橢圓曲線密碼學
與區塊鏈 (上)

陳君明
jmchen@chroot.org
Status of Bitcoin
Bitcoin recognized by Germany as 'private money'

Matt Clinch | @mattclinch81
Monday, 19 Aug 2013 | 10:25 AM ET

Tomohiro Ohsumi | Bloomberg | Getty Images

Virtual currency bitcoin has been recognized by the German Finance Ministry as a "unit of account", meaning it is can be used for tax and trading purposes in the country.

Bitcoin is not classified as e-money or a foreign currency, the Finance Ministry said in a statement, but is rather a financial instrument under German banking rules. It is more akin to "private money" that can be used in "multilateral clearing circles", the Ministry said.

http://www.cnbc.com/id/100971898
歐美作法大不同，比特幣成歐盟認可貨幣，交易視同貨幣流通未來將免稅

比特幣才在上個月正式升格為美國認可的商品，不僅被合法化也納入監管，沒想到昨天歐盟最高法院更宣布，比特幣應視為貨幣的一種，而非商品，因此未來在歐盟各國進行比特幣交易將免收增值稅。

文/ 區騰玉  | 2015-10-23 發表

日本人瘋虛擬貨幣、俄印有望合法化，比特幣登新高

今年 4 月 1 日，日本新版支付服務法（Payment Services Law）生效，承認虛擬貨幣的合法支付地位，包括家電連鎖店 Bic Camera 等均接受比特幣付款。與此同時，俄國當局 4 月表示，最快明年承認比特幣等虛擬貨幣。印度媒體也透露，莫迪政府有意讓虛擬貨幣合法化。

中國原本是比特幣最大炒作國，近來當局嚴格管制比特幣洗錢和市場操縱，交易量大減。但是當地比特幣交易平台提高安全性、嚴防洗錢，可望讓比特幣更為穩定。

Genesis Mining 執行長 Marco Streng 說，諸多微小改變，使得大眾更放心投資比特幣，全球更多國家接受虛擬貨幣，越多正面新聞出現，虛擬貨幣的價格將越高。

https://finance.technews.tw/2017/05/02/bitcoin-ether-popular
## CryptoCurrency Market Capitalizations

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Circulating Supply</th>
<th>Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$140,360,303,975</td>
<td>$8,170.28</td>
<td>$4,222,090,000</td>
<td>17,179,375 BTC</td>
<td>-0.58%</td>
<td><img src="image1" alt="Graph" /></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$46,881,315,962</td>
<td>$464.15</td>
<td>$1,693,350,000</td>
<td>101,005,537 ETH</td>
<td>-0.45%</td>
<td><img src="image2" alt="Graph" /></td>
</tr>
<tr>
<td>3</td>
<td>XRP</td>
<td>$17,801,079,955</td>
<td>$0.452773</td>
<td>$193,020,000</td>
<td>39,315,683,476 XRP*</td>
<td>0.04%</td>
<td><img src="image3" alt="Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>$14,182,148,970</td>
<td>$821.45</td>
<td>$555,628,000</td>
<td>17,264,838 BCH</td>
<td>-0.17%</td>
<td><img src="image4" alt="Graph" /></td>
</tr>
<tr>
<td>5</td>
<td>EOS</td>
<td>$7,336,614,585</td>
<td>$8.19</td>
<td>$627,196,000</td>
<td>896,149,492 EOS*</td>
<td>-1.19%</td>
<td><img src="image5" alt="Graph" /></td>
</tr>
<tr>
<td>6</td>
<td>Stellar</td>
<td>$5,692,274,603</td>
<td>$0.303306</td>
<td>$69,759,100</td>
<td>18,767,431,579 XLM*</td>
<td>-3.27%</td>
<td><img src="image6" alt="Graph" /></td>
</tr>
<tr>
<td>7</td>
<td>Litecoin</td>
<td>$4,842,723,644</td>
<td>$84.03</td>
<td>$281,359,000</td>
<td>57,628,832 LTC</td>
<td>-0.07%</td>
<td><img src="image7" alt="Graph" /></td>
</tr>
<tr>
<td>8</td>
<td>Cardano</td>
<td>$4,157,509,469</td>
<td>$0.160354</td>
<td>$48,248,700</td>
<td>25,927,070,538 ADA*</td>
<td>-1.48%</td>
<td><img src="image8" alt="Graph" /></td>
</tr>
<tr>
<td>9</td>
<td>IOTA</td>
<td>$2,778,332,305</td>
<td>$0.999569</td>
<td>$28,409,200</td>
<td>2,779,530,283 MIOTA*</td>
<td>-2.38%</td>
<td><img src="image9" alt="Graph" /></td>
</tr>
<tr>
<td>20</td>
<td>Zcash</td>
<td>$970,474,156</td>
<td>$217.43</td>
<td>$157,708,000</td>
<td>4,463,469 ZEC</td>
<td>-1.05%</td>
<td><img src="image10" alt="Graph" /></td>
</tr>
</tbody>
</table>
Market Price (USD)

Average USD market price across major bitcoin exchanges.

Source: blockchain.info

https://blockchain.info/charts/market-price?timespan=2years
Birth of Bitcoin
Birth of Bitcoin

- Described by Satoshi Nakamoto (中本聡) 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.
I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

---

In which country do you live?

---

Jacksonville, Florida
zip code 32224
United States
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
UCLA Prof Wants to Nominate Satoshi Nakamoto for Nobel Prize in Economics

"He can write his speech, digitally sign it and send it to me securely."

A professor of finance at the University of California- Los Angeles (UCLA), Bhagwan Chowdhry, wants to nominate Bitcoin’s unknown creator(s), Satoshi Nakamoto, for the Nobel Prize in Economics.
Satoshi Nakamoto Not Eligible For Nobel Prize

Although UCLA Professor Bhagwan Chowdhry chose to nominate the pseudonymous creator of Bitcoin, Satoshi Nakamoto, for the Nobel Prize for Economic Sciences, it appears the The Royal Swedish Academy of Sciences will not consider the nomination unless the legendary Nakamoto were to reveal his identity.

The organization’s press officer, Hans Reuterskiöld, told Inverse.com that the prize is never awarded anonymously nor after someone has died.

The prize, as in this instance, the Sveriges Riksbank Prize in Economic Science in Memory of Alfred Nobel, is never awarded anonymously nor posthumously.

https://www.cryptocoinsnews.com/satoshi-nakamoto-not-eligible-nobel-prize
Cryptography
Cryptography 密碼學
<table>
<thead>
<tr>
<th>比較</th>
<th>貴金屬</th>
<th>法定貨幣</th>
<th>比特幣（加密貨幣）</th>
</tr>
</thead>
<tbody>
<tr>
<td>例子</td>
<td>黃金、白銀等</td>
<td>美元、歐元等</td>
<td>比特幣（加密貨幣）</td>
</tr>
<tr>
<td>存放成本</td>
<td>每年0.15%到1%</td>
<td>由存放款利差所補貼</td>
<td>免費</td>
</tr>
<tr>
<td>交易成本</td>
<td>昂貴</td>
<td>中等</td>
<td>僅需極低廉手續費</td>
</tr>
<tr>
<td>防偽</td>
<td>無法複製或人工合成</td>
<td>防偽技術、法律</td>
<td>密碼學</td>
</tr>
<tr>
<td>運送</td>
<td>昂貴且有安全問題</td>
<td>不方便且有安全問題</td>
<td>安全、方便、便宜、迅速</td>
</tr>
<tr>
<td>存放方式</td>
<td>物理儲存</td>
<td>存放於機構</td>
<td>密碼學及區塊鏈</td>
</tr>
<tr>
<td>發行方式</td>
<td>挖礦</td>
<td>政治(印鈔鑄幣)</td>
<td>演算法</td>
</tr>
<tr>
<td>信用媒介</td>
<td>物理的稀少性</td>
<td>國家政權</td>
<td>演算法及區塊鏈</td>
</tr>
<tr>
<td>記錄儲存</td>
<td>手動</td>
<td>手動</td>
<td>區塊鏈自動記入</td>
</tr>
<tr>
<td>支付結算</td>
<td>昂貴</td>
<td>中心化的</td>
<td>便宜且分散式的</td>
</tr>
<tr>
<td>稀有性</td>
<td>高</td>
<td>主觀的</td>
<td>演算法，最高2100萬個</td>
</tr>
<tr>
<td>鑑定</td>
<td>昂貴的化驗</td>
<td>信賴對方</td>
<td>區塊鏈</td>
</tr>
<tr>
<td>凍結</td>
<td>會被扣押</td>
<td>會被凍結</td>
<td>只要私鑰在，無法被扣押、凍結</td>
</tr>
<tr>
<td>隱私</td>
<td>實名但保密</td>
<td>實名但保密</td>
<td>匿名但公開</td>
</tr>
</tbody>
</table>
Bitcoin Tutorial

- How the Bitcoin protocol actually works
  - Published by Michael Nielsen on December 6, 2013
  - “This is the best explanation of the Bitcoin protocol that I have read” by Bruce Schneier [https://www.schneier.com/blog/archives/2013/12/bitcoin_explana.html](https://www.schneier.com/blog/archives/2013/12/bitcoin_explana.html)

  - “To understand the post, you need to be comfortable with [public key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography), and with the closely related idea of [digital signatures](https://en.wikipedia.org/wiki/Digital_signature). I’ll also assume you’re familiar with [cryptographic hashing](https://en.wikipedia.org/wiki/Cryptographic_hash_function).”

  - “In the world of atoms we achieve security with devices such as locks, safes, signatures, and bank vaults. In the world of bits we achieve security with cryptography. That is why Bitcoin is at heart a cryptographic protocol.”
Public Key Cryptography (PKC)
Caesar Cipher

• Gāius Jūlius Caesar (100 BC – 44 BC)
  • A Roman military and political leader and one of the most influential men in world history
  • He played a critical role in the transformation of the Roman Republic into the Roman Empire

• Caesar Cipher
  • Encode: A ↔ 0, B ↔ 1, C ↔ 2, …, Y ↔ 24, Z ↔ 25
    • Plaintext: SPY (18 15 24)
    • Ciphertext: VSB (21 18 1)
  • Encryption: \( c = p + 3 \mod 26 \)
  • Decryption: \( p = c - 3 \mod 26 \)
Symmetric Cryptography

- Analogy: Safe with a strong lock, only Alice and Bob have a copy of the key
  - Alice encrypts
    → locks message in the safe with her key
  - Bob decrypts
    → uses his copy of the key to open the safe
Symmetric Cryptography

Encryption 鉅密

Plaintext 明文  Symmetric key  Ciphertext 密文

Decryption 解密

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
私密金鑰 與 公開金鑰

Private Key  ↔  Public Key

- For RSA
  - The multiplication of two large primes is easy
  - The factorization of a large integer is hard
Public Key Cryptosystem

Public key

Plaintext 明文 → Encrypt 加密

 Decrypt 解密 ← Ciphertext 密文

Private key

RSA (Rivest – Shamir – Adleman 1977)

ECC (Elliptic Curve Cryptosystem 橢圓曲線密碼系統)
Digital Signature 数位签章

Public key

Signature → Verify 驗章

Sign 簽章 ← Message

Private key

* 資料完整性 (Integrity)
* 身份鑑別性 (Authentication)
* 不可否認性 (Non-Repudiation)
Electronic Signatures Act
Hash Function
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)
Avalanche Effect 雪崩效應

• A desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions
• When an input is changed slightly (e.g., flipping a single bit) the output changes significantly (e.g., half the output bits flip)

Input | Hash function | Hash sum
--- | --- | ---
000 | 8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730
001 | E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72
010 | 47AB9979 443FB7ED 1C193D06 773333BA 7876094F

The SHA-1 hash function exhibits good avalanche effect. When a single bit is changed the hash sum becomes completely different.

https://en.wikipedia.org/wiki/Avalanche_effect
Security Properties

$x = ?$

\[
\begin{align*}
&h \\
&h(x)
\end{align*}
\]

preimage resistance

$x_1 \quad x_2 = ?$

\[
\begin{align*}
&h \\
h(x_1) = h(x_2)
\end{align*}
\]

second preimage resistance

$x_1 = ? \quad x_2 = ?$

\[
\begin{align*}
&h \\
h(x_1) = h(x_2)
\end{align*}
\]

collision resistance
Cryptographic Hash Functions

- $H$ is a function with **one-way property (pre-image resistance)** if given any $y$, it is *computationally infeasible* to find any value $x$ in the domain of $H$ such that $H(x) = y$.

- $H$ is **collision free (resistant)** if it is *computationally infeasible* to find $x' \neq x$ such that $H(x') = H(x)$.

- $H$ is a **cryptographic hash function** if
  - Input: bit strings of arbitrary length
  - Output: bit strings of fixed length
  - $H$ has one-way property
  - $H$ is collision free
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)

<table>
<thead>
<tr>
<th>Algorithm and variant</th>
<th>Output size (bits)</th>
<th>Internal state size (bits)</th>
<th>Block size (bits)</th>
<th>Rounds</th>
<th>Bitwise operations</th>
<th>Security (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1 FIPS 180</td>
<td>160</td>
<td>160</td>
<td>512</td>
<td>80</td>
<td>and, or, add, xor, rot</td>
<td>Theoretical attack $(2^{61})$</td>
</tr>
<tr>
<td>SHA-2 FIPS 180</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-224</td>
<td>224</td>
<td>256</td>
<td>512</td>
<td>64</td>
<td>and, or, xor, shr, rot, add</td>
<td>112 128</td>
</tr>
<tr>
<td>SHA-256</td>
<td>256</td>
<td>(8 × 32)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-384</td>
<td>384</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>192</td>
</tr>
<tr>
<td>SHA-512</td>
<td>512</td>
<td>512</td>
<td>1024</td>
<td>80</td>
<td>and, or, xor, shr, rot, add</td>
<td>256 112 128</td>
</tr>
<tr>
<td>SHA-512/224</td>
<td>224</td>
<td>(8 × 64)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-512/256</td>
<td>256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-3 FIPS 202</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA3-224</td>
<td>224</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>112</td>
</tr>
<tr>
<td>SHA3-256</td>
<td>256</td>
<td>1600</td>
<td>1152</td>
<td>24</td>
<td>and, xor, rot, not</td>
<td>128</td>
</tr>
<tr>
<td>SHA3-384</td>
<td>384</td>
<td>(5 × 5 × 64)</td>
<td>1088</td>
<td></td>
<td></td>
<td>192</td>
</tr>
<tr>
<td>SHA3-512</td>
<td>512</td>
<td></td>
<td>832</td>
<td></td>
<td></td>
<td>256</td>
</tr>
</tbody>
</table>

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:
    - $\text{Ma}(A, B, C) = (A \land B) \oplus (A \land C) \oplus (B \land C)$
    - $\text{Ch}(E, F, G) = (E \land F') \oplus (\neg E \land G')$
    - $\Sigma_0(A) = (A \gg 2) \oplus (A \gg 13) \oplus (A \gg 22)$
    - $\Sigma_1(E) = (E \gg 6) \oplus (E \gg 11) \oplus (E \gg 25)$
  - The bitwise rotation uses different constants for SHA-512
  - The given numbers are for SHA-256
    - is addition modulo $2^{32}$

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 $5 \times 5$ 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
SHA-3 / Keccak: Sponge Construction
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
Abstract Algebra
Group

- **Definition**  A group $(G, *)$ is a set $G$ with an operation $*$, such that the following conditions are satisfied:

  1) **Closure**  $a * b \in G$ for all $a, b \in G$

  2) **Associativity**  $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$

  3) **Identity**  There is an element $e \in G$ such that $a = a * e = e * a$ for each $a \in G$

  4) **Inverse**  For each $a \in G$, there is an element $b \in G$ such that $a * b = b * a = e$
Group

- **Example** Each of the following sets with the specified operation is a group
  - $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with + (addition)
  - $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ with $\times$ (multiplication)
  - $5\mathbb{Z} = \{5a | a \in \mathbb{Z}\}$ with +
  - $\{1, -1\}$ with $\times$
  - $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with + modulo 6
  - $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ with $\times$ modulo 7
  - $\{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}$ with point addition and point doubling laws on elliptic curves
Cyclic Group

• **Definition**  A group \((G, \ast)\) is **cyclic** if there exists a generator \(g \in G\) such that every \(a \in G\) is of the form \(a = g \ast \ldots \ast g\) \((n\) copies\) for some \(n \in \mathbb{Z}\)

• **Example**
  - \((\mathbb{Z}, +)\) is cyclic with generators 1 and \(-1\)
  - \((\mathbb{Z}_7^*, \times)\) is cyclic: \(\{1 = 3^0 = 3^6, 2 = 3^2, 3 = 3^1, 4 = 3^4, 5 = 3^5, 6 = 3^3\}\)
  - \((\mathbb{Z}_9^*, \times)\) is cyclic with generators 2 and 5

• **Example**
  - \((\mathbb{Q}, +)\) is **not** cyclic
  - \((\mathbb{Z}_8^*, \times)\) is **not** cyclic (Klein 4)
Elliptic Curves
Elliptic Curve 椭圓曲線

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

Point Addition

Point Doubling

質數體 (Prime Field) 上的曲線

Addition:
\[(x_3, y_3) = (x_1, y_1) + (x_2, y_2)\]

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

\[
s = \begin{cases} 
\frac{y_2 - y_1}{x_2 - x_1} \mod p & \text{(addition)} \\
\frac{3x_1^2 + a}{2y_1} \mod p & \text{(doubling)} 
\end{cases}
\]

\[
x_3 = s^2 - x_1 - x_2 \mod p
\]

\[
y_3 = s(x_1 - x_3) - y_1 \mod p
\]
Example

- **Given** $E: y^2 = x^3 + 2x + 2 \mod 17$ and point $P = (5, 1)$
- **Goal**: Compute $2P = P + P = (5, 1) + (5, 1) = (x_3, y_3)$

\[
s = \frac{3x_1^2 + a}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \mod 17
\]

- $x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 = 159 \equiv 6 \mod 17$
- $y_3 = s(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \mod 17$

Finally $2P = (5, 1) + (5, 1) = (6, 3)$
Example

- The points on an elliptic curve and the point at infinity \( \mathcal{O} \) form cyclic subgroups

\[
\begin{align*}
2P &= (5, 1) + (5, 1) = (6, 3) \\
3P &= 2P + P = (10, 6) \\
4P &= (3, 1) \\
5P &= (9, 16) \\
6P &= (16, 13) \\
7P &= (0, 6) \\
8P &= (13, 7) \\
9P &= (7, 6) \\
10P &= (7, 11) \\
11P &= (13, 10) \\
12P &= (0, 11) \\
13P &= (16, 4) \\
14P &= (9, 1) \\
15P &= (3, 16) \\
16P &= (10, 11) \\
17P &= (6, 14) \\
18P &= (5, 16) \\
19P &= \mathcal{O}
\end{align*}
\]

This elliptic curve has order \( \#E = |E| = 19 \) since it contains 19 points in its cyclic group.
Double and Add

- Example

\[ 17 \ P = (2P) + P + \ldots + P \]

[1 doubling & 15 additions]

\[ = (10001)_2 \ P = 2(2(2(2P))) + P \]

[4 doublings & 1 addition]
Double and Add

Example: $26P = (11010_2)P = (d_4d_3d_2d_1d_0)_2 P$.

Step

#0 $P = 1_2P$

#1a $P + P = 2P = 10_2P$

#1b $2P + P = 3P = 10^2P + 1_2P = 11_2P$

#2a $3P + 3P = 6P = 2(11_2P) = 110_2P$

#2b

#3a $6P + 6P = 12P = 2(110_2P) = 1100_2P$

#3b $12P + P = 13P = 1100_2P + 1_2P = 1101_2P$

#4a $13P + 13P = 26P = 2(1101_2P) = 11010_2P$

#4b

initial setting

DOUBLE (bit $d_3$)

ADD (bit $d_3 = 1$)

DOUBLE (bit $d_2$)

no ADD ($d_2 = 0$)

DOUBLE (bit $d_1$)

ADD (bit $d_1=1$)

DOUBLE (bit $d_0$)

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:

$$p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFC2F$$

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

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

$$a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000$$

$$b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007$$

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:

$$n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF F poop 8F BAAEDCE6 AF48A03B BFD25E8C$$
$$D0364141$$

$$h = 01$$

椭圆曲线 secp256k1

https://en.bitcoin.it/wiki/Secp256k1
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 $P$
### NIST Curve Standards in FIPS 186

**Table D-1: Bit Lengths of the Underlying Fields of the Recommended Curves**

<table>
<thead>
<tr>
<th>Bit Length of $n$</th>
<th>Prime Field</th>
<th>Binary Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>$161 - 223$</td>
<td>len($p$) = 192</td>
<td>$m = 163$</td>
</tr>
<tr>
<td>$224 - 255$</td>
<td>len($p$) = 224</td>
<td>$m = 233$</td>
</tr>
<tr>
<td>$256 - 383$</td>
<td>len($p$) = 256</td>
<td>$m = 283$</td>
</tr>
<tr>
<td>$384 - 511$</td>
<td>len($p$) = 384</td>
<td>$m = 409$</td>
</tr>
<tr>
<td>$\geq 512$</td>
<td>len($p$) = 521</td>
<td>$m = 571$</td>
</tr>
</tbody>
</table>
NIST Curves over Prime Fields

D.1.2 Curves over Prime Fields

For each prime $p$, a pseudo-random curve

$$E : y^2 \equiv x^3 - 3x + b \pmod{p}$$

of prime order $n$ is listed\(^4\). (Thus, for these curves, the cofactor is always $h = 1$.) The following parameters are given:

- The prime modulus $p$
- The order $n$
- The 160-bit input seed $SEED$ to the SHA-1 based algorithm (i.e., the domain parameter seed)
- The output $c$ of the SHA-1 based algorithm

\(^4\) The selection $a = -3$ for the coefficient of $x$ was made for reasons of efficiency; see IEEE Std 1363-2000.

- The coefficient $b$ (satisfying $b^2 c \equiv -27 \pmod{p}$)
- The base point $x$ coordinate $G_x$
- The base point $y$ coordinate $G_y$

The integers $p$ and $n$ are given in decimal form; bit strings and field elements are given in hexadecimal.
Curve P-256

D.1.2.3 Curve P-256

\[ p = 115792089210356248762697446949407573530086143415290314195533631308867097853951 \]

\[ n = 115792089210356248762697446949407573529996955224135760342122259061068512044369 \]

\[ SEED = c49d3608 86e70493 6a6678e1 139d26b7 819f7e90 \]

\[ c = 7efba166 2985be94 03cb055c 75d4f7e0 ce8d84a9 c5114abc af317768 0104fa0d \]

\[ b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b \]

\[ G_x = 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296 \]

\[ G_y = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5 \]
# NIST Curves over Prime Fields

<table>
<thead>
<tr>
<th>Curve</th>
<th>Equation</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-192</td>
<td>$p = 2^{192} - 2^{64} - 1$, $a = -3$, $h = 1$,</td>
<td>$b = 0x64210519$ E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1</td>
</tr>
<tr>
<td></td>
<td>$n = 0x$ FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831</td>
<td></td>
</tr>
<tr>
<td>P-224</td>
<td>$p = 2^{224} - 2^{96} + 1$, $a = -3$, $h = 1$,</td>
<td>$b = 0xB4050A85$ 0C04B3AB F5413256 5044B0B7 D7BFD8BA 270B3943 2355FFB4</td>
</tr>
<tr>
<td></td>
<td>$n = 0x$ FFFFFFFF FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D</td>
<td></td>
</tr>
<tr>
<td>P-256</td>
<td>$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, $a = -3$, $h = 1$,</td>
<td>$b = 0x5AC635D8$ AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>27D2604B</td>
</tr>
<tr>
<td></td>
<td>$n = 0x$ FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FC632551</td>
</tr>
<tr>
<td>P-384</td>
<td>$p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$, $a = -3$, $h = 1$,</td>
<td>$b = 0xB3312FA7$ E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5013875A C656398D 8A2ED19D 2A85C8ED D3EC2A6F</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$n = 0x$ FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973</td>
</tr>
<tr>
<td>P-521</td>
<td>$p = 2^{521} - 1$, $a = -3$, $h = 1$,</td>
<td>$b = 0x00000051$ 953EB961 8E1C9A1F 929A21A0 B68540EE A2DA725B 99B315F3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B8B48991 8EF109E1 56193951 EC7E937B 1652C0BD 3BB1BF07 3573DF88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3D2C34F1 EF451FD4 6B503F00</td>
</tr>
<tr>
<td></td>
<td>$n = 0x$ FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FFFFFFA 51868783 BF2F966B 7FCC0148 F709A5D0 3BB5C9B8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>899C47AE BB6FB71E 91386409</td>
</tr>
</tbody>
</table>
# Security Level

(NIST) SP 800-57 Part 1

<table>
<thead>
<tr>
<th>Bits of security</th>
<th>Symmetric key algorithms</th>
<th>Finite Field Cryptography (FFC, e.g., DSA, D-H)</th>
<th>Integer Factorization Cryptography (IFC, e.g., RSA)</th>
<th>Elliptic Curve Cryptography (ECC, e.g., ECDSA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>2TDEA*</td>
<td>$L = 1024$  \hspace{1em} $N = 160$</td>
<td>$k = 1024$</td>
<td>$f = 160-223$</td>
</tr>
<tr>
<td>112</td>
<td>3TDEA</td>
<td>$L = 2048$  \hspace{1em} $N = 224$</td>
<td>$k = 2048$</td>
<td>$f = 224-255$</td>
</tr>
<tr>
<td>128</td>
<td>AES-128</td>
<td>$L = 3072$  \hspace{1em} $N = 256$</td>
<td>$k = 3072$</td>
<td>$f = 256-383$</td>
</tr>
<tr>
<td>192</td>
<td>AES-192</td>
<td>$L = 7680$  \hspace{1em} $N = 384$</td>
<td>$k = 7680$</td>
<td>$f = 384-511$</td>
</tr>
<tr>
<td>256</td>
<td>AES-256</td>
<td>$L = 15360$  \hspace{1em} $N = 512$</td>
<td>$k = 15360$</td>
<td>$f = 512+$</td>
</tr>
</tbody>
</table>

* The assessment of at least 80-bits of security for 2TDEA is based on the assumption that an attacker has no more than $2^{40}$ matched plaintext and ciphertext blocks ([ANSX9.52], Annex B).