRP		Trade
Lido Staked Ether STETH	$3,446.10	+1.74%	$33,691,406,869	$97,285,194	9,767,266 STETH		Trade
USDC USDC	$1.00	+0.03%	$32,172,123,278	$6,344,804,784	32.20B USDC		Trade

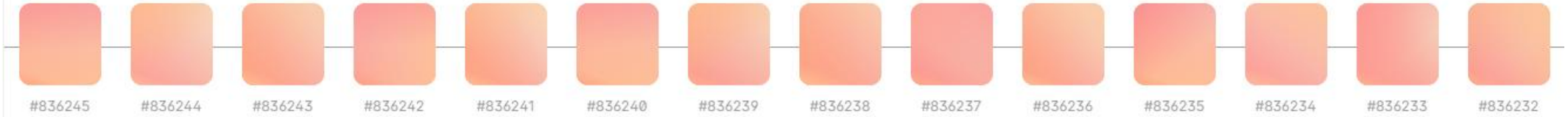
Dogecoin DOGE	$0.17	-0.50%	$24,692,939,524	$2,320,380,608	143.60B DOGE		Trade
Cardano ADA	$0.64	+0.98%	$22,664,737,958	$453,104,293	35.26B ADA		Trade
Avalanche AVAX	$57.86	+7.46%	$21,864,537,168	$949,727,462	377,416,611 AVAX		Trade
Toncoin TON	$5.51	+11.34%	$19,078,923,906	$396,600,741	3.47B TON		Trade
Shiba Inu SHIB	$0.00003	-1.11%	$16,321,074,070	$825,435,846	589265.17B SHIB		Trade
Polkadot DOT	$9.47	+2.65%	$12,749,372,949	$231,931,513	1.34B DOT		Trade
Chainlink LINK	$18.93	+3.06%	$11,131,317,327	$399,872,322	587,099,971 LINK		Trade
Wrapped Bitcoin WBTC	$67,086.00	+2.39%	$10,441,049,341	$262,965,344	155,475 WBTC		Trade
TRON TRX	$0.12	-0.37%	$10,413,990,680	$387,722,065	87.78B TRX		Trade

Home
Prices
Charts
NFTs
DeFi
Academy
News
Developers
Wallet
Exchange

Bitcoin
Ethereum
Bitcoin Cash

English

Latest BTC Blocks



Number	Hash	Miner	Mined	Tx Count	Nonce	Fill	Size	Total Sent	Total Fees
836245	0000-e49f	Unknown	32m 57s	2,567	2,250,773,337	153.66%	1,611,215 Bytes	4,516 BTC	0.14BTC
836244	0000-d85e	Unknown	36m 17s	3,564	1,274,478,626	153.99%	1,614,693 Bytes	22,818 BTC	0.22BTC
836243	0000-a2f7	Unknown	1h 2m 21s	2,586	1,885,092,154	179.58%	1,882,984 Bytes	12,224 BTC	0.21BTC
836242	0000-1782	Unknown	1h 23m 37s	2,886	2,623,066,711	163.64%	1,715,901 Bytes	5,835 BTC	0.14BTC
836241	0000-7979	ViaBTC	1h 34m 43s	2,879	2,120,079,646	152.28%	1,596,788 Bytes	7,178 BTC	0.15BTC
836240	0000-c8ac	ViaBTC	1h 49m 43s	1,272	1,614,313,504	166.89%	1,749,963 Bytes	1,387 BTC	0.08BTC
836239	0000-04d4	Unknown	1h 52m 59s	2,588	535,465,905	155.47%	1,630,233 Bytes	4,925 BTC	0.13BTC
836238	0000-eb24	Unknown	2h 5m 46s	2,789	1,966,420,860	225.41%	2,363,558 Bytes	285 BTC	0.07BTC
836237	0000-b6fc	Unknown	2h 6m 14s	2,478	2,223,084,330	157.29%	1,649,261 Bytes	21,565 BTC	0.13BTC

Bitcoin Block 836,245

Mined on March 25, 2024 08:54:19 • All Blocks

Unknown

Coinbase Message •
,z>mmo}"w>r$ YEy;:MEZKA1dd51,# p /F2Pool/d :A27

A total of 4,515.95 BTC ($302,852,898) were sent in the block with the average transaction being 1.7592 BTC ($117,977). Unknown earned a total reward of 6.25 BTC $419,143. The reward consisted of a base reward of 6.25 BTC $419,143 with an additional 0.1427 BTC ($9,569.87) reward paid as fees of the 2,567 transactions which were included in the block.

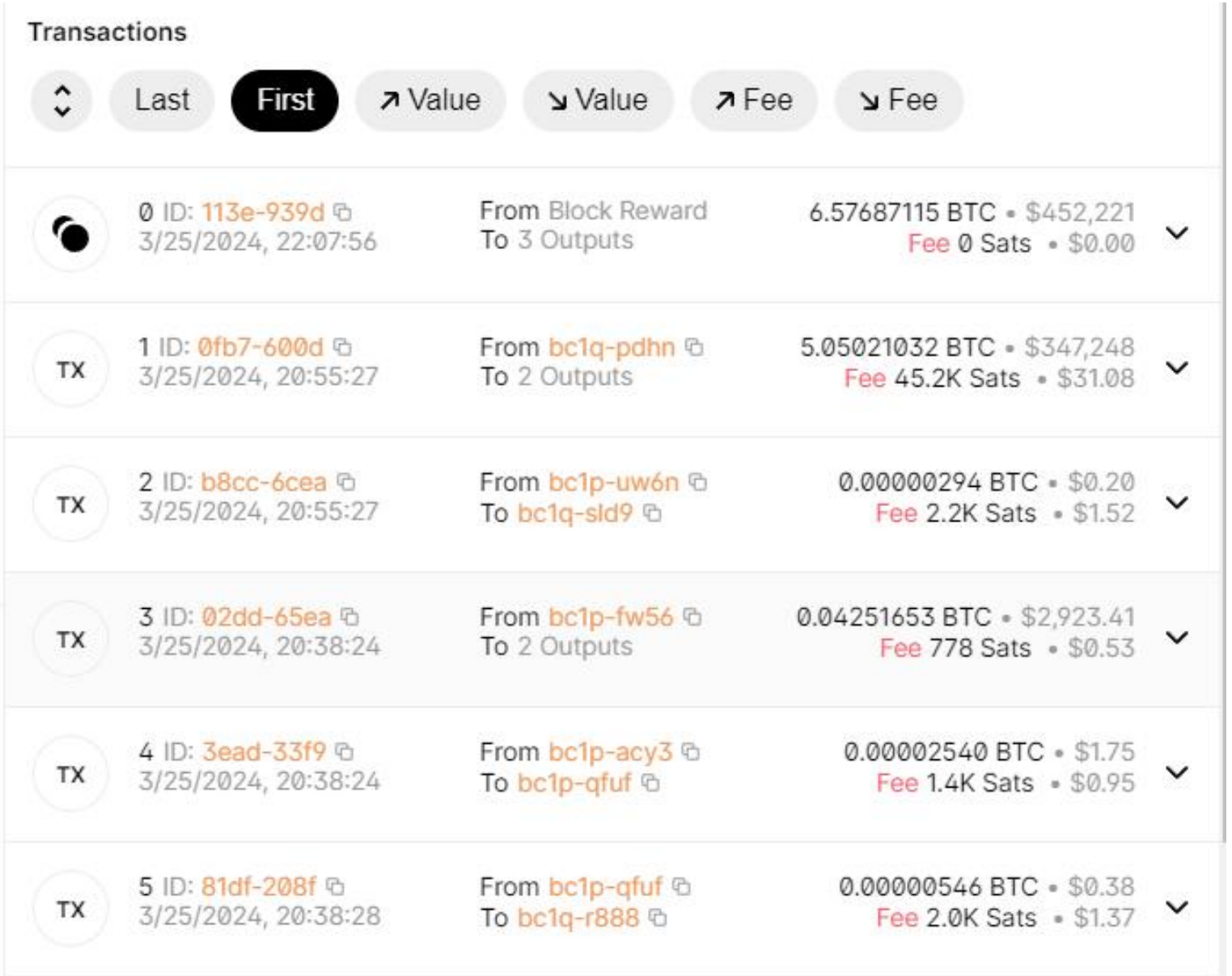
Details

Hash	00000-ae49f	Depth	1
Capacity	153.66%	Size	1,611,215
Distance	33m 58s	Version	0×34000000
BTC	4,515.9543	Merkle Root	cf-74
Value	$302,852,898	Difficulty	83,947,913,181,361.55
Value Today	$302,378,090	Nonce	2,250,773,337
Average Value	1.7592342239 BTC	Bits	386,095,705
Median Value	0.00788848 BTC	Weight	3,998,018 WU
Input Value	4,516.10 BTC	Minted	6.25 BTC
Output Value	4,522.35 BTC	Reward	6.39271849 BTC
Transactions	2,567	Mined on	2024年3月25日 20:54:19
Witness Tx's	2,414	Height	836,245
Inputs	8,541	Confirmations	1
Outputs	8,134	Fee Range	0-320 sat/vByte
Fees	0.14271849 BTC	Average Fee	0.00005560
Fees Kb	0.0000886 BTC	Median Fee	0.00002314
Fees kWU	0.0000357 BTC	Miner	Unknown

Transactions

Last | First | ↗ Value | ↘ Value | ↗ Fee | ↘ Fee

	0 ID: 2221-7aa4 3/25/2024, 20:54:19	From Block Reward To 6 Outputs	6.39271849 BTC • $428,714 Fee 0 Sats • $0.00
TX	1 ID: 4325-0906 3/25/2024, 20:54:19	From 1JRh-YocL To 4 Outputs	0.04943450 BTC • $3,315.22 Fee 701 Sats • $0.47
TX	2 ID: c0eb-2800 3/25/2024, 20:54:19	From bc1q-pdhn To 2 Outputs	5.05396991 BTC • $338,933 Fee 45.2K Sats • $30.31
TX	3 ID: e2d2-cf94 3/25/2024, 20:53:03	From bc1q-hsfv To 2 Outputs	3.83698258 BTC • $257,319 Fee 45.2K Sats • $30.31
TX	4 ID: b1b4-23b8 3/25/2024, 20:53:42	From bc1q-pdhn To 2 Outputs	5.06134511 BTC • $339,428 Fee 45.2K Sats • $30.31
TX	5 ID: 6c3a-b610 3/25/2024, 20:52:28	From 18zk-skNz To bc1q-jc86	0.01525444 BTC • $1,023.01 Fee 70.7K Sats • $47.42
TX	6 ID: 21a1-718e 3/25/2024, 20:52:21	From 1M4n-y8mp To bc1q-f5zp	1.29955400 BTC • $87,151.83 Fee 44.6K Sats • $29.91
TX	7 ID: 81cb-aaa2 3/25/2024, 20:51:08	From bc1q-80s6 To 24 Outputs	14.73703600 BTC • $988,308 Fee 141.4K Sats • $94.83
TX	8 ID: 3cfa-f0e1 3/25/2024, 20:51:04	From 1M9e-RhwJ To bc1q-r5qw	0.03474215 BTC • $2,329.91 Fee 25.8K Sats • $17.29


Transactions
Last
First
↗ Value
↘ Value
↗ Fee
↘ Fee
0 ID: 113e-939d
3/25/2024, 22:07:56
From Block Reward
To 3 Outputs
6.57687115 BTC • $452,221
Fee 0 Sats • $0.00
TX
1 ID: 0fb7-600d
3/25/2024, 20:55:27
From bc1q-pdhn
To 2 Outputs
5.05021032 BTC • $347,248
Fee 45.2K Sats • $31.08
TX
2 ID: b8cc-6cea
3/25/2024, 20:55:27
From bc1p-uw6n
To bc1q-sld9
0.00000294 BTC • $0.20
Fee 2.2K Sats • $1.52
TX
3 ID: 02dd-65ea
3/25/2024, 20:38:24
From bc1p-fw56
To 2 Outputs
0.04251653 BTC • $2,923.41
Fee 778 Sats • $0.53
TX
4 ID: 3ead-33f9
3/25/2024, 20:38:24
From bc1p-acy3
To bc1p-qfuf
0.00002540 BTC • $1.75
Fee 1.4K Sats • $0.95
TX
5 ID: 81df-208f
3/25/2024, 20:38:28
From bc1p-qfuf
To bc1q-r888
0.00000546 BTC • $0.38
Fee 2.0K Sats • $1.37

TX

USD

Bitcoin Transaction

Broadcasted on 25 Mar 2024 10:07:56 GMT+8

Hash ID
113e59f69954a8559cb5a71c79b2198c3661d0cde969f17cde4696e4da07939d

Amount	6.57687115 BTC • $453,600
Fee	0 SATS • $0.00
From	Block Reward
To	3 Outputs

Confirmed

This transaction has 5 Confirmations. It was mined in Block 836,246

This transaction is efficient, no issues detected.

Decoded OP_Return
RSKBLOCK:-k<2I0Dx$ ^

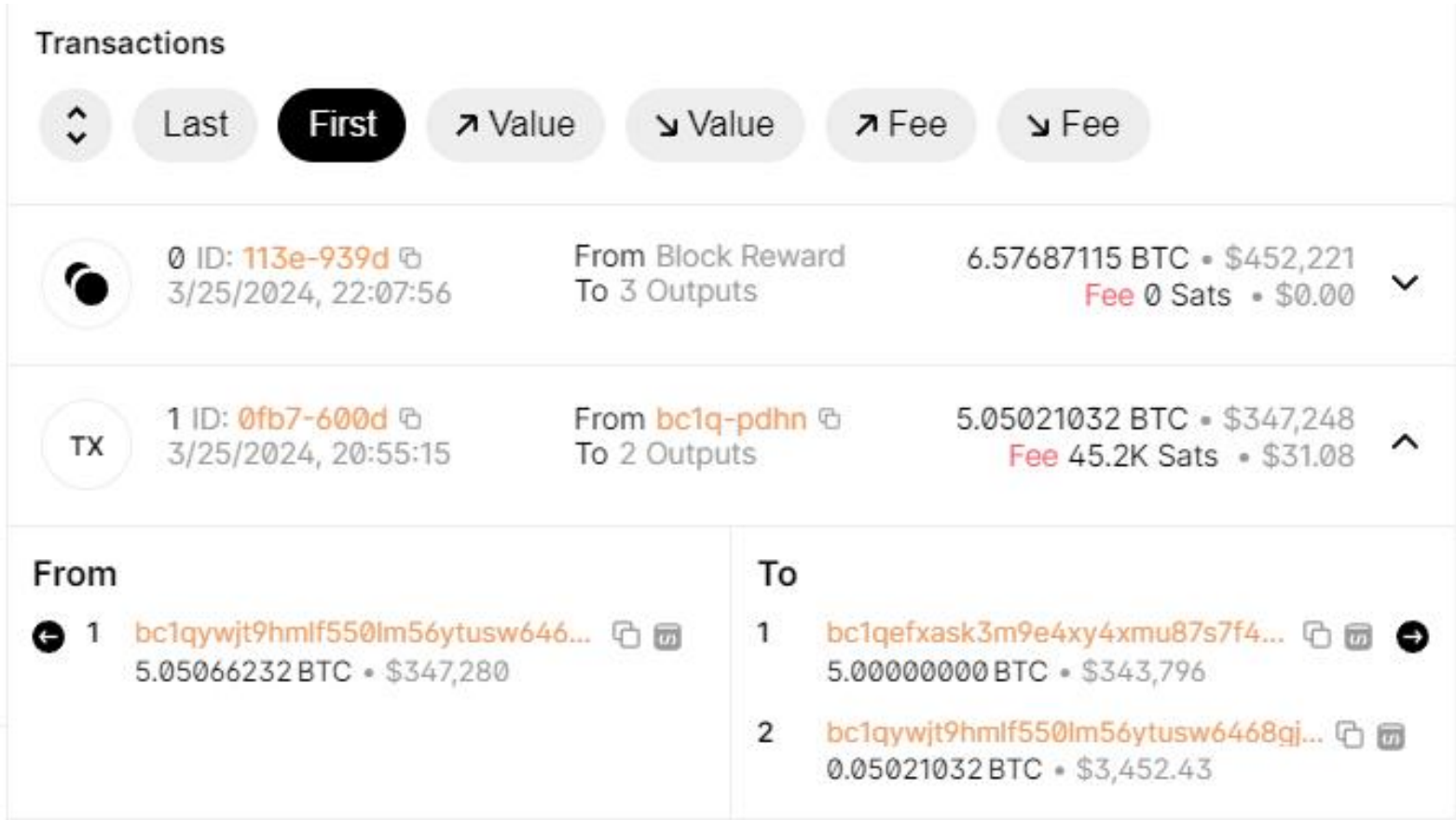
Summary

This transaction was first broadcasted on the Bitcoin network on March 25, 2024 at 10:03 AM GMT+8. The transaction currently has 5 confirmations on the network. The current value of this transaction is now $453,600.

Advanced Details

Hash	113e-939d	Block ID	836,246
Time	25 Mar 2024 10:07:56	Age	35m 37s
Inputs	1	Input Value	—
Outputs	3		$0.00
Output Value	6.57687115 BTC	Fee	0 BTC
	$453,600		$0.00
Fee/B	-	Fee/VB	-
Size	299 Bytes	Weight	1,088
Weight Unit	-	Coinbase	Yes
Witness	Yes	RBF	No
Locktime	0	Version	1
BTC Price	$68,969.06		


Overview
JSON
From
1
Block Reward
0.00 BTC • $0.00
To
1
ViaBTC
6.57687115 BTC • $453,600
2
Unknown
0.00000000 BTC • $0.00
3
Unknown
0.00000000 BTC • $0.00


Transactions
Last
First
↗ Value
↘ Value
↗ Fee
↘ Fee
0 ID: 113e-939d
3/25/2024, 22:07:56
From Block Reward
To 3 Outputs
6.57687115 BTC • $452,221
Fee 0 Sats • $0.00
1 ID: 0fb7-600d
3/25/2024, 20:55:15
TX
From bc1q-pdhn
To 2 Outputs
5.05021032 BTC • $347,248
Fee 45.2K Sats • $31.08
From
1 bc1qywjt9hmlf550lm56ytusw646...
5.05066232 BTC • $347,280
To
1 bc1qefxask3m9e4xy4xmu87s7f4...
5.00000000 BTC • $343,796
2 bc1qywjt9hmlf550lm56ytusw6468gj...
0.05021032 BTC • $3,452.43

Summary

This transaction was first broadcasted on the Bitcoin network on March 25, 2024 at 08:03 AM GMT+8. The transaction currently has 6 confirmations on the network. The current value of this transaction is now $349,179.

Advanced Details

Hash	0fb7-600d	Block ID	836,246
Position	1	Time	25 Mar 2024 08:55:27
Age	1h 54m 3s	Inputs	1
Input Value	5.05066232 BTC	Outputs	2
	$349,211	Output Value	5.05021032 BTC
Fee	0.00045200 BTC		$349,179
	$31.25	Fee/B	202.691 sat/B
Fee/VB	320.567 sat/vByte	Size	223 Bytes
Weight	562	Weight Unit	80.427 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	2	BTC Price	$69,141.67


Overview
JSON
From
1 bc1qywjt9hmlf550lm56ytusw6468gjpfpaeq0pdhn
5.05066232 BTC • $349,937
To
Funds were spent, click to view transaction.
1 bc1qefxask3m9e4xy4xmu87s7f4gdllmruewz7p0er
5.00000000 BTC • $346,427
2 bc1qywjt9hmlf550lm56ytusw6468gjpfpaeq0pdhn
0.05021032 BTC • $3,478.85


Overview
JSON
From
1 bc1qefxask3m9e4xy4xmu87s7f4gdllmruewz7p0er
5.00000000 BTC • $346,427
To
1 bc1q7znglrlh9z7p80dy5aggvy4gpraelmllpg9a6g
4.99997800 BTC • $346,426

Address

USD BTC

This address has transacted 1,001,526 times on the Bitcoin blockchain. It has received a total of 3,138,303.33351950 BTC ($63,168,867,903.25) and has sent a total of 3,138,287.00172058 BTC ($63,168,539,171.08). The current value of this address is 16.33179892 BTC ($328,732.16).

Address	bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7...
Format	BECH32 (P2WSH)
Transactions	1,001,526
Total Received	3138303.33351950 BTC
Total Sent	3138287.00172058 BTC
Final Balance	16.33179892 BTC

Transactions

Fee 0.00040000 BTC
(105.263 sat/B - 52.770 sat/WU - 380 bytes)
(210.526 sat/vByte - 190 virtual bytes)

-0.00832982 BTC

UNCONFIRMED

Hash 6688cb8d1580ba35f11e868016538c906f59f834f40b27...

2022-09-27 17:08

bc1qwqdg6squsna38e46795at95yu... 3.79047560 BTC

3NPhh279wpt8FNmhGrQGEQg9gxJ... 0.00792982 BTC

bc1qwqdg6squsna38e46795at95yu... 3.78214578 BTC

Fee 0.00040000 BTC
(104.712 sat/B - 52.219 sat/WU - 382 bytes)
(208.333 sat/vByte - 192 virtual bytes)

-0.00980000 BTC

UNCONFIRMED

Hash 0f910f13f4327a6506a0df069f0e0fddfa9a18aa70aaa225...

2022-09-27 17:08

bc1qwqdg6squsna38e46795at95yu... 0.03199530 BTC

1Cf85sZiSLV8Xv2P4RAMRhPJJm6h... 0.00940000 BTC

bc1qwqdg6squsna38e46795at95yu... 0.02219530 BTC

ETH Price: $3,610.13 (+5.29%) Gas: 17 Gwei

Etherscan

Home | Blockchain | Tokens | NFTs | Resources | Developers | More | Sign In

The Ethereum Blockchain Explorer

All Filters | Search by Address / Txn Hash / Block / Token / Domain Name

Sponsored: - Harambe Token Presale: The first A.I powered hedged fund with 100% APY! Get in early.

ETHER PRICE
$3,610.13 @ 0.051409 BTC (+5.29%)

MARKET CAP
$433,483,071,335.00

TRANSACTIONS
2,309.84 M (15.3 TPS)

LAST FINALIZED BLOCK
19515307

MED GAS PRICE
17 Gwei ($1.29)

LAST SAFE BLOCK
19515371

TRANSACTION HISTORY IN 14 DAYS

Latest Blocks

Customize

19515398 14 secs ago	Fee Recipient beaverbuild 78 txns in 12 secs	0.02667 Eth
19515397 26 secs ago	Fee Recipient Lido: Execution La... 224 txns in 12 secs	0.06807 Eth

Latest Transactions

Customize

0x5548adb5a2... 14 secs ago	From 0x95222290...5CC4BAfe5 To 0x388C818C...7ccB19297	0.02762 Eth
0x0ba378df211... 14 secs ago	From 0x2c154c5E...69b69850b To 0x11111112...0f8842A65	0 Eth

- 比特币和以太坊是两种最主要的加密货币
- 比特币是区块链1.0，以太坊是区块链2.0
- 以太坊基于比特币的一些运行问题进行了改进
  - ✓ 出块时间15s左右，减小交易延迟
  - ✓ mining puzzle对内存要求高（限制ASIC使用）
  - ✓ 使用PoS，代替PoW
- 第一个支持智能合约的区块链系统

回顾：传统合约

在了解智能合约前，先回顾传统合约：

- 传统合约如果没有定量标准，将无法正常执行
- 当双方有分歧，需要有可信任的公证人。
- 现实社会中合约需要通过政府、司法手段来维护。

自动化维度	**条件满足，但交易未必会继续**
主客观维度	**公证人的主观意识会影响合约规则**
执行时间维度	**整个合约执行过程繁琐，浪费时间**
违约惩罚维度	**一方违约，未必会收到惩罚， 难以追责**

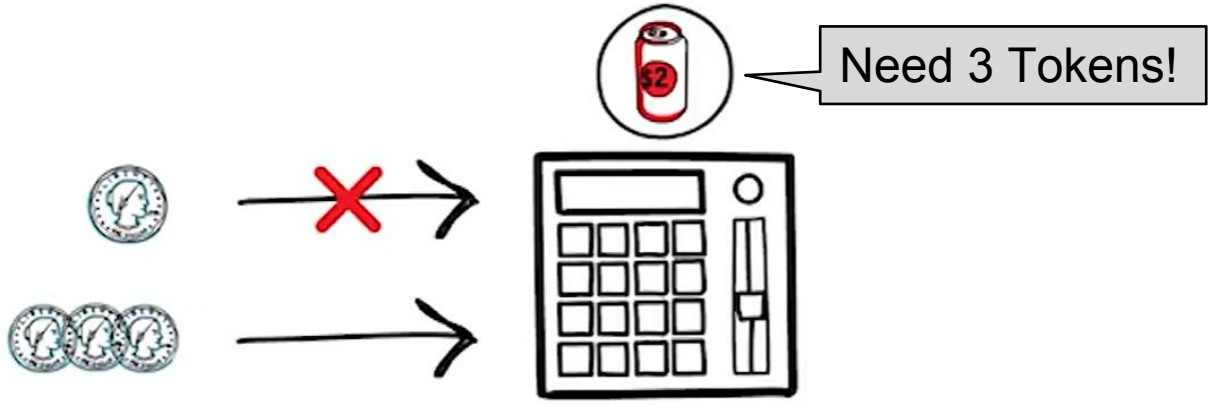
传统合约会受到各种维度的影响

智能合约

- 为了解决传统合约的弊端，尼克·萨博提出智能合约。
  - 一般认为，智能合约指能够自动执行合约条款的计算机程序，其概念由尼克·萨博在1994年提出，具有事件驱动、价值转移、自动执行等特性。

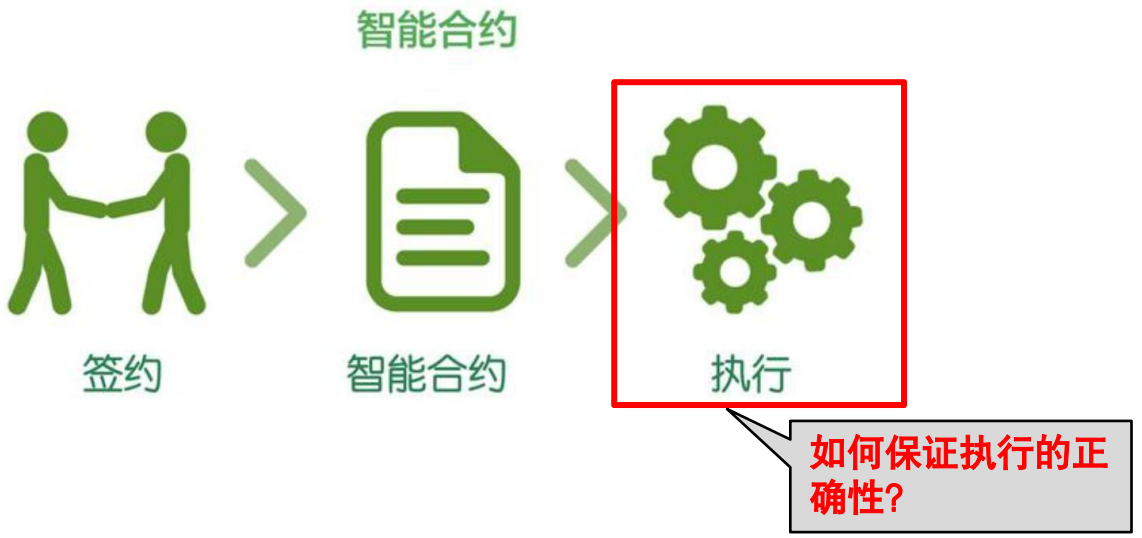
智能合约

- 将自动售货机视为智能合约
  - 事件驱动：合约以投币等动作作为输入，触发其动作执行；
  - 价值转移：外部以钱币为输入，合约输出饮料、食品等商品，完成了价值的交换或转移；
  - 自动执行：这一履约行为是完全自动的，不需要人在其中干预（投币动作除外）



智能合约

- 智能合约依赖于环境的可靠性
  - 售货机这一“智能合约”依赖的就是机器，其执行的可靠性除了合约本身，还依赖于执行环境的可靠性，一旦执行环境出错，则合约的执行也将出错

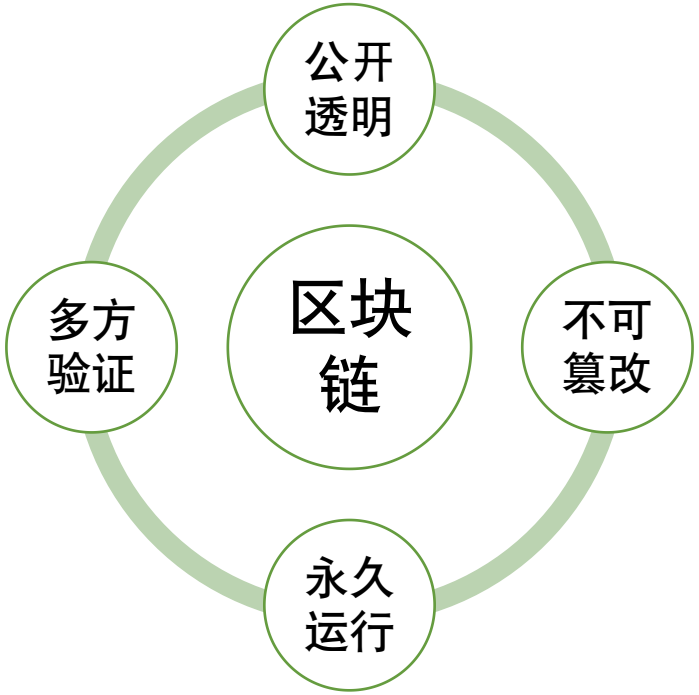


智能合约

- 中心化环境的弊端
  - 容易受到篡改：可以人为地修改自动售货机的程序，使其免费出售商品
  - 出错后难以追溯恢复：一旦售货机程序被篡改，篡改的源头是往往无法追溯的，因为恶意篡改人已经掌握了整个机器的控制权

智能合约

- 应用在区块链上的智能合约
  - 区块链是一种能使多方间达成状态一致的有效手段，那么将智能合约应用到区块链上，就能使得智能合约具备更高的可靠性。



智能合约

❑以太坊智能合约

- 以太坊在多个节点组成的点对点网络中，维护共同的区块链数据，通过区块链上的交易来进行智能合约的创建、调用、结束等操作。
- 由于多个节点所维护的区块链状态是一致的，因此，多个节点上所运行的智能合约的过程和结果也是一致的。

智能合约的出现解决了传统合约的信任问题，大幅降低了信任成本。

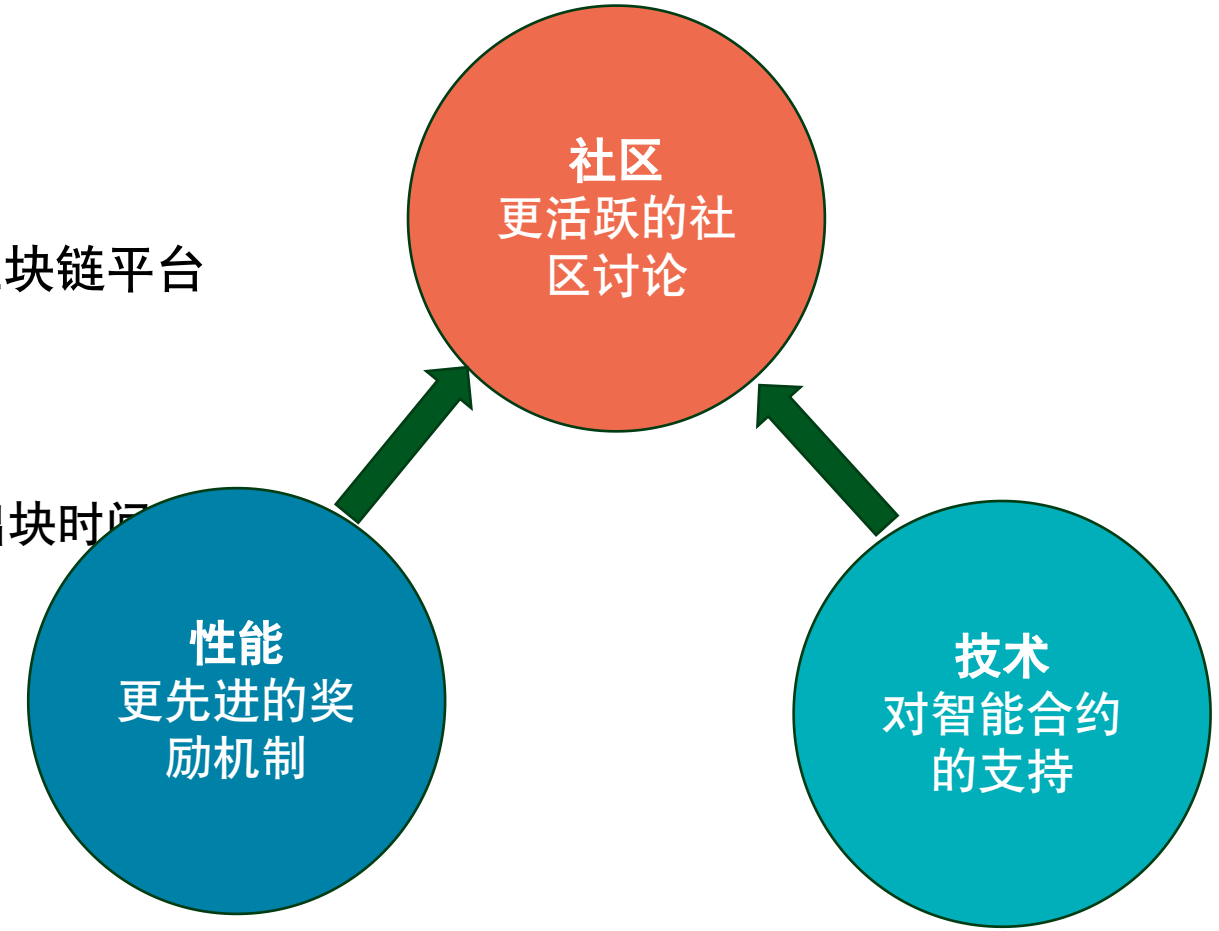
Code is law!

以太坊简介

- 第一个支持智能合约的区块链系统
- 使用Ether作为加密数字货币
- 是生态社区最活跃的区块链系统，出现了大量去中心化自治组织（DAOs）和去中心化应用（Dapps），促进了区块链技术在发币以外的应用
  - 超过30,000个github开源项目
  - 超过 3000 个基于以太坊的 Dapp

以太坊与比特币对比

- 技术：
  - 支持智能合约
  - 通用的Dapp的底层区块链平台
  - 账户模型
- 性能：
  - 增加叔块奖励，减少出块时间
  - Ghost共识机制
- 社区：
  - 更加活跃的社区
  - 超过35k的开源项目



以太坊特色与应用

- 溯源存证
- 数字资产发行和流通
- 数据共享
- 多种应用Dapp

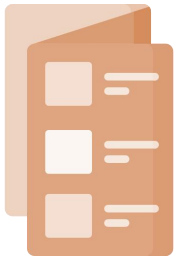
表 3.1　以太坊当前最流行的十个区块链应用

名称	类别	功能描述
MakerDAO	金融	去中心化借贷应用
Chainlink	安全	去中心化预言机
KyberNetwork	交换	代币交换协议
Status	钱包	DApp 浏览器发行的代币
My Crypto Heroes	游戏	角色扮演游戏
Uniswap	交换	代币交换协议
Axie Infinity	游戏	宠物养成游戏
Synthetix	金融	去中心化合成资产平台
Basic Attention Token	钱包	Brave 浏览器的激励代币
Knight Story	游戏	角色扮演游戏

Outline

1. 什么是 加密货币/数字货币

2. 典型 加密/数字货币 有哪些



山寨币

1. 算法改进

- 莱特币于2011年11月9日上线
- **莱特币（LiteCoin代码LTC）Scrypt 算法**
- 确认时间减少到2.5分钟
- 货币总量增加到8400万个

2. 模式改进

- 点点币于2012年8月19日上线
- **点点币引入了权益证明（POS）模式**
- 权益证明就是挖矿的产出取决于：拥有点点币的数量乘以拥有的时间

3. 用途改进

- 质数币于2013年7月12日上线
- **质数币工作量证明（寻找质数）**
- 质数币的另一个创新是挖矿奖励的数量，同工作量的难度相关，不像比特币是固定的。

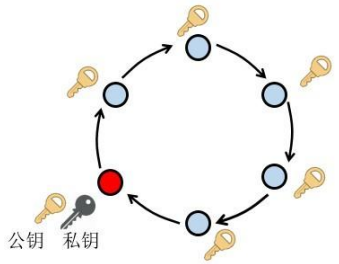
其他山寨币

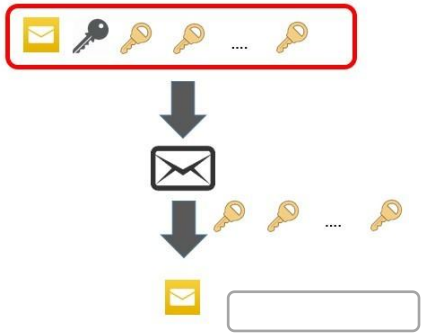
- **格雷德币**（GridCoin 代码 GRC）分布式科学计算
- **夸克币**（Quark 代码 QRK）多种加密
- **万事达币**（MasterCoin 代码 MSC）提供分布式资产平台
- **合约币**（Counterparty 代码 XCP）烧钱模式
- **比特股**（BitShares 代码 BTS）与事物挂钩
- **极光币**（Auroracoin 代码 AUR）免费发放
- **…**

匿名币

1. 门罗币

- 门罗币于 2014 年 4 月上线
- 通过 隐蔽地址 实现 不可链接性
- 通过 环签名技术 实现 不可追踪性





2. DASH币

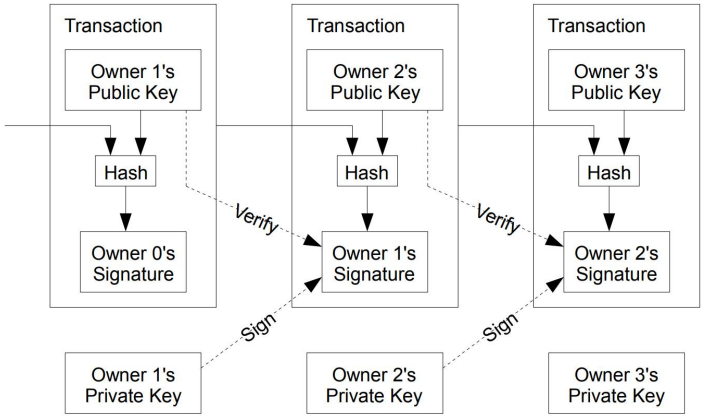
- 2014 年发布白皮书，发行总量为1890万个
- 基于 CoinJoin 实现了一种 隐私保护策略

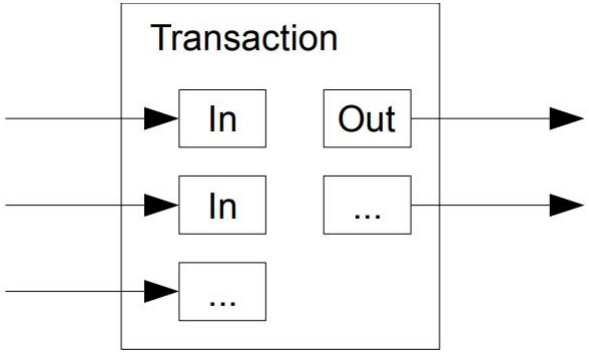
3. 大零币

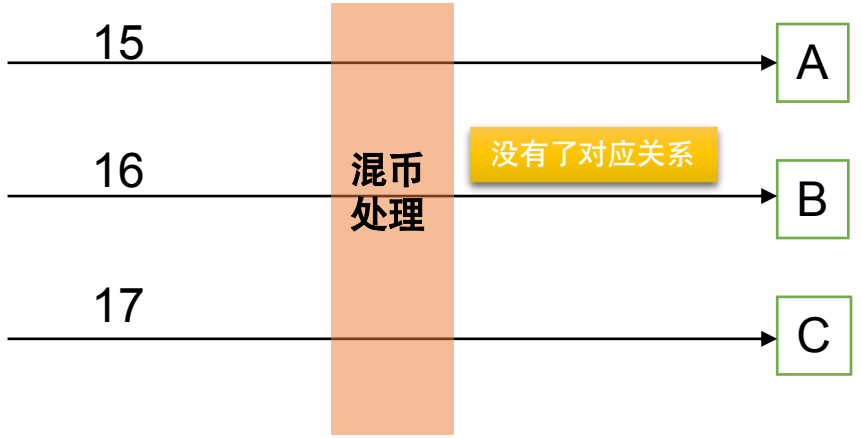
- 大零币上线于 2016 年10月28日
- Zerocoin 通过 零知识证明 让用户只是通过 加密货币本身进行交互来 隐藏交易信息

CoinJoin

混币：将多笔交易的输入和输出进行混合，让生成的交易无法溯源达到有效的保护交易隐私的目的。







瑞波币

- Ripple 是一个开放的支付网络，主要用于货币兑换和汇款。
- XRP 是 Ripple 网络系统中的原生代币。
- Ripple 网关 是 Ripple 网络的重要组成部分也是通过 Ripple 网络交易的关键所在
- 瑞波网络 提出的高度中心化模型，创造出了新型的第三方信任，没有消除中心化第三方信任的需要

☆	4	USD Coin USDC	Buy	$1.00
☆	5	BNB BNB		$284.55
☆	6	XRP XRP	Buy	$0.4739
☆	7	Binance USD BUSD		$1.00
☆	8	Cardano ADA	Buy	$0.4567

IFO: 分叉币

IFO（Initial Fork Offerings），首次分叉发行

- 指通过分叉比特币等主流加密货币生成新的代币
- 一些社区或集团为了改进比特币的机制而分叉出一条新的区块链，这实际是一种硬分叉的场景
- 2017年区8月1号，Bitcoin Cash（BCH）区块链成功在区块高度478559与主链分离。这一新的加密货币默认区块大小为8MB，并且可以实现块容量的动态调整。

BCH：跌幅78%
BTG：跌幅84%
BCD：跌幅96%
SBTC：跌幅98%
BTF：跌幅90%
BTN：跌幅99.96%
BTP：跌幅89%
BTV：跌幅99.47%
UBTC：跌幅97%
BTH：跌幅99%
BCX：跌幅67%
LBTC：跌幅86%
BCK：跌幅99.75%
GOD：跌幅90%

矿霸，比特大陆支持

IFO: 分叉币

比特币的五次重要分叉

第一次：2017年8月1日，被称为比特币现金（Bitcoin Cash）。这次分叉的主要原因是比特币社区对于比特币的扩容问题产生了分歧。比特币现金采用了更大的区块大小，使得交易速度更快，手续费更低，但也带来了一些安全性和去中心化程度的问题。

第二次：2017年10月24日，被称为比特币黄金（Bitcoin Gold）。这次分叉的主要目的是改变比特币的挖矿算法，使得普通用户也能够参与挖矿，增加去中心化程度。然而，比特币黄金在分叉后面临了一系列安全性问题，使得其发展受到了限制。

第三次：2017年12月23日，被称为比特币钻石（Bitcoin Diamond）。这次分叉的主要目的是改善比特币的性和交易速度。比特币钻石采用了更大的区块大小和更快的交易确认时间，但也存在着一些技术和安全性问题。

第四次：2018年10月24日，被称为比特币SV（Bitcoin SV）。这次分叉的主要原因是对比特币扩容问题的分歧，比特币SV主张采用更大的区块大小来提高交易速度和扩展性。然而，比特币SV的发展受到了一些技术和社区的争议。

第五次：2019年11月15日，被称为比特币现金ABC（Bitcoin Cash ABC）和比特币现金SV（Bitcoin Cash SV）。这次分叉的主要原因是比特币现金社区对于链上协议的改变产生了分歧。比特币现金ABC和比特币现金SV分别代表了不同的发展方向，两者之间展开了一场激烈的竞争。

韭菜必知：ICO、IFO、IMO、IEO

- ICO（Initial Coin Offering），首次代币发行，指区块链项目首次向公众发行代币，募集比特币、以太坊等主流加密货币以获得项目运作的经费。
  - 用未来的产品向未来的用户“众筹”

- IFO（Initial Fork Offerings），首次分叉发行，指通过分叉比特币等主流加密货币生成新的代币。
- IEO（Initial Exchange Offerings），首次交易发行，指以交易所为核心发行代币；代币跳过 ICO 这步，直接上线交易所。
- IMO（Initial Miner Offerings），首次矿机发行，指首次通过售卖硬件/矿机来发行代币。

Eth 以太坊、以太币

- 2013年， Vitalik Buterin发帖

  比特币区块链功能太少，因为比特币区块原则上只能写几十个字节，几乎写不下任何程序

- 2014年，以太币发起众筹

  以太币众筹价格31591个比特币，换成人民币是2.8元

- 2015年7月30日，以太坊基金会开始发布Frontier

  意味着以太坊可以在世界各地的交易所交易，2.8涨到17元

可编程货币

比特币

内嵌脚本

支撑加密数字货币

可编程合约

以太坊

智能合约

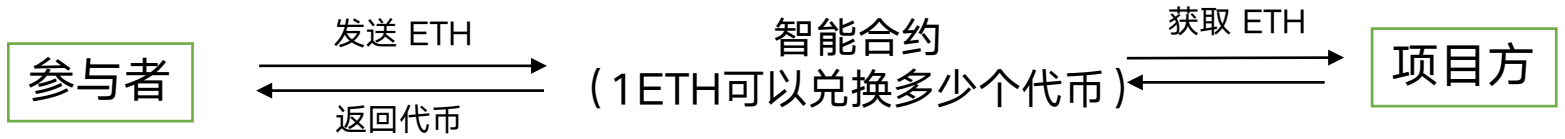
支撑智能合约

以太币 计量单位

1. *wei* Wei Dai 戴伟 密码学家，发表 B-money
2. 10^3: *lovelace* Ada Lovelace 洛夫莱斯 世界上第一位程序员、诗人拜伦之女
3. 10^6: *babbage* Charles Babbage 巴贝奇 英国数学家、发明家兼机械工程师，提出了差分机与分析机的设计概念，被视为计算机先驱。
4. 10^9: *shannon* Claude Elwood Shannon 香农 美国数学家、电子工程师和密码学家，被誉为信息论的创始人
5. 10^12: *szabo* Nick Szabo 尼克萨博 密码学家、智能合约的提出者
6. 10^15: *finney* Hal Finney 芬尼 密码学家、工作量证明机制（PoW）提出
7. 10^18: *ether* 以太

以太坊的 ICO

基于以太坊的 **发币** ICO (Initial Coin Offering)



	ICO	IPO
资料	白皮书	非常繁琐
投资者获得权力	项目代币，使用权	企业所有权
融资速度	快	慢
监管	不允许	允许
跨国	支持	不支持
发行门槛	无	很高
退出方式	**上数字货币交易所**	**上市**
人数	无	不大于200人

以太坊的 ICO

2017 年 9 月 4 日，七部委发布公告禁止 ICO

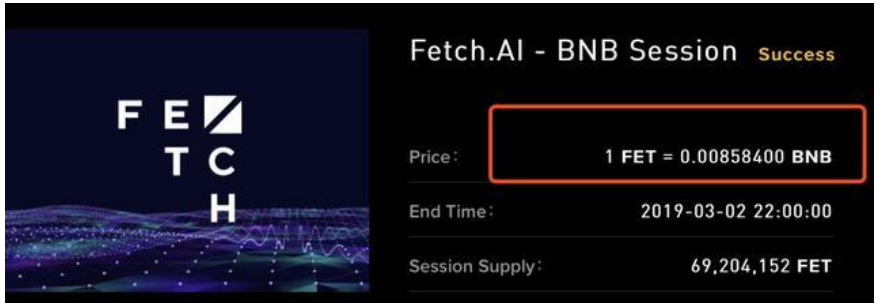
IEO：首次交易发行

IEO 的特点是 “近水楼台先得月”，没有融资认购的过程，省掉了ICO、空投推广等环节，直接在加密货币交易所上市交易

ICO　成功的第一步是上交易所

项 目 白 皮 书
团 队
代 码
社 区
募 资 情 况

IEO　交 易 所 直 接 发 行



1 FET = 0.05 BNB

1 FET = 0.01414 BNB

FET (Fetch.AI)，总量：11.53亿，2019年2月份在币安IEO的项目，当时开盘直接5倍拉升，FET是一个基于人工智能与区块链搭建的一个数字化的经济网络平台

交易所代币

火币的 HT、币安的 BNB、OKEx 的 OKB 等由加密货币交易所发行的平台币，均属 IEO。

火 币 HT

币 安 BNB

以太坊的共识

PoW -> PoS

POS

Proof of Stake

质 押（Staking）一定数量的币便可以拥有出块权利

「币量」or 「币量」 *「币龄」

Peercoin、 NXT、 Blackcoin、 Neblio

DPOS

Delegate Proof of Stake

质 押 、 用 户 投 票 、 组 织 实 力

轮流（Round-robin）出块

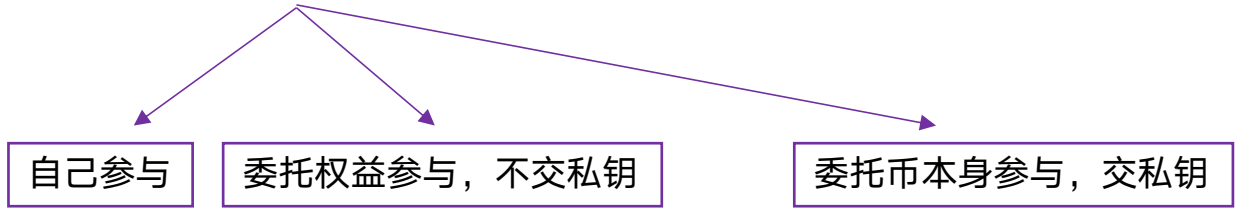
PoS生态

增 发 下 的 经 济 模 式

Staking

Staking：指持币人通过「Staking」执行了自己持有币所相关的权益

只要持币人参与 Staking 的过程，就可以享有不同链增发不同比例的奖励



Staking Economy

金融衍生品：借贷

项 目 方

保 护 网 络 安 全

锁 仓，利 于 币 价 稳 定

参 与 者

持 币 生 息

行 使 权 益

价 格 涨 了，还 有 额 外 的 收 益

价 格

短 期 收 益 在 分 成，长 期 收 益 在 生 态

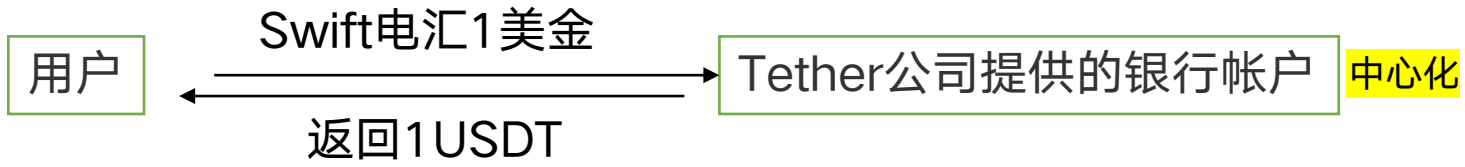
稳定币

稳定币：用来购买数字货币、市场行情不好时，用来避险、跨境支付

去中心化

USDT 是 Tether 公司推出的基于稳定价值货币美元（USD）的代币 Tether USD（下称 USDT).

Omni-USDT，ERC-USDT，TRC-USDT



1. 与审计公司合作终止
2. 19年4月，Tether 总法律顾问承认，只有约 74% 的 USDT 由现金及等价物支撑
3. 19年7月，Tether 在波场上又一次性增发 50亿 枚 USDT，官方出来澄清仅仅只想发布5000万枚，按错小数点，并及时将多余的 USDT 销毁。

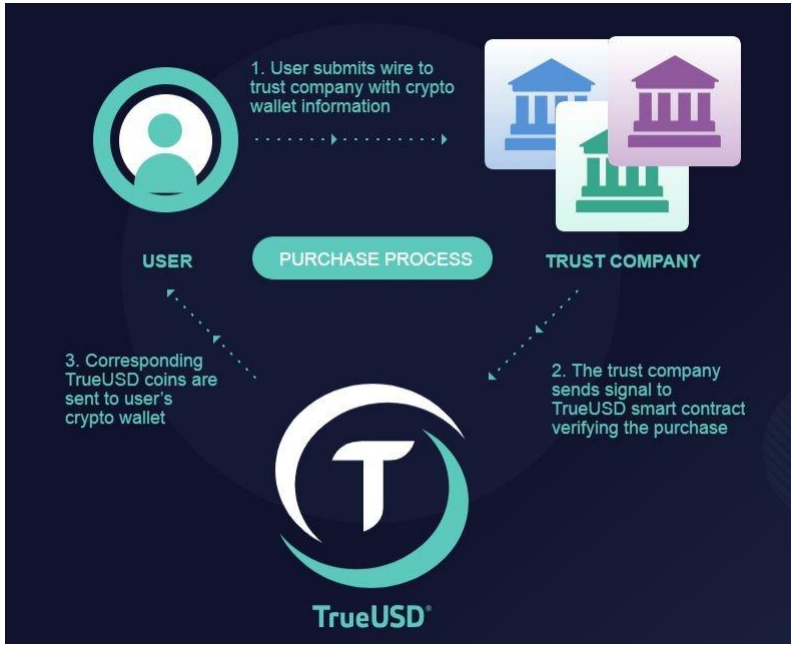
审计不公开、中心化、涉嫌超额发行

稳定币

TUSD, TrueUSD

代币 / 稳定币

1. 保证完全**美元**储备，提供定期审计。
2. 实行严格标准的KYC/AML验证。
3. 独立托管，不需要经手 TrueUSD 项目团队。



GUSD Gemini Dollar

PAX Paxos Standard Token

USDC USD Coin

稳定币

1. 基于 数字货币 的 稳定币（质押贷款）

用户 ⇄ 智能合约（1.5ETH；返回价值 1ETH 的 Dai）

付利息

Dai上升，降低利率

Dai下降，升高利率

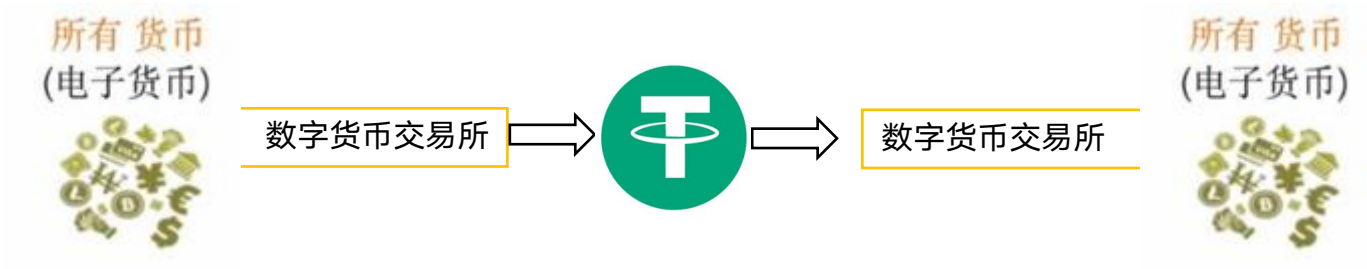
2. 基于 算法 的 稳定币

1. 智能合约发稳定币，市场价格高，多发行稀释，价格低，回购。
2. 回购的钱不足，发行一种股票，让别人购买。

稳定币

截至2019年10月总量超过40亿美金

大部分资金是炒币



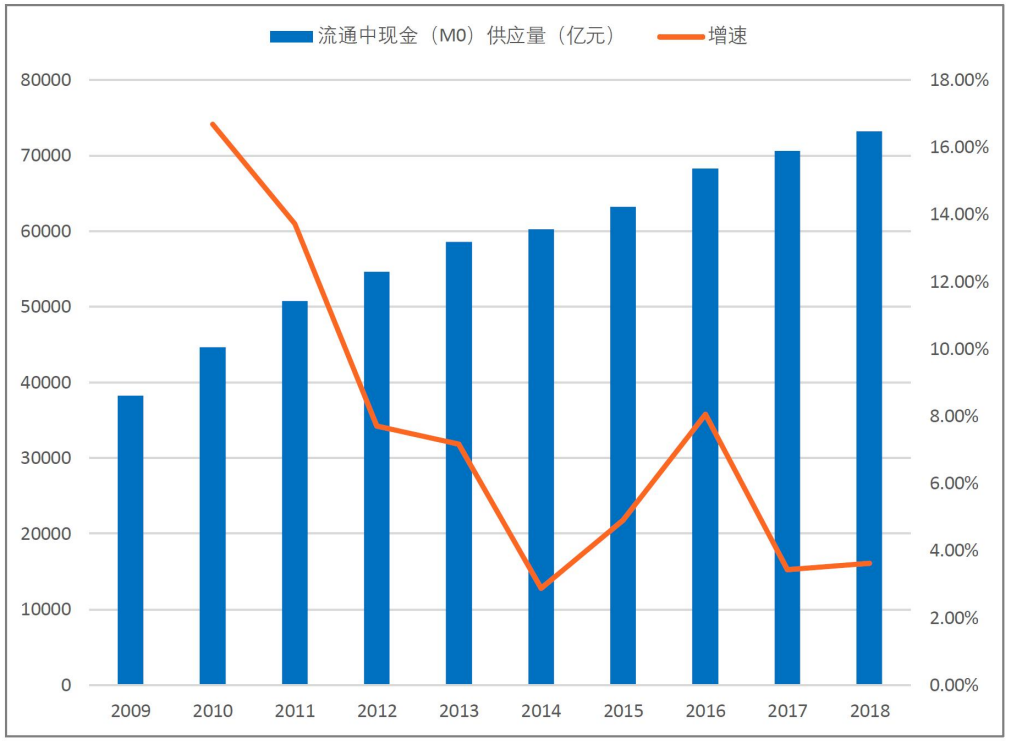
22万亿美元跨境支付市场

合规通向更大的规模

DCEP：央行数字货币

在电子支付已经这么发达的情况下，为什么还要发行央行的数字货币？

- 纸币的应用越来越少
- 纸钞、硬币的印制、发行、贮藏等各环节成本相对数字货币都非常高，还需要不断投入成本进行防伪技术研发（防止洗钱） 替代M0
- 基于现有银行账户 紧耦合模式的电子支付，无法满足公众匿名支付的需求



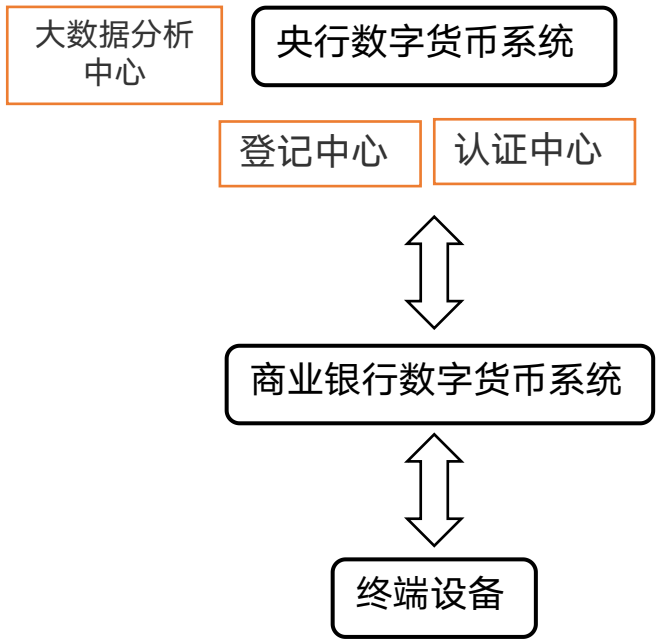
图：中国近 10 年来 M0 的数量及增速情况

央行数字货币

数字货币　　电子支付

Digital Currency Electronic Payment

DCEP



双层运营投放体系（1 币 2 库 3 中心）

登记中心

印制

转移

销毁

回笼

1. 记录数字货币的归属
2. 记录交易流水表

认证中心

CA认证中心（商业银行）

IBC认证中心（钱包服务）

大数据分析中心

反洗钱

满足零售级别的高并发性能

区块链平台无法满足零售所需的吞吐量（至少30万笔/秒）

技术中性：商业银行的体验决定

央行数字货币

匿名性

银行 和 商家 相互勾结也不能跟踪数字货币的使用
但数字货币的 发行方 可跟踪数字货币的使用

M||m

M = 交易代码 || 发送者公钥 ||D 币信息 || 支付金额 || 接受者公钥

Hash（M）签名得到m

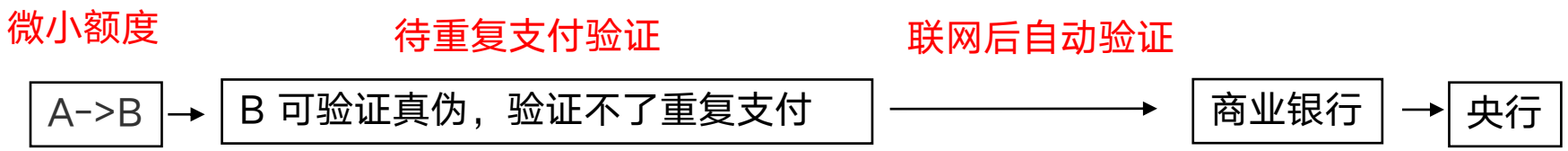
分级匿名

D-RMB 芯片卡支持匿名发卡和实名发卡

央行数字货币

双离线离线支付

近场支付:



通过滞后重复支付检查来发现并追责

对不良记录将录入征信系统以作惩戒

央行数字货币

第一，它能更准确地帮助 计算 宏观经济指标，如通货膨胀率等

第二，它增加了 收集实时数据的可能性，如货币的创建、记账和流通，为货币政策制定者提供了更加有用的参考

第三，通过使用其 大数据中心，它能 帮助监管机构 打击洗钱、恐怖融资和逃税等违法行为

第四，它能够帮助 降低 金融机构 和 监管机构 之间 的 信息不对称问题。