查詢比特幣全帳本的資訊

盧瑞山 教授

rslu2000@gmail.com

複習上節課的觀念

- 上週透過紙上的模擬，我們已經認識了什麼比特幣，比特幣如何記帳？

- 任何一筆比特幣交易，都會被某節點給廣播讓全網的節點都知道

- 比特幣大約每十分鐘結算一次，也就是每十分鐘打包一次，生出一個新的區塊

- 每生出一個區塊，我們稱挖出一個區塊

- 每挖出一個區塊就會額外生產出一批新的比特幣出來，記載在帳本上

- 搶記帳權就是挖礦

- 搶記帳權需要耗費運算資源

- 比特幣的帳本是全網公開的

- 只要是全節點，都擁有一份完整的歷史帳本
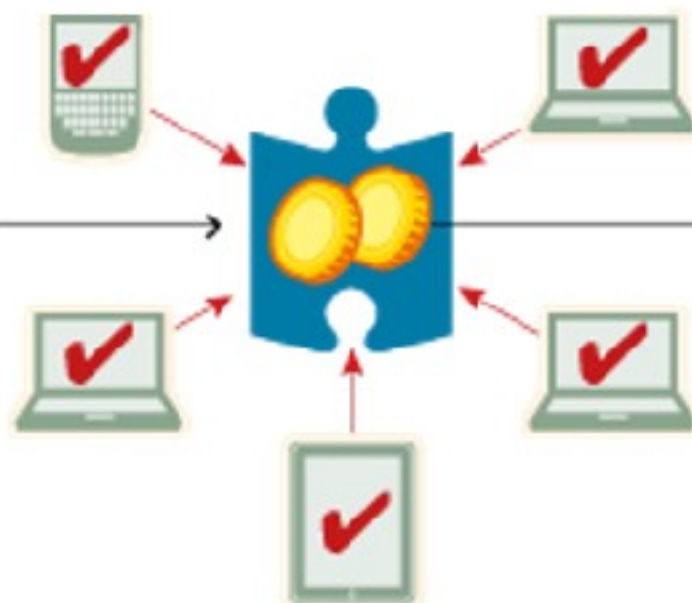
区块链如何工作

1 A想要发送钱给B

2 这笔交易在网络上以一个"区块"作为代表

3 该区块广播给网络里的所有参与者

4 参与者同意交易有效

5 该区块然后被添加到链上这条链提供永久和透明的交易记录

6 资金从A转移到B

FT

如何查詢比特幣公開帳本的資訊？

透過三個不同的全節點來查相同的帳本內容

- 假設我們想查歷史上第100000個區塊的內容

- 我們試著用瀏覽器透過網路去查詢以下三個全節點：

  1. https://blockchain.info

  2. https://blockexplorer.com

  3. http://192.192.140.25

- 從以上三個網站，輸入100000按下Enter去查詢內容

http://blockchain.info

https://blockexplorer.com

安全 https://blockexplorer.com ☆ IP

Bitcoin   Blocks   Status   *Search for block, transaction or address*   ✔ · Conn 68 · Height 472289   Scan   BTC ▾

Latest Blocks

Height	Age	Transactions	Mined by	Size
472289	14 minutes ago	2211		999094
472288	38 minutes ago	2590		998264
472287	an hour ago	2413		998234
472286	an hour ago	2087	AntMiner	998201
472285	2 hours ago	2427		998244

See all blocks

Latest Transactions

Hash	Value Out
2b4bdd3a3af59600bdc0125b182beb397d54a8292949...	0.23623983 BTC
bde29e779b77b9c1922fe449c32871d08b29476b7986...	2.75359982 BTC
1a45fa7dd46bc97cda0b4ce133bc9a7e6a9f4abf5e114b..	0.01617228 BTC
bf2da7b0771ecd5746ca2b71269e9cc2fbe840d5aac9e...	0.254341 BTC
1086573a7194e92aefb89ceb3273b6422904f2b918ccb...	0.00557887 BTC
be29dc4f308bc8104dcde02359929cf72e9a1727e2271...	0.4297238 BTC

About Block Explorer

Bitcoin Block Explorer is an open source web tool that allows you to view information about blocks, addresses, and transactions on the Bitcoin blockchain. The source code is on GitHub.

If you are new to Bitcoin, check out We Use Coins and Bitcoin.org.

Public Bitcoin API: Machine readable stats & blockchain info can be accessed directly through the REST and Websockets APIs.

Testnet is Bitcoin's sandbox. Block Explorer supports viewing both the testnet and mainnet blockchains.

Other projects: BitKey - The Bitcoin swiss army knife

Thanks to Private Internet Access for hosting the site. They provide a VPN Service that accepts Bitcoin.

Powered by

bitcore   A   levelDB   node

開始拿同一個區塊去不同的網站上去查詢

Bitcoin 100000

Short Link: http://192.192.140.25/b/C2G1437Bp

Hash: 000000000003ba27aa200b1cecaac478d2b00432346c3f1f3986da1afd33e506
Previous Block: 000000000002d01c1fccc21636b607dfd930d31d01c3a62104612a1719011250
Next Block: 000000000000080b66c911bd5ba14a74260057311eaeb1982802f7010f1a9f090
Height: 100000
Version: 1
Transaction Merkle Root: f3e94742aca4b5ef35488dc37c06c3282295ffec960994b2c0d5ac2a25a95766
Time: 1293623863 (2010-12-29 19:57:43)
Difficulty: 14 484.383 (Bits: 1b04864c)
Cumulative Difficulty: 105 171 839.321
Nonce: 274148111
Transactions: 4
Value out: 103.01
Transaction Fees: 0
Average Coin Age: 248.914 days
Coin-days Destroyed: 349.79967997
Cumulative Coin-days Destroyed: 16.7896%

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
8c14f0db3d...	0	0.135	Generation: 50 + 0 total fees	1HWqMzw1jfpXb3xyuUZ4uWXY4tgL2cW47J: 50
fff2525b89...	0	0.259	1BNwxHGaFbeUBitpjy2AsKpJ29Ybxntqvb: 50	1JqDybm2nWTENrHvMyafbSXXtTk5Uv5QAn: 5.56 1EYTGtG4LnFfiMvjJdsU7GMGCQvsRSjYhx: 44.44
6359f08681...	0	0.257	15vScfMHNrXN4QvWe54q5hwfVoYwG79CS1: 3	1H8ANdafjpqYntniT3Ddxh4xPBMCSz33pj: 0.01 1Am9UTGfdnxabvcywYG2hvzr6qK8T3cUZT: 2.99
e9a66845e0...	0	0.225	1JxDJCyWNakZ5kECKdCU9Zka6mh34mZ7B2: 0.01	16FuTPaeRSPVxxCnwQmdyx2PQWxX6HWzhQ: 0.01

blockchain.info 上查詢到第100000個區塊內的資訊

Block #100000

Summary

Number Of Transactions	4
Output Total	103.01 BTC
Estimated Transaction Volume	5.58 BTC
Transaction Fees	0 BTC
Height	100000 (Main Chain)
Timestamp	2010-12-29 11:57:43
Received Time	2010-12-29 11:57:43
Relayed By	Unknown
Difficulty	14,484.16
Bits	453281356
Size	0.957 KB
Version	1
Nonce	274148111
Block Reward	50 BTC

Hashes

Hash	000000000003ba27aa200b1cecaad478d2b00432346c3f1f3986da1afd33e506
Previous Block	000000000002d01c1fccc21636b607dfd930d31c01c3a621046f2a1719011250
Next Block(s)	00000000000080b66c911bd5ba14a74260057311eaeb1982802f7010f1a9f090
Merkle Root	f3e94742aca4b5ef8548dc37c06c3282295ffec960994b2c0d5ac2a25a95766

blockchain.info 上查詢到第100000個區塊內的資訊

Transactions

8c14f0db3df150123e6f3dbbf30f8b955a3249b62ac1d1ff16284sefa3d06d87	(Size: 135 bytes) 2010-12-29 11:57:43
No Inputs (Newly Generated Coins) ➡	1HWqMzw1jfpXb3xyuUZ4uWXY4tqL2cW47J - (Spent) 50 BTC
	50 BTC

fff2525b8931402dd09222c50775608f75787bc2b87e56995a7bdd30f79702c4	(Fee: 0 BTC - Size: 259 bytes) 2010-12-29 11:57:43
1BNwxHGaFbeUBitpjy2AsKpJ29Ybxntqvb (50 BTC - Output) ➡	1JqDybm2nWTENrHvMyafbSXXtTk5Uv5QAn - (Spent) 5.56 BTC
	1EYTGIG4LnFfiMvjJdsU7GMGCQvsRSjYhx - (Spent) 44.44 BTC
	50 BTC

6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4	(Fee: 0 BTC - Size: 257 bytes) 2010-12-29 11:57:43
15vScfMHNrXN4QvWe54q5hwfVoYwG79CS1 (3 BTC - Output) ➡	1H8ANdafjpqYntniT3Ddxh4xPBMCSz33pj - (Spent) 0.01 BTC
	1Am9UTGfdnxabvcywYG2hvzr6qK3T3oUZT - (Spent) 2.99 BTC
	3 BTC

e9a66845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b80c1d	(Fee: 0 BTC - Size: 225 bytes) 2010-12-29 11:57:43
1JxDJCyWNakZ5kECKdCU9Zka6mh34mZ7B2 (0.01 BTC - Output) ➡	16FuTPaeRSPVxxCnwQmdyx2PQWxX6HWzhQ - (Spent) 0.01 BTC
	0.01 BTC

在blockexplorer.com 上查詢到第100000個區塊內的資訊

在blockexplorer.com 上查詢到第100000個區塊內的資訊

https://blockexplorer.com/block/000000000003ba27aa200b1cecaad478d2b00432346c3f1f3986da1afd33e5O6

Bitcoin

Blocks   Status   *Search for block, transaction or address*   ✔ · Conn 68 · Height 472289   Scan   BTC ▾

Block #100000

BlockHash 000000000003ba27aa200b1cecaad478d2b00432346c3F1F3986da1afd33e506

Summary

Number Of Transactions	4	Difficulty	14484.16236122
Height	100000 (Mainchain)	Bits	1b04864c
Block Reward	50 BTC	Size (bytes)	957
Timestamp	Dec 29, 2010 7:57:43 PM	Version	1
Mined by		Nonce	274148111
Merkle Root	f3e94742aca4b5ef85488dc37c06c3...	Next Block	100001
Previous Block	99999		

在blockexplorer.com 上查詢到第10000個區塊內的資訊

從以上查詢結果，發現什麼？

在不同節點上，查到的內容都一樣
這就是區塊鏈的特性，分散式帳本技術的
特點就是全網帳本都是一樣的，
達到不可否認性，不可篡改性