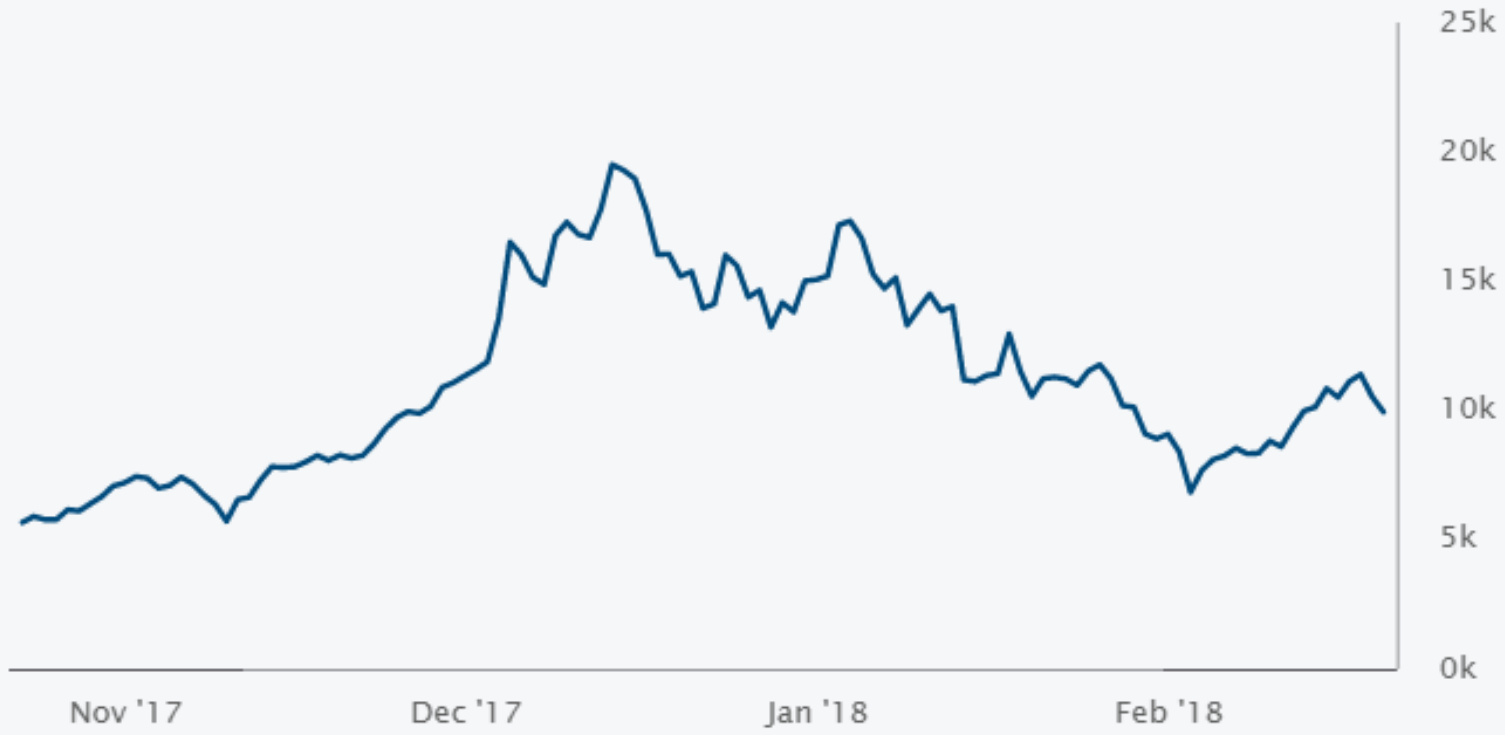
比特幣的原理 - 區塊鏈的應用

交大資訊工程系 陳榮傑

https://blockchain.info

1 BTC = $10,098.52

Interactive Chart →



Outline

1. Birth of Bitcoin 比特幣誕生
2. Mining 挖礦
3. Hash 雜湊函數
4. Blockchain 區塊鏈
5. Transaction 交易
6. Consensus 共識
7. PKC 公鑰密碼

Birth of Bitcoin

比特幣誕生

Birth of Bitcoin

- Described by Satoshi Nakamoto (中本聰) in 2008
- Introduced as open-source software on the evening of January 3, 2009

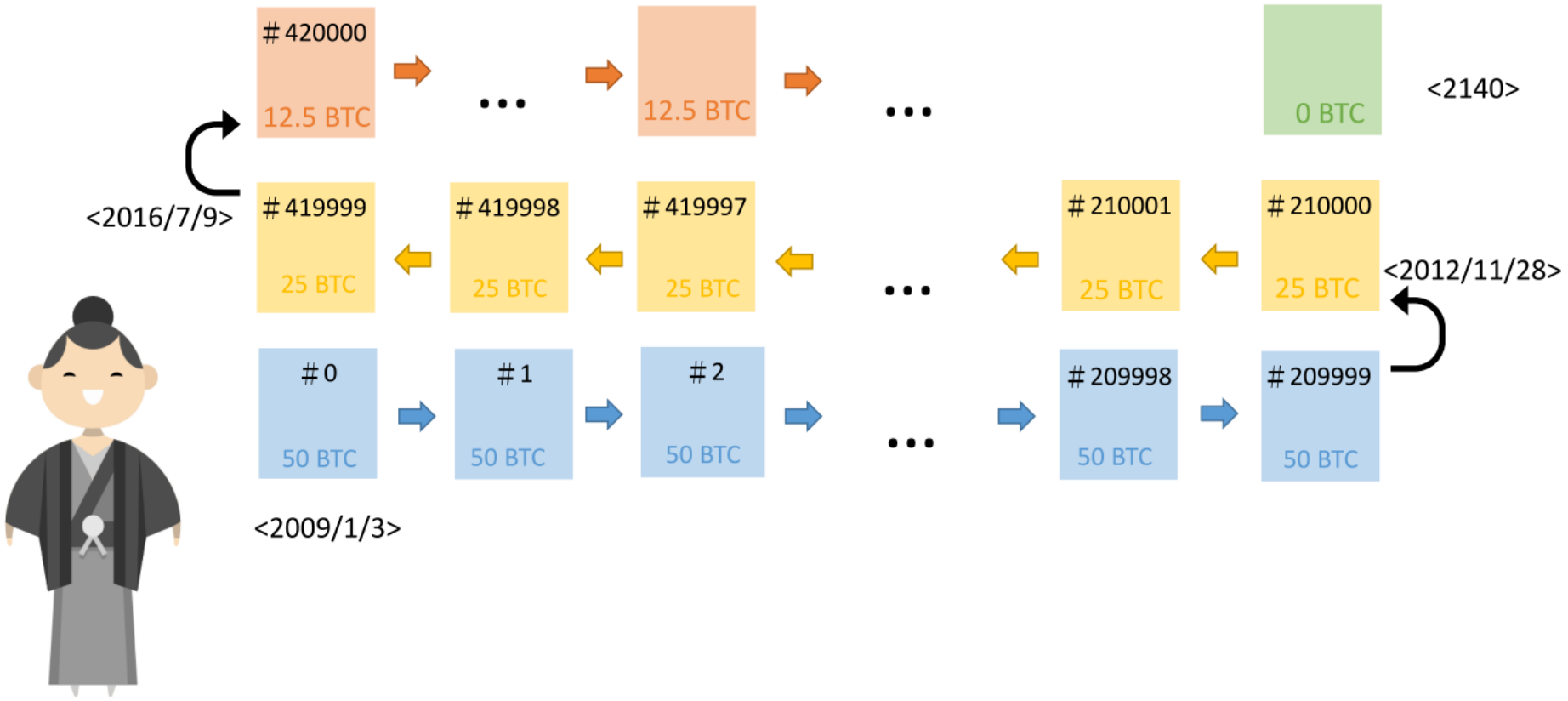
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

http://bitcoin.org/bitcoin.pdf 中本聰

比特幣的區塊鏈當作公用帳本(public ledger)



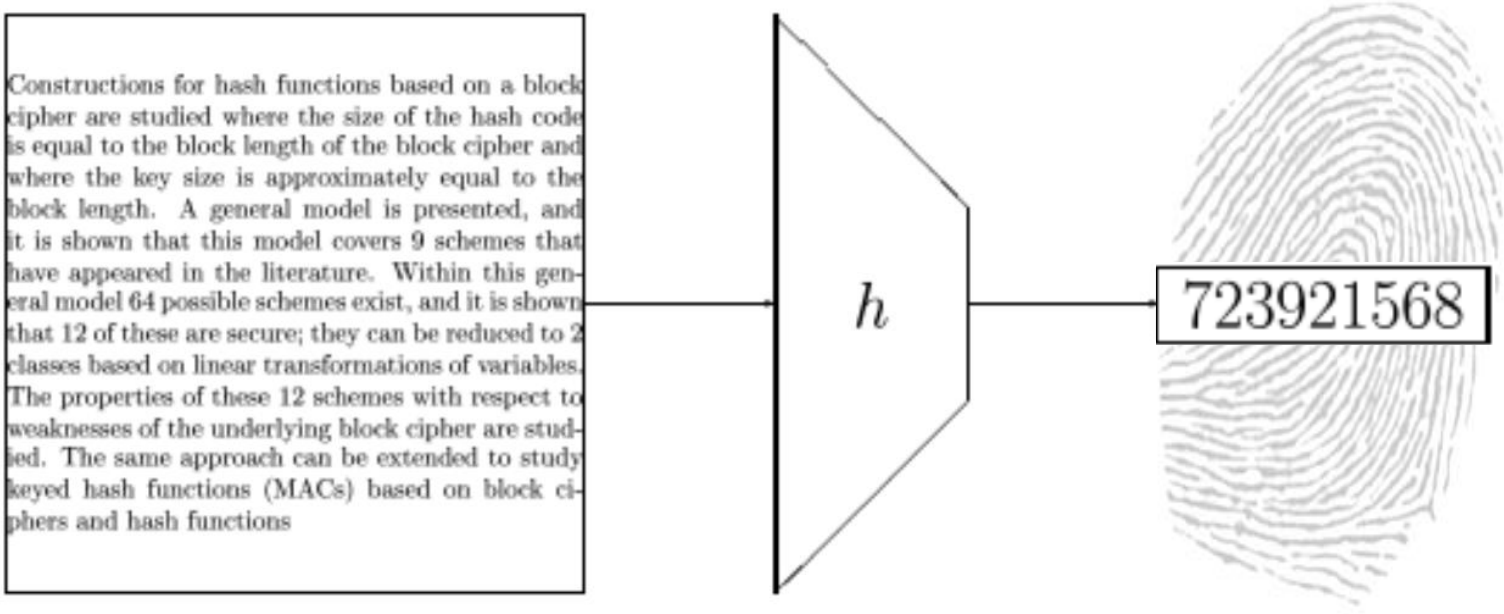
Block#0 的挖礦困難度(difficulty)為1 即hash後前面32個bits為0, 以後每2016個blocks(約兩週)調整一次, 使約每十分鐘產生一block

32

000…000 | xxx……xxxxxxxxxx

Hash Function 雜湊函數

- An efficient function mapping binary strings of **arbitrary length** to binary strings of **fixed length**, called the **hash-value** or **hash-code** (fingerprint, checksum)



SHA: Secure Hash Algorithm

- The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Bitwise operations	Security (bits)
SHA-1 **FIPS 180**		160	160	512	80	and, or, add, xor, rot	Theoretical attack (2^{61})
SHA-2 **FIPS 180**	SHA-224	224	256 (8×32)	512	64	and, or, xor, shr, rot, add	112
	SHA-256 Bitcoin	256					128
	SHA-384	384	512 (8×64)	1024	80	and, or, xor, shr, rot, add	192
	SHA-512	512					256
	SHA-512/224	224					112
	SHA-512/256	256					128
SHA-3 **FIPS 202**	SHA3-224	224	1600 ($5 \times 5 \times 64$)	1152	24	and, xor, rot, not	112
	SHA3-256 Ethereum (Keccak 256)	256		1088			128
	SHA3-384	384		832			192
	SHA3-512	512		576			256

https://en.wikipedia.org/wiki/Secure_Hash_Algorithm

Merkle-Damgård Construction for SHA-1 / SHA-2

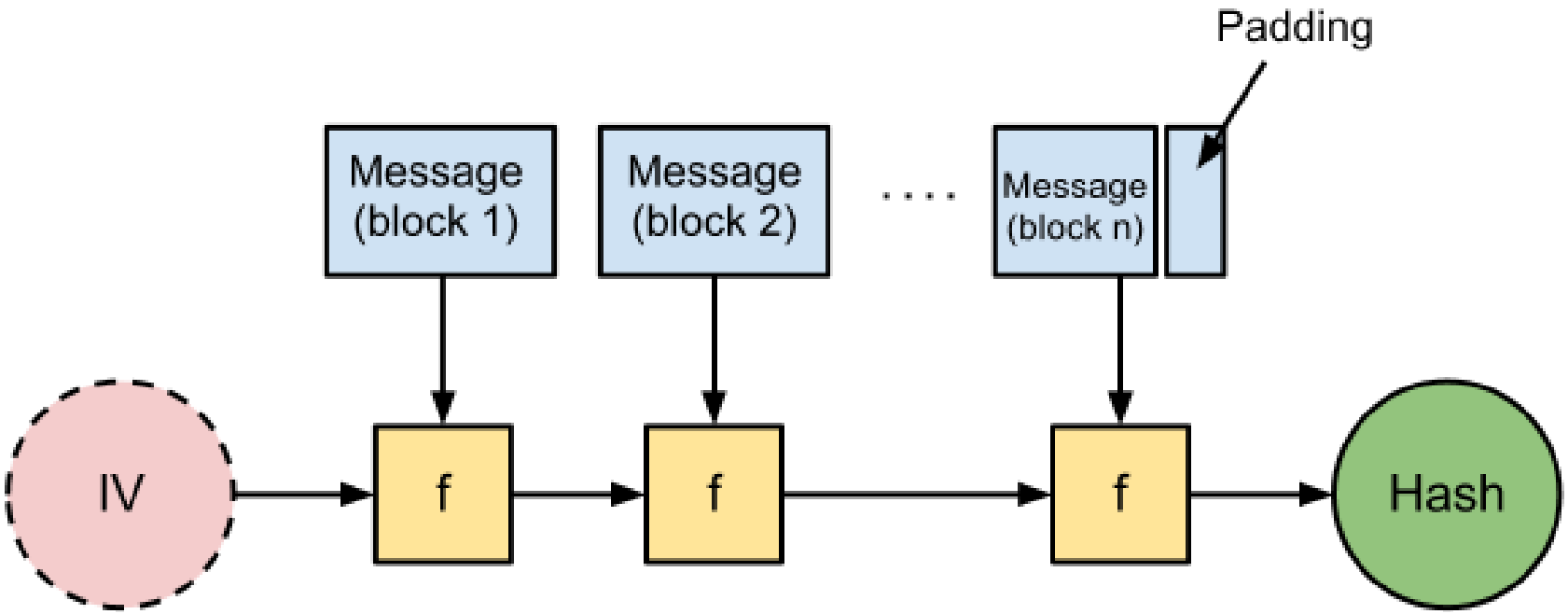


Image Courtesy http://joncave.co.uk/2012/08/i-captured-the-flag

SHA-256

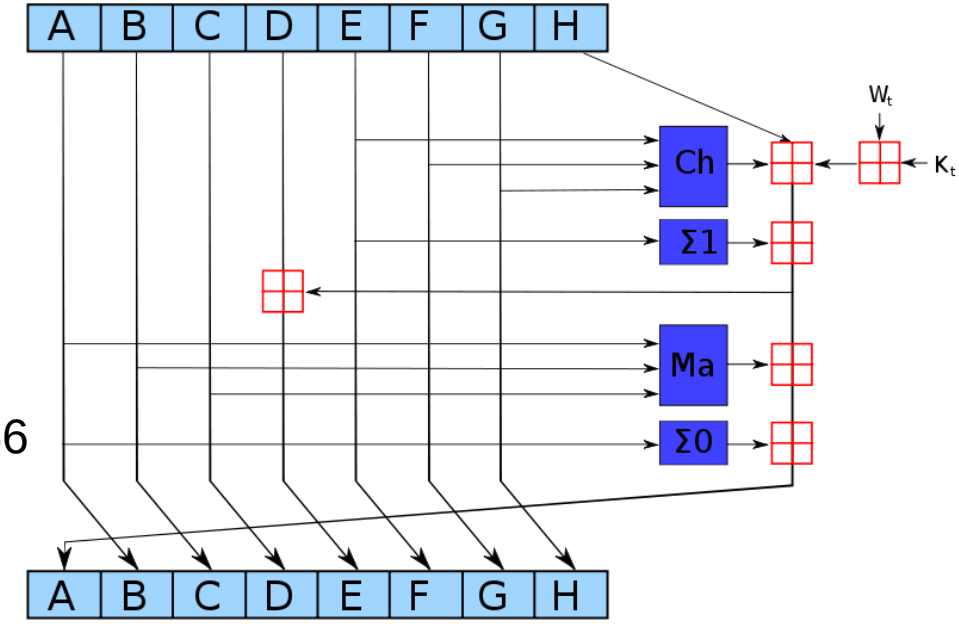
- One iteration in a SHA-2 family compression function
  - The blue components perform the following operations

$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$

$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$

$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$



- The bitwise rotation uses different constants for SHA-512
- The given numbers are for SHA-256
  - ⊞ is addition modulo 2^{32}

http://en.wikipedia.org/wiki/SHA-2

Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

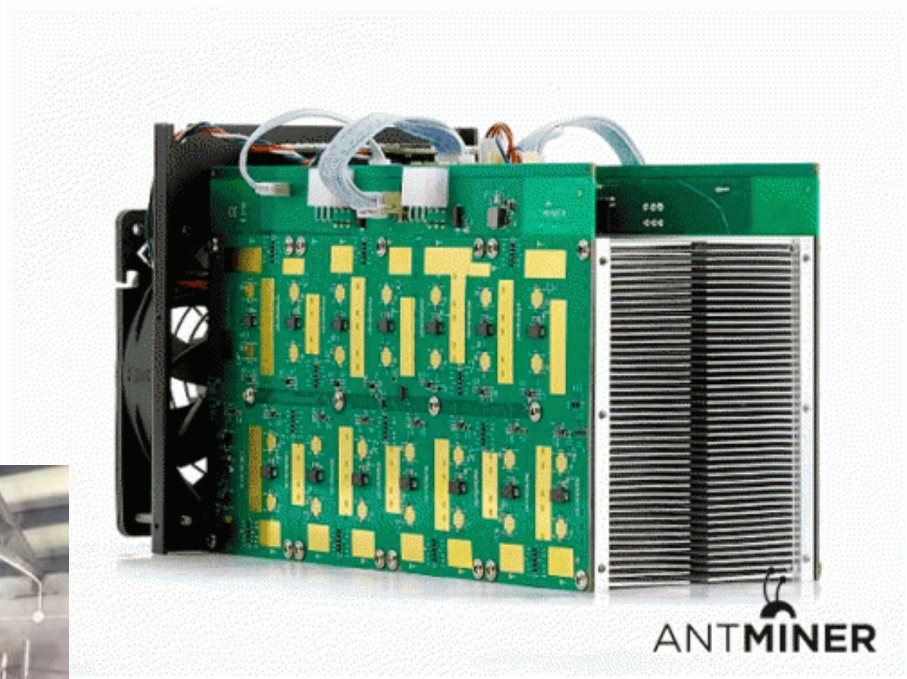
Transactions

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b — **2009-01-03 18:15:05**

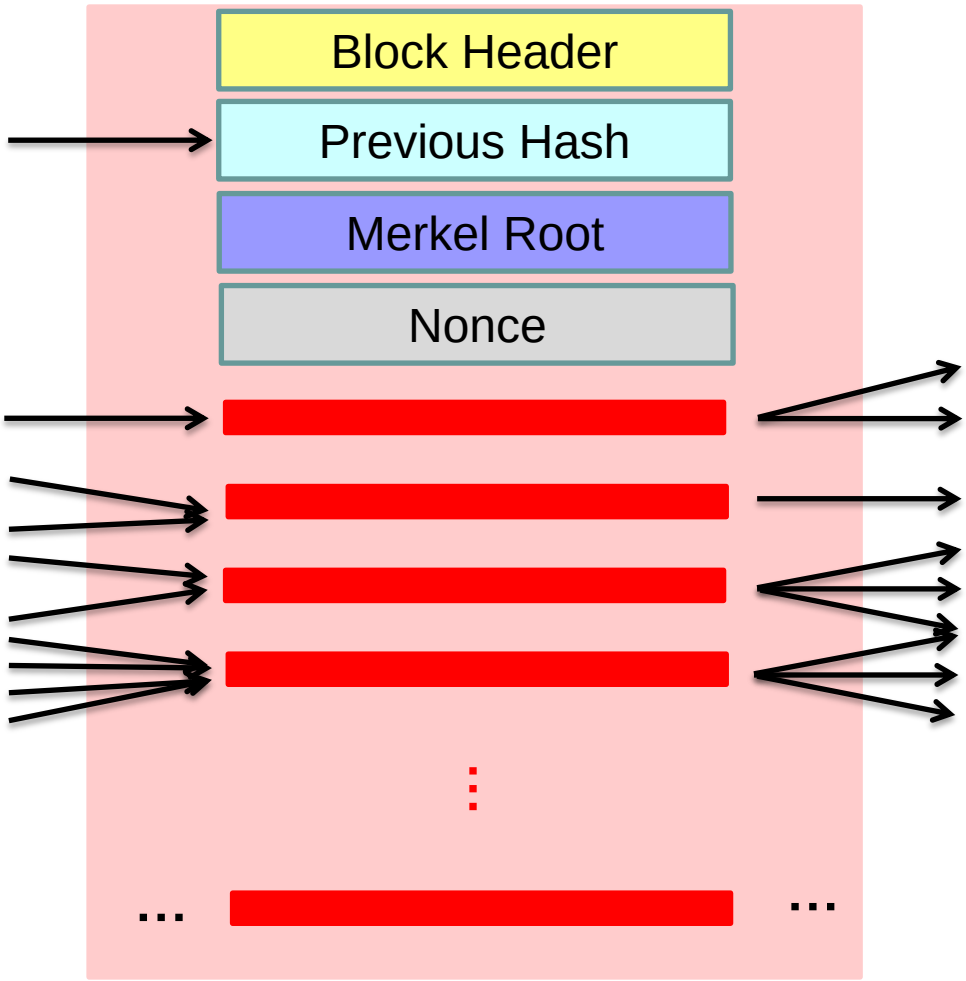
No Inputs (Newly Generated Coins) → 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa 50 BTC

50 BTC

比特幣礦機



Block 區塊



http://bitcoin.org/bitcoin.pdf 中本聰

Block #534200

Summary	
Number Of Transactions	169
Output Total	624.18996341 BTC
Estimated Transaction Volume	7.13403894 BTC
Transaction Fees	0.01235101 BTC
Height	534200 (Main Chain)
Timestamp	2018-07-29 03:59:19
Received Time	2018-07-29 03:59:19
Relayed By	SlushPool
Difficulty	5,178,671,069,072.25
Bits	389437975
Size	67.031 kB
Weight	225.103 kWU
Version	0x20000000
Nonce	1962295696
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000035f53ec665dfcb65b6d946215d8dee6421d19f43373436
Previous Block	0000000000000000014cbbac6073eaaba44a63b6d78754a2bee4f9a065aa399
Next Block(s)	
Merkle Root	01296f783cf96ed0b71f5f5ca241ae6cc55b0842dad4e0a7d3cad43cb43a6af9

Transactions

ff50337f00af30b0a6c5c572a91f15b03a2bbab03af6fde094d031e55d6a23e5			**2018-07-29 03:59:19**
No Inputs (Newly Generated Coins)	→	1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE Unable to decode output address Unable to decode output address	12.51235101 BTC 0 BTC 0 BTC
			12.51235101 BTC
18163d2c86d300881c4306c78436e8d9c53ba1ff40eb7ffd899a067621238354			**2018-07-29 03:57:17**
1159SzdZyyqBwG1TG9KRJDwfaqZt4xdM3L 1Eb8buAUHvNtHA5XJu9CF6VAhrrGDnyXom 1N6EPcV47BRG8HmNTvPeyJ7sV3mUWqitsK	→	1BuV7TDJ7ysr1BBFvTVf2AnD9rHYVDvuRv 36EQt6kESVT9X9oXMTj2PEyzxmm4n6owKy	0.00840876 BTC 0.02142695 BTC
			0.02983571 BTC
795a3f5cc0ee990813c3dafde94404a06a5c9507bc80b650d09c238ffc22f7f0			**2018-07-29 03:58:23**
18bY4zkJfErgmds7Wd1Q2d8uhPWqWyJDhE 1ABkcFYkXtZ3uLYJ4dxkG96P3T5ffAdpMa	→	1FzzXCEWm6sxxEDeebnFoTCTuSNGDMbfcU 34eFgSe3in1h4WsyftY4reDMkQaqaVrb14	0.24257527 BTC 0.60312843 BTC
			0.8457037 BTC

比特幣發明人果然是他！澳洲企業家Craig Steven Wright終於坦言證實

中本聰一直是個謎樣的人物，2008年發表比特幣（Bitcoin）論文後，不僅創造出全新的金融模式，也發明了如今讓全球金融科技都瘋狂的區塊鏈技術

文/ 王宏仁 | 2016-05-02 發表

http://www.ithome.com.tw/news/105677

比特幣發明者是誰？Wright是中本聰還是騙子？

儘管部份人士相信澳洲企業家Craig Steven Wright就是比特幣發明者，但仍有資安專家、開發者質疑Wright是中本聰的真實性，認為Wright所提出的證據薄弱，要求提出的更有力的證據，例如展示第0區塊的相關私鑰才能證明他真的是中本聰。

文/ 陳曉莉 | 2016-05-03 發表

http://www.ithome.com.tw/news/105687

承認是中本聰後質疑聲四起，Wright不想再證明了

Wright向媒體承認自己是中本聰後謠言四起，Wright說，他的能力與性格都受到攻擊，當這些指控被駁回時，新的指控又出現了，他知道他承受不起...向相信他的人道歉。

文/ 陳曉莉 | 2016-05-06 發表

http://www.ithome.com.tw/news/105769

Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000 BTC

May 22, 2014 at 19:16 by Grace Caffyn

Today, bitcoiners the world over will celebrate the anniversary of the most expensive pizzas in history.

Bought on 22nd May 2010 by Laszlo Hanyecz, the programmer paid a fellow Bitcoin Talk forum user 10,000 BTC for two Papa John's pizzas. Back then – when the technology was just over a year old – that equated to roughly $25, but is $5.12m by today's exchange rate.

http://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc

貨幣發行與交易確認

- 比特幣透過挖礦(mining)發行貨幣。每一區塊挖礦成功礦工得一筆酬金(reward)至2140共發行21,000,000 BTCs
  - 2009.1.3 ~ 2012.11.28 (Block #0 ~ #209999): 50 bitcoins per block
  - 2012.11.28 ~ 2016.7.9 (#210000 ~ #419999): 25 bitcoins per block
  - …… Done in 2140: All 21,000,000 bitcoins are issued
- 礦工確認新的交易(transactions)並把它們登錄在區塊鏈新產生的區塊內。
- 每筆交易要付手續費(transaction fee)給被確認的礦工。

現在已發行多少比特幣?

- 全部比特幣共 2100萬 BTCs
- 前21萬blocks共發行 1050萬 BTCs 佔 1/2
- 前42萬blocks共發行 3/4
- 前63萬blocks共發行 7/8
- 前51萬blocks(約現在)發行

  3/4 + (9/21)*(1/8)=0.804

  約八成

多少種密碼貨幣?

- 密碼貨幣(Cryptocurrency)

使用密碼學原理來確保交易安全及控制交易單位創造的交易媒介。密碼貨幣是數位貨幣(或稱虛擬貨幣)的一種。比特幣在2009成為第一個去中心化的密碼貨幣，這之後密碼貨幣一詞多指此類設計。自此之後數種類似的密碼貨幣被創造，它們通常被稱作altcoins。2018/5統計共有altcoins一千八百種，Ethereum，Ripple，Litecoin ...

在全家便利商店就可以將現金換成比特幣

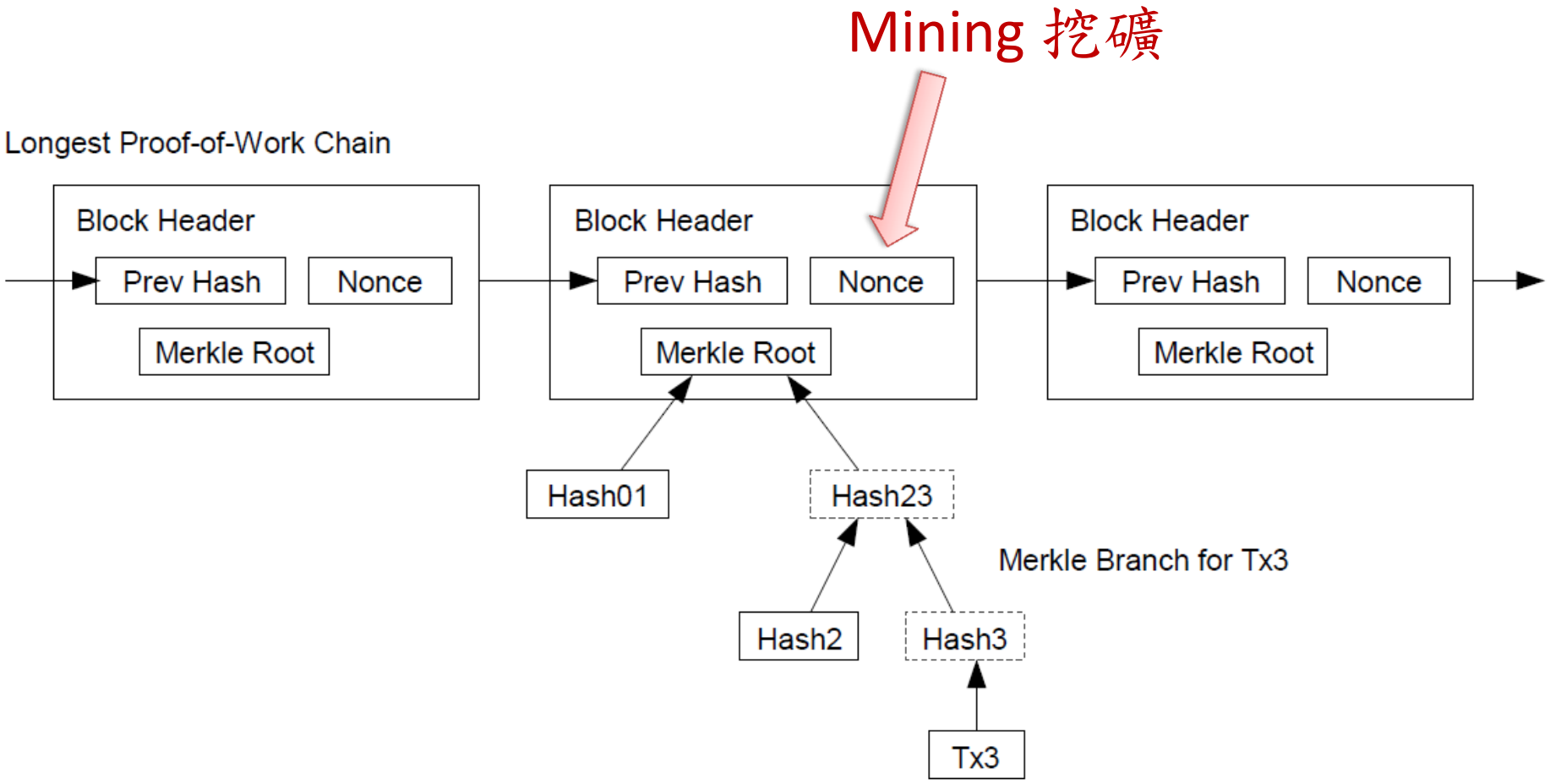
台灣第一家可以用加密貨幣買蛋糕的店 Coin Cake 開幕。

https://www.inside.com.tw/2017/10/18/coin-cake

The Book “Mastering Bitcoin”

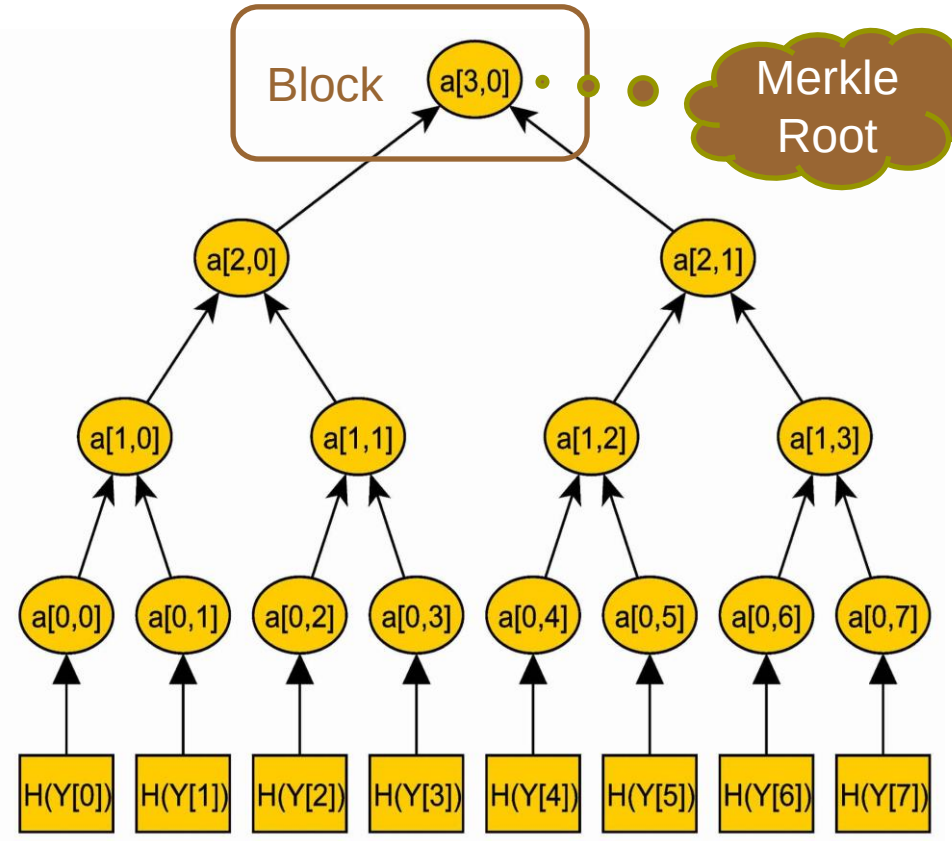
MINING 挖礦

Block Chain

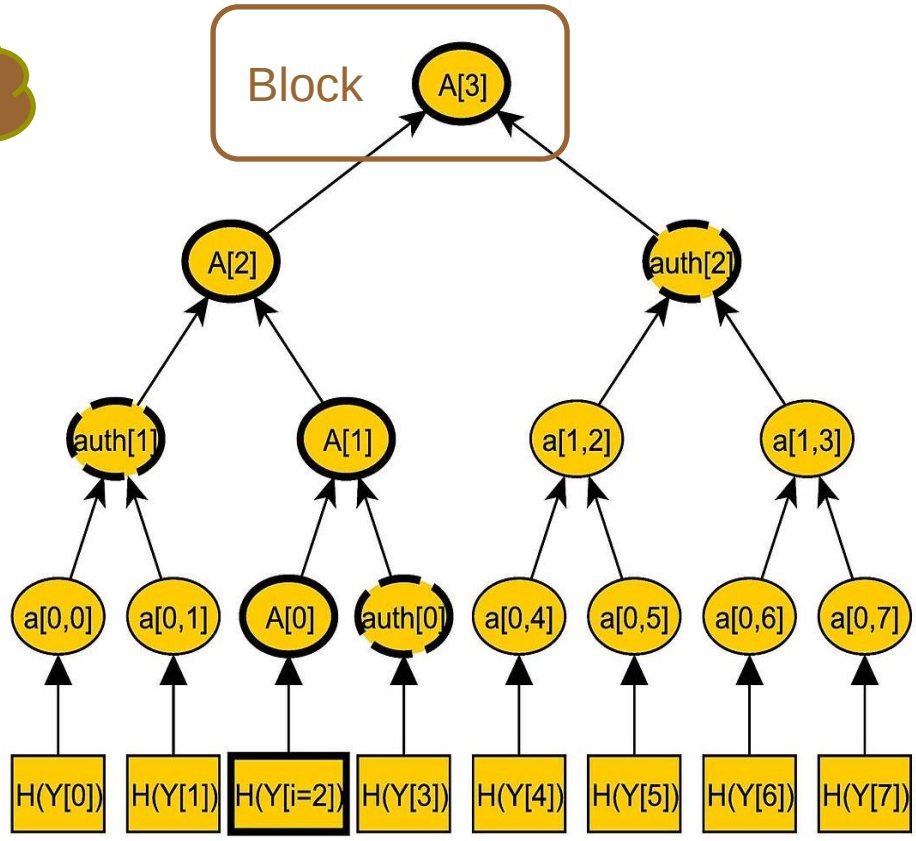


http://bitcoin.org/bitcoin.pdf 中本聰

Merkle Tree / Hash Tree



Merkle Root



http://commons.wikimedia.org/wiki/File:MerkleTree1.jpg

http://commons.wikimedia.org/wiki/File:MerkleTree2.jpg

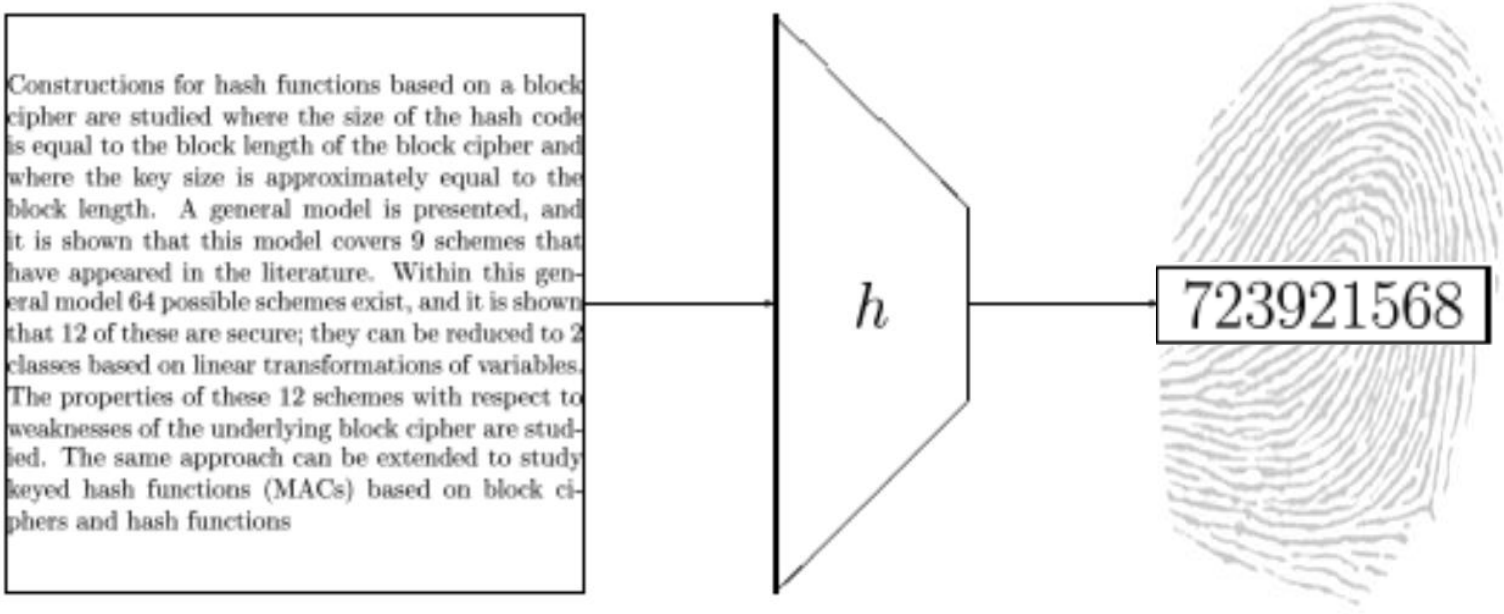
Proof-of-Work 工作量證明

- “The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits.”

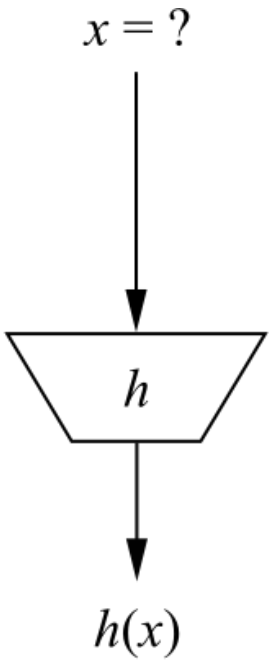
HASH 雜湊函數

Hash Function 雜湊函數

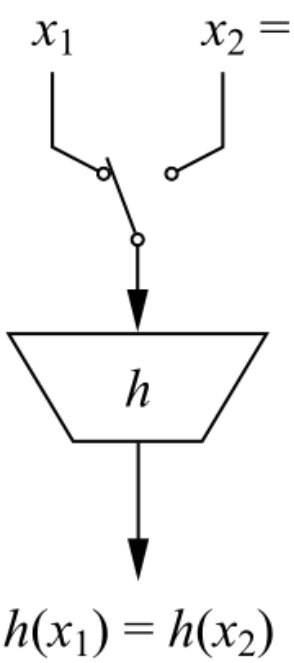
- An efficient function mapping binary strings of **arbitrary length** to binary strings of **fixed length**, called the **hash-value** or **hash-code** (fingerprint, checksum)



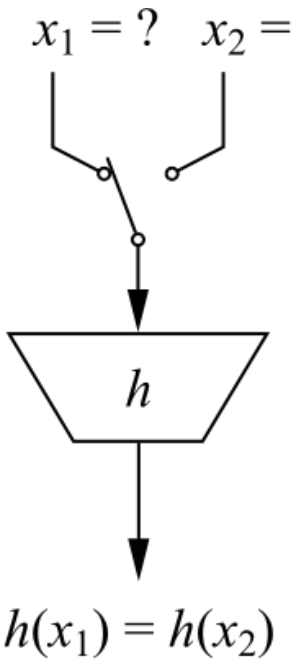
Security Properties



preimage resistance



second preimage resistance



collision resistance

SHA-3 Competition Winner: Keccak

- Designers:
  - Guido Bertoni (Italy) of STMicroelectronics
  - Joan Daemen (Belgium) of STMicroelectronics
  - Gilles Van Assche (Belgium) of STMicroelectronics
  - Michaël Peeters (Belgium) of NXP Semiconductors
- Not very fast in software implementation, but in hardware implementations it is notably faster than all other finalists
- In its largest instance, the state consists of a 5×5 array of 64-bit words, 1600 bits total
  - Reduced versions are defined for smaller power-of-2 word sizes w down to 1 bit (25 bits total state)
  - Smaller state sizes can be used to test cryptanalytic attacks
  - Intermediate state sizes (e.g., from $w = 4$, 100 bits, to $w = 32$, 800 bits) also provide practical, lightweight, alternatives

Applications

- Verifying the Integrity of Files or Messages
- Password Verification
- File or Data Identifier
- Pseudorandom Generation & Key Derivation
- Proof-of-Work (POW)

https://en.wikipedia.org/wiki/Cryptographic_hash_function

Hash Function Usages

- Double SHA256, i.e., SHA256(SHA256())
  - Merkle Tree
  - Block Hash
  - Transaction ID
- RIPEMD160(SHA256())
  - Bitcoin Address

Bitcoin Address

- Address = RIPEMD160(SHA256(public key representation))
- Example
  - ECDSA private key = 18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725
  - Public key *P* = 04 50863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B235 22CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6
  - SHA256(*P*) = 600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B408
  - RIPEMD160(SHA256(*P*)) = 010966776006953D5567439E5E39F86A0D273BEE
  - Address (Base58Check encoded): 16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM
  - https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses#How_to_create_Bitcoin_Address
- Base58 is a set of lower and capital letters and numbers without (0, O, l, I), i.e., 0 (number zero), O (capital o), l (lower L), I (capital i)

BLOCKCHAIN 區塊鏈

比特幣交易登錄於區塊鏈的程序

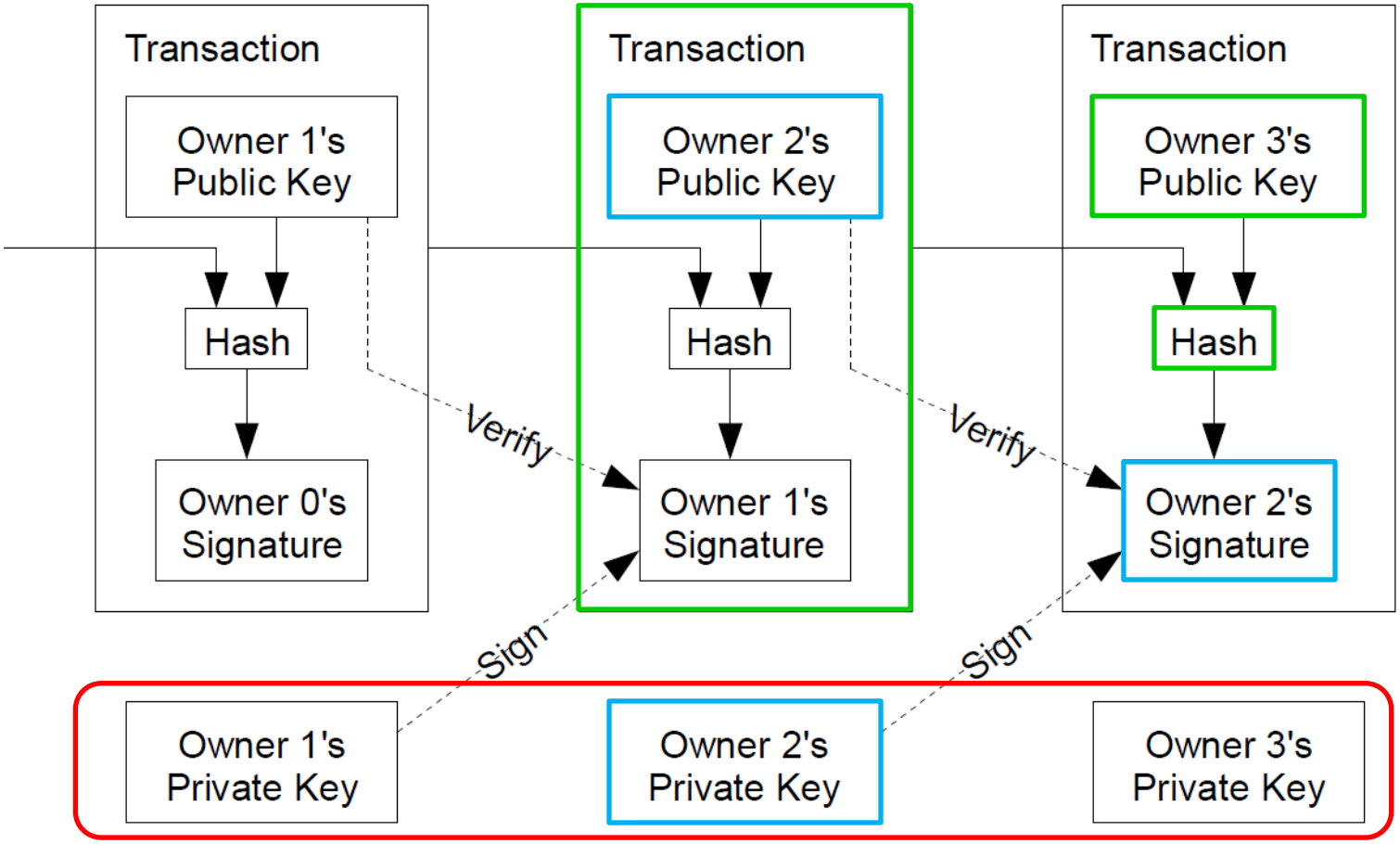
1. 當有一筆新的交易產生, 會通知所有的節點
2. 每個挖礦節點會將新的交易紀錄存到一個區塊中
3. 每個挖礦節點會執行工作量證明
4. 當節點執行完工作量證明後, 會將區塊資訊告知其他節點
5. 若區塊裡的所有交易皆為合法且尚未失效, 節點將接受此區塊
6. 若區塊被驗證為完成工作量證明, 則此區塊內容的hash將被當作下一個區塊的previous hash

區塊鏈 Block Chain

- 區塊鏈技術是 Bitcoin 的基礎，受全世界重視的程度已經超越 Bitcoin 本身
- 一言以蔽之：「以 hash function 串接資料」
  - Hash function – 雜湊函數、赫序函數、哈希函數
- 探討區塊鏈的文獻極多，大部分著墨於應用，鮮少講清楚最根本的 hash function
  - Hash function 是基礎密碼演算法，實務應用非常普遍

TRANSACTIONS 交易

Bitcoin Transactions 交易

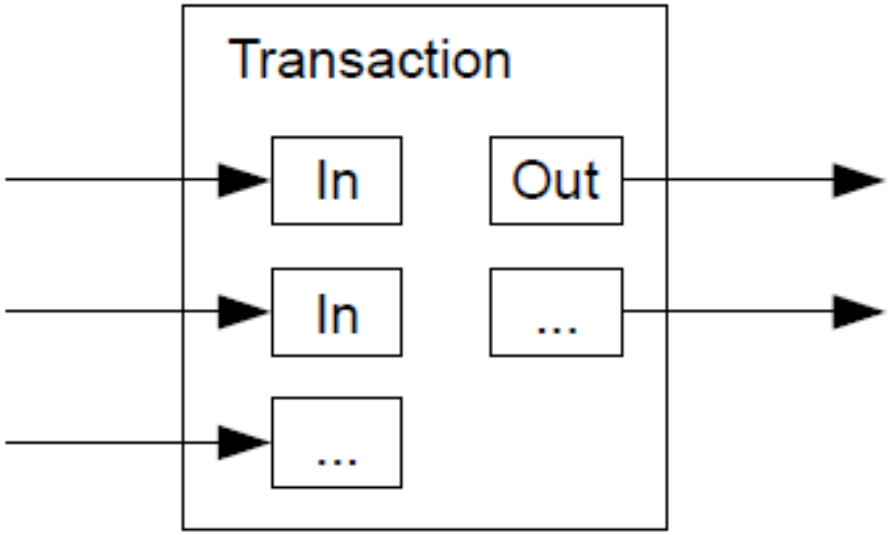


Must be protected very well!!!

http://bitcoin.org/bitcoin.pdf 中本聰

Combining & Splitting Value

- "To allow value to be split and combined, transactions contain multiple inputs and outputs."



http://bitcoin.org/bitcoin.pdf 中本聰

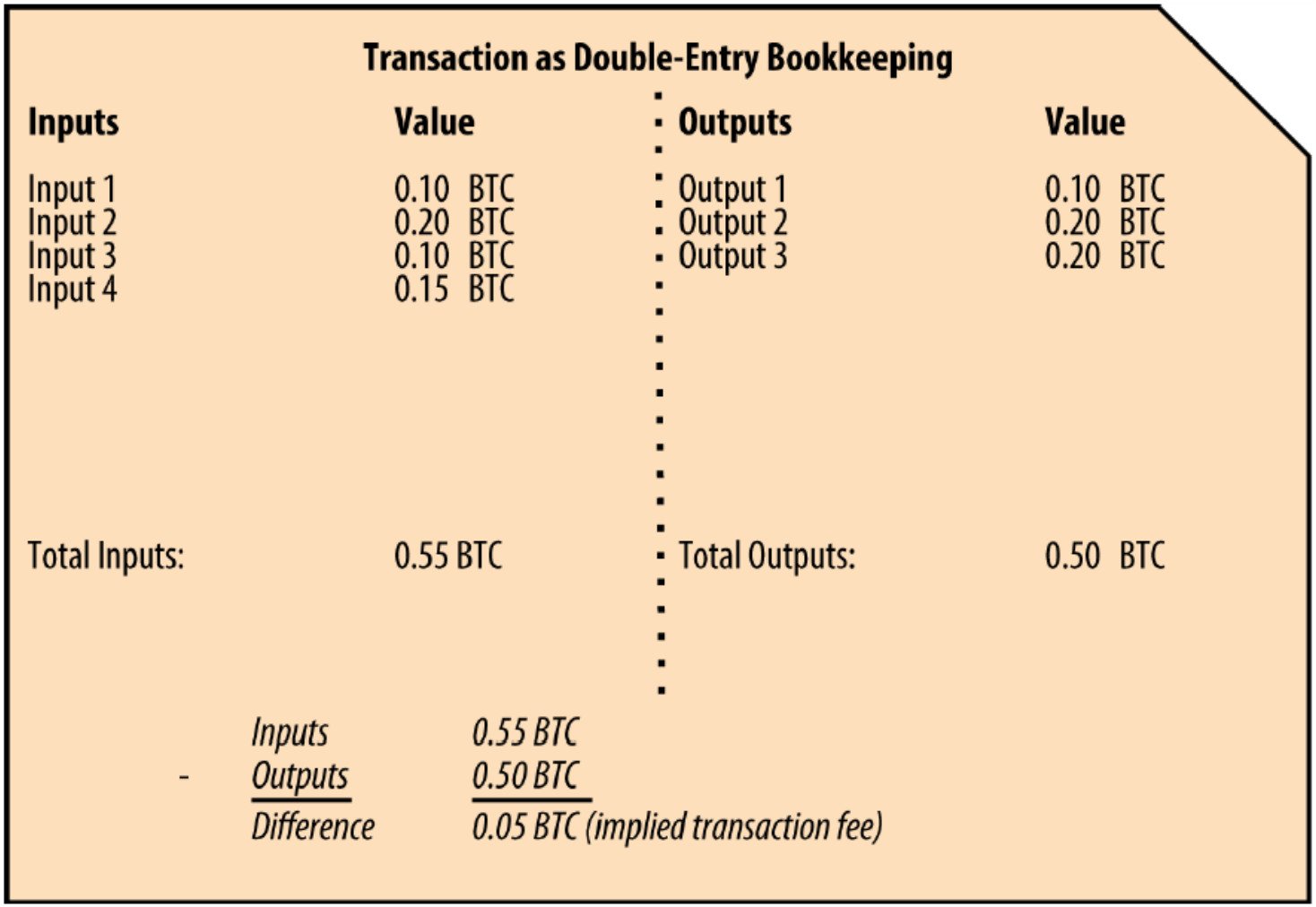


Figure 2-3. Transaction as double-entry bookkeeping

"Mastering Bitcoin" by Andreas M. Antonopoulos

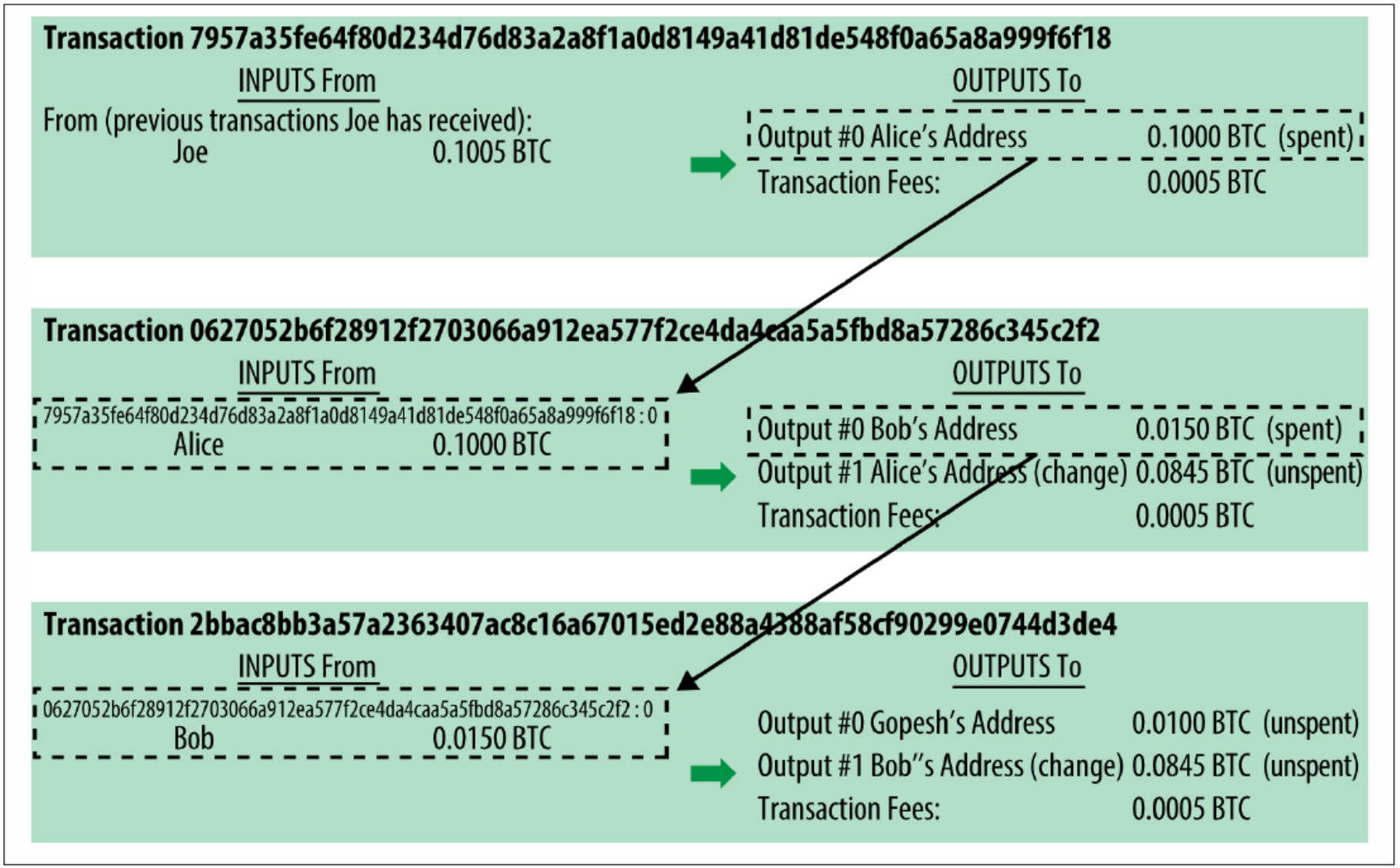


Figure 2-4. A chain of transactions, where the output of one transaction is the input of the next transaction

"Mastering Bitcoin" by Andreas M. Antonopoulos

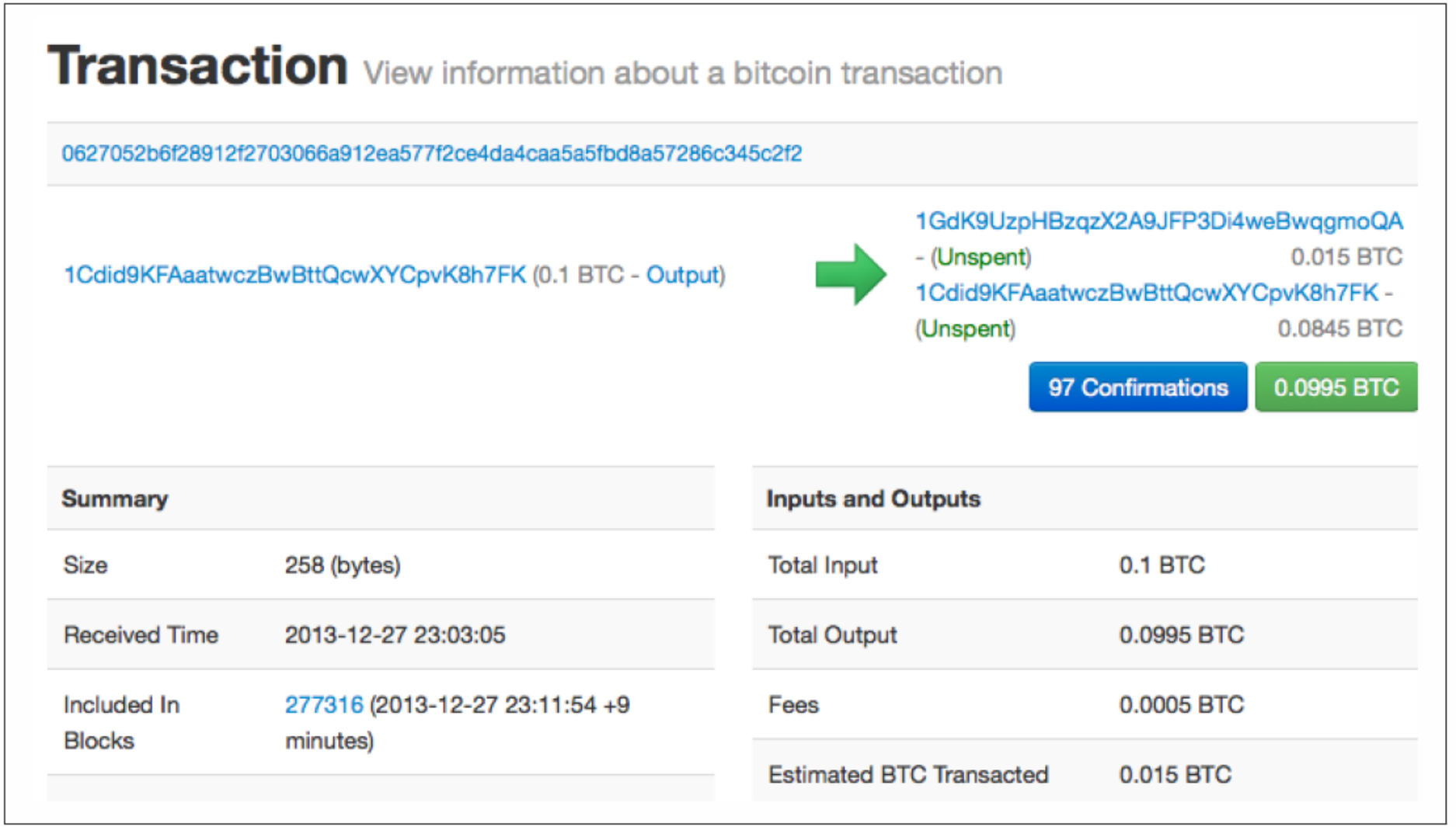


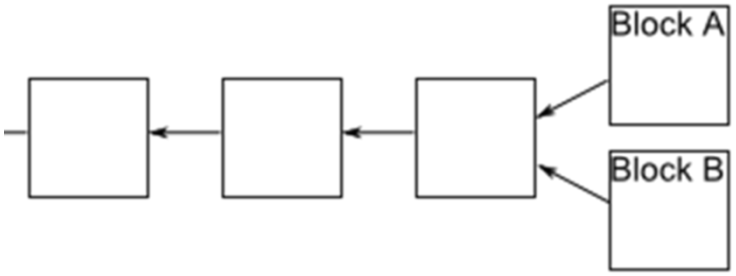
Figure 2-8. Alice's transaction to Bob's Cafe

"Mastering Bitcoin" by Andreas M. Antonopoulos

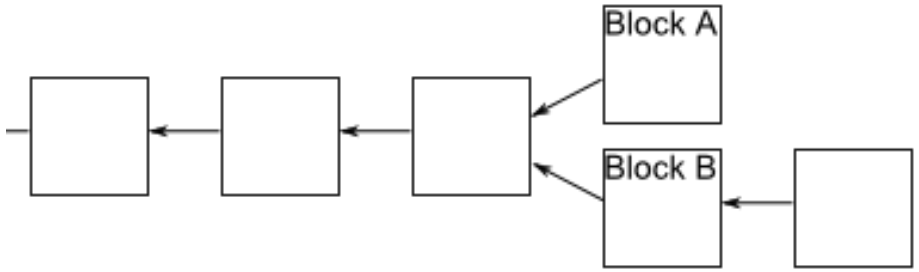
CONSENSUS 共識

Block Forking 區塊分岔

- Occasionally, a fork appears in the block chain, i.e., two miners happen to validate a block of transactions near-simultaneously

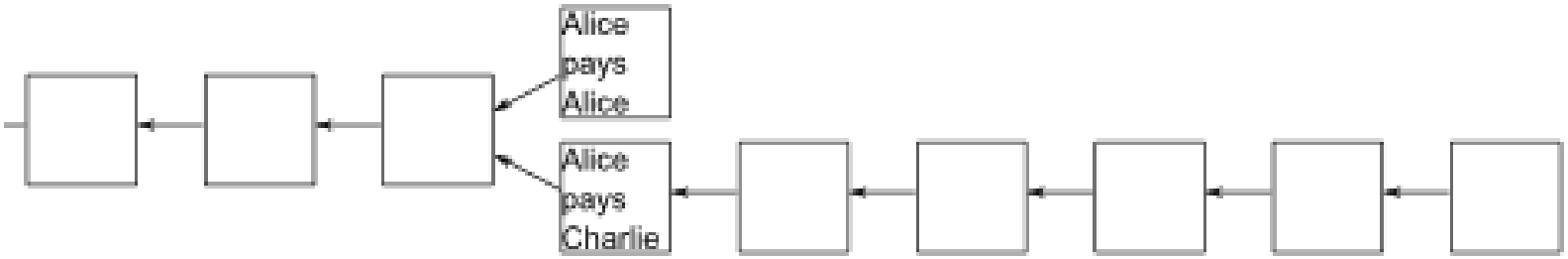


- If a fork occurs, people on the network keep track of both forks
- Miners only work to extend whichever fork is longest in their copy of the block chain



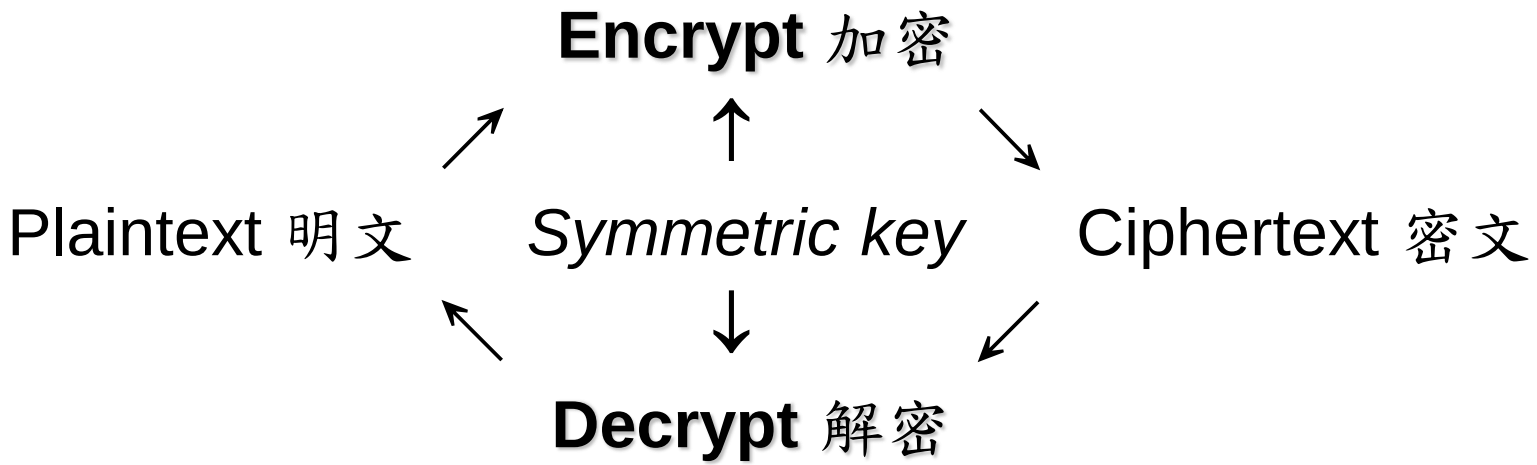
Confirmations

- A transaction is not considered confirmed until
  - It is part of a block in the longest fork
  - At least 5 blocks follow it in the longest fork
  - In this case, we say that the transaction has "6 confirmations"
- 10 minutes per block (in average)
- Payee must wait 60 minutes



PUBLIC KEY CRYPTOGRAPHY (PKC)公鑰密碼

Symmetric Cryptography



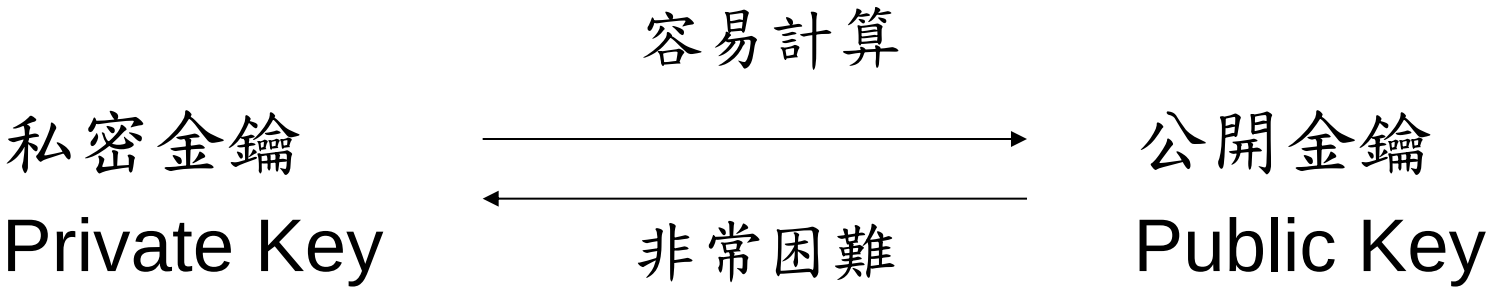
DES (Data Encryption Standard)

AES (Advanced Encryption Standard)

Asymmetric Cryptography

- New Idea: Use the “mailbox” principle
  - Everyone can drop a letter
  - But only the owner has the correct key to open the box
- 1976: first publication of such an algorithm by Whitfield Diffie and Martin Hellman

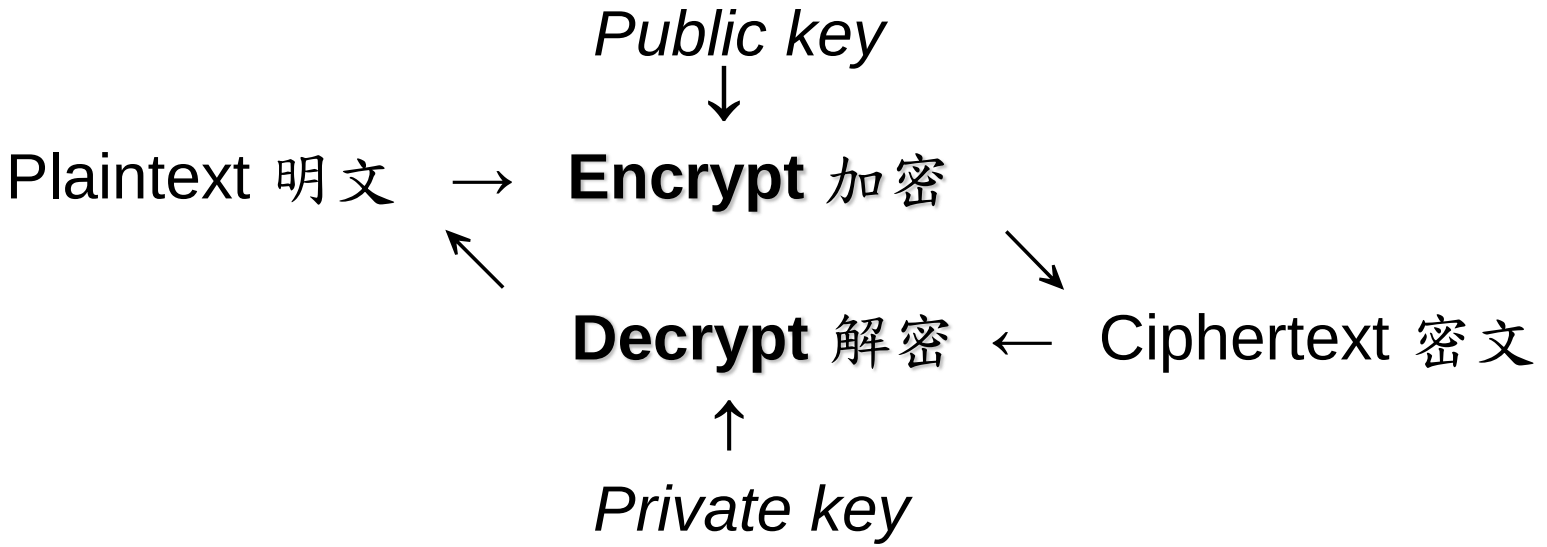
私密金鑰 與 公開金鑰



藉由數學工具達成此目的

Whit Diffie 和 Martin Hellman 於 1976 年提出此觀念

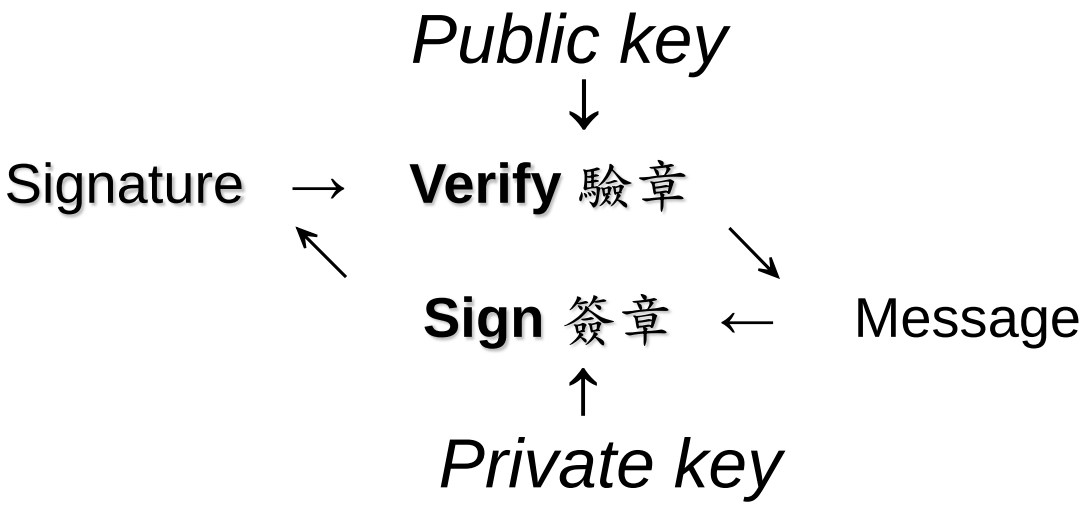
Public Key Cryptosystem 公鑰密碼系統



RSA (Rivest – Shamir – Adleman 1977)

ECC (Elliptic Curve Cryptosystem 橢圓曲線密碼系統)

Digital Signature 數位簽章

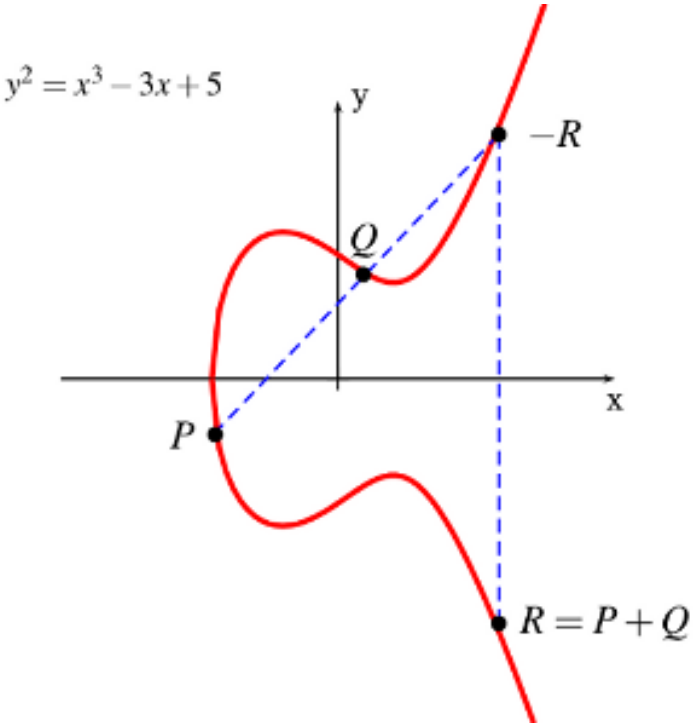


* 資料完整性 (Integrity)
* 身份鑑別性 (Authentication)
* 不可否認性 (Non-Repudiation)

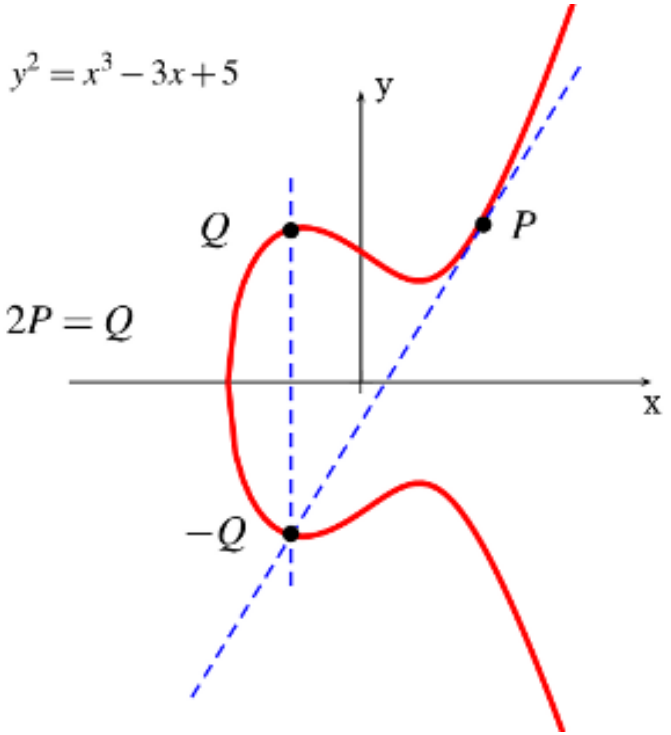
Elliptic Curve

Elliptic Curve 橢圓曲線

- The rich and deep theory of Elliptic Curves has been studied by mathematicians over 150 years
- Elliptic Curve over $\boldsymbol{R}$: $y^2 = x^3 + ax + b$



Point Addition



Point Doubling

Image Courtesy: http://www.embedded.com/design/safety-and-security/4396040/An-Introduction-to-Elliptic-Curve-Cryptography

質數體 (Prime Field) 上的曲線

Addition:

$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$

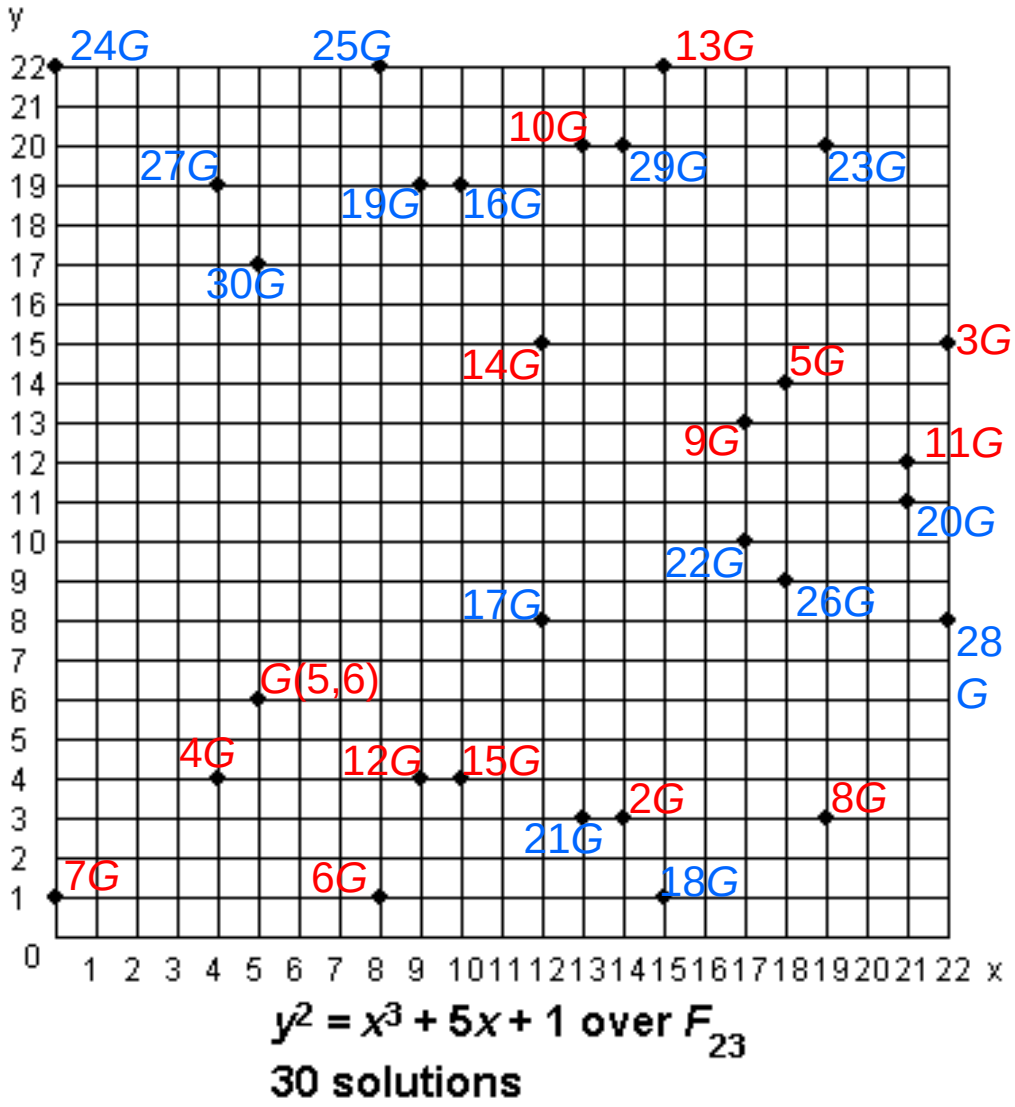
Doubling:

$(x_3, y_3) = [2]\,(x_1, y_1)$

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p & \text{(addition)} \\ \dfrac{3x_1^2 + a}{2y_1} \bmod p & \text{(doubling)} \end{cases}$$

$$x_3 = s^2 - x_1 - x_2 \bmod p$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$



Double and Add

Example: $26P = (11010_2)P = (d_4 d_3 d_2 d_1 d_0)_2\, P$.

Step		
#0	$P = \mathbf{1}_2 P$	inital setting
#1*a*	$P + P = 2P = \mathbf{10}_2 P$	DOUBLE (bit d_3)
#1*b*	$2P + P = 3P = 10^2 P + 1_2 P = \mathbf{11}_2 P$	ADD (bit $d_3 = 1$)
#2*a*	$3P + 3P = 6P = 2(11_2 P) = \mathbf{110}_2 P$	DOUBLE (bit d_2)
#2*b*		no ADD ($d_2 = 0$)
#3*a*	$6P + 6P = 12P = 2(110_2 P) = \mathbf{1100}_2 P$	DOUBLE (bit d_1)
#3*b*	$12P + P = 13P = 1100_2 P + 1_2 P = \mathbf{1101}_2 P$	ADD (bit d_1=1)
#4*a*	$13P + 13P = 26P = 2(1101_2 P) = \mathbf{11010}_2 P$	DOUBLE (bit d_0)
#4*b*		no ADD ($d_0 = 0$)

Bitcoin 和 Ethereum 使用的曲線

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

256-bit prime

The curve E: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

橢圓曲線 secp256k1

https://en.bitcoin.it/wiki/Secp256k1

The base point G in compressed form is:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

and in uncompressed form is:

G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order n of G and the cofactor are:

n = FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

256-bit prime

h = 01

Key Pairs 金鑰對

- The base point *G* is fixed on the given Elliptic Curve
- $P = [m]\,G$
  - Given *m*, it is **easy and fast** to find the point *P*
    - Using “double and add” for scalar multiplication
  - Given *P*, it is **extremely hard** to find the integer *m*
    - Elliptic Curve Discrete Logarithm Problem (橢圓曲線離散對數問題)
  - A randomly generated integer *m* is a **private key**
    - A private key is used to sign Bitcoin transactions with ECDSA
  - The point *P* is the **public key** corresponding to *m*
    - A public key is used by other nodes to verify Bitcoin transactions
    - **A Bitcoin address is the hash value of a public key *P***