比特幣的過去現在與未來

講者：陳伯韋 Chen Po Wei
Email：powei.chen@pku.edu.cn
日期：2019. 7. 11
地點：計資中心106教室
網站：https://cypherpunks-core.github.io/

關於我

關於我（1）

學歷：

- 學士,銘傳大學 資訊工程, 2011.9-2016.7
- 碩士,北京大學 軟體工程,2016.9-2018.7

工作經驗：

- Organizer, Cypherpunks Taiwan, 2019.01-present
- 技術顧問, Turing Chain, 2019.01-present
- 技術顧問, BlockTempo, 2018.09-present
- 研究助理, 科技部, 2014.07-2018.09
- 訪問學生, 中央研究院 資訊科學所, 2017.09-2018.02
- 教學助理, 銘傳大學, 2015.07-2016.06
- Intern, 中央研究院 資訊科學所, 2015.07-2015.09

關於我（2）

社群：

- Co-organizer, Taipei Bitcoin Meetup, 2014.12-present
- Co-organizer, Bitcoin 比特幣中文, 2014.08-present
- Co-organizer, Taipei Ethereum Meetup, 2016.12-present
- Moderator, IOTA 愛好者中文社群 , 2017.12-present

Research Interest：

- Bitcoin
- Blockchain
- Cryptocurrency
- address generation
- Cryptography
- Firewall rules sniffing
- Onion network

相關著作

- Jan-Ming Ho, Po-Wei Chen, Chia-Hui Wang. “Feasibility Study on Sniffering and Breakthrough of Firewall Rules behind Non-free Networks over Internet.”, 2018 International Conference for Leading and Young Computer Scientists（IC-LYCS）. 2018.
- Chen, Po-Wei, Bo-Sian Jiang, and Chia-Hui Wang. “Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet.” 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications（WiMob）. IEEE, 2017.
- 江柏憲，陳伯韋，王家輝，何建明。<匿名加密貨幣與實名商家交易的有效行動支付監督平臺之建置與實作 - 以比特幣為例>。 “TANET2017臺灣網際網路研討會，20171001” 東海大學（編）。臺灣：東海大學，2017.1-6。 “華藝線上圖書館” 。網路.2018年2月11日.doi：10.6728 / TANET.201710.0001，TANET2017

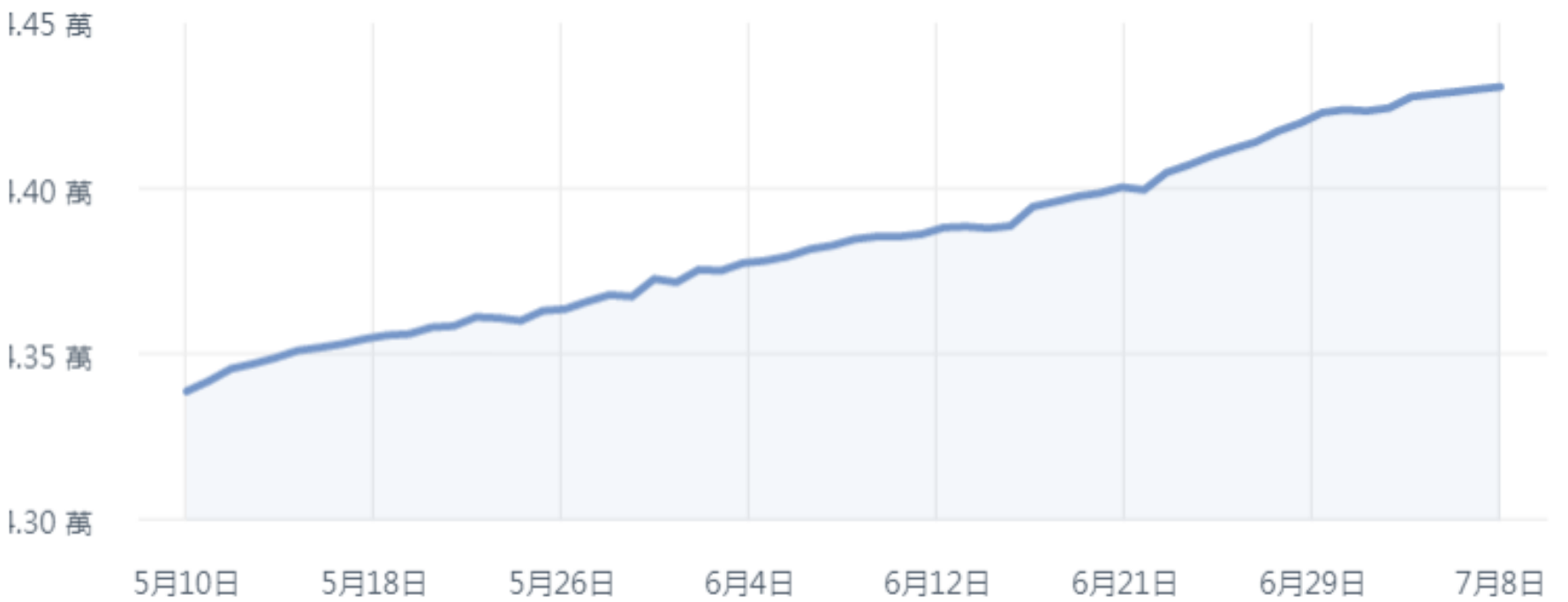
Bitcoin比特幣中文社團

四萬四千多人

成員總數

5 月 10, 2019 ~ 7 月 8, 2019

4.4 萬 成員



44,310

成員總數

+2%

bitcoin taiwan

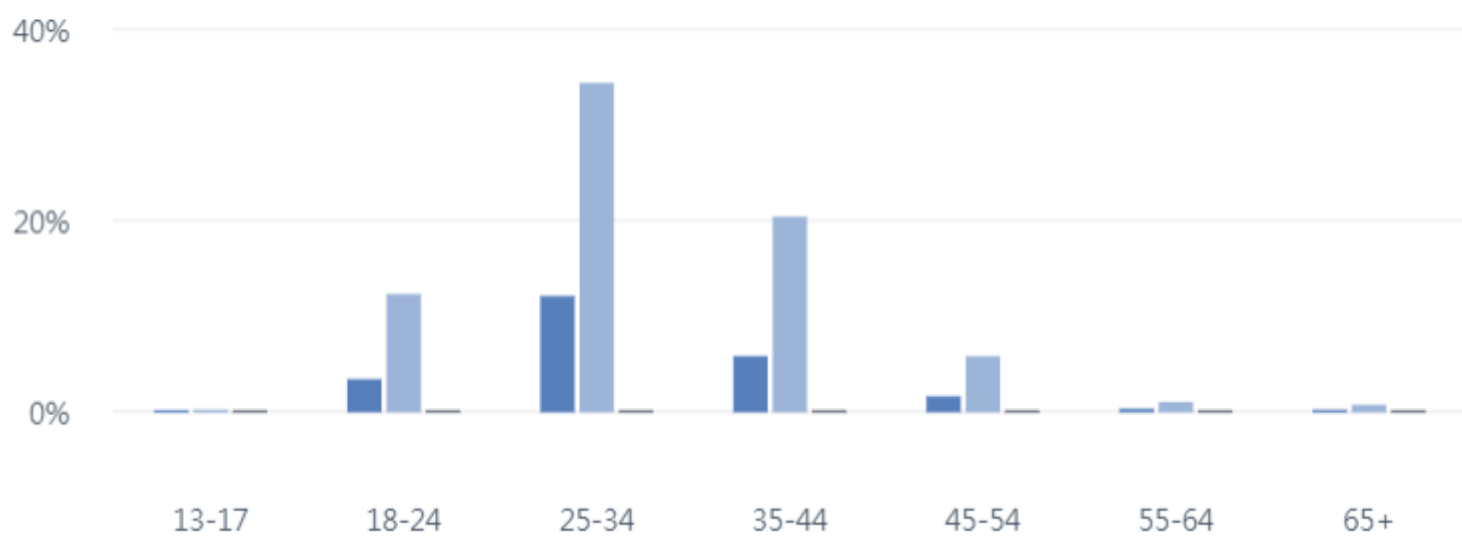
- 本版的『工人』智慧過濾些貼文如以下相關內容：
  - 高收益投資方案(High Yield Investment Program,HYIP)
  - 水龍頭
  - 賣(雲)礦機(託管)
  - 賣加密貨幣
  - 洗留言（廣告性質）
  - 有廣告 推廣連結

最常發言的成員	貼文	留言
唐O萱	1	68
謝O佑	13	4
邱O維	11	3
金O賢	3	40
林O鈞	8	12
Ling O Lee	8	8
孫O盛	1	39
柯O濱	1	35
Justin O	2	29
張O遠	2	27
Joynior O	2	23
鍾O京	6	3
陳O群	0	32
王O駿	1	26
Henry O	6	0

bitcoin taiwan

年齡與性別

24.1% 女性　75.7% 男性　0.2% 自訂



24.1%
女性

75.7%
男性

0.2%
自訂

bitcoin taiwan

國家 / 地區排名		城市排行榜	
台灣	34,029	臺北市	14,029
中國	2,609	臺中市	4,905
香港	2,447	高雄市	3,388
馬來西亞	1,128	桃園區，桃園市	2,780
美國	819	香港香港	2,436
澳大利亞	290	臺南市	2,351
越南	265	新北市，New Taipei City	2,079
日本	205	新竹市	1,230

bitcoin taiwan

Before Bitcoin

What is a Cypherpunk?

Cypherpunks郵寄清單始於1992年，到1994年有700名訂閱者。在高峰時期，它是一個非常活躍的論壇，其技術討論涉及 **“數學、密碼學、計算器科學、政治、哲學”** 討論，個人論證和攻擊等，並引發了一些垃圾郵件。

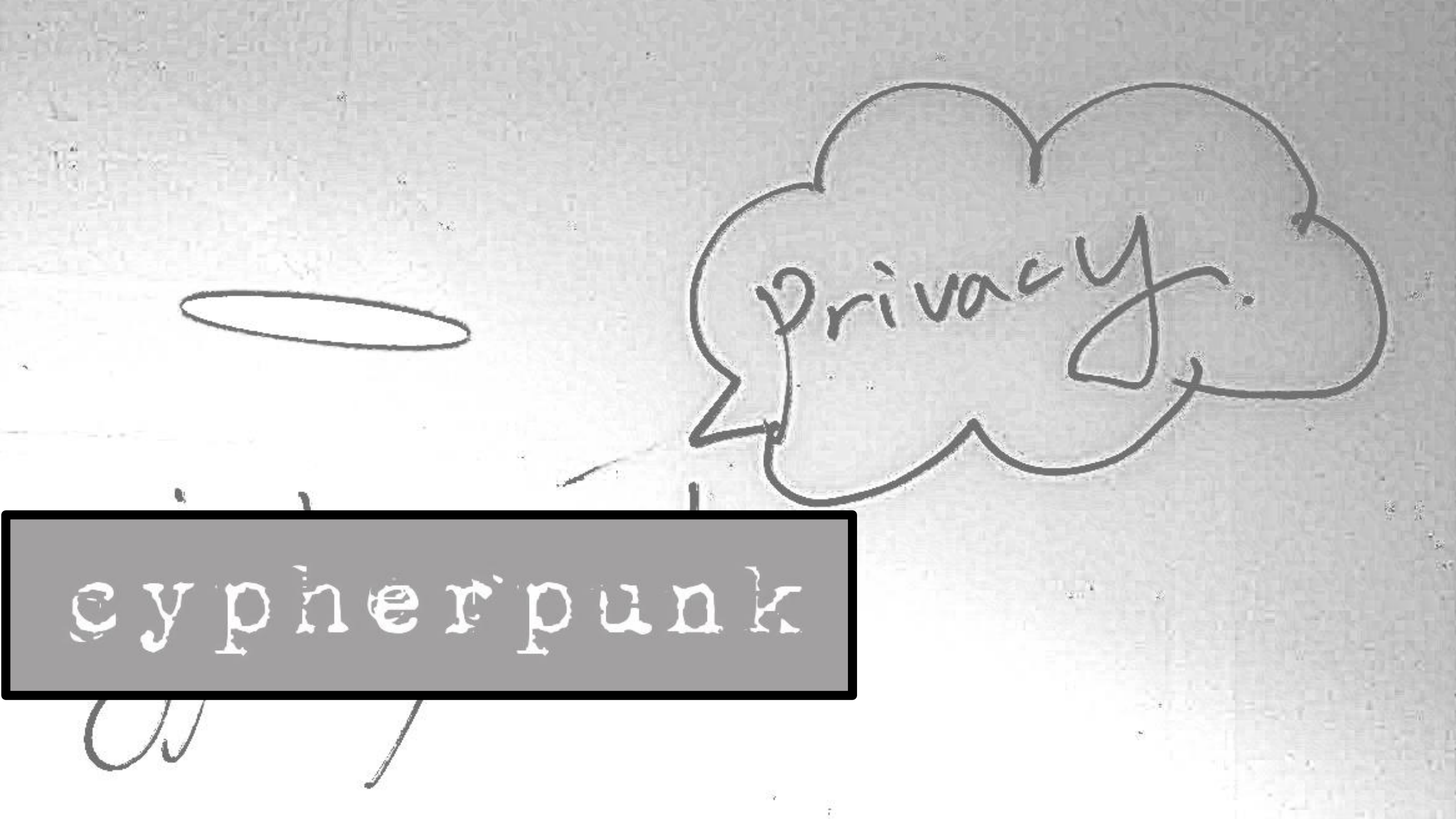
Cypherpunk 宣言

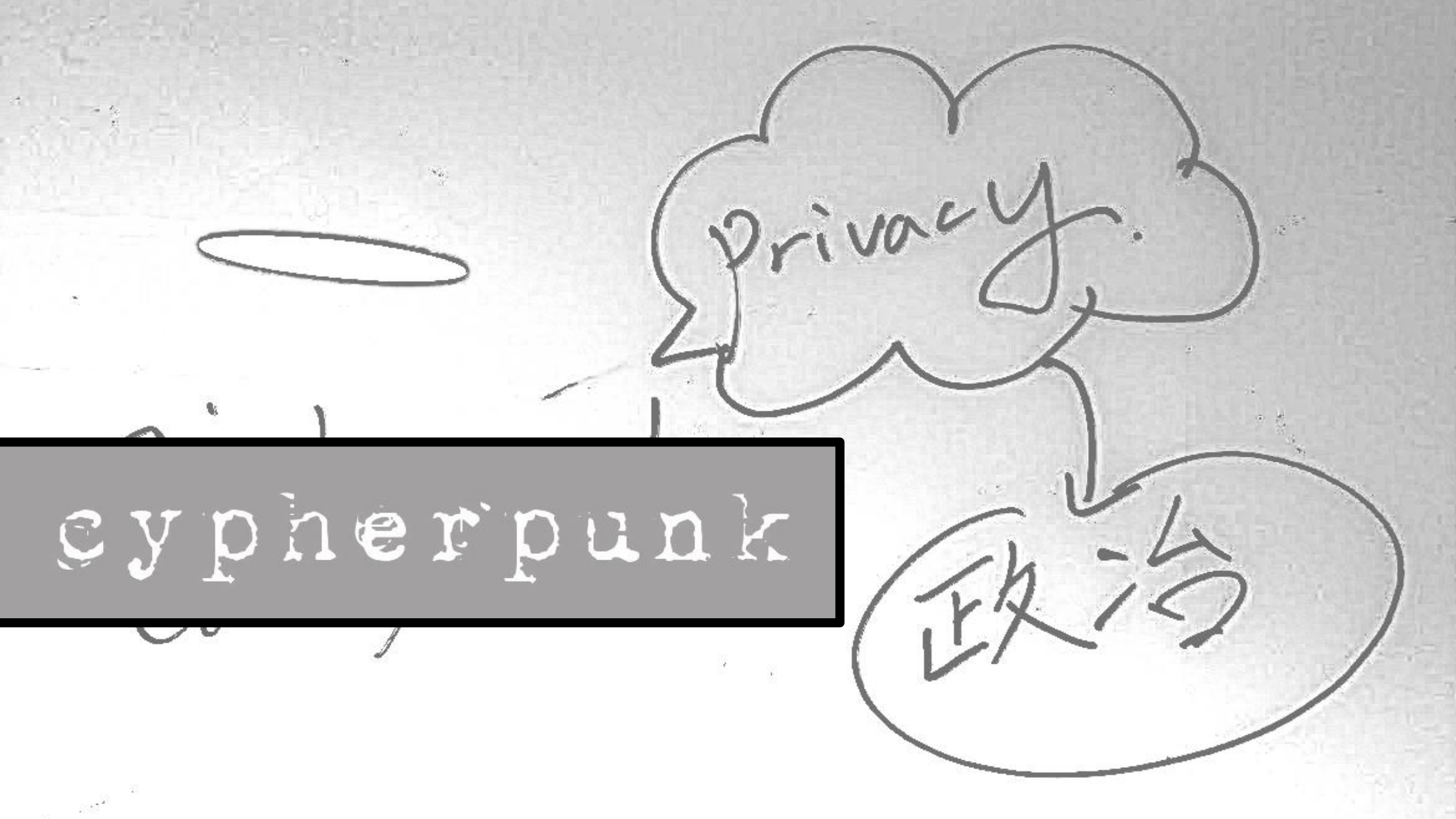
隱私是電子時代開放社會所必需的.....我們不能指望政府，企業或其他大型，不露面的組織給予我們 隱私...**如果我們希望有任何保護，我們必須保護自己的隱私**。... Cypherpunks編寫代碼。我們知道有人必須編寫軟體來保護隱私，並且...我們將編寫它。

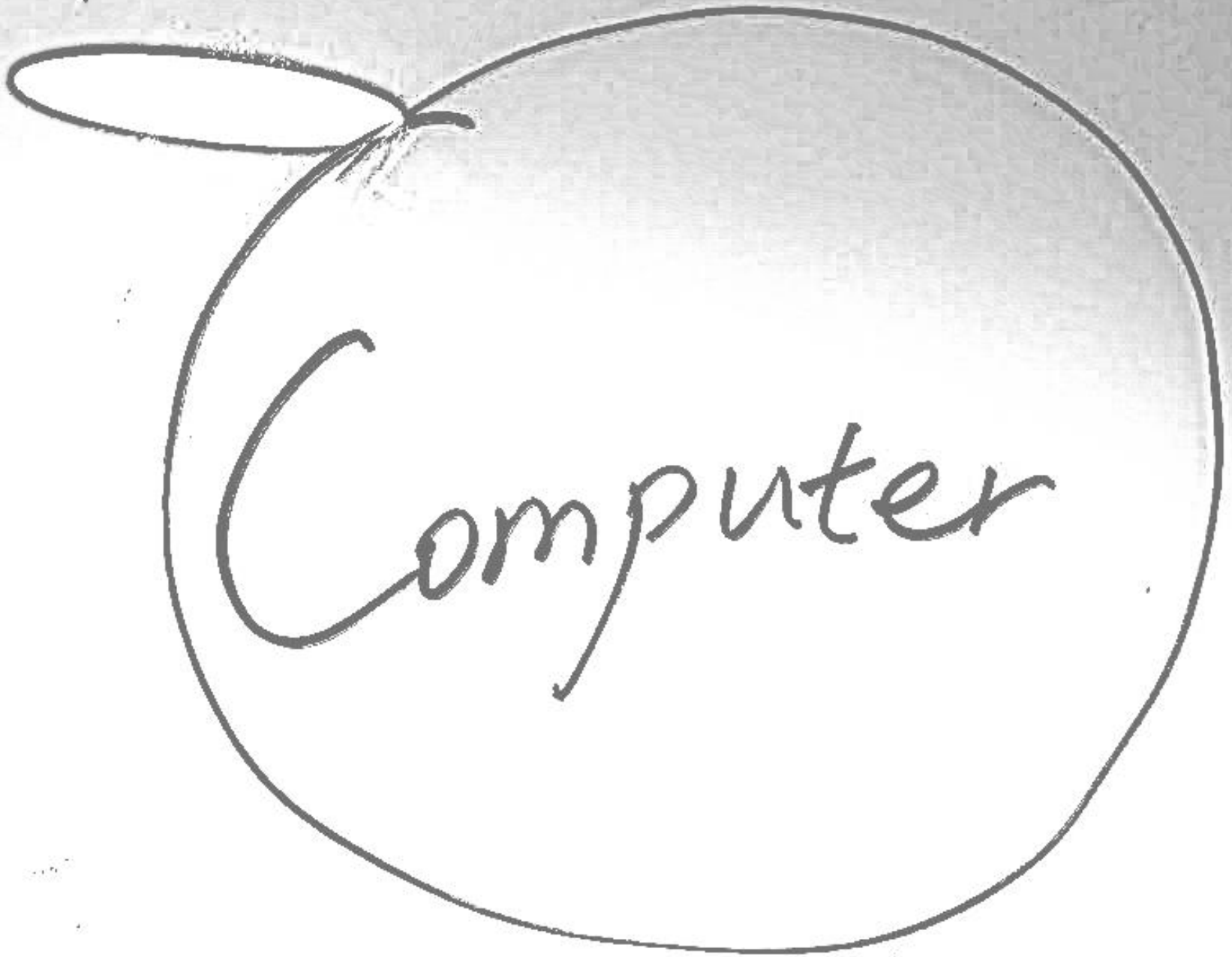
密碼無政府狀態

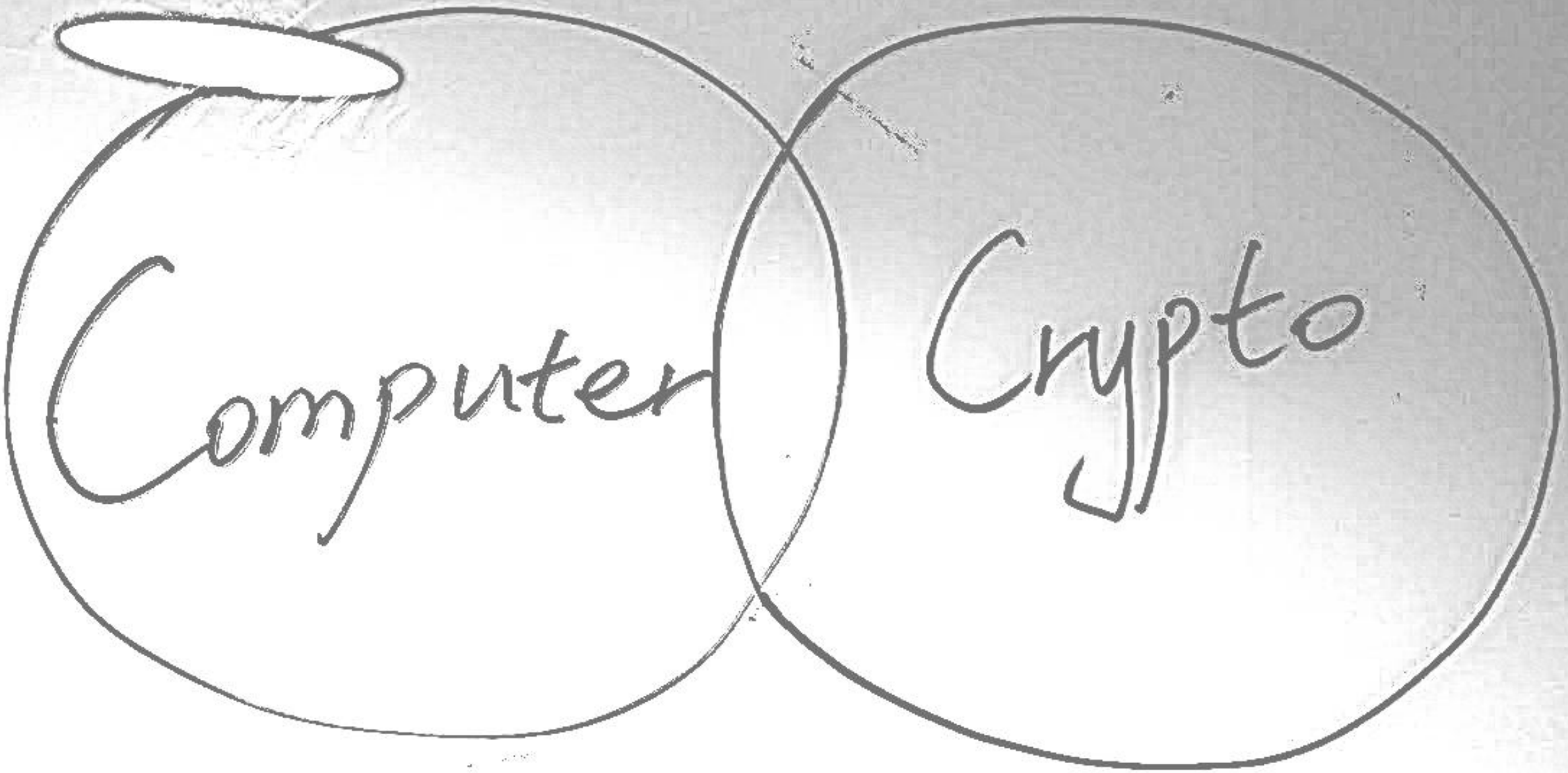
- 加密
- 數位貨幣
- 匿名網路
- 數字假名
- 零知識
- 聲譽
- 訊息市場
- 黑市
- 政府崩潰。

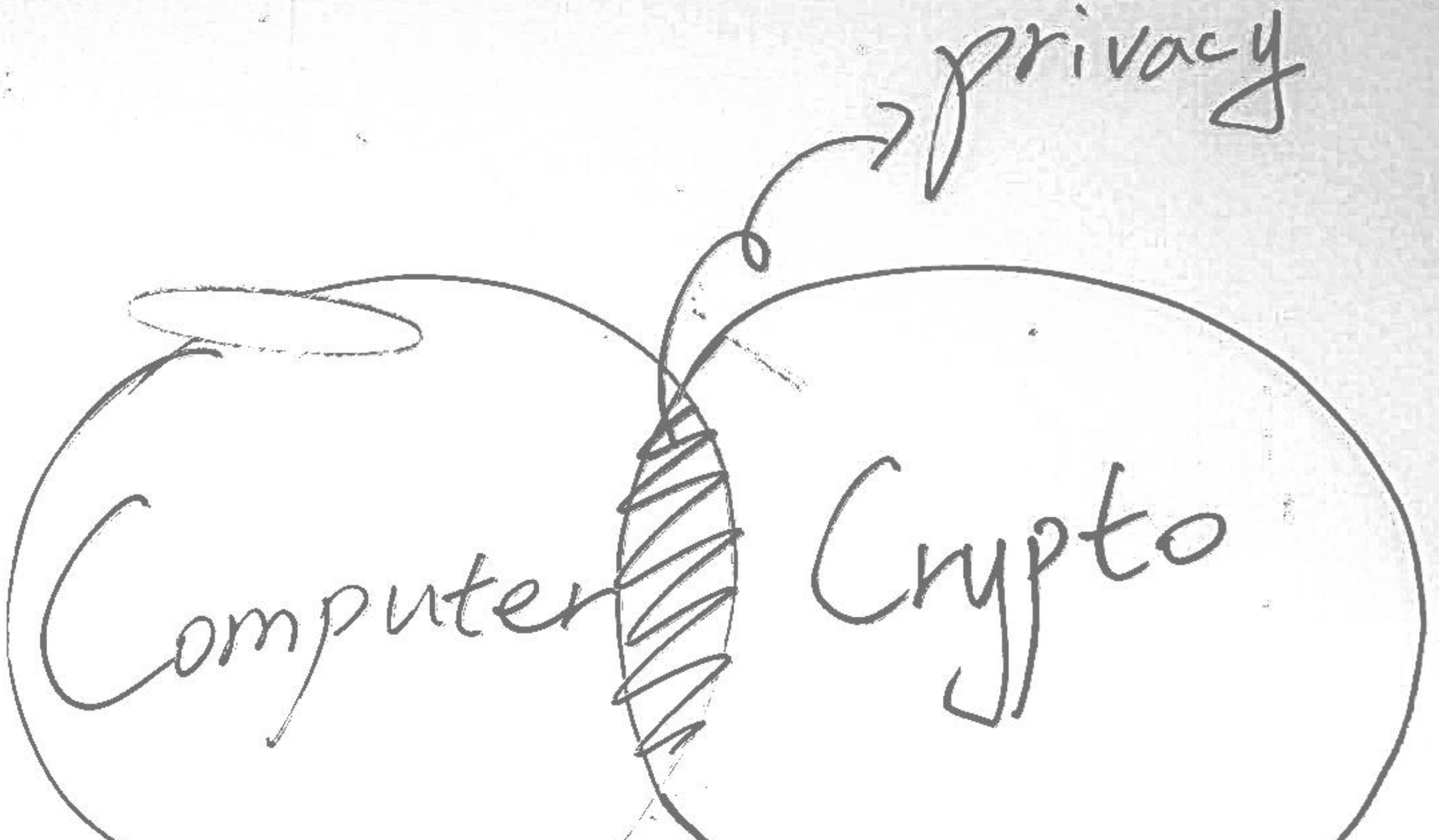
cypherpunk


Privacy
cypherpunk

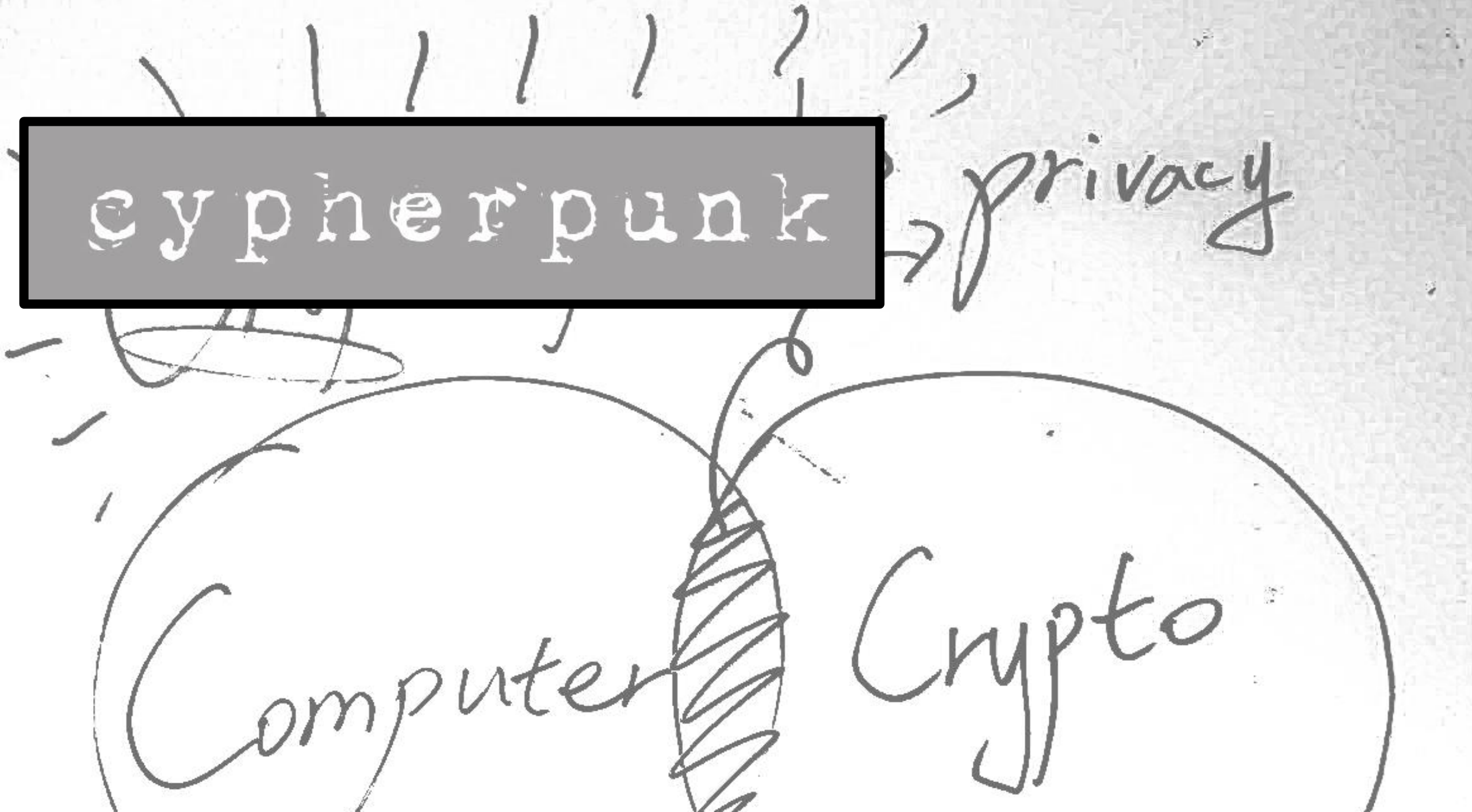

Privacy.
cypherpunk
政治


Computer


Computer
Crypto


privacy
Computer
Crypto

cypherpunk



why privacy ?

Why privacy?

不相信

(1) 政府

(2) 企業

Cypherpunks 精神

密碼學使自由隱私再次偉大

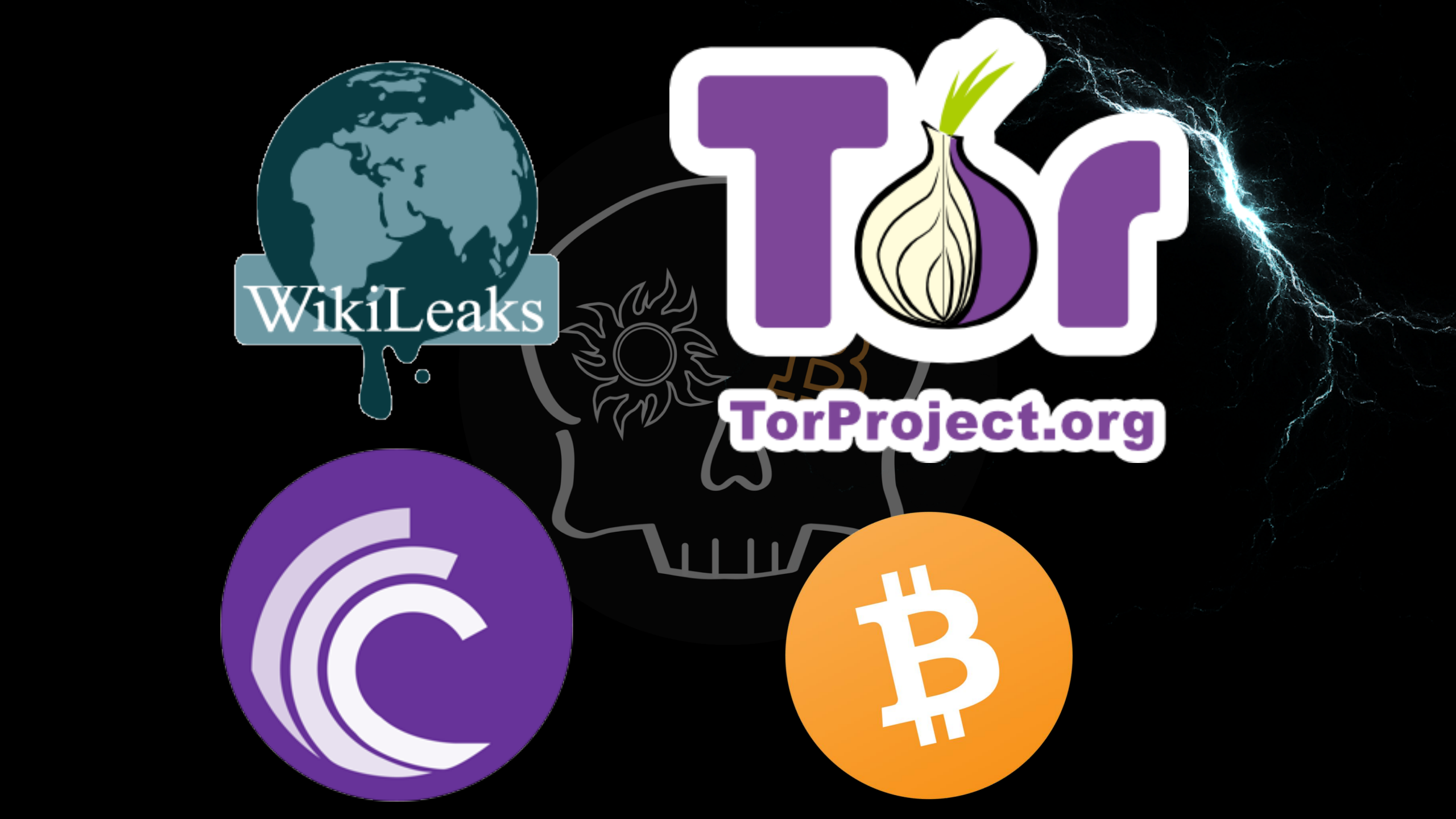
Not Trump

cypherpunk

1) Tor

2) Torrent

3) 非對稱密碼


WikiLeaks
Tor
TorProject.org

TorProject.org

Tor：暗網！

how do i get to the...

WHAT IS WikiLeaks?

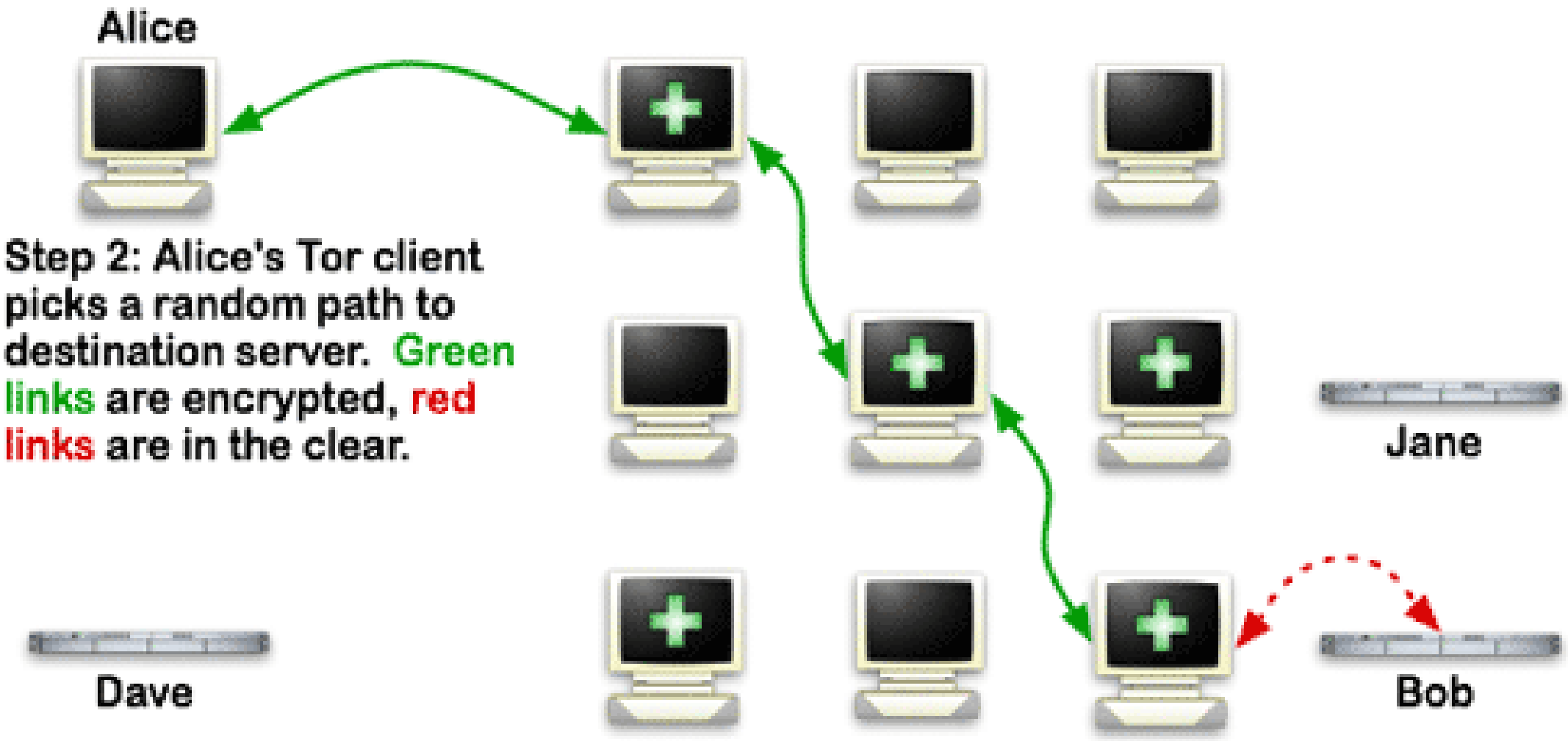
說出　不可以說的真相

2010
2011
2012
2013
2014
2015
2016
2017
2018
2019

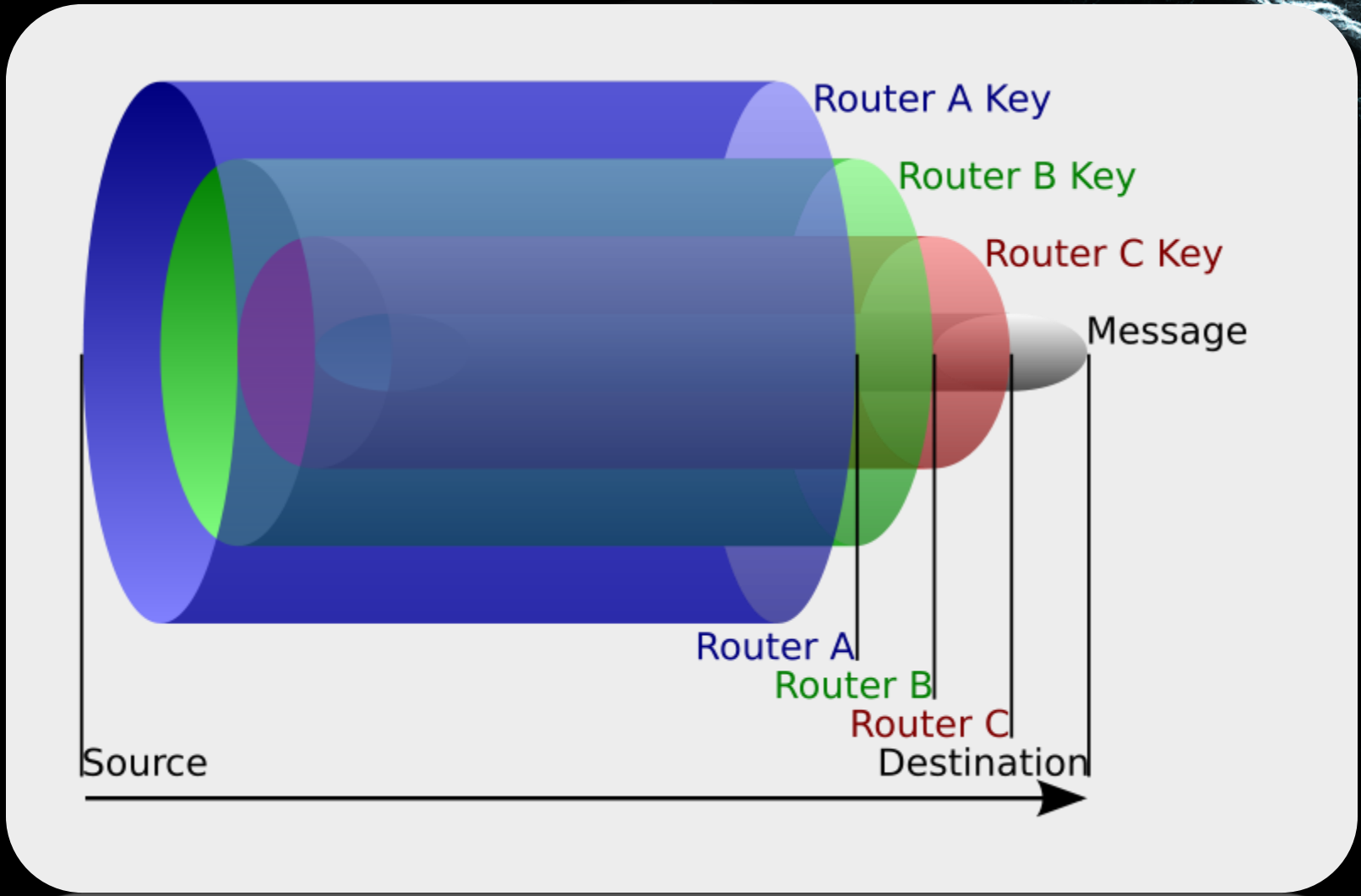
How Tor Works: 1

https://2019.www.torproject.org/about/overview.html.en

How Tor Works: 2



https://2019.www.torproject.org/about/overview.html.en


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Bitcoin 存在的隱私問題

- 區塊鏈同步的過程中，暴露ＩＰ
- 發起比特幣交易的過程中，暴露ＩＰ

2015 IEEE Symposium on Security and Privacy

提到針對這樣的議題進行開發全新的貨幣，如Anoncoin，BitTor，Torcoin，Stealthcoin

Bitcoin over Tor isn't a good idea

文中提出多個 bitcoin 使用tor 網路的攻擊手法 並加以分析

Alex Biryukov
University of Luxembourg
Email: alex.biryukov@uni.lu

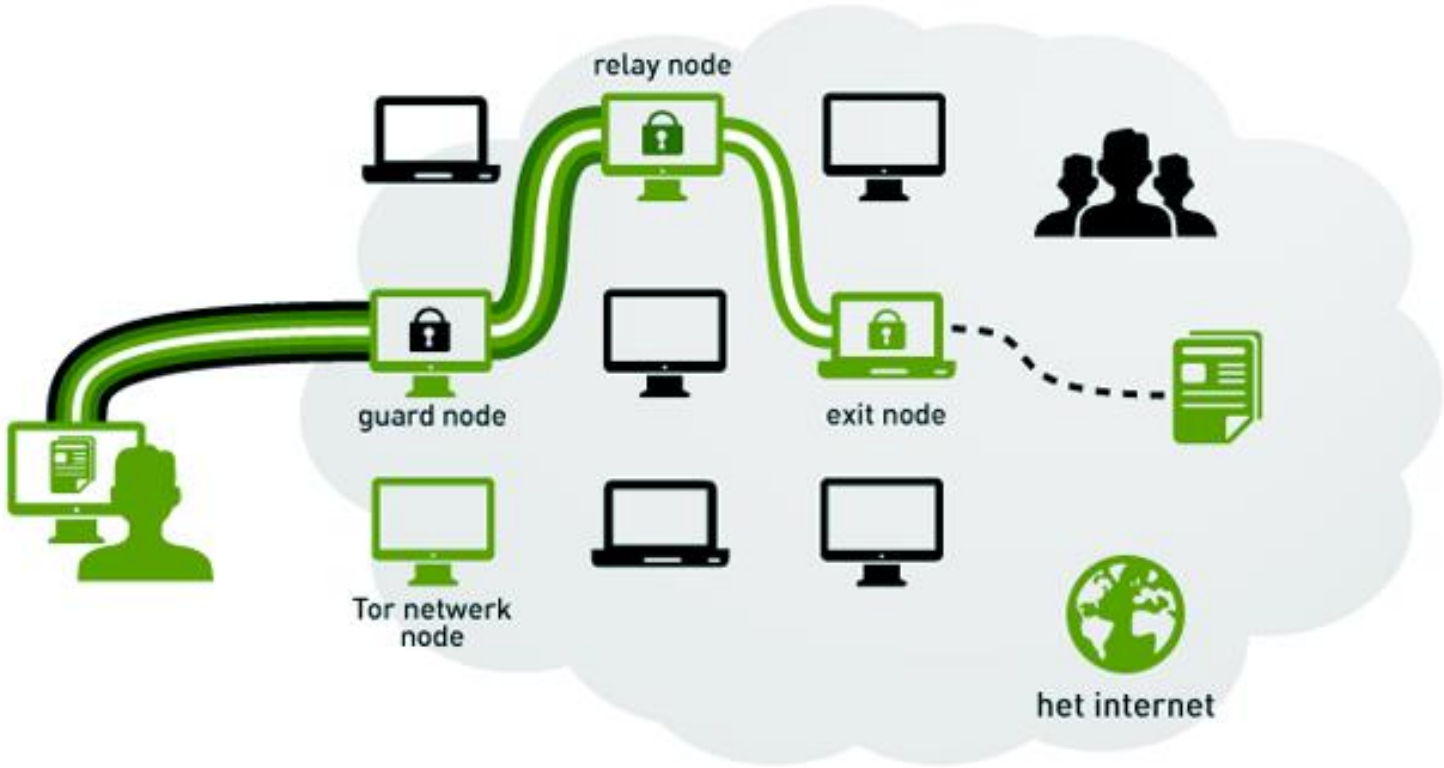
Ivan Pustogarov
University of Luxembourg
Email: ivan.pustogarov@uni.lu

***Abstract*—Bitcoin is a decentralized P2P digital currency in which coins are generated by a distributed set of miners and transactions are broadcasted via a peer-to-peer network. While Bitcoin provides some level of anonymity (or rather pseudonymity) by encouraging the users to have any number of random-looking Bitcoin addresses, recent research shows that this level of anonymity is rather low. This encourages users to connect to the Bitcoin network through anonymizers like Tor and motivates development of default Tor functionality for popular mobile SPV clients. In this paper we show that combining Tor and Bitcoin creates a new attack vector. A low-resource attacker can gain full control of information flows between all users who chose to use Bitcoin over Tor. In particular the attacker can link together user's transactions regardless of pseudonyms used, control which Bitcoin blocks and transactions are relayed to user and can delay or discard user's transactions and blocks. Moreover, we show how an attacker can fingerprint users and**

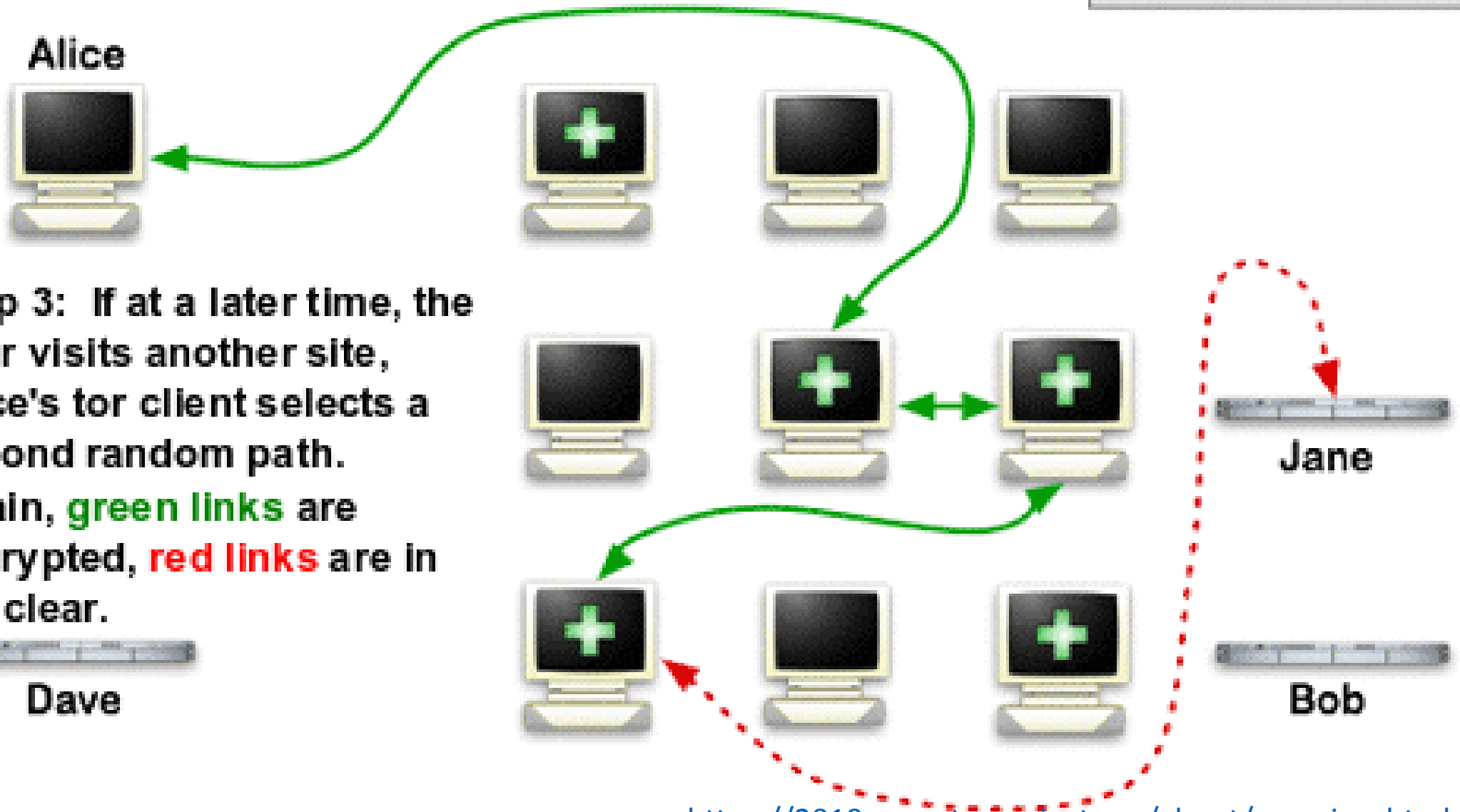
already foreseen in the original Bitcoin whitepaper, see Section 8 of [18]. Since such popular clients [5], [11] (around 1 Million expected userbase [13]) are vulnerable to spoofing attacks which may result in double-spending (see appendix B), the current trend is to bundle them with Tor by default to avoid spoofing[2] and man-in-the-middle attacks. Tor can also be a solution for services and online shops that want to prevent DoS attacks against their public IP. Finally Tor is seen as a countermeasure if Internet neutrality towards Bitcoin will start to erode [7].

Tor is not a panacea however and not all applications are anonymized equally well when combined with Tor. The biggest effort has been made so far on improving protection of the HTTP(S) protocol on top of Tor. Other protocols are not researched that well. There were several documented

Ways to UnMask Tor Users without Cracking Encryption



How Tor Works: 3



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

https://2019.www.torproject.org/about/overview.html.en

~~暗網~~

保護 1) User IP

2) 訪問 service 路徑.

暗網 - 洗錢

OnionWallet Simple and secure Bitcoin wallet

Home | Login | Register | FAQ

Your anonymous Tor Bitcoin Wallet and Laundry

OnionWallet Features:

- **Free Bitcoin Mixer! You will always get get completely different Bitcoins on withdrawals with no "taint" to your recieving address.**
- Safe storage: we keep most of the bitcoins in secure encrypted offline storage.
- Protect your funds with a transaction PIN.
- Anonymous registration: We do not need any private data.
- Very simple user interface, no complicated options and settings.
- NO FEES except the bitcoin network fee!

Get started using Bitcoins in 2 simple steps:

- Register an account on OnionWallet and write down your username, password and optionally PIN at a secure place.
- Purchase Bitcoins to your Bitcoin address in your OnionWallet account using for example one of the following exchange services:

暗網 - 洗錢

EasyCoin
Your rocket fast Bitcoin wallet
Tor
easycoinsayj7p5l.onion
Home
Login
Register
Buy Bitcoins
FAQ
Welcome to EasyCoin Bitcoin Wallet
Now with free Bitcoin mixer, you will always get new coins back when you withdraw from your EasyCoin wallet!
You only pay the Bitcoin transaction fee.
We also support completely free account to account transfers.
Click here to sign up now!

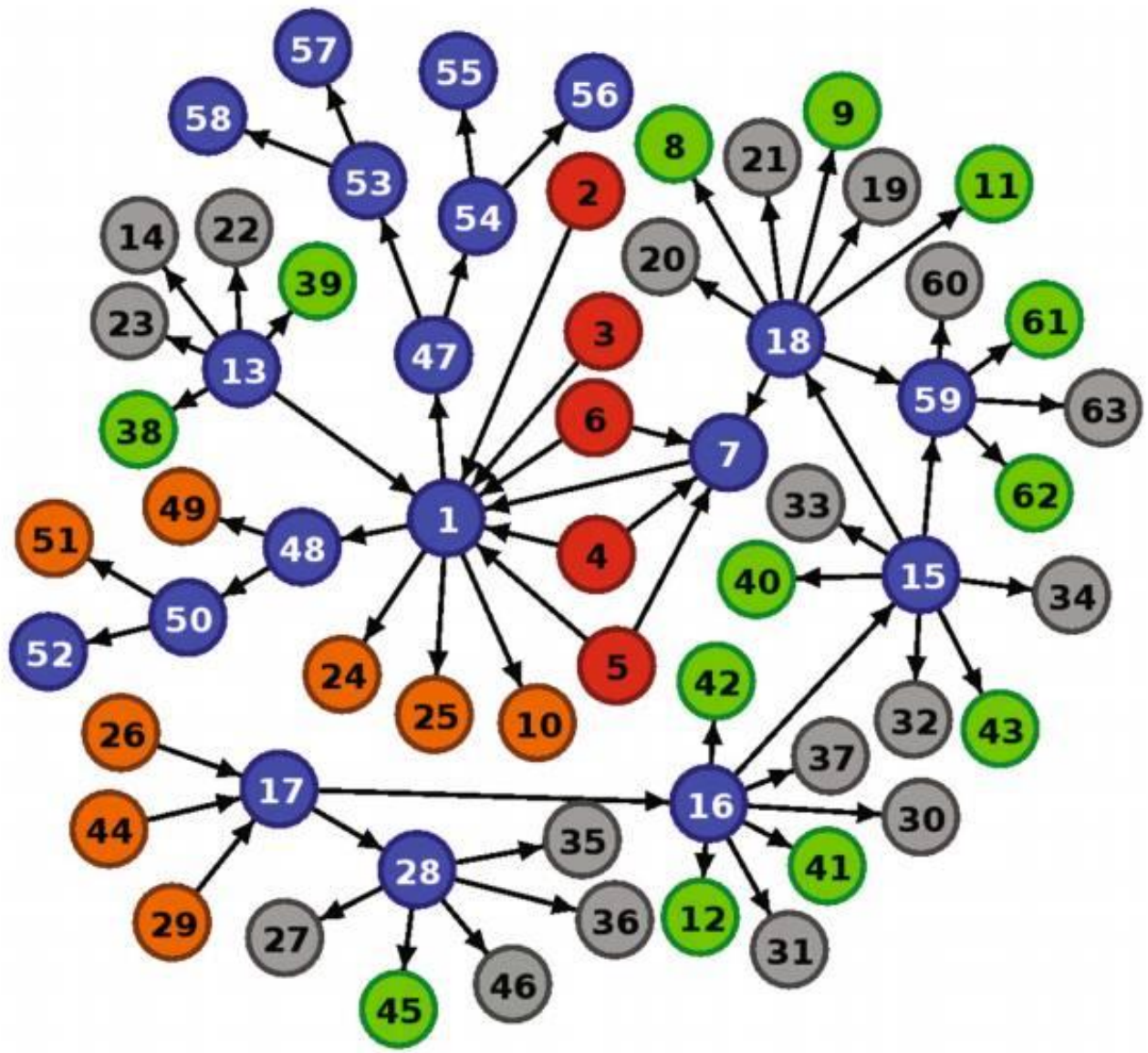


Fig. 8. Darklaunder workflow

bitcoin taiwan

Dream Market

- Down or Up: Up / Online
- Total Listing: 120262
- Drug Listings: 61457
- Entry: Open
- Description: Dream Market 自2013年下半年以來一直在運作。

暗網 - 駭客服務

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.079 ฿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.158 ฿	1 X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.284 ฿	1 X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.063 ฿	1 X Buy now

暗網 - 帳戶買賣

ccPal Store

Products | FAQs | Register | Login

ccPal Store - PayPals, CCs, CVV2s, Ebay accounts

We are the ccPal hackers group. We got more accounts than we can ever sell from old hacks and phishing. And we also get huge new lists every few days so get them while supply lasts and prices are cheap!
All lists are totally random, some paypals or CCs will have 0 balance, some will have $5000 balance or more. We don't have the time to check them all before we sell them.
80%+ working guarantee, we will replace if more than 20% don't work!

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.027 ฿	1 X Buy now
100 Ebay accounts	100 USD = 0.027 ฿	1 X Buy now
100 CCs with CVV2	150 USD = 0.040 ฿	1 X Buy now

暗網 - 護照

Products | Login | Register | FAQs

UK Passports

Your UK Passport - Name of your choice!

We are selling original UK Passports made with your info/picture.
Your info will get entered into the official passport database.
So it's possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your information and pictures will be given after purchase!

You can even enter the UK/EU with our passports, we will add a stamp for the country you are in before we send you your passport to any country!
Ideal for people who want to work in the EU/UK.

Product	Price	Quantity
Your original UK passport with your info/pictures This is 50% of the final price, you pay the other 50% once we show you pictures of your new passport	1000 GBP = 0.343 ฿	1 X Buy now
NEW: UK bank account with online banking and card. Great for cashing out bitcoin. Accounts are created in a secure way to make sure they don't get banned.	700 GBP = 0.240 ฿	1 X Buy now

暗網 - 身分證

USfakeIDs

Products FAQs Register Login

US Fake Drivers Licenses - Scannable, Holograms, UV etc

Our fake drivers licenses are all scannable, contain original hologram and UV, microprint, laser engraving etc.
Shipping from the US within 48 hours!
We only sell the best quality, you will not find better IDs anywhere.

Product	Price	Quantity
Delaware	200 USD = 0.053 ฿	1 X Buy now
Illinois	200 USD = 0.053 ฿	1 X Buy now

Bitcoin Core

檔案(F)

總覽

餘額

可用金額

未定金額

總金額

選項

主要(M) | 錢包(A) | 網路(N) | 視窗(W) | 顯示(D)

- [ ] 用 UPnP 設定通訊埠對應
- [x] 接受外來連線(G)
- [ ] 透過 SOCKS5 代理伺服器連線(預設代理伺服器 C):

代理位址(I): 127.0.0.1 埠號(P): 9050

用來跟其他節點聯絡的中介: IPv4 IPv6 Tor

- [ ] 透過另外的 SOCKS5 代理伺服器來連線到 Bitcoin 網路中的 Tor 隱藏服務:

代理位址(I): 127.0.0.1 埠號(P): 9050

Options set in this dialog are overridden by the command line or in the configuration file:

無

開啟設定檔

重設選項(R)

好(O) 取消(C)

正在同步前導資料(2.9%)中... 落後 10 年又 26 星期

BTC HD

Tor V2 and Tor V3 address

Bitcoin Address

雜湊函數

- 雜湊函數 = 散列函數 = 哈希函數 = Hash Function
- 包括：
  - 訊息摘要(Message Digest，MD)
  - 安全雜湊演算法(Secure Hash Algorithm，SHA)
  - RIPEMD-160
- 特色
  - **擴散性**(Diffusion)　只要有一個bit的變化就會完全不同
  - **不可逆性**(Irreversible)　如 1TB的檔案做SHA-256 很難反推
  - **抗碰撞性**(Collision resistance)　很難遇到不同的輸入　有同樣的輸出

SHA函式對比

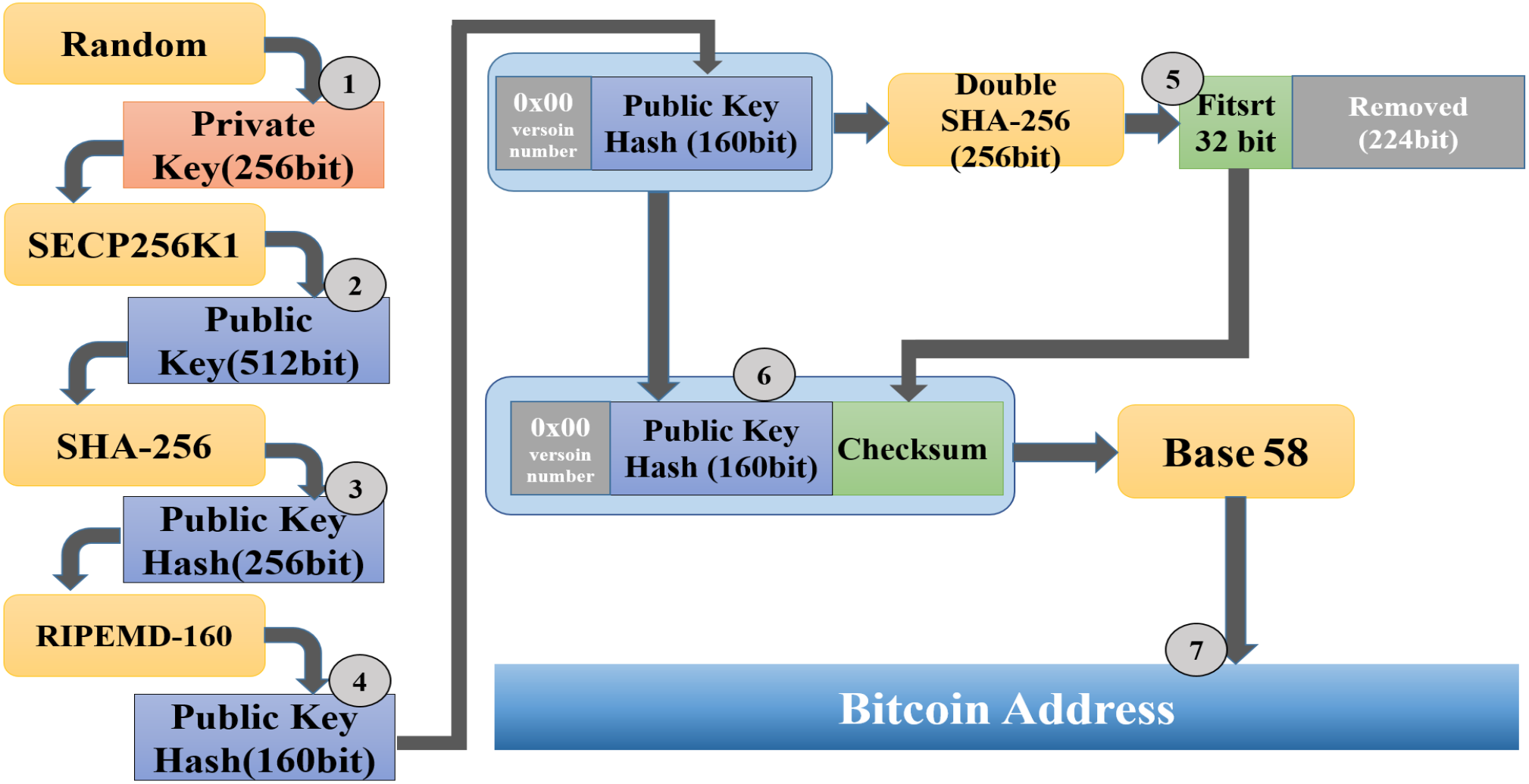
演算法和變體		輸出雜湊值長度（bits）	中繼雜湊值長度（bits）	資料區塊長度（bits）	最大輸入訊息長度（bits）	迴圈次數	使用到的運算子	碰撞攻擊（bits）	效能範例[3] (MiB/s)
MD5（作為參考）		128	128 (4 × 32)	512	無限[4]	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 （發現碰撞）	335
SHA-0		160	160 (5 × 32)	512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<80 （發現碰撞）	-
SHA-1		160	160 (5 × 32)	512	$2^{64} - 1$	80		<80[5] （發現碰撞[6]）	192
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	139
	SHA-384 *SHA-512* *SHA-512/224* *SHA-512/256*	384 512 224 256	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256 112 128	154
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	無限[7]	24[8]	And, Xor, Rot, Not	112 128 192 256	-
	SHAKE128 *SHAKE256*	*d* (arbitrary) *d* (arbitrary)		1344 1088				min(*d*/2, 128) min(*d*/2, 256)	-

Base58

- Base58字母表，Base58就是由不包括（0，O，l，I）的大小寫字母和數字組成。
- 123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

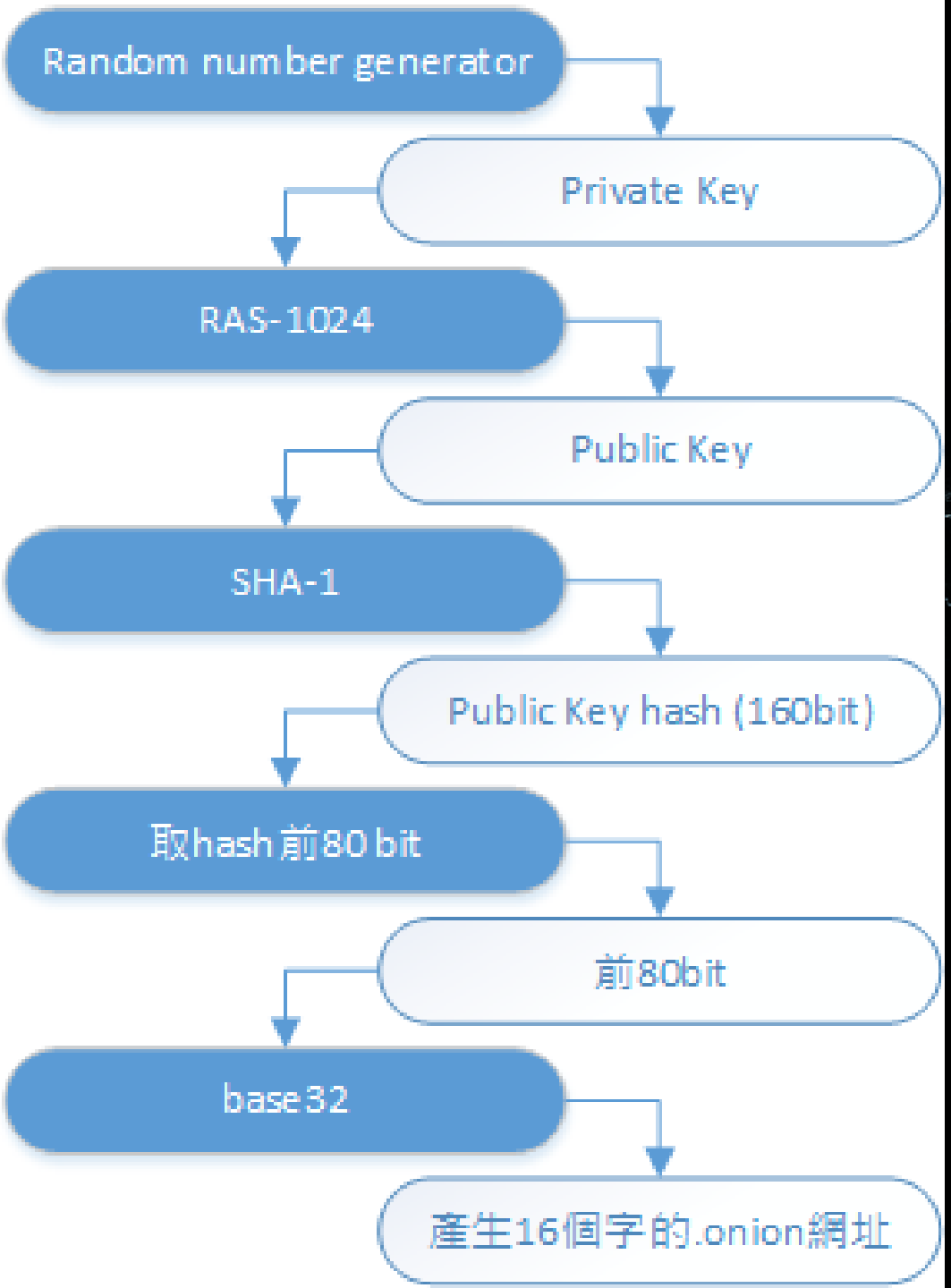
Value	Character	Value	Character	Value	Character	Value	Character
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

Bitcoin Address 生成 過程

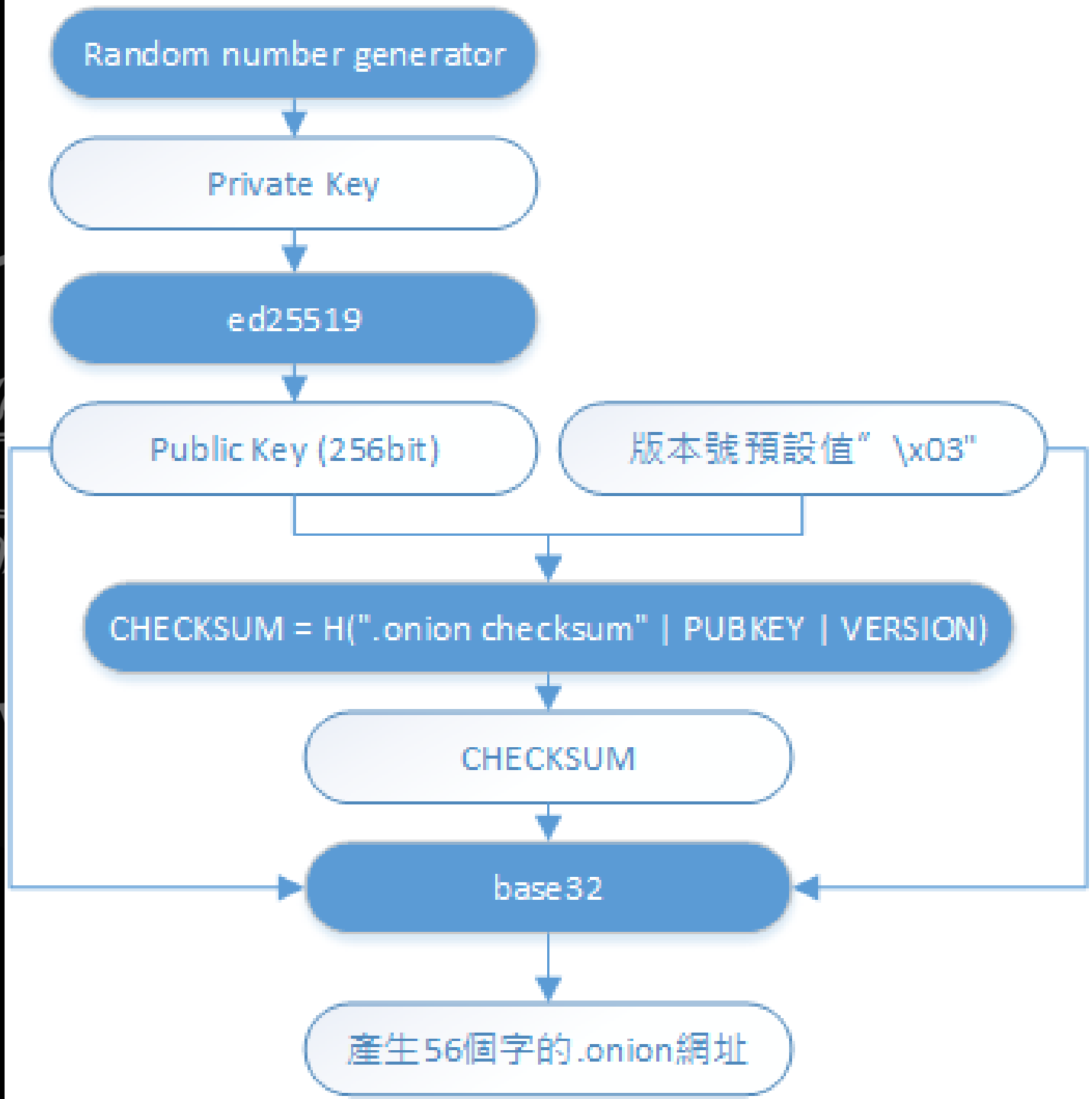


1KwA4fS4uVuCNjCtMivE7m5ATbv93UZg8V

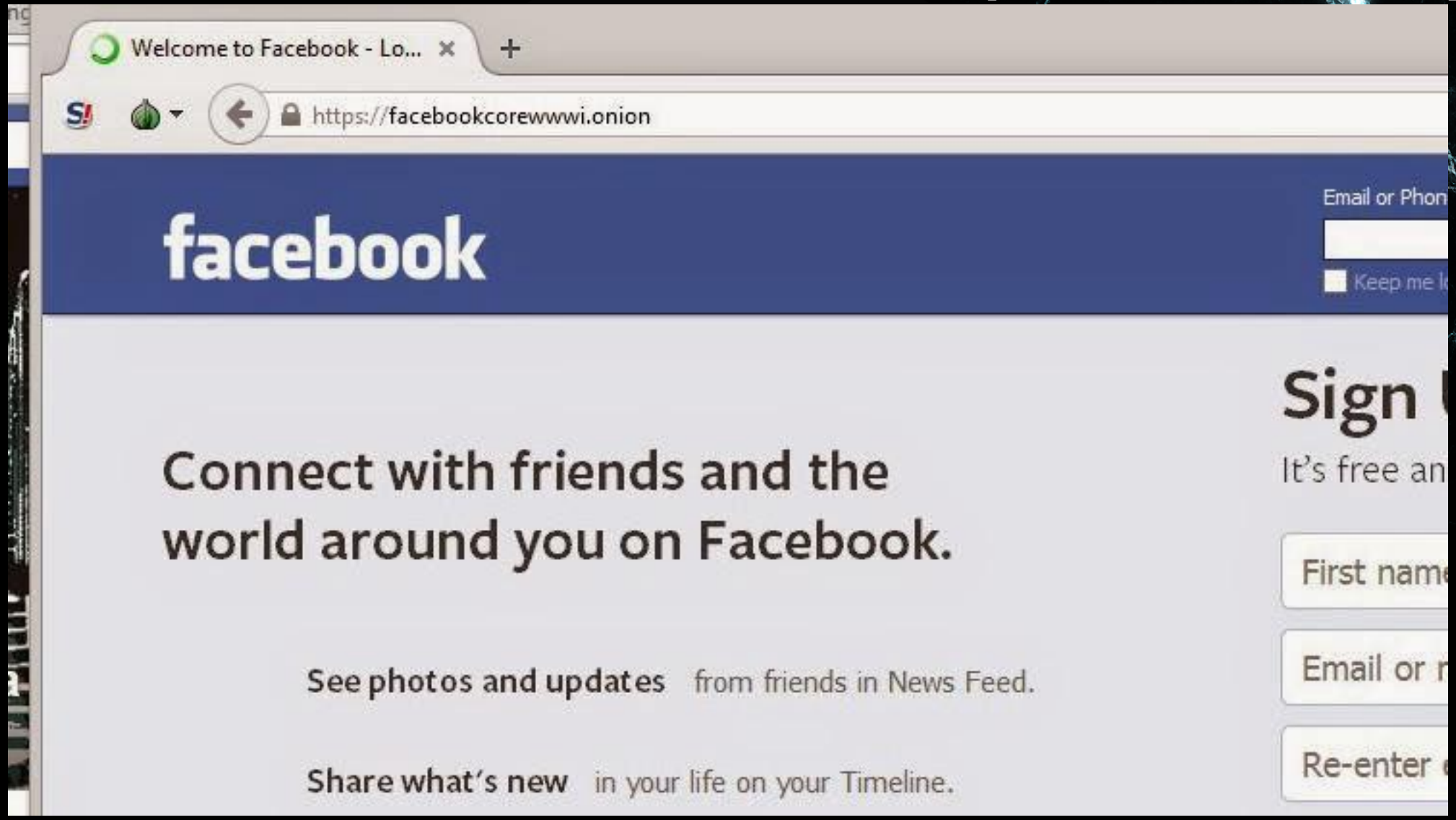
Tor V2 address



TorV3 address



暴力生成美麗的.onion域名(tor v2 & v3)

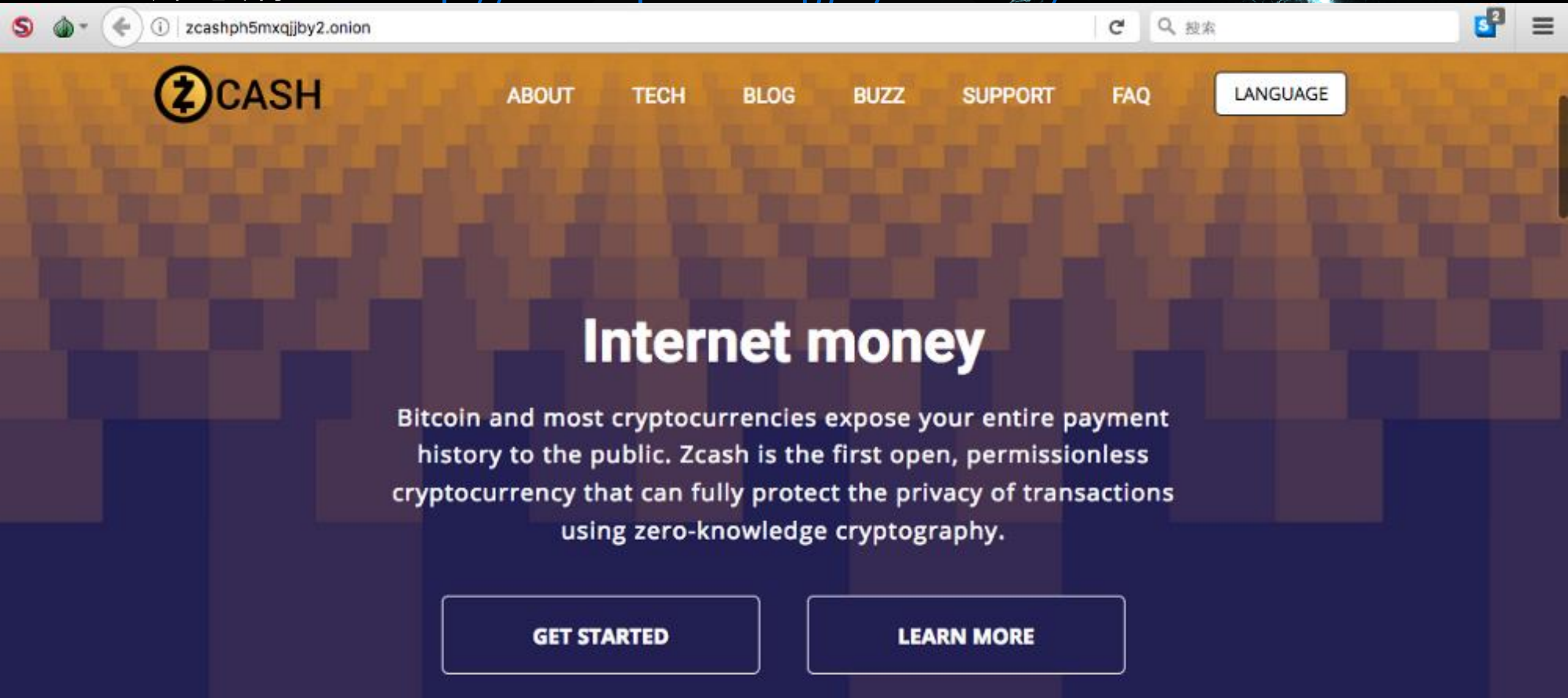


生成所需時間

characters	time to generate (approx.)
1	less than 1 second
2	less than 1 second
3	less than 1 second
4	2 seconds
5	1 minute
6	30 minutes
7	1 day
8	25 days
9	2.5 years
10	40 years
11	640 years
12	10 millenia
13	160 millenia
14	2.6 million years

> *katmagic/Shallot：應該算是早期的版本，用CPU慢慢算*
>
> *lachesis/scallion：開始有人覺得不夠快啦，通通改寫成GPU啦*
>
> *cathugger/mkp224o：因為大家都開始意識到rsa、sha1快要撐不下去了，在今年一月十號左右tor project表示，新的洋蔥v3將會有ecc ，而這個倉庫是以v3 的協議 去做的 爆破*

- 選擇性公開讓大家來看交易內容，與門羅幣不同的是，門羅是以混合為基礎，zcash也是可以不加密。
- 洋蔥網址：http://zcashph5mxqjjby2.onion/



- GreenAddress的簽署，是以一個第三方公正的方式，去保證他簽署過的地址不會是“雙花攻擊”，使得收款的商家可以安心的接受“零確認交易”。
- 洋蔥網址：http://s7a4rvc6425y72d2.onion/en/

- 一個老字號的比特幣區塊鏈檢視器網站，也有自己的錢包服務，做了許多區塊鏈的分析並且畫成圖表。
- 洋蔥地址：https://blockchainbdgpzk.onion/

Blockchain Luxembourg S.A.R.L (LU) | https://blockchainbdgpzk.onion

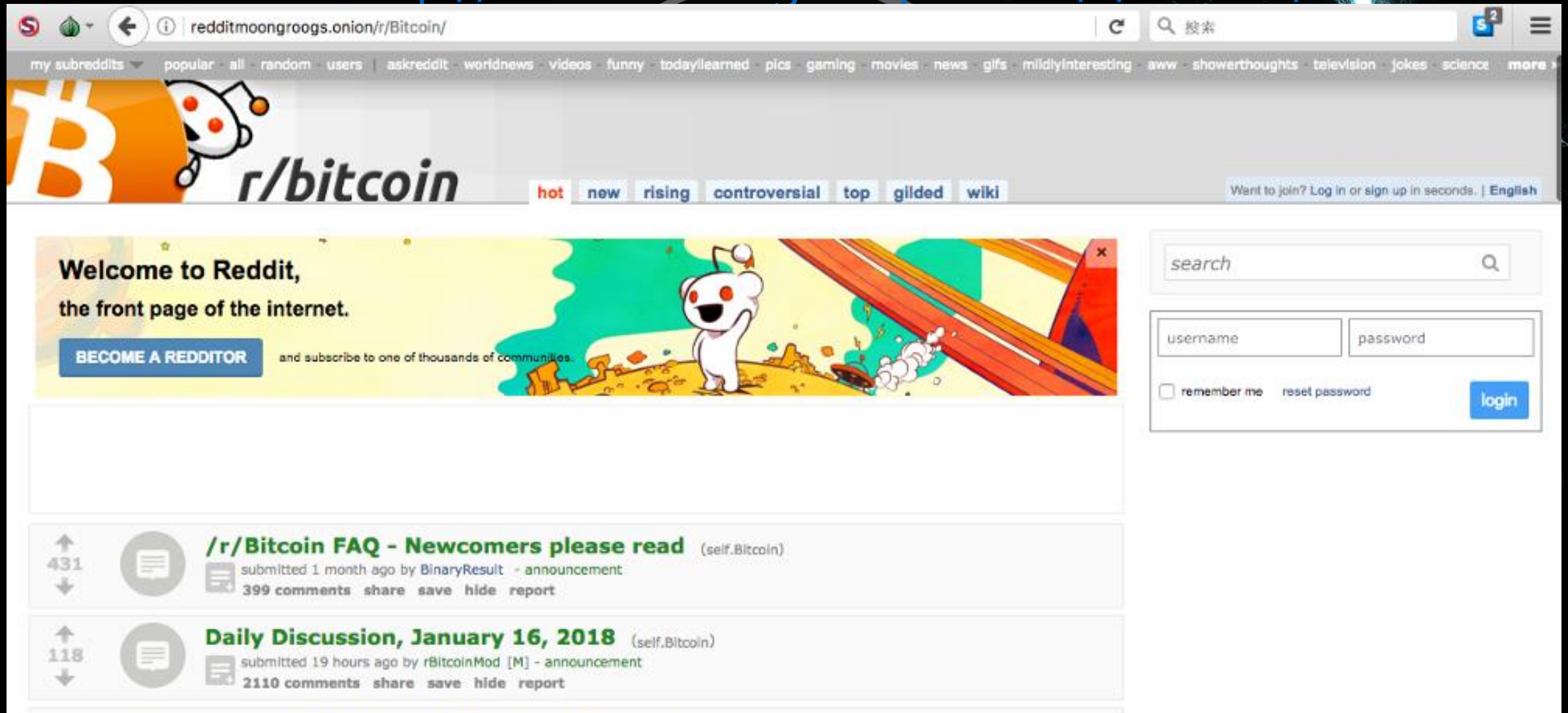
BLOCKCHAIN WALLET DATA API ABOUT BLOCK, HASH, TRANSACTION, ETC... GET A FREE WALLET

LATEST BLOCKS

SEE MORE →

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
504602	4 minutes	2188	20,036.19 BTC	AntPool	1,107.34	3,992.51
504601	19 minutes	2265	30,936.33 BTC	BTC.com	1,074.68	3,992.87
504600	34 minutes	1651	6,332.99 BTC	BTCC Pool	1,092.63	3,992.82
504599	38 minutes	2622	23,924.45 BTC	GBMiners	1,079.33	3,993.04

- 這論壇討論比特幣的程度比bitcointalk來得踴躍很多。這網站因為很注重個人隱私，所以也讓很注重隱私的tor用戶願意在這裡開版。
- 洋蔥地址：http://redditmoongroogs.onion/r/Bitcoin/



暴力生成 個性化Bitcoin 地址 and alt coin

- 效果：1PWChenM8isYz1Z7TpBXdiWn2VDTshPaVr

- [1]https://github.com/samr7/vanitygen
- [2]https://en.bitcoin.it/wiki/Vanitygen
- [3]https://github.com/exploitagency/vanitygen-plus

https://github.com/samr7/vanitygen

基於 CPU 計算

```
Terminal
Fichier  Edition  Affichage  Rechercher  Terminal  Aide
┌─[ ]─[Chiheb@NeXus]─[~/Bureau/vanitygen-master]
└──╼ [>] ./vanitygen 1c
Difficulty: 1353
Pattern: 1c
Address: 1cTfsNtYUKumSharFCKyurX9f6dDsYXy4
Privkey: 5JFHSpPnN7Ky1ZpeLQCNJTMSWkKcB7fmr9M4kvX7Kd1mTngoQWp
┌─[Chiheb@NeXus]─[~/Bureau/vanitygen-master]
└──╼ [>] ./vanitygen 1ch
Difficulty: 78508
Pattern: 1ch
Address: 1chX9kHtsBWfq8jAr8Xehu331qnqGdtEG
Privkey: 5JFbtie16rdVFYNQAWkpJzhFB91Fir7uG2XDDTXyvoLKtpCjFs5
┌─[Chiheb@NeXus]─[~/Bureau/vanitygen-master]
└──╼ [>] ./vanitygen 1chi
Difficulty: 4553521
Pattern: 1chi
Address: 1chiAHAt3hvbXWE7WXrL5ynErUbwVYG21
Privkey: 5J6dKvQDWbRJXT35povuUXbUZZ72TUmGdGYN5VahArYuLqyNQBB
┌─[Chiheb@NeXus]─[~/Bureau/vanitygen-master]
└──╼ [>] |
```

vanity	difficulty	average time
1B	22	< 1s
1Bi	1,330	< 1s
1Bit	77,178	< 1s
1Bitc	4,476,342 (4.48E+6)	< 10s
1Bitco	259,627,881 (2.6E+8)	3 minutes
1Bitcoi	15,058,417,127 (1.506E+10)	3 hours
1Bitcoin	8.7339E+11	1 week
1BitcoinE	5.0657E+13	1 year
1BitcoinEa	2.9381E+15	60 years
1BitcoinEat	1.7041E+17	3,500 years
1BitcoinEate	9.8837E+18	200,000 years
1BitcoinEater	5.7325E+20	11,700,000 years
1BitcoinEaterAddressDontSend	1.6209E+47	3.3E+33 or 3.3 decillion years.

https://github.com/exploitagency/vanitygen-plus

基於 GPU計算 & 多貨幣支持

Current List of Available Coins for Address Generation

Argument(UPPERCASE)	Coin	Address Prefix
42	42coin	4
AC	Asiacoin	A
ACM	Actinium	N
AIB	Advanced Internet Block by IOBOND	A
ANC	Anoncoin	A
ARS	Arkstone	A
ATMOS	Atmos	N
AUR	Auroracoin	A
AXE	Axe	R

Tor: → 出現 .onion → 相似 Bitcoin Address

~~暗網是~~

保護 1) User IP

2) 訪問 service 路徑.

public key = Base 32

出現 .onion

相似 Bitcoin Address

Tor:

~~暗網 ?~~

保護 User IP

Torrent

去中心化

檔案共享.

Torrent

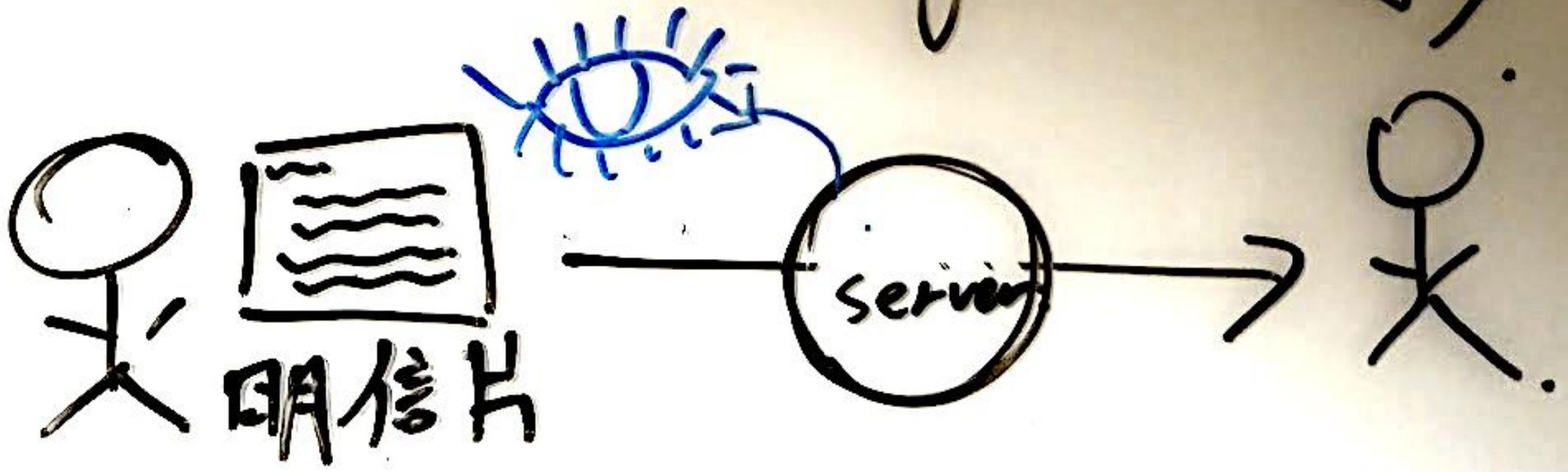
Bitcoin

P2P

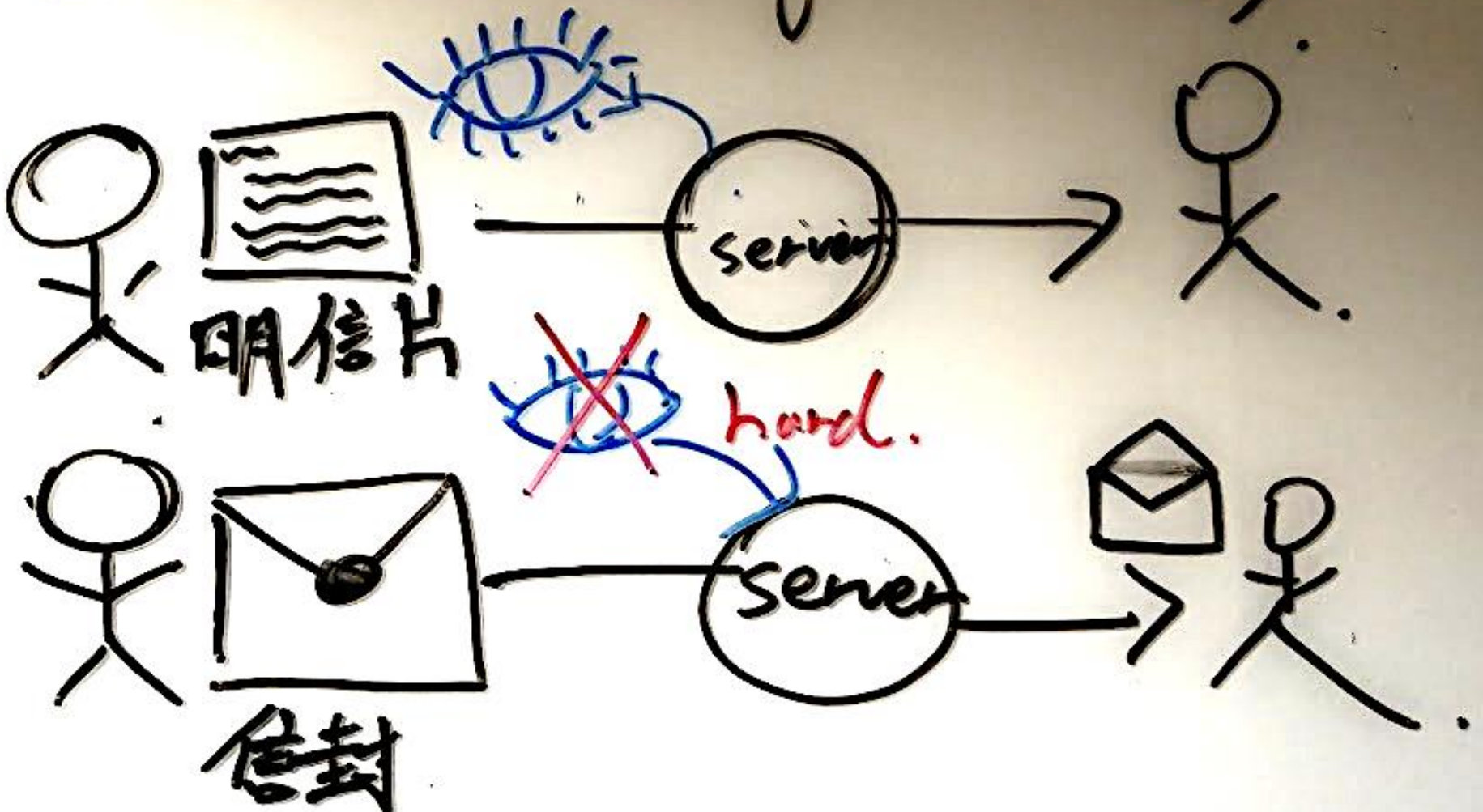
去中心化

檔案共享.

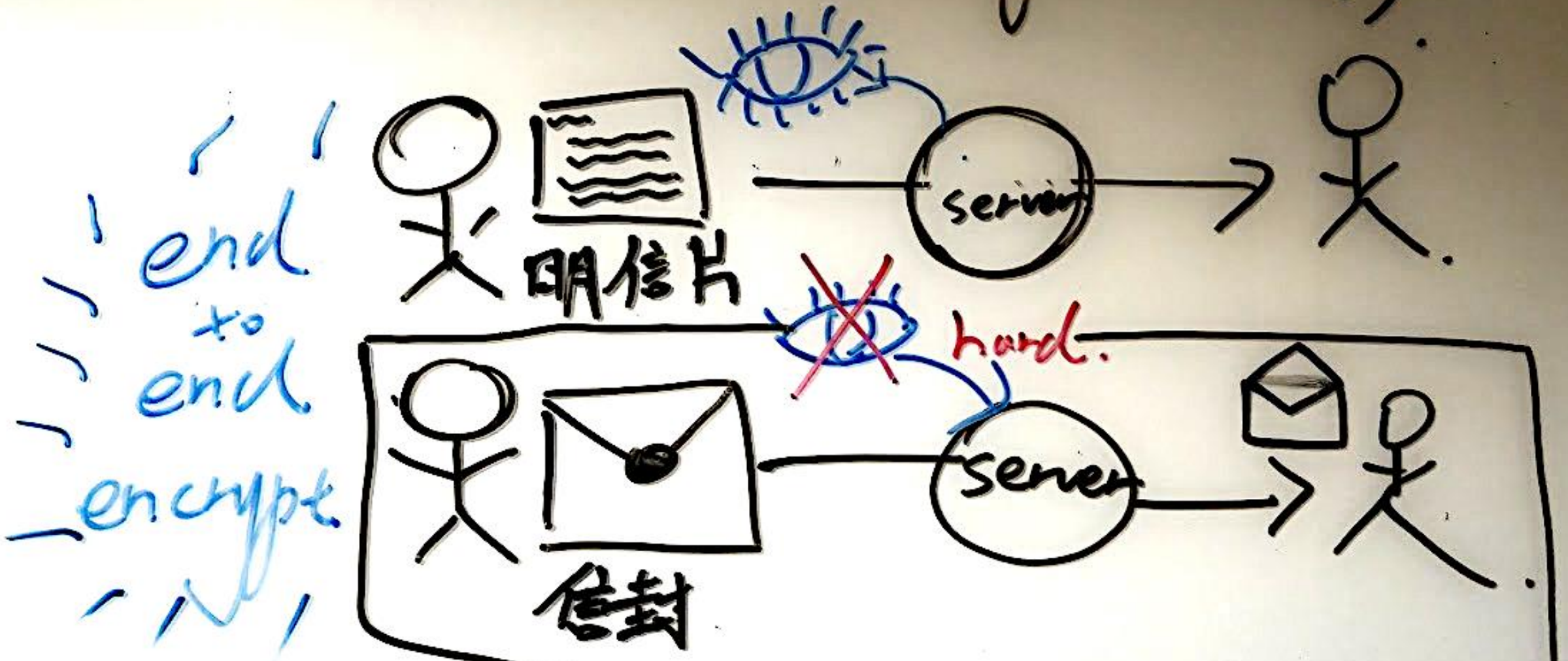
pgp (pretty good privacy)



PGP (pretty good privacy)



pgp (pretty good privacy)



Google

Gmail

More

COMPOSE

Inbox

Starred

Sent Mail

Drafts (5)

More

Test

Electronic Frontier Fo

Electronic Frontier Foundation Software Projects - Tor M...

Electronic Frontier Foundation Soft...

Electronic Frontier Foundation Softwar...

Available

5:29:59 PM – The current conversation is not private.

Electronic Frontier Foundatio...

Secure | https://hangouts.google....

Electronic Frontier Foundation Soft

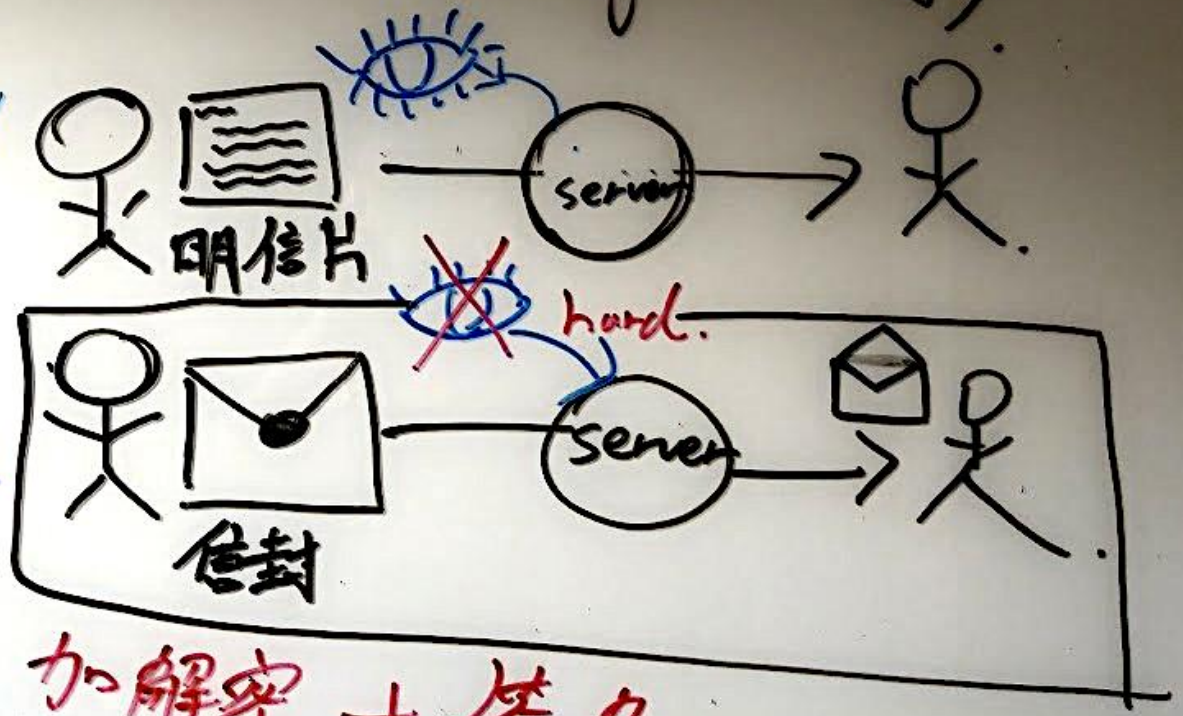
Send a message

n here.

Bitcoin = 簽名

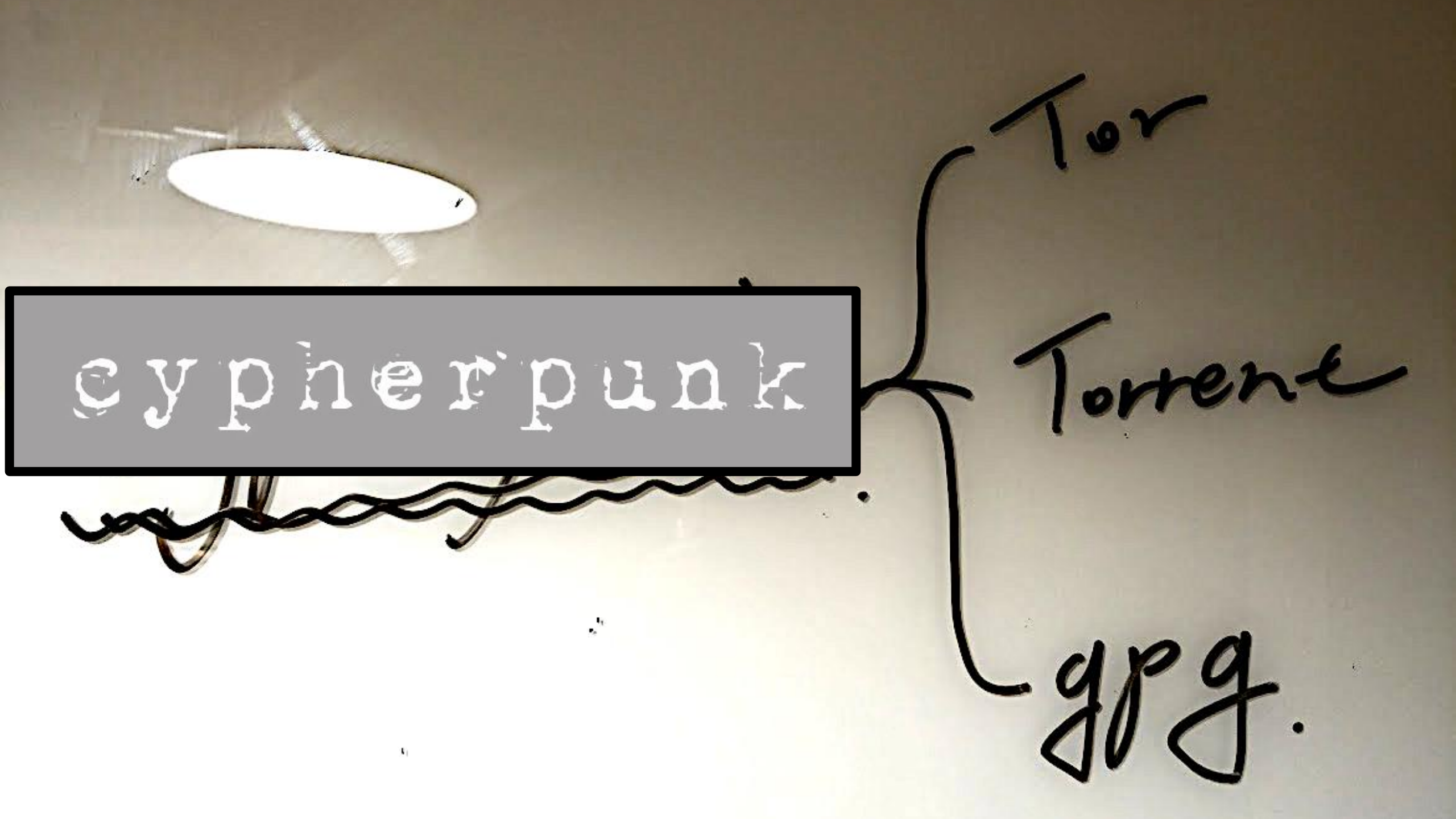
pgp (pretty good privacy)

end to end encrypt



加解密 + 簽名.

end-to-end encrypt.		
default	手動.	Null
1) line.	1) telegram	1) wechat
2) whatsapp	2) Riot	2) QQ
3) signal.	3) Facebook	
4) Keybase		


cypherpunk
Tor
Torrent
gpg.

cypherpunk

- Tor
  - "onion"
- Torrent
  - P2P
- gpg.
  - 签名

cypherpunk

Tor
"onion" ⇒ Address.

Torrent
P2P ⇒ Network.

gpg.
签名 ⇒ Tx

cypherpunk

Bitcoin

- Tor "onion" ⇒ Address
- Torrent P2P ⇒ Network
- gpg 簽名 ⇒ Tx

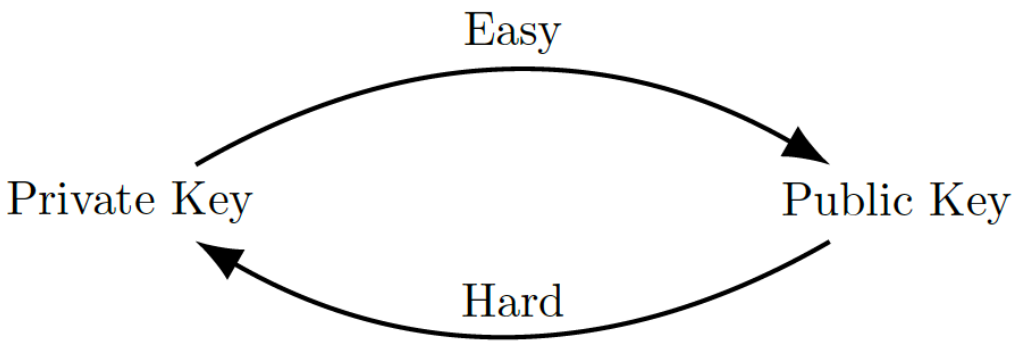
區塊鏈相關技術

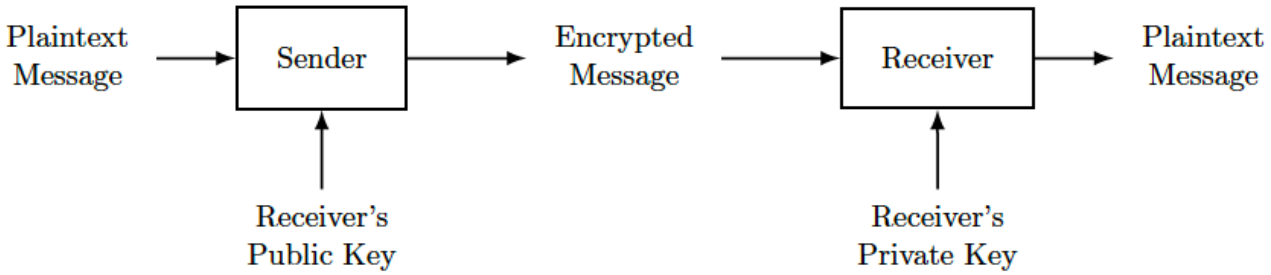
相關技術

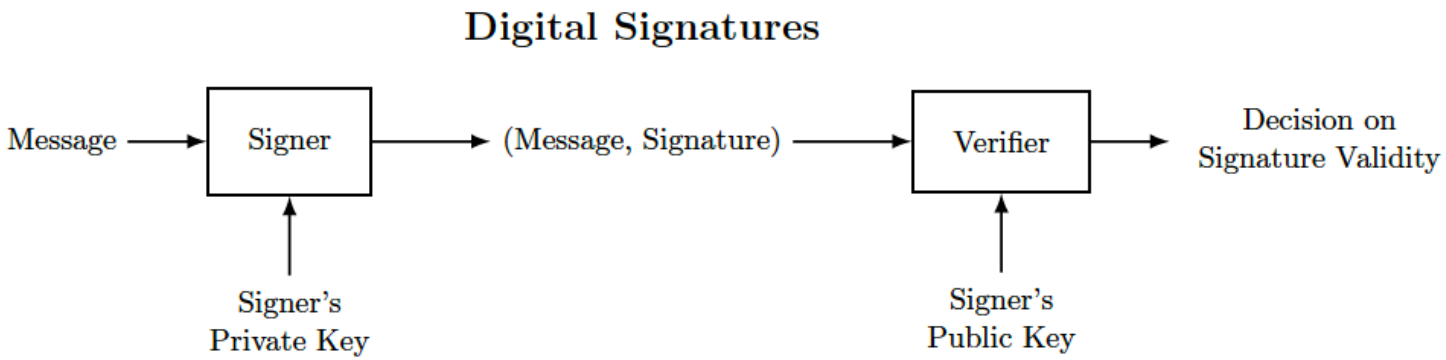
- 密碼學 (Cryptography)
  - 對稱密鑰密碼學(Symmetric key cryptography)
    -~~DES, 3DES~~, AES
  - 非對稱密鑰密碼學(Asymmetric key cryptography)
    -~~RSA~~, ECC
  - Hash=雜湊函數=哈希函數=散列函數
    -~~MD5, SHA-0, SHA-1~~, SHA-2, ~~SHA-3~~
- P2P network

Bitcoin 相關技術

- 密碼學 (Cryptography)
  - 非對稱密鑰密碼學
    - ~~公鑰加密。私鑰解密~~
    - 私鑰簽名。公鑰驗證
  - Hash
- P2P network

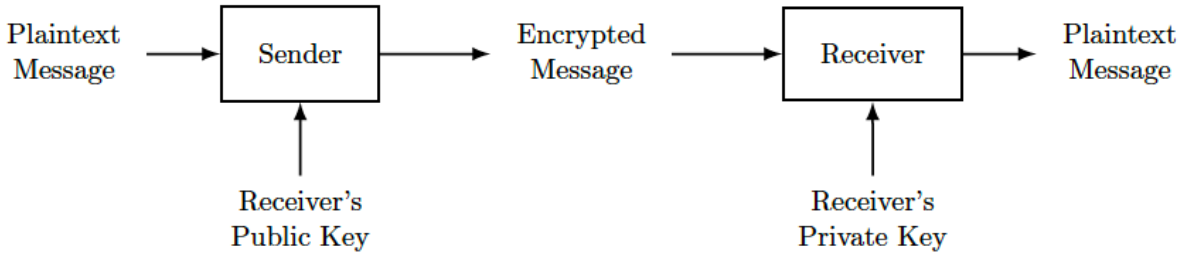


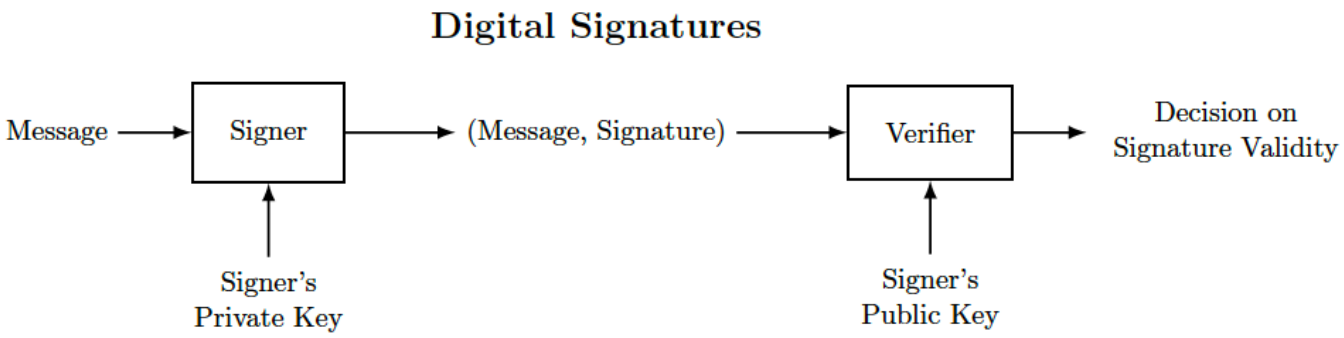




Bitcoin 相關技術

- 密碼學 (Cryptography)
  - 非對稱密鑰密碼學
    - ~~公鑰加密，私鑰解密~~
    - 私鑰簽名，公鑰驗證
      - 生成比特幣地址
      - 簽署比特幣交易
  - Hash
    - Hash Pointer
    - Proof of Work (Mining)
- P2P network





比特幣的開始

比特幣 “論文”

- 2008年11月1日 Satoshi Nakamoto, 發送了一封名為 “Bitcoin P2P e-cash paper” 的電子郵件

- 主要特性：
  - 通過 P2P網路 防止雙重支付。
  - 沒有 造幣廠 或是其他 可信任方 。
  - 參與者可以是匿名的。
  - 新貨幣是由Hashcash類型的工作量證明生成。
  - 新一代貨幣的工作量證明也為網絡提供能量以防止雙重支出。

http://satoshinakamoto.me/2008/11/01/bitcoin-p2p-e-cash-paper/#selection-95.0-107.36

比特幣 “論文”

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. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of

bitcoin taiwan

https://bitcoin.org/bitcoin.pdf

比特幣：一種點對點的電子現金系統

簡中翻譯 李笑來 繁中翻譯 Chen Po Wei

作者：中本聰 satoshin@gmx.com www.bitcoin.org 2008.10.31.

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. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

摘要：一個純粹的點對點版本的電子現金系統，將允許線上支付直接從一方傳送到另一方，而無需通過金融機構。數字簽名雖然提供了部分解決方案，但，若是仍然需要被信任的第三方來防止雙重支付的話，那麼電子支付的主要優勢就被抵消了。我們提出一個方案，使用點對點網路去解決雙重支付問題。點對點網路將為每筆交易標記時間戳，方法是：把交易的雜湊資料錄入一個不斷延展的、以雜湊為基礎的工作量證明鏈上，形成一個如非完全重做就不可能改變的記錄。最長鏈，一方面用來證明已被見證的事件及其順序，與此同時，也用來證明它來自於最大的 CPU 運算能力池。只要絕大多數 CPU 運算能力被良性節點控制 —— 即，它們不與那些嘗試攻擊網路的節點合作 —— 那麼，良性節點將會生成最長鏈，並且在速度上超過攻擊者。這個網路本身需要最小化的結構。資訊將以最大努力為基本去傳播，節點來去自由；但，加入之時總是需要接受最長的工作量證明鏈作為它們未參與期間所發生之一切的證明。

https://github.com/ChenPoWei/bitcoin_whitepaper_zh

比特幣 “第一個版本”

- 2009年1月3日 Satoshi Nakamoto, 發布了"Bitcoin v0.1 released”
- 一開始的Bitcoin 是託管在 sourceforge 上
  - https://sourceforge.net/p/bitcoin/news/2009/01/bitcoin-v01-released---p2p-e-cash/

Bitcoin does not use any encryption.
by Satoshi Nakamoto

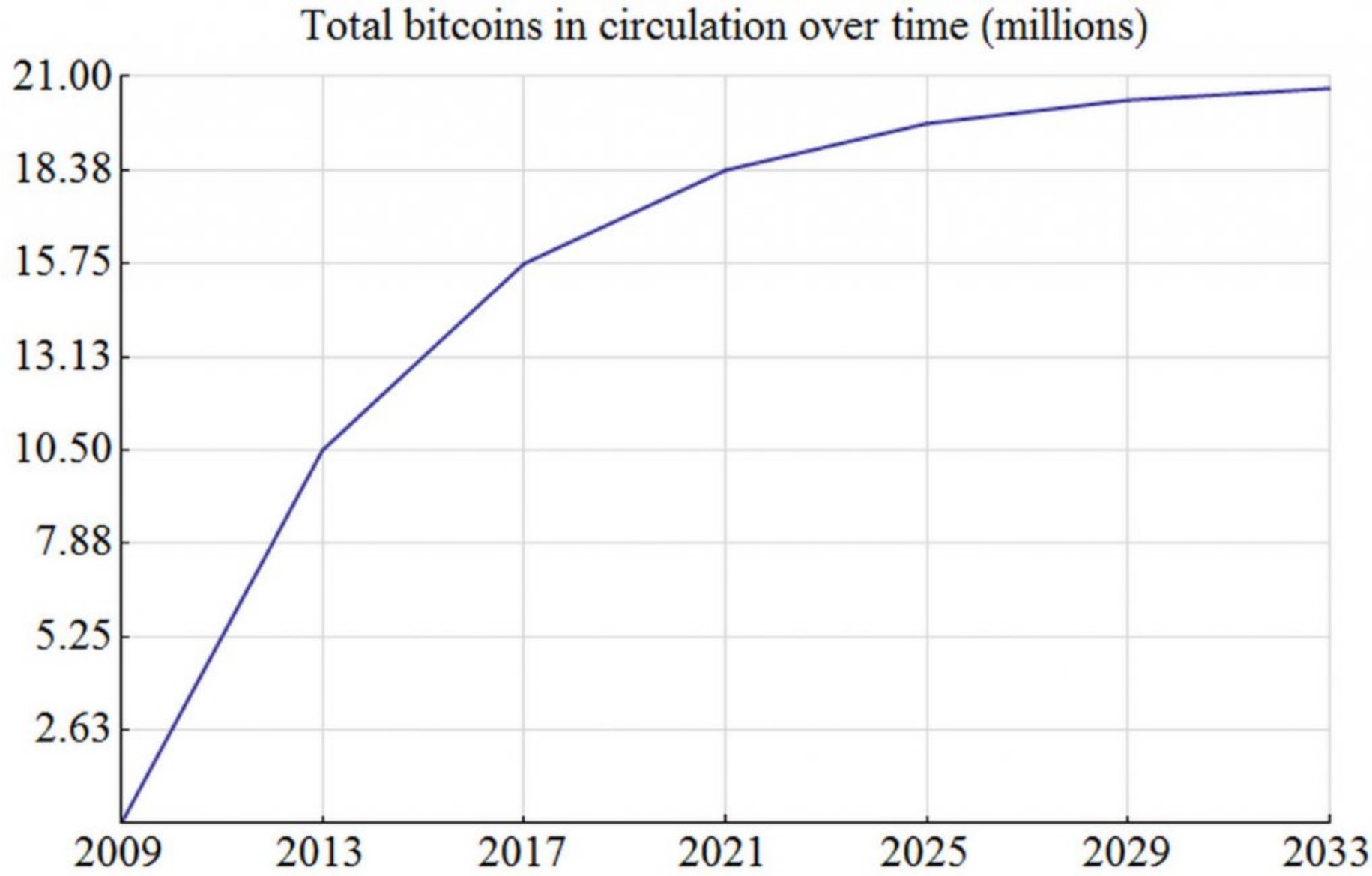
```
BitCoin v0.1.5 ALPHA

Copyright (c) 2009 Satoshi Nakamoto
Distributed under the MIT/X11 software license, see the accompanying
file license.txt or http://www.opensource.org/licenses/mit-license.php.
This product includes software developed by the OpenSSL Project for use in
the OpenSSL Toolkit (http://www.openssl.org/).  This product includes
cryptographic software written by Eric Young (eay@cryptsoft.com).


Compilers Supported
-------------------
MinGW GCC (v3.4.5)
Microsoft Visual C++ 6.0 SP6


Dependencies
------------
Libraries you need to obtain separately to build:

              default path   download
wxWidgets      \wxWidgets     http://www.wxwidgets.org/downloads/
OpenSSL        \OpenSSL       http://www.openssl.org/source/
Berkeley DB    \DB            http://www.oracle.com/technology/software/products/berkeley-db/index.html
Boost          \Boost         http://www.boost.org/users/download/

Their licenses:
wxWidgets      LGPL 2.1 with very liberal exceptions
OpenSSL        Old BSD license with the problematic advertising requirement
Berkeley DB    New BSD license with additional requirement that linked software must be free open source
Boost          MIT-like license


OpenSSL
-------
Bitcoin does not use any encryption.  If you want to do a no-everything
build of OpenSSL to exclude encryption routines, a few patches are required.
(OpenSSL v0.9.8h)
```

比特幣簡介

論文發佈	2008年11月1日	挖礦類型	Proof of Work
開始時間	2009年1月3日	雜湊函數	SHA-256
貨幣總量	趨近2100顆	出塊時間	平均10分鐘
維護團隊	BitcoinCore	開源軟體	MIT license
託管平台	Github	開發作者	SatoshiNakamoto

bitcoin taiwan

總發行量為 2100萬個



比特幣 “第一個區塊”

Block #0

BlockHash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Summary

Number Of Transactions	1	**Difficulty**	1
Height	0 (Mainchain)	**Bits**	1d00ffff
Block Reward	50 BTC	**Size (bytes)**	285
Timestamp	Jan 4, 2009 2:15:05 AM	**Version**	1
Mined by		**Nonce**	2083236893
Merkle Root	4a5e1e4baab89f3a32518a8...	**Next Block**	1

https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

bitcoin taiwan

比特幣“第一筆交易”

Summary

Height	0	Version	1	Block Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	558,506	Difficulty	2.54 K / 1.00	Prev Block	N/A
Size	285 Bytes	Bits	0x1d00ffff	Next Block	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Stripped Size	285 Bytes	Nonce	0x7c2bac1d	Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Weight	1,140	Relayed By	unknown		V 1
Tx Count	1	Time	2009-01-04 02:15:05	Other Explorers	BLOCKCHAIR

Transactions

Sort: Tx block id | Tx hash | Fee | Sigops | Size | Weight | Inputs count | Inputs value | Outputs count | Outputs value | Witness hash

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b 0.00000000 BTC 2009-01-04 02:15:05

Coinbase → 1A1zP1eP5QGefi2... (Genesis of B...) 50.00000000

50.00000000

https://www.blockchain.com/btc/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

比特幣“第一則訊息”

- Base16：04ffff001d01044554686520546 96d65732030332f4a616e2f3230303920436861 6e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73
- Base64：BP//AB0BBEVUaGUgVGltZXMgMDMvSmFuLzIwMDkgQ2hhbmNlbGxvciBvbiBicmluayBvZiBzZWNvbmQgYmFpbG91dCBmb3IgYmFua3M=

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

https://www.blockchain.com/btc/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Bitcoin.org

誰擁有bitcoin.org？

開始 1

2011-2012 2

2014 3

今天 4

Satoshi Nakamoto和Martti Malmi

Bitcoin.org最初由比特幣的前兩位開發商Satoshi Nakamoto和Martti Malmi註冊並擁有。當Nakamoto離開項目時，他將域名的所有權交給了與比特幣開發者分開的其他人，以分散責任並防止任何一個人或團隊輕易獲得對比特幣項目的控制權。

bitcoin taiwan

誰擁有bitcoin.org？

開始 1

2011-2012 2

2014 3

今天 4

BitcoinCore

從2011年到2013年，該網站主要用於發布現在稱為BitcoinCore的軟件的新版本。2013年，該網站進行了重新設計，添加了大量頁面，列出了額外的比特幣軟件，並創建了翻譯系統。

bitcoin taiwan

誰擁有bitcoin.org？

開始 1

開發人員文檔於2014年添加

歡迎來自社區成員的更新，修復，建議和改進。

2011-2012 2

Site是一個獨立的開源項目

今天，該網站是一個獨立的開源項目，來自世界各地的貢獻者。最終發布權限由共同所有者持有，但所有常規活動都是通過公共拉取請求流程組織的，並由站點共同維護者管理。

2014 3

今天 4

bitcoin taiwan

bitcoin

介紹 資源 創新 參與 常見問題

Bitcoin 是一個創新的支付網路以及一種新的貨幣。

開始使用 Bitcoin

選擇你的錢包

What is Bitcoin?

https://bitcoin.org/zh_TW/

2014-04-08

Bitcoin Core version 0.9.1 released

Read more

2014-03-19

Bitcoin Core version 0.9.0 released

Read more

2013-12-09

Bitcoin-Qt version 0.8.6 released

Read more

2013-09-13

Bitcoin-Qt version 0.8.5 released

Read more

BitcoinCore

BitcoinCore

- BitcoinCore是一個開源項目，維護和發布名為“BitcoinCore”的比特幣客戶端軟件。
- 它是Satoshi Nakamoto在發佈著名的比特幣白皮書後發布的原始比特幣軟件客戶端的直系後代。
- BitcoinCore包括“全節點”軟體，用於完全驗證區塊鏈以及比特幣錢包。該項目目前還維護相關軟件，如加密庫libsecp256k1和其他位於GitHub的軟件。

Bitcoin Core

ABOUT DOWNLOAD BLOG RELEASES FAQS DEVELOPMENT CONTACT

English

Recent Posts

Bitcoin Core 0.17.1 Released

Bitcoin Core 0.17.1, a maintenance release bringing bug fixes and minor improvements, is now available.

Bitcoin Core 0.17.0 Released

We're pleased to announce the release of Bitcoin Core 0.17, a major new version containing many new features as well as bug fixes and other improvements.

CVE-2018-17144 Full Disclosure

https://bitcoincore.org/

Bitcoin 於github 的倉庫

bitcoin / **bitcoin**

Watch 3,379 | Star 32,646 | Fork 19,626

Code | Issues 545 | Pull requests 265 | Projects 7 | Insights

Bitcoin Core integration/staging tree https://bitcoin.org/en/download

bitcoin c-plus-plus p2p cryptocurrency cryptography

17,420 commits | **7** branches | **197** releases | **551** contributors | MIT

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

jonasschnelli Merge #13439: rpc: Avoid "duplicate" return value for invalid submitb... ··· Latest commit 3f398d7 a day ago

.github	Make default issue text all comments to make issues more readable	7 months ago
.tx	tx: Update transifex slug for 0.16	5 months ago

什麼是BIP？

- BIP 代表 “比特幣改進提案”
- BIP 是一種設計文檔，為比特幣社區提供信息或描述比特幣或其流程或環境的新功能
- BIP 應提供該功能的**簡明技術規範**和**該功能的基本原理**

BIP有三種

- 標準跟踪BIP描述了影響大多數或所有比特幣實施的任何變更，例如
  - 網路協議、區塊、交易有效性規則、交互
- 描述比特幣設計問題，或向比特幣社區提供一般指導，但不提出新功能。
- 流程BIP描述了圍繞比特幣的流程，或者建議改變流程（或交易）。

Number	Layer	Title	Owner	Type	Status
1		BIP Purpose and Guidelines	Amir Taaki	Process	Replaced
2		BIP process, revised	Luke Dashjr	Process	Active
8		Version bits with lock-in by height	Shaolin Fry	Informational	Draft
9		Version bits with timeout and delay	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	Informational	Final
10	Applications	Multi-Sig Transaction Distribution	Alan Reiner	Informational	Withdrawn
11	Applications	M-of-N Standard Transactions	Gavin Andresen	Standard	Final
12	Consensus (soft fork)	OP_EVAL	Gavin Andresen	Standard	Withdrawn

已經實行的BIP

- BIP: 11 Title: M-of-N Standard Transactions
- BIP: 22 Title: getblocktemplate - Fundamentals
- BIP: 23 Title: get
- BIP: 32 Title: Hierarchical Deterministic Wallets blocktemplate - Pooled Mining
- BIP: 37 Title: Connection Bloom filtering
- BIP: 42 Title: A finite monetary supply for Bitcoin
- BIP: 50 Title: March 2013 Chain Fork Post-Mortem

> A successful DOUBLE SPEND US$10000 against OKPAY this morning.

已經實行的BIP

- BIP: 70, 71, 72, 73 Payment Protocol
- BIP: 91, 141, 143, 144, 145, 147, 148 segwit

比特幣的區塊鏈, 區塊, 交易

Height ...	Time	Miner	# tx	Block Value	Total Fees	Size
528,343	4m ago - 20-Jun 17:52	Unknown	841	2,505.05575921	1.37753575	985,857 B
528,342	7m ago - 20-Jun 17:50	Unknown	2074	11,390.46648083	1.81488291	950,607 B
528,341	25m ago - 20-Jun 17:32	Unknown	2239	9,268.41368369	1.70567569	940,643 B
528,340	40m ago - 20-Jun 17:16	Unknown	1360	4,897.24872002	1.80000492	962,899 B
528,339	50m ago - 20-Jun 17:07	Slush	1964	12,042.46277209	1.62265418	960,874 B
528,338	56m ago - 20-Jun 17:01	Unknown	1906	6,210.30767808	1.64552247	962,671 B
528,337	57m ago - 20-Jun 17:00	F2Pool	2161	11,939.13530581	2.02098421	940,242 B
528,336	1h 09m ago - 20-Jun 16:47	Unknown	863	3,420.28980220	2.09191382	948,850 B
528,335	1h 16m ago - 20-Jun 16:40	Unknown	880	3,986.74517838	2.16830965	972,063 B
528,334	1h 26m ago - 20-Jun 16:31	AntPool	984	5,755.03560284	2.36948038	962,973 B
528,333	1h 49m ago - 20-Jun 16:08	Unknown	334	1,827.13524539	2.06183228	990,685 B
528,332	1h 55m ago - 20-Jun 16:02	AntPool	670	3,149.85127925	2.42199304	980,942 B
528,331	2h 09m ago - 20-Jun 15:47	Slush	323	1,936.73753814	2.19454876	988,511 B

‹ Block 528,343

Technical

Block	06/20/18 17:52:51 (12 minutes ago)
Time	
Confirmations	1
Miner	Unknown
Chain	Main
Hash	0000000000000000028e98ab056e5d047578813063a4f380bf1e4976adffbc0
Difficulty	5.08T
Nonce	4,119,056,028
Size	985,857 B
Fee/size	139.72977318 sat/B
Version	536870912

Monetary

Transaction Count	841
Avg. Transaction	2.96568836
Volume	
Transaction Volume	2,491.17822346
Mining Fees	1.37753575
Block Reward	12.50000000
Output Volume	2,505.05575921
Price (XBX)	$6643.34

Date	Inputs	Outputs			Fee	Size	Tx Hash
06/20/18 17:52	Coinbase		2 outputs	13.87753575	0.00000000	207	7bad...
06/20/18 17:51	1 input	-15.92003183	6 outputs	15.91786081	0.00217102	391	2f18b...
06/20/18 17:51	3 inputs	-0.01359914	2 outputs	0.01077906	0.00282008	521	bc7b...
06/20/18 17:51	2 inputs	-0.40586000	1 output	0.40483000	0.00103000	172	8a62...
06/20/18 17:50	1 input	-1.49079799	5 outputs	1.48979839	0.00099960	236	d358...
06/20/18 17:51	1 input	-4.77279566	2 outputs	4.77227548	0.00052018	116	d46d...
06/20/18 17:50	1 input	-1.09495930	2 outputs	1.09424740	0.00071190	226	4463f...
06/20/18 17:50	2 inputs	-0.04304856	2 outputs	0.04187426	0.00117430	373	c418...
06/20/18 17:51	1 input	-0.09130000	2 outputs	0.09028864	0.00101136	335	ea56...
06/20/18 17:52	3 inputs	-0.00749911	2 outputs	0.00592789	0.00157122	521	80da...
06/20/18 17:51	1 input	-0.52875489	2 outputs	0.52807463	0.00068026	226	d326...
06/20/18 17:50	2 inputs	-1.01528015	2 outputs	1.01428015	0.00100000	372	ef323...
06/20/18 17:50	2 inputs	-8.76847094	2 outputs	8.76747094	0.00100000	373	543d...
06/20/18 17:51	1 input	-0.10900000	1 output	0.10850000	0.00050000	190	e70b...

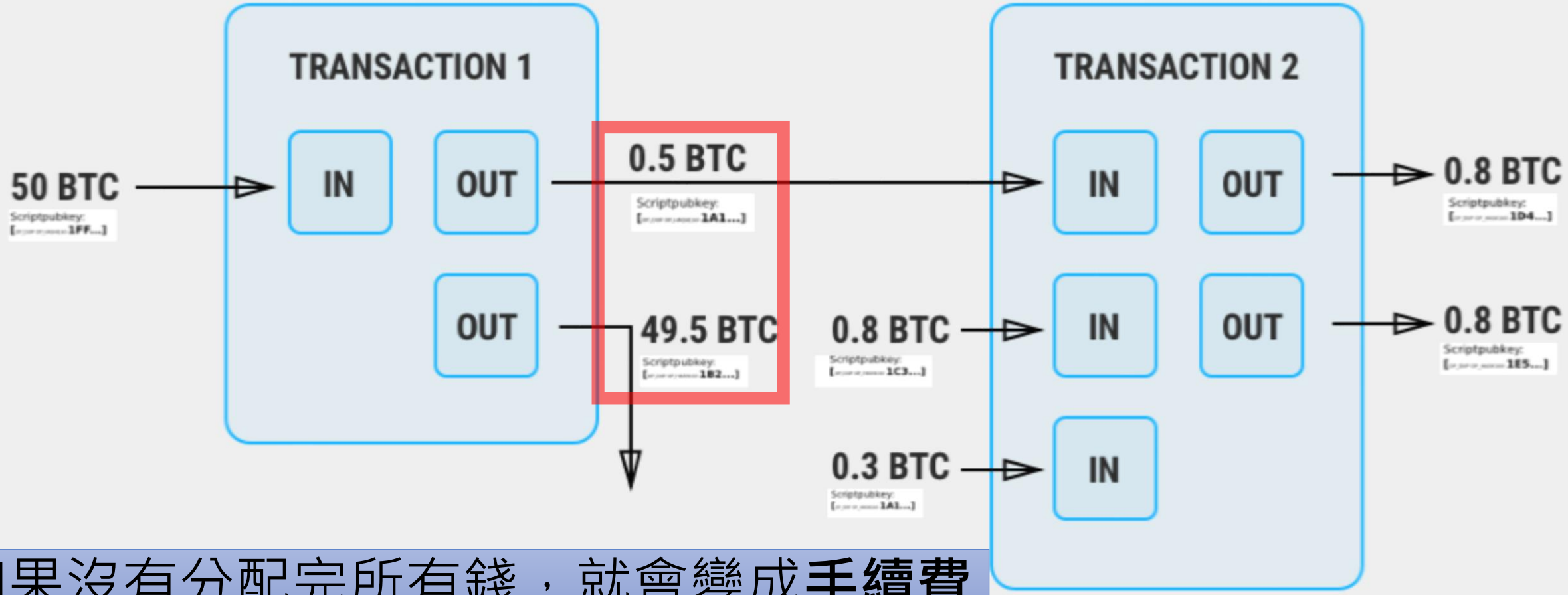
Mining Fees	1.37753575
Block Reward	12.50000000

Date	Inputs	Outputs		Fee	Size	Tx Hash
06/20/18 17:52	Coinbase	2 outputs	13.87753575	0.00000000	207	7bad…
	Coinbase	1C1mCxRukix1KfegAY5zQQJV7s…	13.87753575			
		Nonstandard	0.00000000			
		Fee	0.00000000			

Date	Inputs		Outputs		Fee	Size	Tx Hash
06/20/18 17:51	1 input	-15.920031836	6 outputs	15.91786081	0.00217102	391	2f18b…
	< 17A16QmavnUfCW11DAApiJxp7…	-15.920031831	1E9eDiY9BM8thoCyAr1f25kLyeLk…	> 0.01086559			
			3JhosXz884M4fHTXrbQB76pVHP…	0.02256391			
			1HpXPHkGFQPaehe6cZ9vWCiihA…	0.06000000			
			1KGxbjLAetieW37zk9dUPzkZS3U…	0.29950000			
			1N6hxno8Gfm7mJwbR8urtR5NM…	3.74950000			
			17A16QmavnUfCW11DAApiJxp7…	>11.77543131			
			Fee	0.00217102			
			Hide outputs				
06/20/18 17:51	3 inputs	-0.01359914	2 outputs	0.01077906	0.00282008	521	bc7b…
	< 1GpaAsKqPbr9dR72zfVzH2XYxJ…	-0.00686667	1LPWwMmaP283169a5gHNghpS…	0.01074761			
	< 14SFTEWKsUhpeMDHg9p7no3ut…	-0.00163333	16bQFAeXtWtk3SkCowr7frC4q6m…	0.00003145			
	< 1N6NHcwypFavYfZKRKQR228zZ…	-0.00509914	Fee	0.00282008			
06/20/18 17:51	2 inputs	-0.40586000	1 output	0.40483000	0.00103000	172	8a62…
	< 3989V1uCKhP1N3yM2Xnubs9f3r…	-0.07546000	17hDkWDhknAPdo93KfzC4Vuahi…	0.40483000			
	< 32QYcpCVFsXhcSC9rXJBQ2FeN…	-0.33040000	Fee	0.00103000			
06/20/18 17:50	1 input	-1.49079799	5 outputs	1.48979839	0.00099960	236	d358…
06/20/18 17:51	1 input	-4.77279566	2 outputs	4.77227548	0.00052018	116	d46d…

比特幣的交易

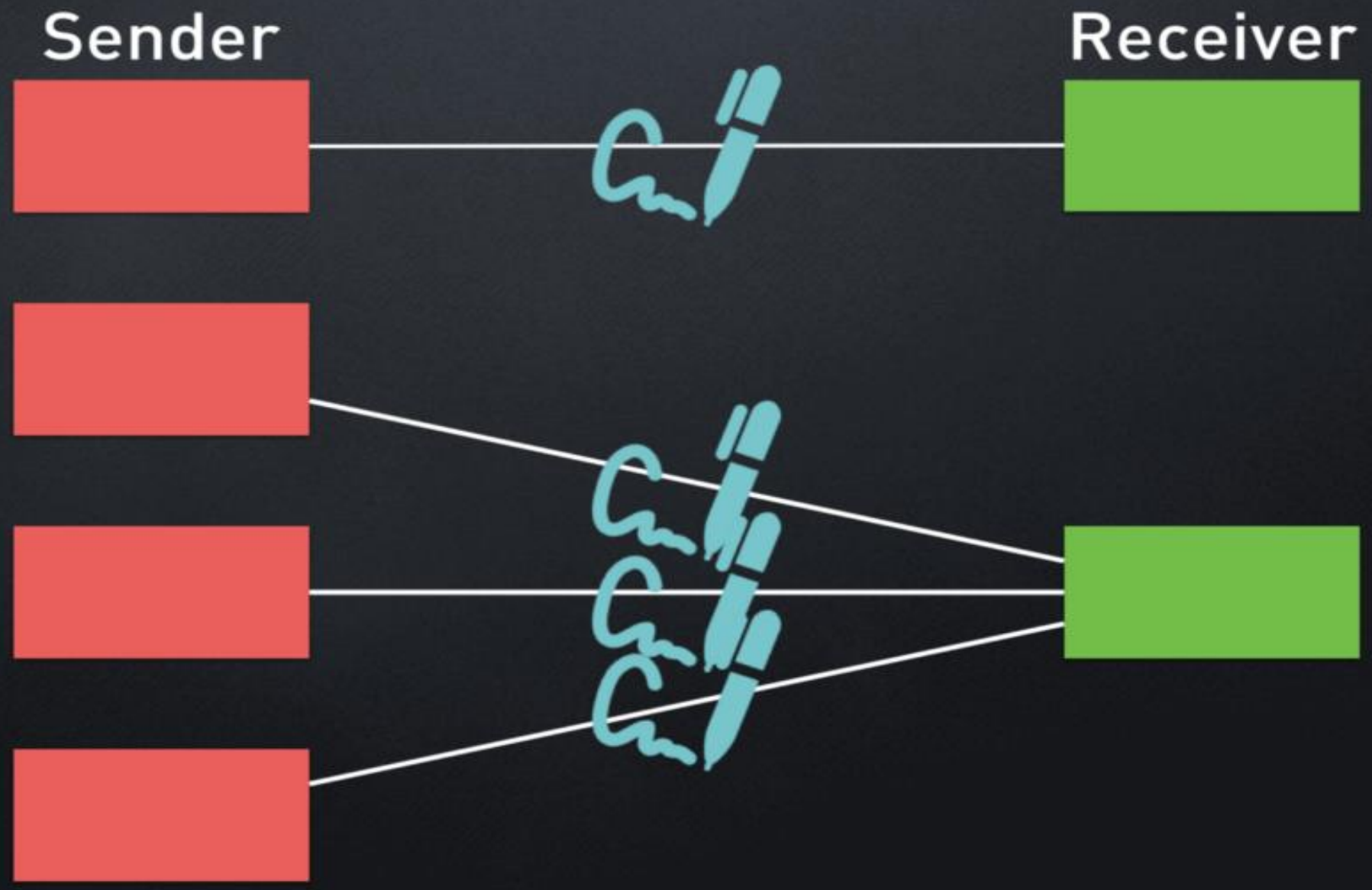
https://steemit.com/eos/@iang/the-message-is-the-medium



如果沒有分配完所有錢，就會變成**手續費**

Figure 4 - The UTXO or Unspent Transaction Outputs Model

Date	Inputs		Outputs		Fee	Size	Tx Hash
06/20/18 17:51	1 input	-15.92003183	6 outputs	15.91786081	0.00217102	391	2f18b…
	< 17A16QmavnUfCW11DAApiJxp7…	-15.92003183	1E9eDiY9BM8thoCyAr1f25kLyeLk…	> 0.01086559			
			3JhosXz884M4fHTXrbQB76pVHP…	0.02256391			
			1HpXPHkGFQPaehe6cZ9vWCiihA…	0.06000000			
			1KGxbjLAetieW37zk9dUPzkZS3U…	0.29950000			
			1N6hxno8Gfm7mJwbR8urtR5NM…	3.74950000			
			17A16QmavnUfCW11DAApiJxp7…	>11.77543131			
			Fee	0.00217102			
			Hide outputs				
06/20/18 17:51	3 inputs	-0.01359914	2 outputs	0.01077906	0.00282008	521	bc7b…
	< 1GpaAsKqPbr9dR72zfVzH2XYxJ…	-0.00686667	1LPWwMmaP283169a5gHNghpS…	0.01074761			
	< 14SFTEWKsUhpeMDHg9p7no3ut…	-0.00163333	16bQFAeXtWtk3SkCowr7frC4q6m…	0.00003145			
	< 1N6NHcwypFavYfZKRKQR228zZ…	-0.00509914	Fee	0.00282008			
06/20/18 17:51	2 inputs	-0.40586000	1 output	0.40483000	0.00103000	172	8a62…
	< 3989V1uCKhP1N3yM2Xnubs9f3r…	-0.07546000	17hDkWDhknAPdo93KfzC4Vuahi…	0.40483000			
	< 32QYcpCVFsXhcSC9rXJBQ2FeN…	-0.33040000	Fee	0.00103000			
06/20/18 17:50	1 input	-1.49079799	5 outputs	1.48979839	0.00099960	236	d358…
06/20/18 17:51	1 input	-4.77279566	2 outputs	4.77227548	0.00052018	116	d46d…


Sender
Receiver

比特幣區塊鏈的分佈,大小,版本

比特幣區塊鏈的分佈

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Jun 20 2018 19:47:20 GMT+0800 (中國標準時間).

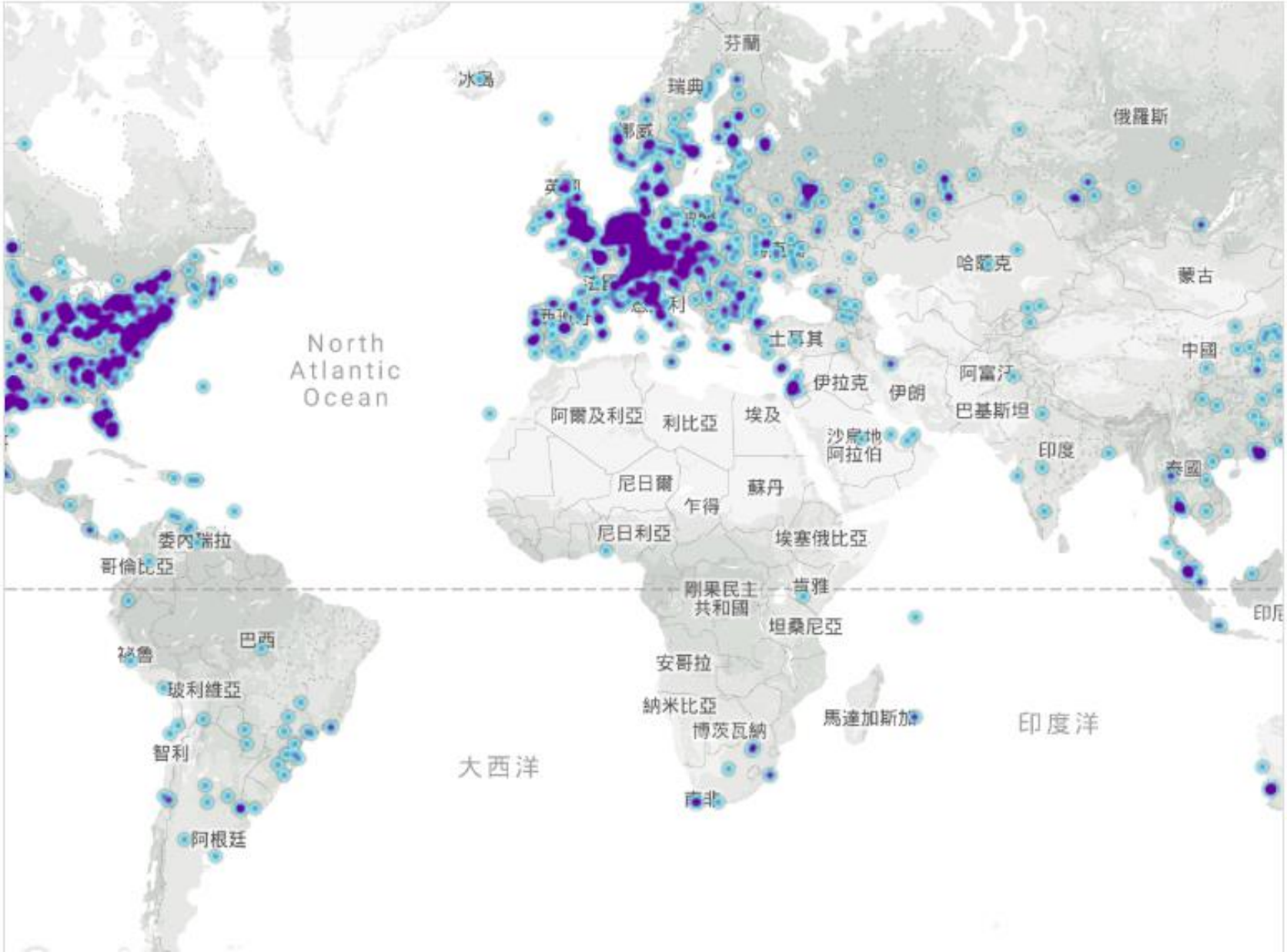
9952 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2453 (24.65%)
2	Germany	1746 (17.54%)
3	China	857 (8.61%)
4	France	661 (6.64%)
5	Netherlands	462 (4.64%)
6	Canada	372 (3.74%)
7	n/a	370 (3.72%)
8	United Kingdom	304 (3.05%)
9	Russian Federation	297 (2.98%)
10	Japan	225 (2.26%)

More (103) »



比特幣有多種版本

There are currently **9588*** nodes running on the Bitcoin network.

9046 Bitcoin Core

WHAT IS BITCOIN CORE?

222 Bitcore nodes

WHAT IS BITCORE?

90 Bitcoin UASF nodes

WHAT IS BITCOIN UASF?

49 bcoin nodes

WHAT IS BCOIN?

48 Bitcoin Unlimited

WHAT IS BITCOIN UNLIMITED?

40 btc1 nodes

WHAT IS BTC1?

38 btcd nodes

WHAT IS BTCD?

25 Bitcoin Knots nodes

WHAT IS BITCOIN KNOTS?

10 Bitcoin Classic

WHAT IS BITCOIN CLASSIC?

10 TRB nodes

WHAT IS TRB?

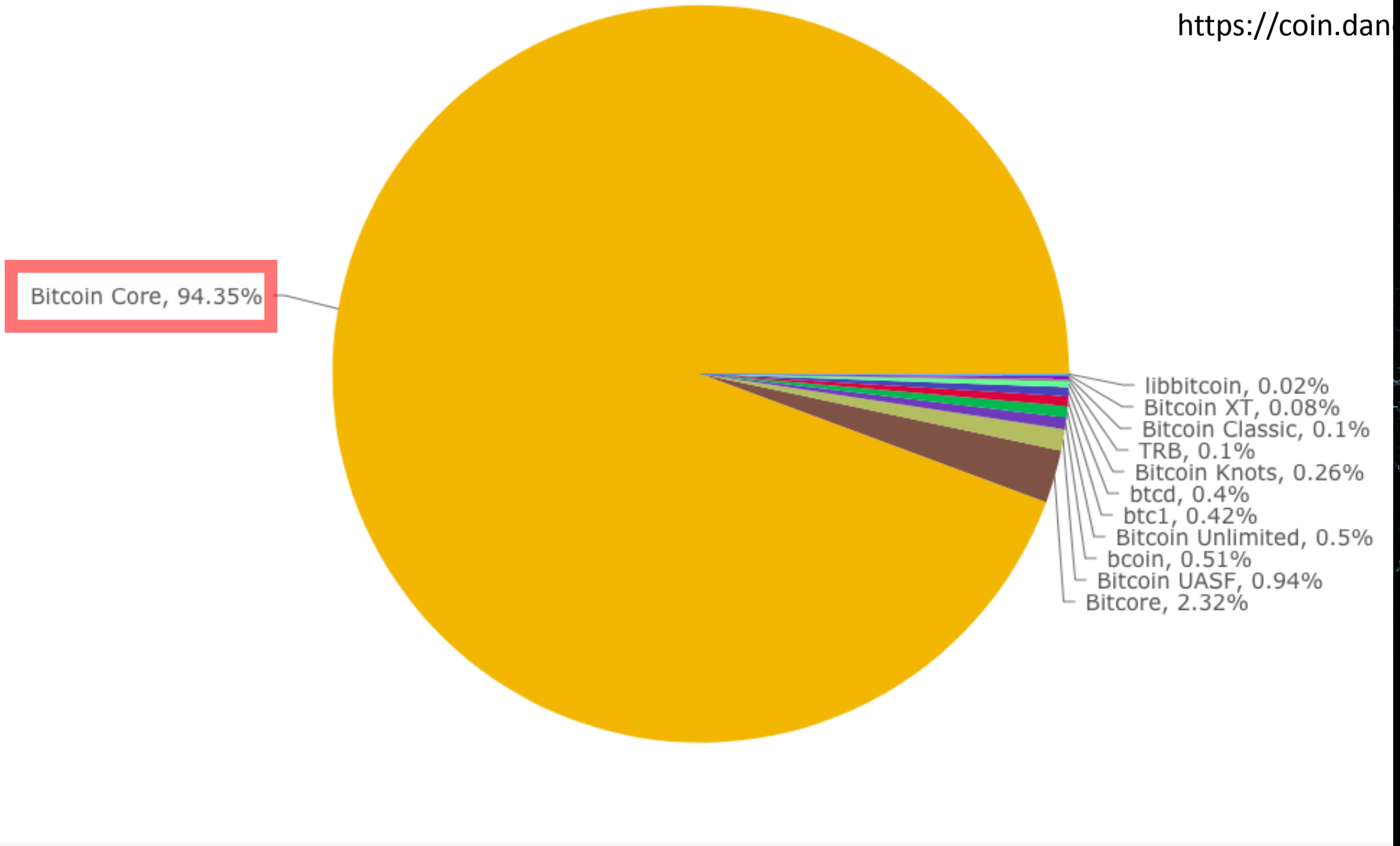
8 Bitcoin XT nodes

WHAT IS BITCOIN XT?

2 libbitcoin nodes

WHAT IS LIBBITCOIN?

https://coin.dan



bitcoin / bips

Watch 541 | Star 2,582 | Fork 1,376

Code | Pull requests 64 | Projects 0 | Wiki | Insights

Bitcoin Improvement Proposals http://bitcoin.org

1,721 commits | 5 branches | 0 releases | 172 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

luke-jr Merge pull request #683 from kallewoof/bip-178-abstract ... Latest commit 7158648 on 22 May

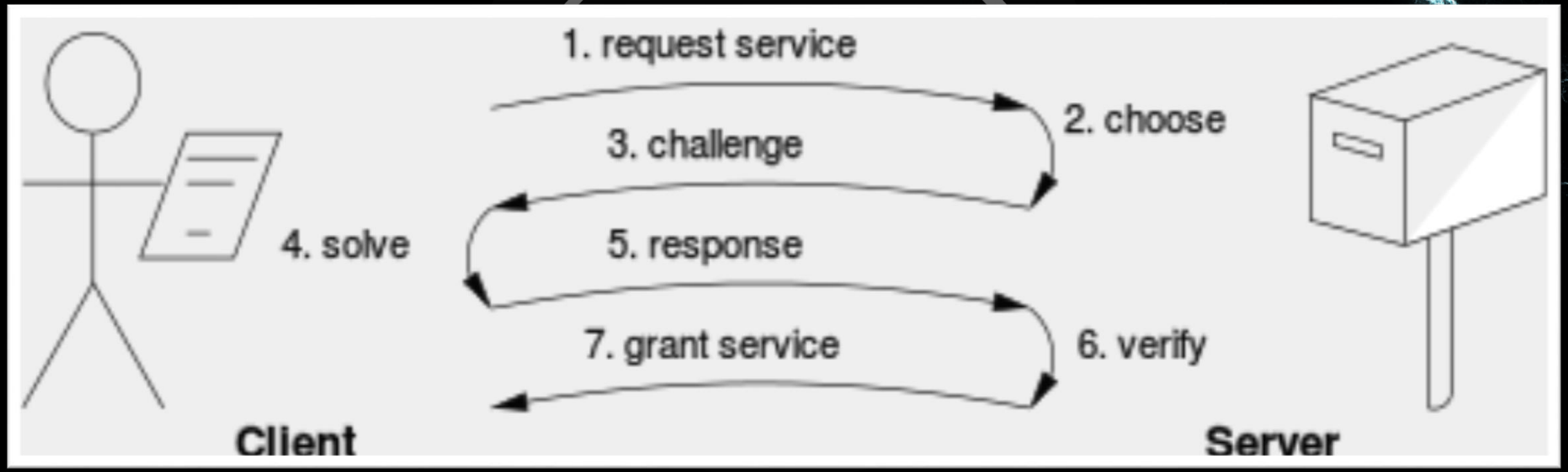
bip-0001	Fix formatting	5 years ago
bip-0002	Add obsolete status to process image	a year ago
bip-0008	Amend BIP8 by height	a year ago
bip-0009	BIP 9: Misplaced table cells typo	4 months ago
bip-0016	Archive Revision as of 19:50, 9 March 2012	5 years ago
bip-0032	Fix formatting	5 years ago

Number	Layer	Title	Owner	Type	Status
1		BIP Purpose and Guidelines	Amir Taaki	Process	Replaced
2		BIP process, revised	Luke Dashjr	Process	Active
8		Version bits with lock-in by height	Shaolin Fry	Informational	Draft
9		Version bits with timeout and delay	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	Informational	Final
10	Applications	Multi-Sig Transaction Distribution	Alan Reiner	Informational	Withdrawn
11	Applications	M-of-N Standard Transactions	Gavin Andresen	Standard	Final
12	Consensus (soft fork)	OP_EVAL	Gavin Andresen	Standard	Withdrawn
13	Applications	Address Format for pay-to-script-hash	Gavin Andresen	Standard	Final
14	Peer Services	Protocol Version and User Agent	Amir Taaki, Patrick Strateman	Standard	Final
15	Applications	Aliases	Amir Taaki	Standard	Deferred
16	Consensus (soft fork)	Pay to Script Hash	Gavin Andresen	Standard	Final

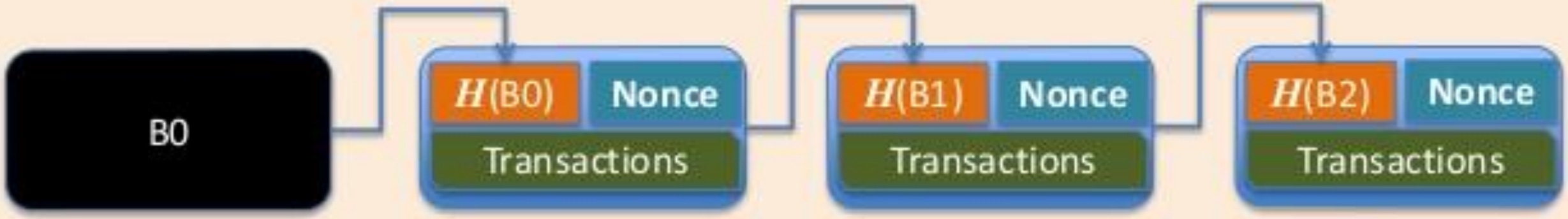
Name	Features	Introduced On	Details	Last Commit Date
Bitcoin Core	SegWit, RBF, libsecp256k1, Version bits w/ timeout & delay, BIP 68, CHECKSEQUENCEVERIFY, BIP 113, Compact Blocks, JSON RPC API, Automatic blockchain pruning, Manual blockchain pruning, ZeroMQ notifications, Transaction fee bumping, Mandatory spam filters	2009-01-03	VIEW	2018-06-19 (yesterday)
Bitcore	Advanced API	2015-11-04	VIEW	2018-05-10 (40 days ago)
Bitcoin UASF	SegWit, RBF, libsecp256k1, Version bits w/ timeout & delay, BIP 68, CHECKSEQUENCEVERIFY, BIP 113, Compact Blocks, JSON RPC API, Automatic blockchain pruning, Manual blockchain pruning, ZeroMQ notifications, Transaction fee bumping, Mandatory spam filters, BIP 148	2017-03-25	VIEW	2017-07-08 (347 days ago)
bcoin	RBF, libsecp256k1, Advanced API, CHECKSEQUENCEVERIFY, Runs in-browser, Compact Blocks, BIP 151, BIP 150, JSON RPC API	2016-12-21	VIEW	2018-06-14 (6 days ago)
Bitcoin Unlimited	libsecp256k1, Emergent Consensus, Xthin Blocks, Traffic-shaping, Xpedited Block Forwarding, Targeted Bloom Filters, JSON RPC API, Automatic blockchain pruning, ZeroMQ notifications, Mandatory spam filters	2015-09-04	VIEW	2018-05-04 (47 days ago)

比特幣的挖礦

工作量證明 proof of work



Bitcoin's Proof-of-Work



Find a nonce x such that:

SHA-256(SHA-256(r || x)) < T/d

r = header includes H(previous block)
root of Merkle tree of transactions

target

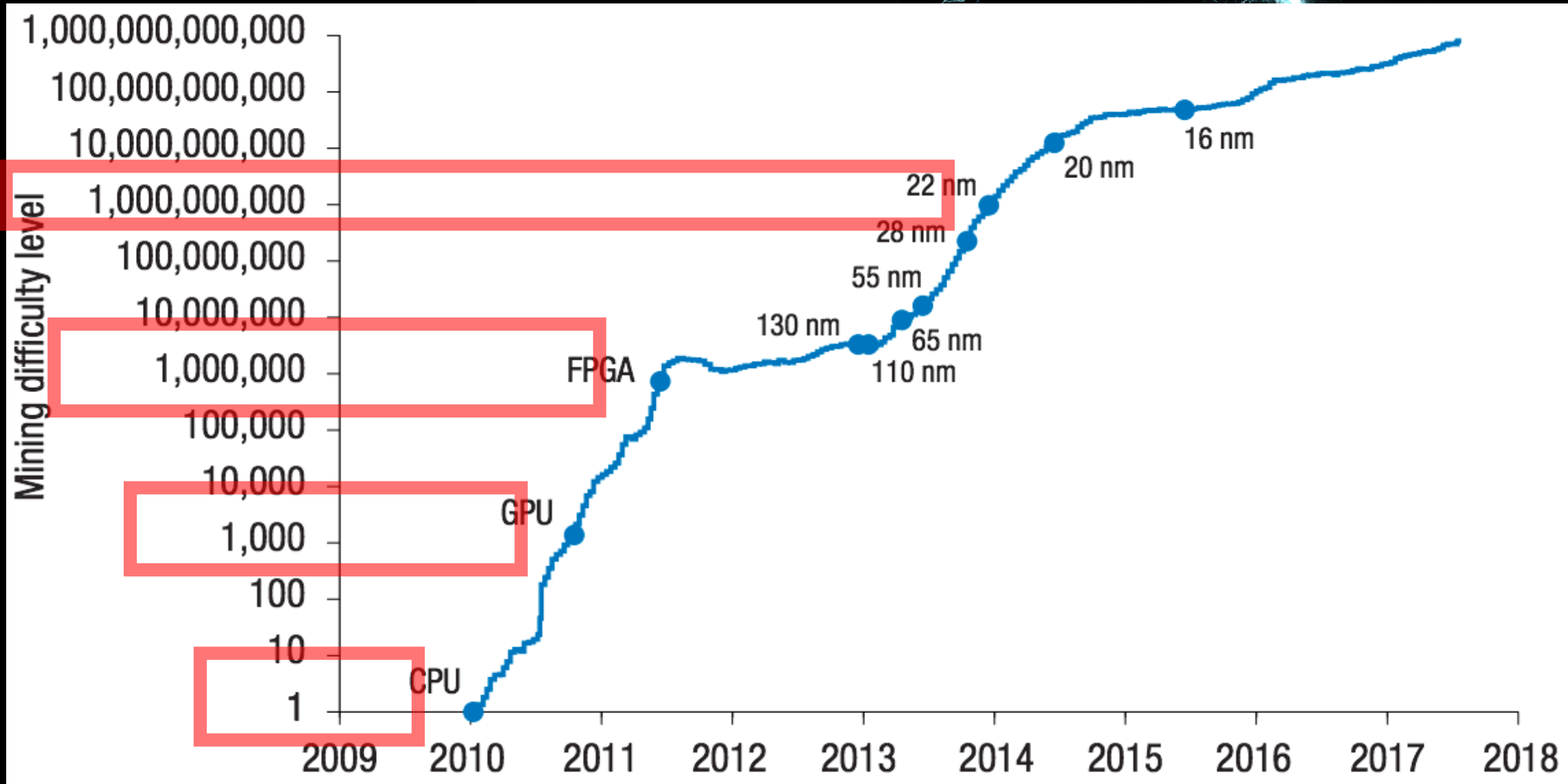
```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

挖礦

- **解出問題的人**可以取得許可權
  - 問題是以工作量證明(proof of work)為基礎，一個難以計算，卻簡單驗算的題目。
    - hash puzzle
    - 素數-費馬測試（Fermat Test），通過則再進行歐拉-拉格朗日-立夫習茲測試（Euler-Lagrange-Lifchitz Test）
    - 因數分解
- 取得許可權的人可以**創建區塊**並且得到獎勵
- 該問題源自於最新的區塊

http://ieeexplore.ieee.org/document/8048662/

挖礦設備



挖礦的演進

CPU

GPU

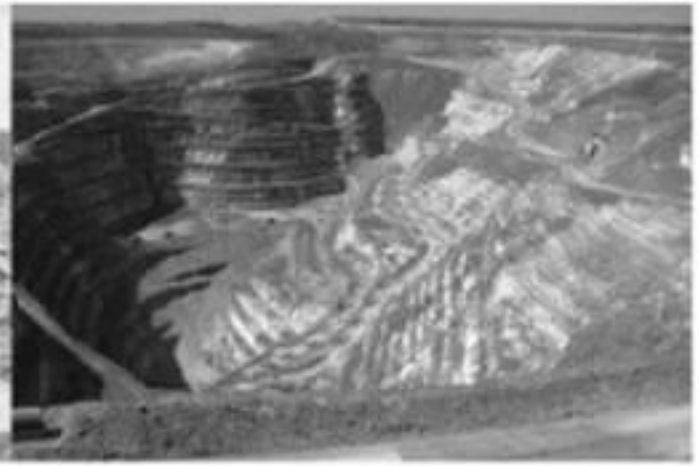
FPGA

ASIC

淘金用的盘

流沙槽

水冲刷淘金



露天机械化挖矿

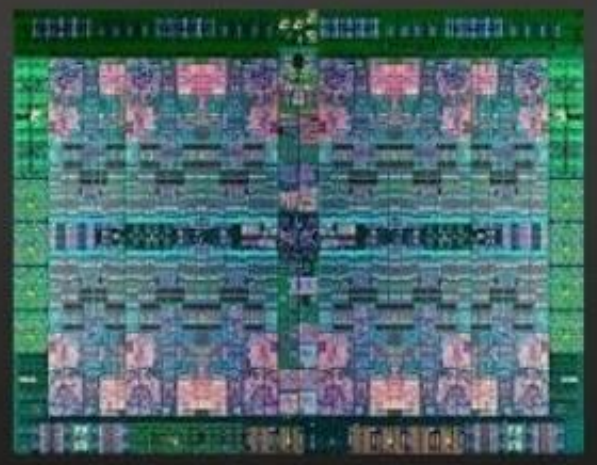
8. 挖礦硬體演進

CPU

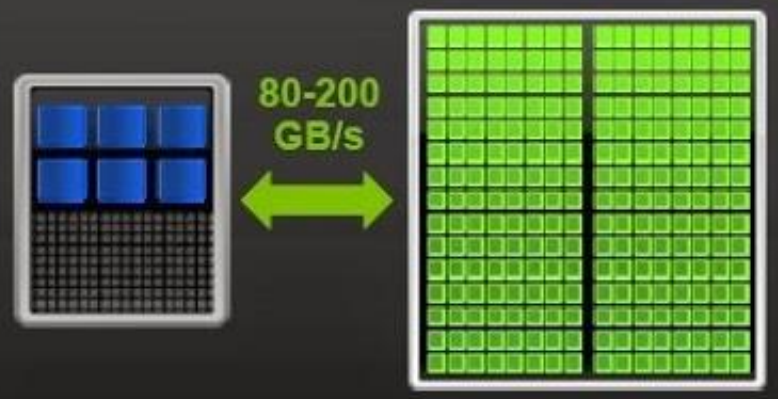
intel
Intel® Core™ i7

GPU

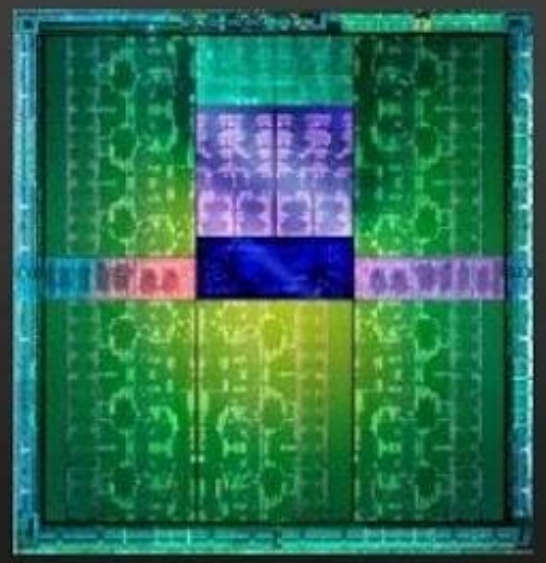
Accelerated Computing
5x Higher Energy Efficiency



IBM POWER CPU
Most Powerful Serial Processor

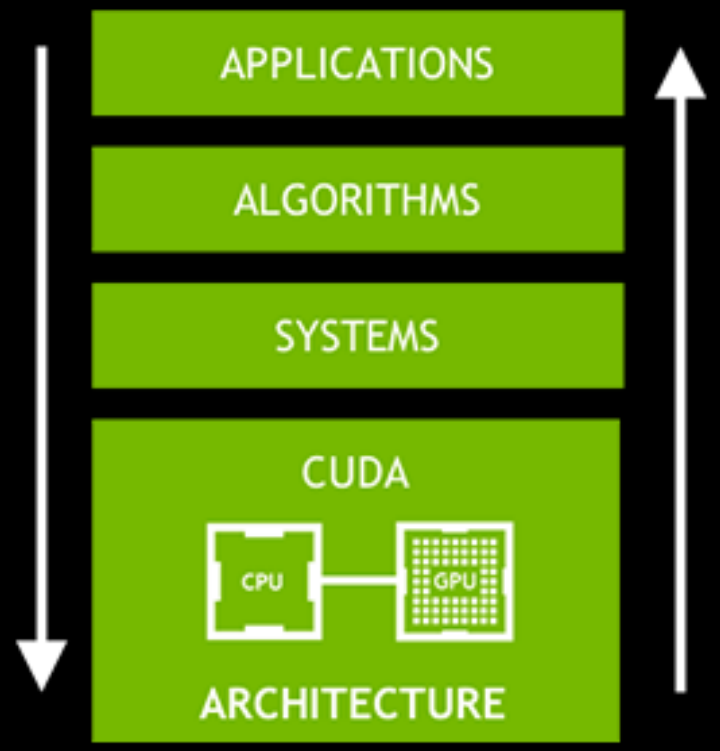


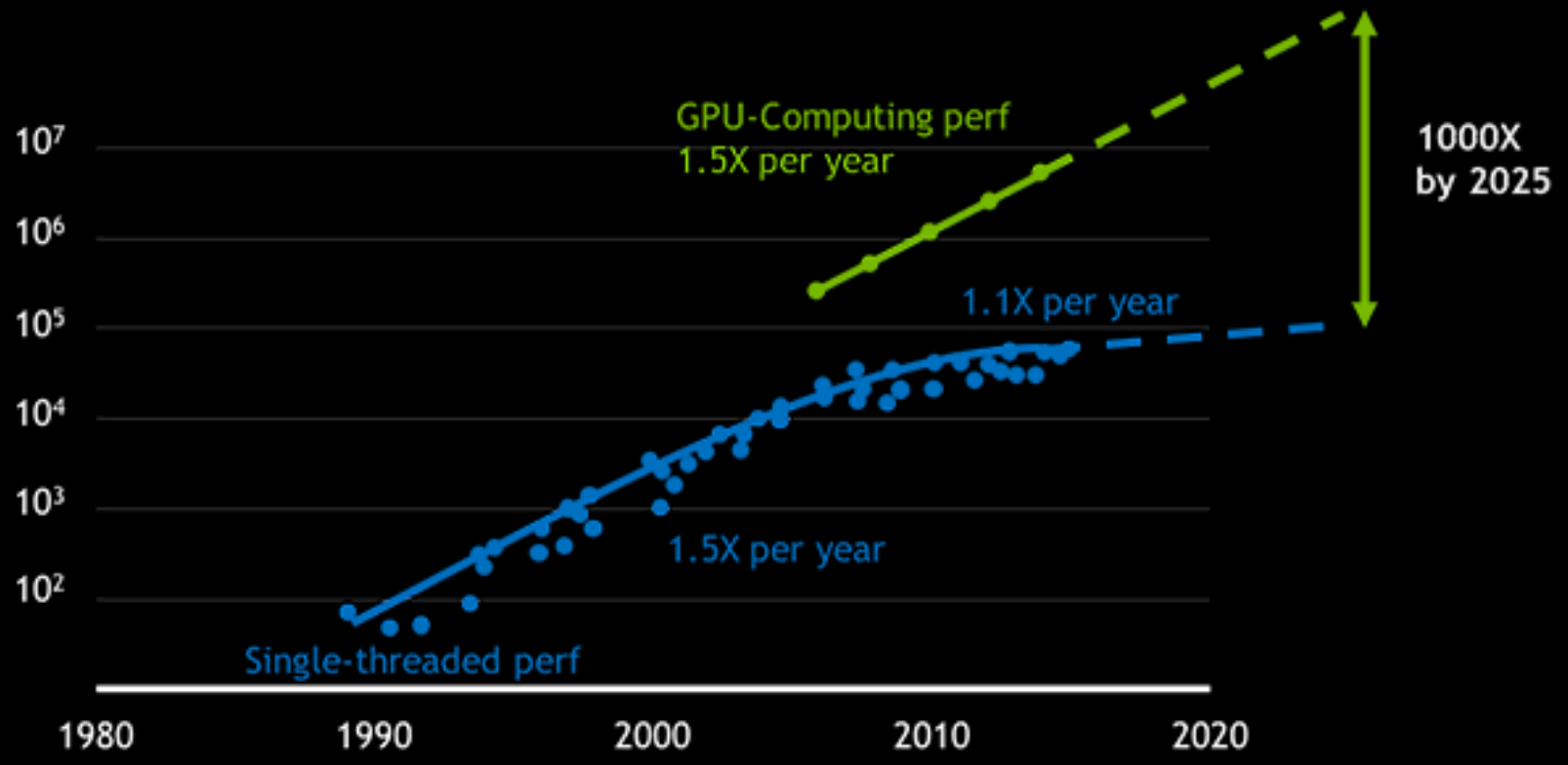
NVIDIA NVLink
Fastest CPU-GPU Interconnect



NVIDIA Volta GPU
Most Powerful Parallel Processor

RISE OF GPU COMPUTING

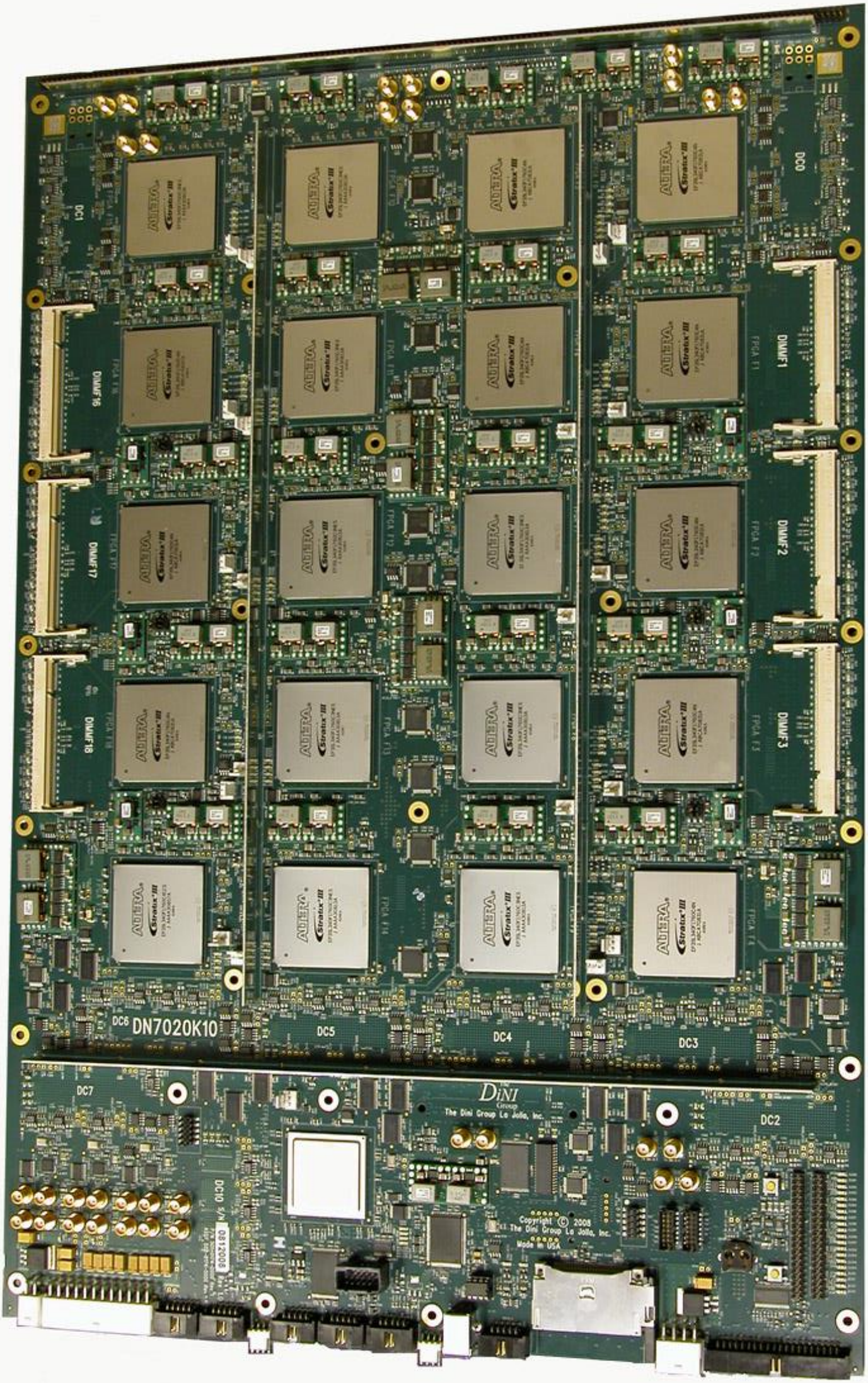




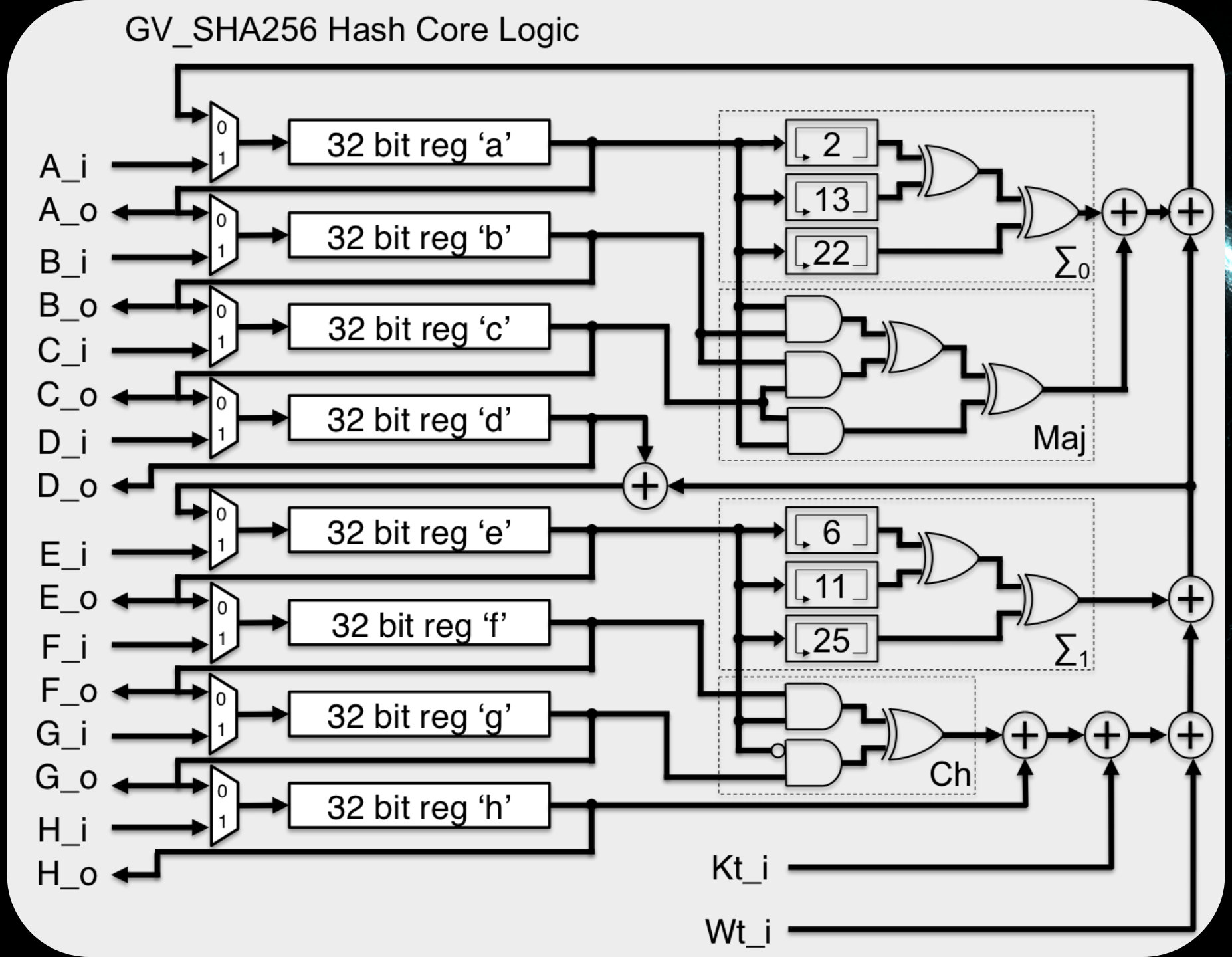
Original data up to the year 2010 collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten New plot and data collected for 2010-2015 by K. Rupp

AORUS

FPGA


DC1
DC0
DIMMF16
DIMMF1
DIMMF17
DIMMF2
DIMMF18
DIMMF3
DC6 DN7020K10
DC5
DC4
DC3
DC7
DC2
DiNI
Group
The Dini Group La Jolla, Inc.
DC10 S/N
Copyright © 2008
The Dini Group La Jolla, Inc.
Made in USA

ASIC


GV_SHA256 Hash Core Logic
A_i
A_o
B_i
B_o
C_i
C_o
D_i
D_o
E_i
E_o
F_i
F_o
G_i
G_o
H_i
H_o
0
1
32 bit reg 'a'
32 bit reg 'b'
32 bit reg 'c'
32 bit reg 'd'
32 bit reg 'e'
32 bit reg 'f'
32 bit reg 'g'
32 bit reg 'h'
2
13
22
Σ_0
Maj
6
11
25
Σ_1
Ch
Kt_i
Wt_i

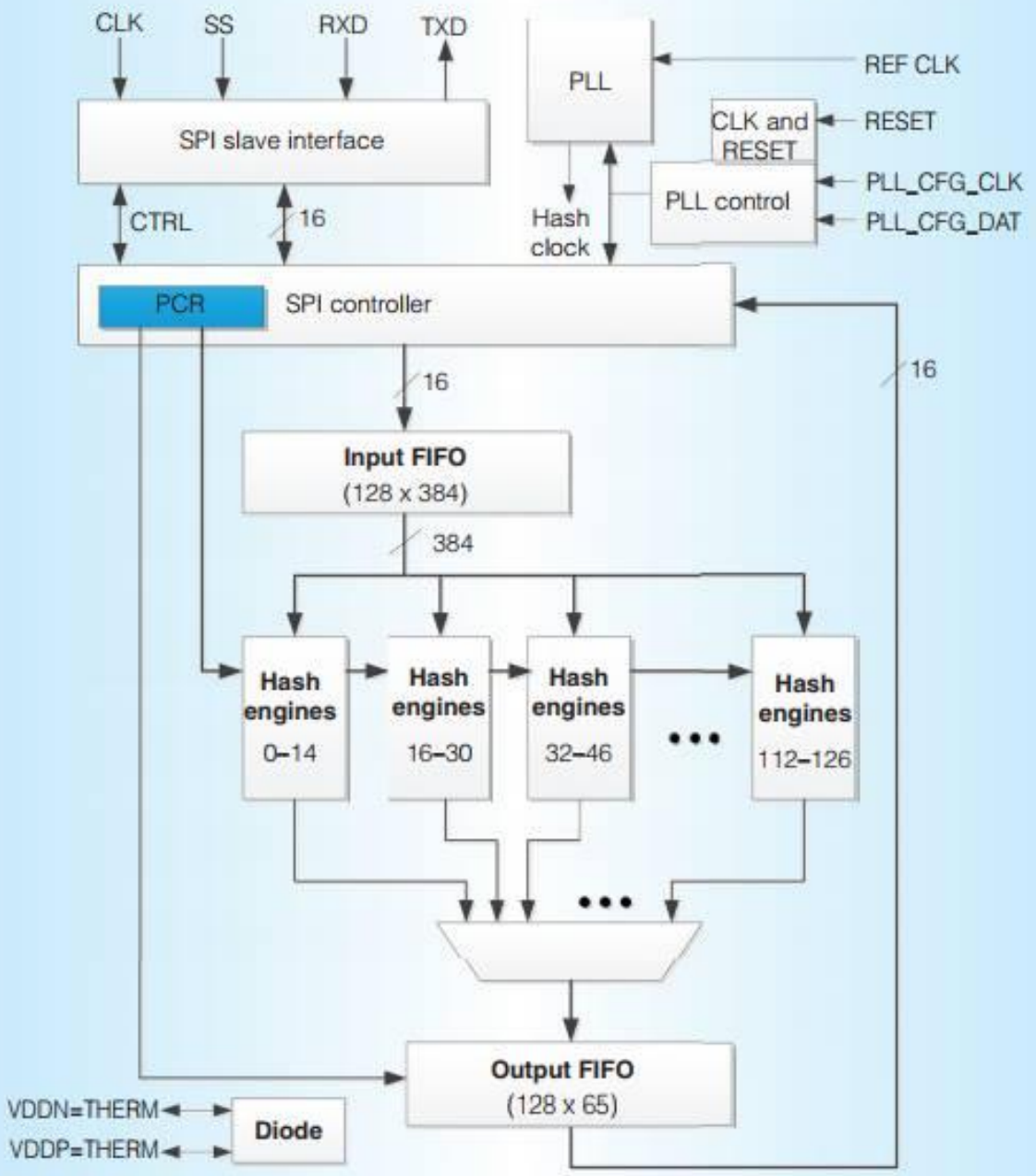
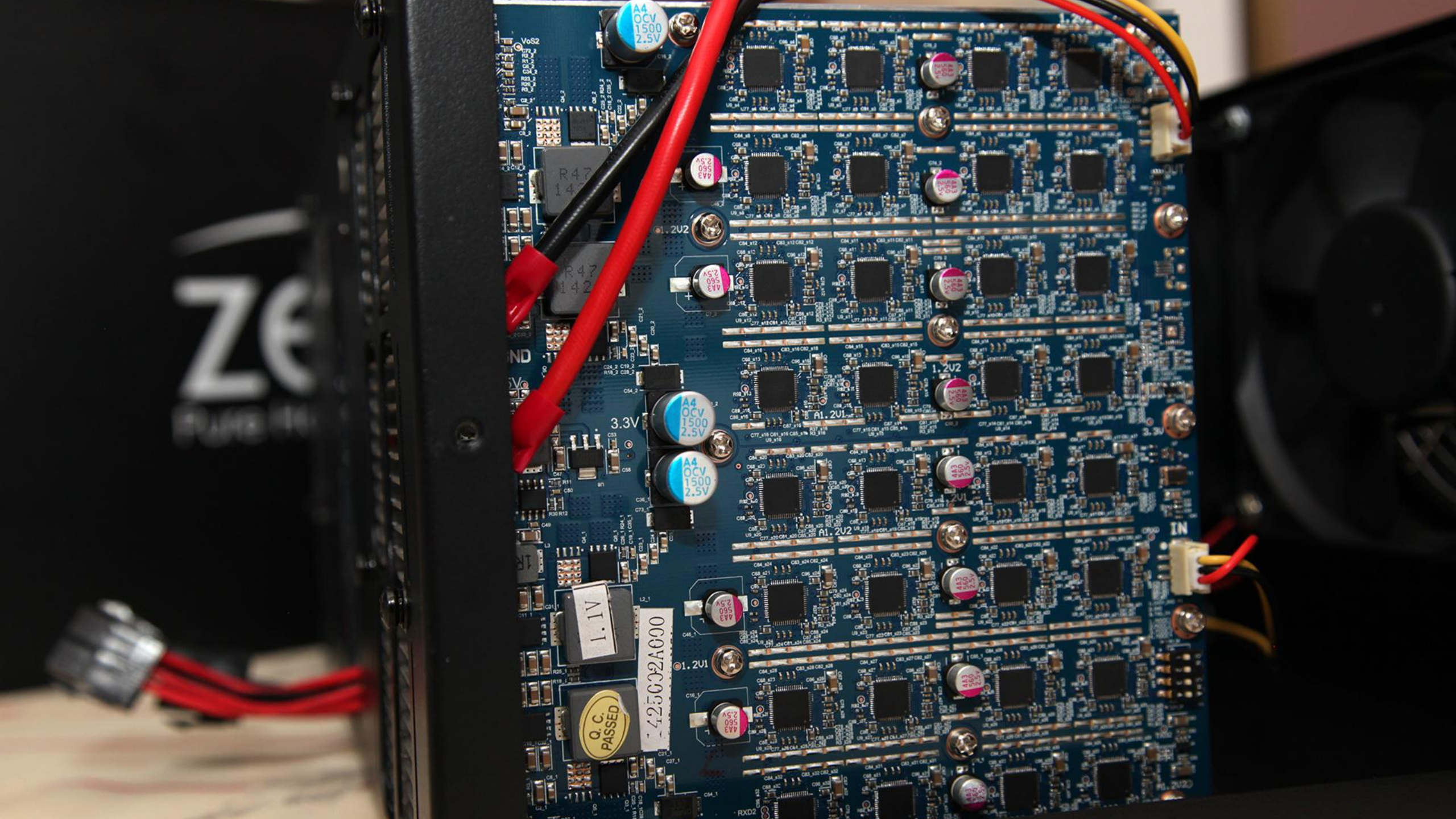


Figure 2. Block diagram of the Goldstrike 1 architecture. Each of the 120 hash engines is working independently on a separate problem.

AVALON
A3222-Q56
T8A9891434EMAA

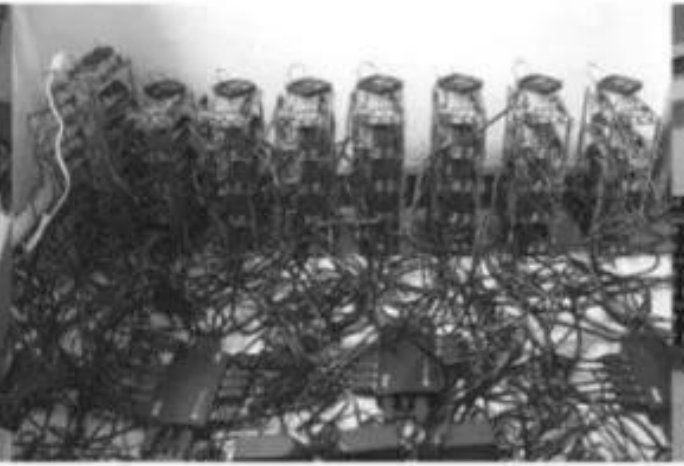
cool
.385
A
V

hot
.405
A
V


A4
OCV
1500
2.5V
VoS2
R47
142
1.2V2
3.3V
A1.2V1
A1.2V2
1.1V
1.2V1
Q.C.
PASSED
IN
OUT

CPU

GPU



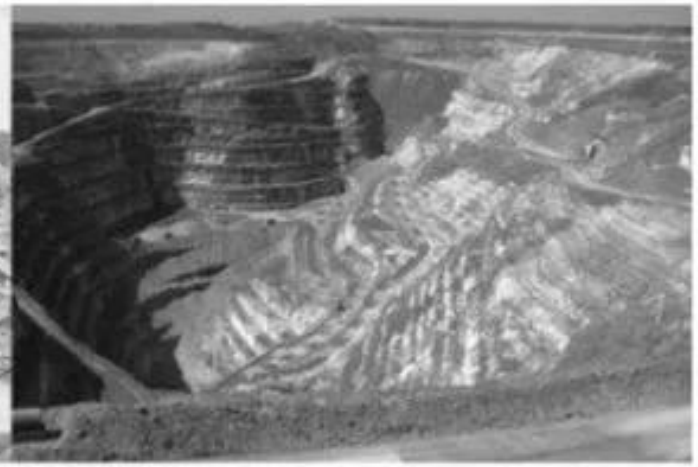
FPGA

ASIC

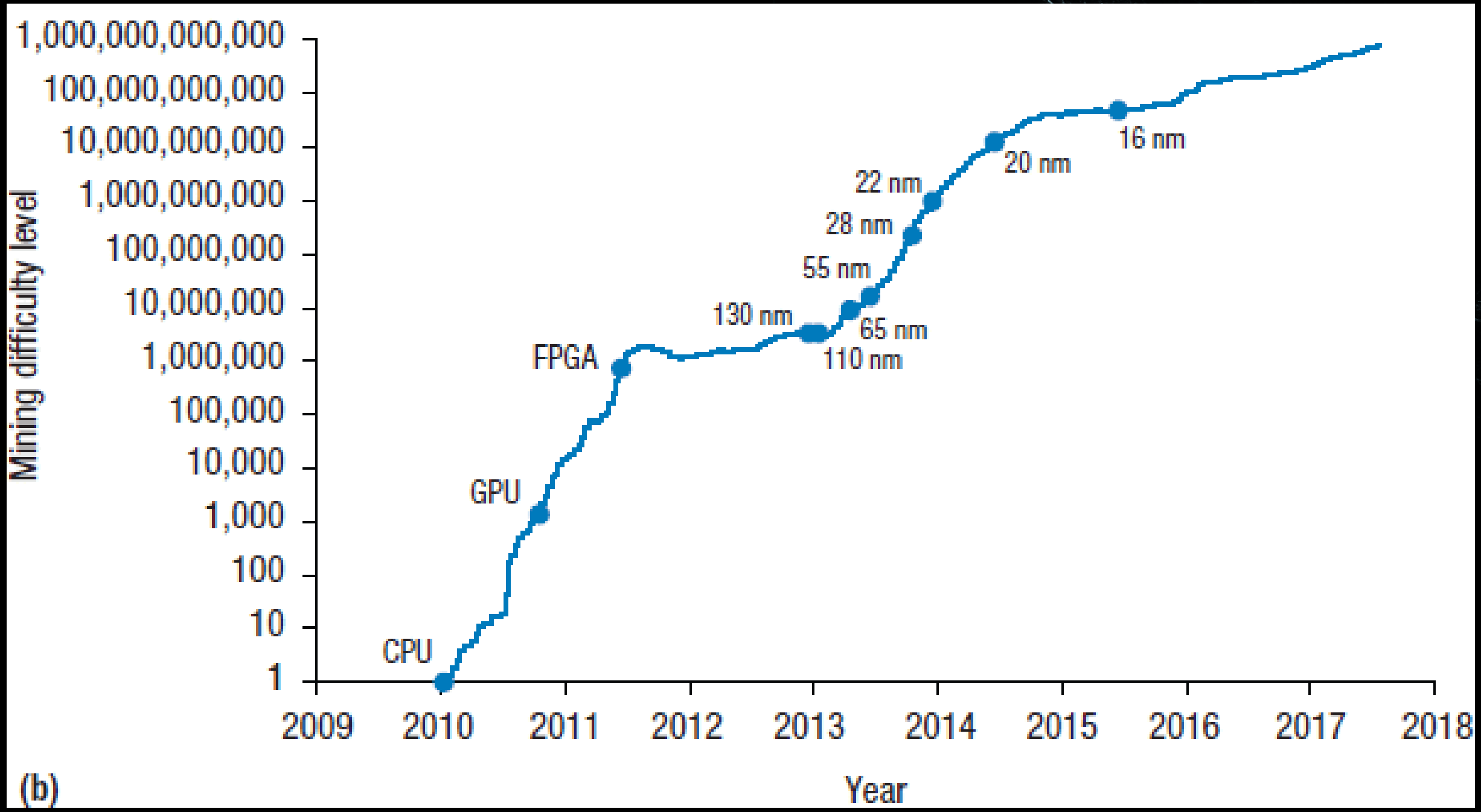
淘金用的盘

流沙槽

水冲刷淘金



露天机械化挖矿


1,000,000,000,000
100,000,000,000
10,000,000,000
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
Mining difficulty level
CPU
GPU
FPGA
130 nm
110 nm
55 nm
65 nm
28 nm
22 nm
20 nm
16 nm
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Year
(b)

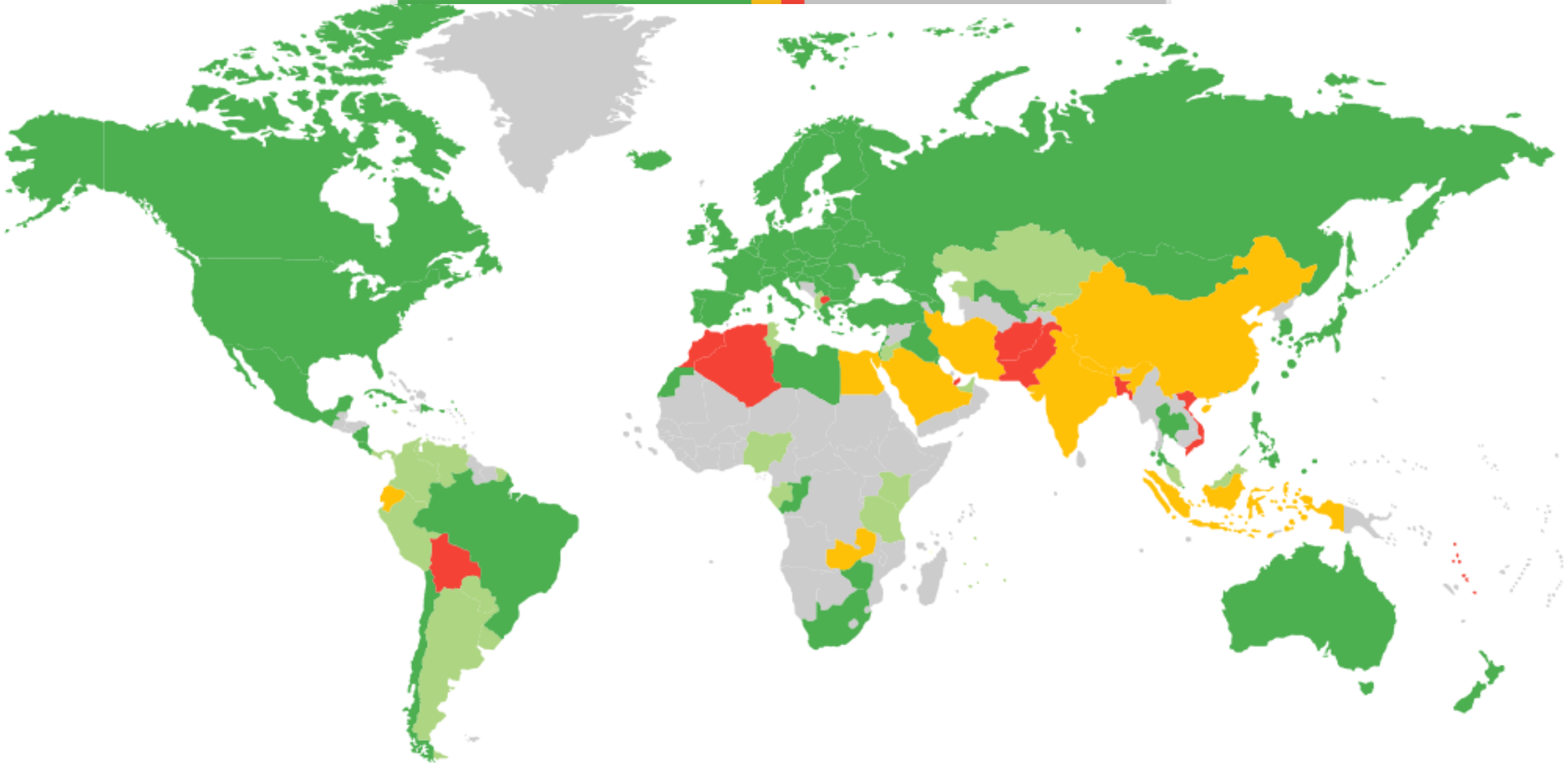
5,000
2,000
1,000
500
200
100
50
20
10
5
2
1
0.5
0.2
0.1
0.05
BTC-to-USD exchange rate
2010
2011
2012
2013
2014
2015
2016
2017
2018
Year

(a)

Bitcoin 在不同國家

Global Bitcoin Legality

Bitcoin is unrestricted in 115 of 251 countries/regions.



Legal Alegal Restricted Illegal Unknown

Stay Up to Date on Crypto & Blockchain With Our Suite of Newsletters. Subscri

Taiwan Financial Regulator Says Bitcoin Isn't Banned

Stan Higgins

Nov 13, 2015 at 20:20 UTC • Updated Nov 13, 2015 at 20:48 UTC

NEWS

In a new statement, Taiwan's Financial Supervisory Commission (FSC) – its top banking, insurance and securities regulator – has indicated its stance on bitcoin remains neutral despite recent speculation it was moving toward more restrictive policies.

比特幣之外

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ Exchanges ▾ Watchlist USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$219,439,933,485	$12,320.95	$30,564,603,964	17,810,312 BTC	-1.89%	
2	Ethereum	$30,749,117,507	$287.80	$11,213,613,311	106,843,630 ETH	-7.43%	
3	XRP	$15,443,401,992	$0.362806	$2,068,316,376	42,566,596,173 XRP *	-8.20%	
4	Bitcoin Cash	$6,957,177,201	$389.01	$1,807,800,072	17,884,225 BCH	-6.64%	
5	Litecoin	$6,787,899,274	$108.43	$4,383,261,716	62,602,337 LTC	-9.24%	
6	EOS	$4,855,334,686	$5.26	$3,069,631,326	922,657,131 EOS *	-11.16%	
7	Binance Coin	$4,465,361,511	$31.63	$256,543,538	141,175,490 BNB *	-4.02%	

8	Tether	$3,840,454,515	$1.00	$30,873,021,477	3,838,668,473 USDT *	-0.45%		•••
9	Bitcoin SV	$3,369,842,863	$188.73	$382,947,856	17,854,986 BSV	-8.64%		•••
10	TRON	$2,130,865,611	$0.031956	$759,412,407	66,682,072,191 TRX	-7.22%		•••
11	Cardano	$1,881,792,764	$0.072580	$120,341,998	25,927,070,538 ADA	-6.95%		•••
12	Stellar	$1,832,517,861	$0.094334	$372,630,558	19,425,802,089 XLM *	-7.43%		•••
13	Monero	$1,623,472,957	$95.01	$130,642,336	17,086,582 XMR	-6.18%		•••
14	UNUS SED LEO	$1,529,094,967	$1.53	$12,653,327	999,498,893 LEO *	-4.47%		•••
15	Dash	$1,339,011,822	$150.20	$281,185,824	8,914,932 DASH	-4.03%		•••

16	NEO	$1,136,003,350	$16.10	$508,572,899	70,538,831 NEO *	-7.21%		•••
17	Chainlink	$1,072,856,392	$3.07	$143,307,727	350,000,000 LINK *	0.31%		•••
18	IOTA	$1,019,814,652	$0.366902	$21,307,525	2,779,530,283 MIOTA *	-7.41%		•••
19	Cosmos	$858,396,278	$4.50	$139,232,992	190,688,439 ATOM *	-9.66%		•••
20	Ethereum Classic	$816,330,281	$7.30	$665,491,388	111,846,378 ETC	-7.34%		•••
21	Tezos	$779,128,088	$1.18	$6,602,173	657,649,139 XTZ *	-1.39%		•••
22	NEM	$743,476,561	$0.082609	$60,299,567	8,999,999,999 XEM *	-8.15%		•••
23	Crypto.com Chain	$715,954,958	$0.091159	$3,909,089	7,853,881,279 CRO *	14.59%		•••

DICCOM

24	Maker	$692,055,049	$692.06	$2,205,700	1,000,000 MKR *	-6.06%		•••
25	Zcash	$671,432,615	$96.75	$354,458,535	6,940,169 ZEC	-4.30%		•••
26	Ontology	$663,441,707	$1.24	$162,161,087	533,255,142 ONT *	-8.51%		•••
27	Bitcoin Gold	$500,906,622	$28.60	$18,388,155	17,513,924 BTG	-2.50%		•••
28	Dogecoin	$411,571,376	$0.003422	$48,277,685	120,288,603,867 DOGE	-3.66%		•••
29	Qtum	$403,385,208	$4.21	$368,103,215	95,857,256 QTUM *	-11.95%		•••
30	Basic Attenti...	$396,707,957	$0.311631	$34,975,569	1,273,006,300 BAT *	6.48%		•••

bitcoin taiwan

31	VeChain	$393,753,044	$0.007100	$40,609,052	55,454,734,800 VET *	-2.79%		•••
32	Egretia	$378,062,262	$0.089828	$252,584,505	4,208,736,606 EGT *	17.23%		•••
33	USD Coin	$377,347,489	$1.00	$174,351,345	377,013,861 USDC *	0.13%		•••
34	Decred	$329,623,208	$32.76	$3,940,999	10,061,490 DCR	-1.03%		•••
35	V Systems	$320,837,170	$0.182983	$12,285,935	1,753,368,158 VSYS *	1.79%		•••
36	OmiseGO	$308,217,695	$2.20	$92,744,059	140,245,398 OMG *	-11.09%		•••
37	BitTorrent	$261,501,898	$0.001233	$57,192,555	212,116,500,000 BTT *	-4.75%		•••
38	Holo	$216,463,741	$0.001625	$18,057,265	133,214,575,156 HOT *	-3.76%		•••

DICCOIN

39	HedgeTrade	$212,252,947	$0.735984	$1,167,308	288,393,355 HEDG *	-1.56%		•••
40	TrueUSD	$208,320,902	$1.00	$243,594,934	207,815,163 TUSD *	0.15%		•••
41	Bitcoin Diamond	$203,410,481	$1.09	$4,492,706	186,492,898 BCD	-5.47%		•••
42	Huobi Token	$196,181,539	$3.92	$107,932,518	50,000,200 HT *	-2.17%		•••
43	Pundi X	$184,762,136	$0.000776	$5,707,680	237,959,087,583 NPXS *	-4.63%		•••
44	Lisk	$180,020,840	$1.52	$8,027,565	118,406,991 LSK *	-5.58%		•••
45	Ravencoin	$179,835,557	$0.045582	$18,472,627	3,945,290,000 RVN	-4.93%		•••
46	HyperCash	$178,511,976	$4.10	$11,234,186	43,529,781 HC	-9.41%		•••

DICCOIN

平台幣

#	Name	Platform	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Tether	Omni	$3,843,319,650	$1.00	$30,942,744,587	3,838,668,473	-0.37%	
2	UNUS SED LEO	Ethereum	$1,525,971,318	$1.53	$12,666,523	999,498,893	-4.65%	
3	Chainlink	Ethereum	$1,063,333,009	$3.04	$144,668,651	350,000,000	-0.66%	
4	Crypto.com ...	Ethereum	$712,560,183	$0.090727	$3,917,507	7,853,881,279	14.12%	
5	Maker	Ethereum	$690,882,205	$690.88	$2,205,397	1,000,000	-6.20%	
6	Basic Atten...	Ethereum	$392,858,683	$0.308607	$35,243,619	1,273,006,300	5.42%	
7	Egretia	Ethereum	$377,536,772	$0.089703	$252,383,711	4,208,736,606	17.10%	
8	USD Coin	Ethereum	$377,183,635	$1.00	$174,497,108	377,013,861	0.08%	
9	OmiseGO	Ethereum	$308,532,790	$2.20	$92,852,843	140,245,398	-11.00%	

10	BitTorrent	TRON	$261,603,108	$0.001233	$57,237,841	212,116,500,000	-4.70%	
11	Holo	Ethereum	$214,590,210	$0.001611	$17,767,271	133,214,575,156	-4.51%	
12	HedgeTrade	Ethereum	$212,769,930	$0.737777	$1,167,811	288,393,355	-1.30%	
13	TrueUSD	Ethereum	$208,270,600	$1.00	$243,829,069	207,815,163	0.13%	
14	Huobi Token	Ethereum	$196,045,002	$3.92	$107,963,288	50,000,200	-2.25%	
15	Pundi X	Ethereum	$184,934,956	$0.000777	$5,771,497	237,959,087,583	-4.47%	
16	Augur	Ethereum	$172,626,699	$15.69	$12,481,700	11,000,000	-3.79%	
17	Qubitica	Ethereum	$169,772,921	$60.42	$85,408	2,809,830	-8.15%	
18	Aurora	Ethereum	$169,716,686	$0.025941	$8,713,648	6,542,330,148	1.45%	

交易量修正

Cryptocurrencies ▾ | **Exchanges ▾** | Watchlist | USD ▾ | Next 100 →

#	Name	Volume (24h)	Volume (7d)	Volume (30d)	No. Markets	Change (24h)	Vol Graph (7d)	Launched
1	BitMax	$11,664,391,924	$51,651,227,993	$186,509,965,726	139	5.66%		Jul 2018
2	BitMEX	$7,212,037,984	$31,355,688,231	$166,140,916,080	1	11.06%		Apr 2014
3	Binance	$2,557,626,965	$11,086,538,500	$68,632,398,908	517	10.33%		Jul 2017
4	OKEx	$2,489,088,578	$10,281,892,432	$57,055,829,385	423	33.61%		Jan 2014
5	Huobi Global	$2,276,550,877	$9,410,146,864	$50,579,916,217	457	12.29%		Sep 2013
6	LBank	$2,193,971,175	$8,447,789,134	$43,993,429,982	111	40.59%		Oct 2017
7	ZBG	$1,902,520,192	$10,018,272,023	$52,192,501,700	31	-4.02%		Jul 2018
8	BitForex	$1,870,440,083	$8,001,407,095	$42,666,520,146	181	23.60%		Jun 2018

Cryptocurrencies ▾ | **Exchanges ▾** | Watchlist | USD ▾ | Next 100 →

#	Name	Adj. Vol (24h)*	Volume (24h)	Volume (7d)	Volume (30d)	No. Markets	Change (24h)	Vol Graph (7d)	Launched
1	Binance	$2,554,889,680	$2,554,889,680	$11,086,538,500	$68,632,398,908	516	10.12%		Jul 2017
2	OKEx	$2,491,178,399	$2,491,178,399	$10,281,892,432	$57,055,829,385	423	33.67%		Jan 2014
3	Huobi Global	$2,277,907,674	$2,277,907,674	$9,410,146,864	$50,579,916,217	457	12.31%		Sep 2013
4	LBank	$2,193,924,849	$2,193,924,849	$8,447,789,134	$43,993,429,982	111	40.27%		Oct 2017
5	BitForex	$1,872,936,111	$1,872,936,111	$8,001,407,095	$42,666,520,146	181	23.74%		Jun 2018
6	DigiFinex	$1,787,068,876	$1,787,068,876	$7,316,090,238	$47,531,386,703	176	20.04%		Apr 2018
7	DOBI Exchange	$1,747,378,544	$1,747,378,544	$9,471,581,592	$41,540,928,015	29	6.10%		May 2018
8	CoinTiger	$1,662,970,630	$1,662,970,630	$6,574,042,956	$37,648,440,504	131	13.81%		Dec 2017

Cryptocurrencies | Exchanges | W

#	Name	Volume (24h)
1	BitMax	$11,664,391,924
2	BitMEX	$7,212,037,984
3	Binance	$2,557,626,965
4	OKEx	$2,489,088,578
5	Huobi Global	$2,276,550,877
6	LBank	$2,193,971,175
7	ZBG	$1,902,520,192
8	BitForex	$1,870,440,083

Cryptocurrencies | Exchanges | Watchlist

#	Name	Adj. Vol (24h)*	Volume (24h)	Volume (7d)	Volume (30d)	No. Markets	Change
1	Binance	$2,554,889,680	$2,554,889,680	$11,086,538,500	$68,632,398,908	516	10
2	OKEx	$2,491,178,399	$2,491,178,399	$10,281,892,432	$57,055,829,385	423	33
3	Huobi Global	$2,277,907,674	$2,277,907,674	$9,410,146,864	$50,579,916,217	457	12
4	LBank	$2,193,924,849	$2,193,924,849	$8,447,789,134	$43,993,429,982	111	40
5	BitForex	$1,872,936,111	$1,872,936,111	$8,001,407,095	$42,666,520,146	181	23
6	DigiFinex	$1,787,068,876	$1,787,068,876	$7,316,090,238	$47,531,386,703	176	20
7	DOBI Exchange	$1,747,378,544	$1,747,378,544	$9,471,581,592	$41,540,928,015	29	6
8	CoinTiger	$1,662,970,630	$1,662,970,630	$6,574,042,956	$37,648,440,504	131	13

Bitcoin

比特幣的未來

閃電網路

Lightning Network

Bitcoin 存在的問題

- 比特幣區塊鏈 出塊時間 平均為 10 分鐘
  - 沒塞車：發起一筆交易 平均十分鐘
  - 塞車：天荒地老 可以是一天 、一週、數個月
  - 嚴重塞車：發起的交易就此消失

  - 小結：僅支持每秒七筆交易的比特幣，難成為 生活中的支付
- 比特幣區塊鏈 達到250GB
  - 去中心化：龐大的資料 難 讓志願者願意儲存
  - 同步過程：同步速度 太久 驗算交易

閃電網絡是一個小額交易協議，提供瞬時廉價的比特幣交易服務。

小額交易

閃電網絡使得安全的全球小額交易成為現實。從數字商品銷售到隨叫隨到的在線服務，無數新的數字商業模式將首次成為可能。要了解更多應用例子，可以查看我們已經創建的一些閃電網絡應用(LApps)。

隱私政策

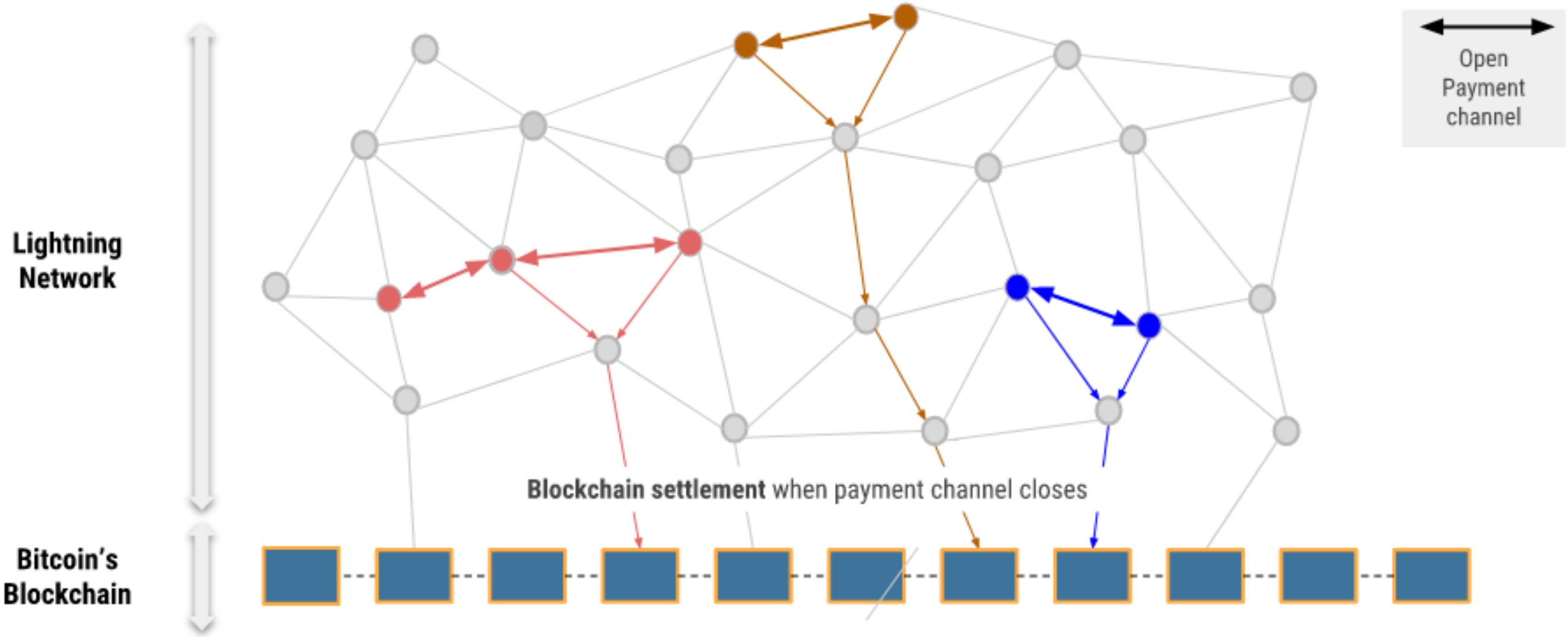
閃電網絡上的交易不會被記錄在區塊鏈上，默認使用洋蔥路由器進行分享，和標準的比特幣交易相比，這種交易方式能夠更好地保護用戶隱私。

還記得 比特幣的最小單位？

1 Satoshi	= 0.00000001 ฿	
10 Satoshi	= 0.00000010 ฿	
100 Satoshi	= 0.00000100 ฿	= 1 Bit / µBTC (you-bit)
1,000 Satoshi	= 0.00001000 ฿	
10,000 Satoshi	= 0.00010000 ฿	
100,000 Satoshi	= 0.00100000 ฿	= 1 mBTC (em-bit)
1,000,000 Satoshi	= 0.01000000 ฿	= 1 cBTC (bitcent)
10,000,000 Satoshi	= 0.10000000 ฿	
100,000,000 Satoshi	= 1.00000000 ฿	

閃電網路 使1 Satoshi的交易變得可行

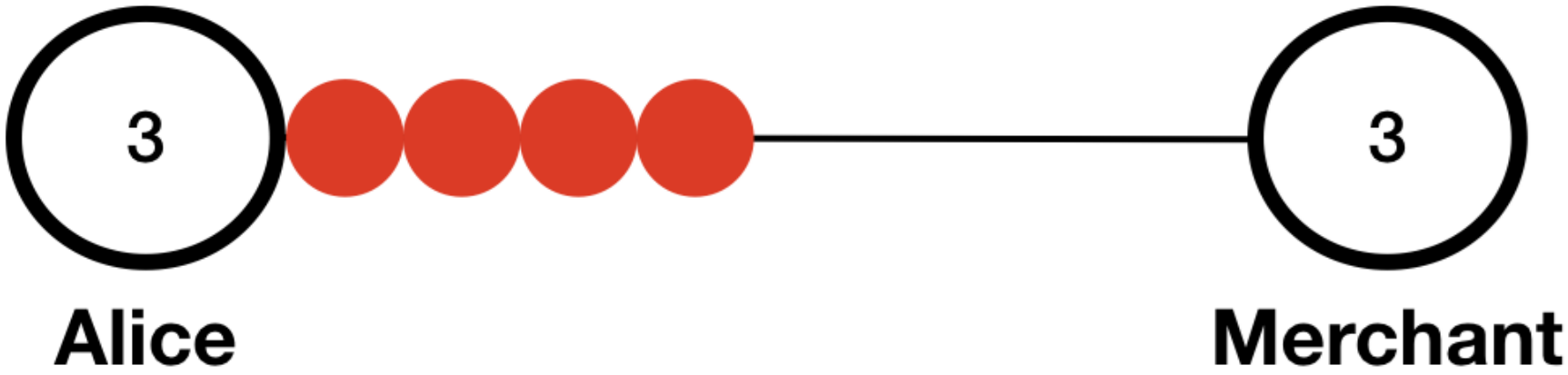
Lightning Network



© TheBlockPro.com

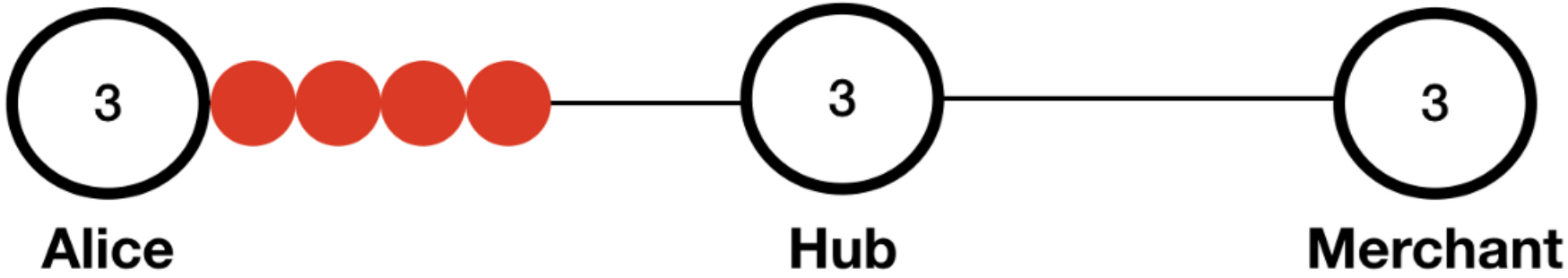
Multisig
Address
Alice's
BTC Address
DIRECTION OF PAYMENT
Carol's
BTC Address

Regular thinking



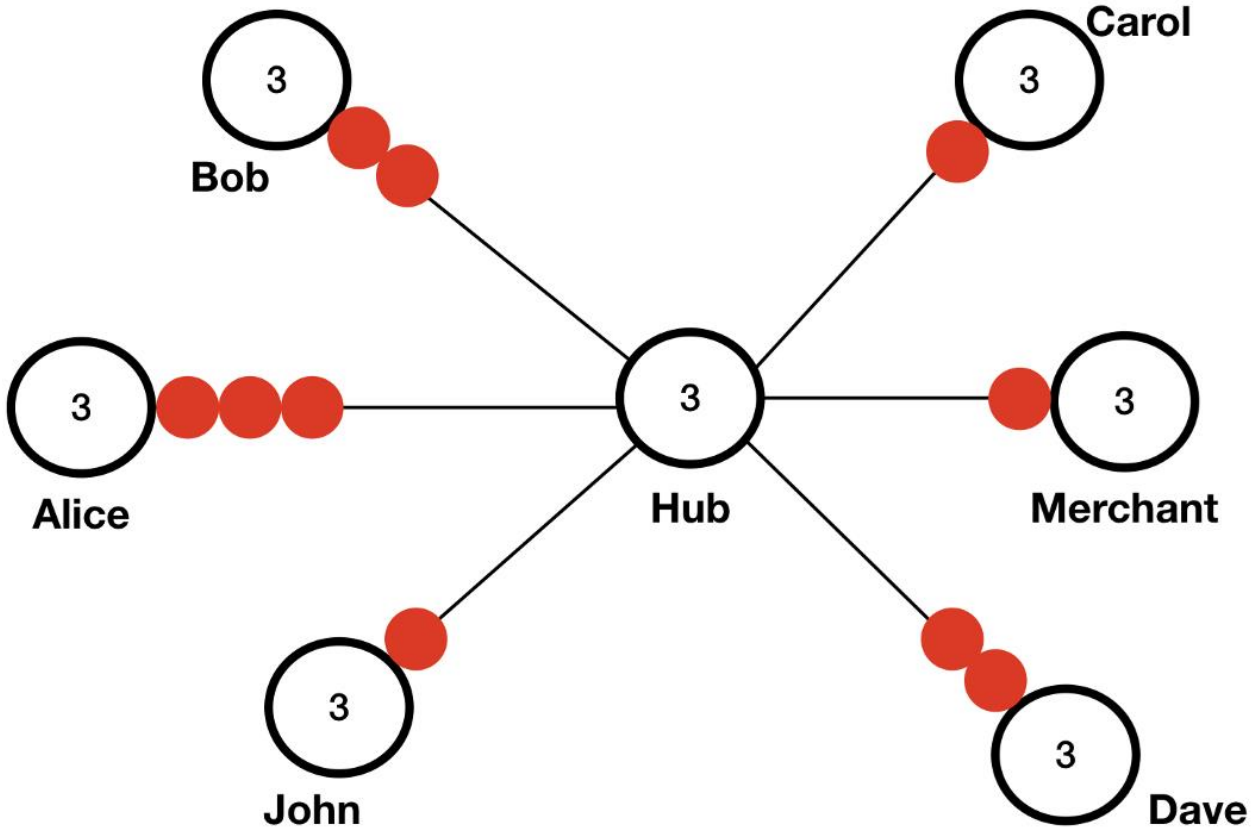
bitcoin taiwan

Lightning Network reality



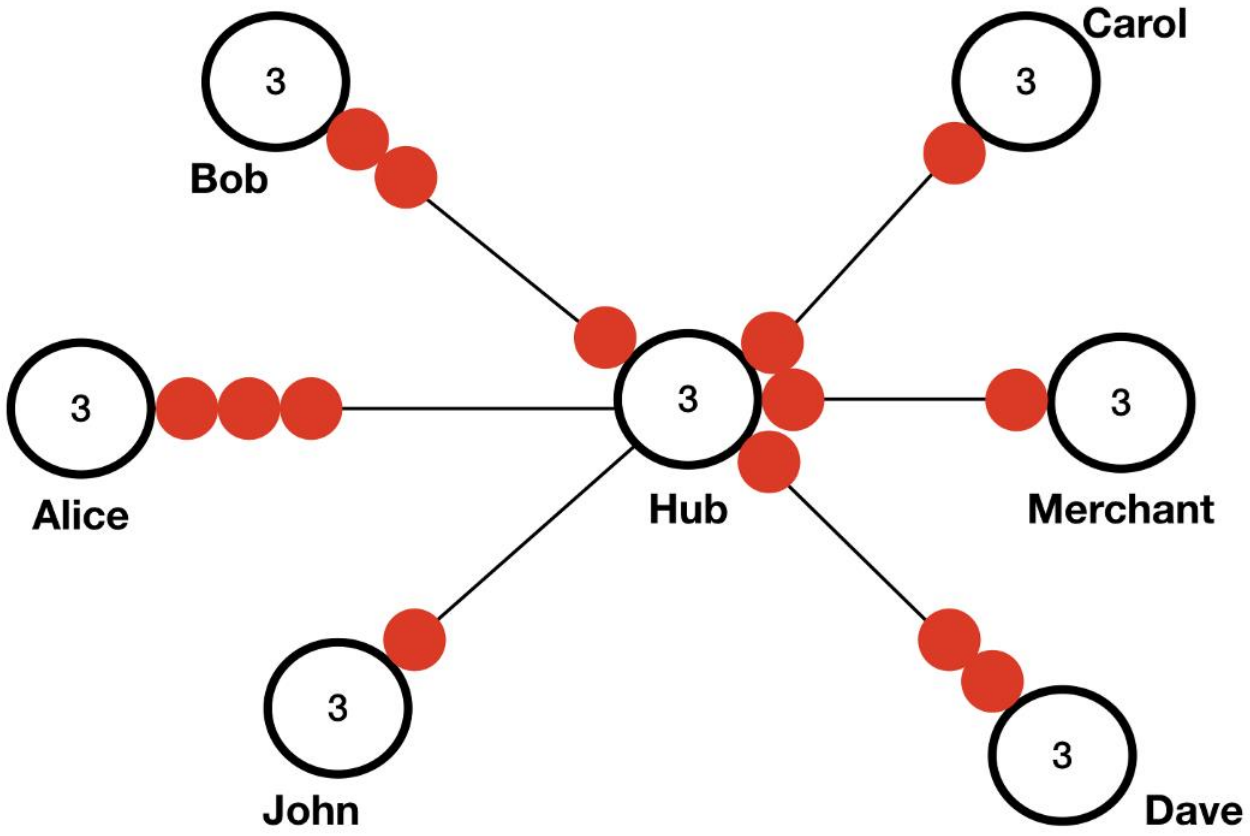
bitcoin taiwan

How much can Alice send?



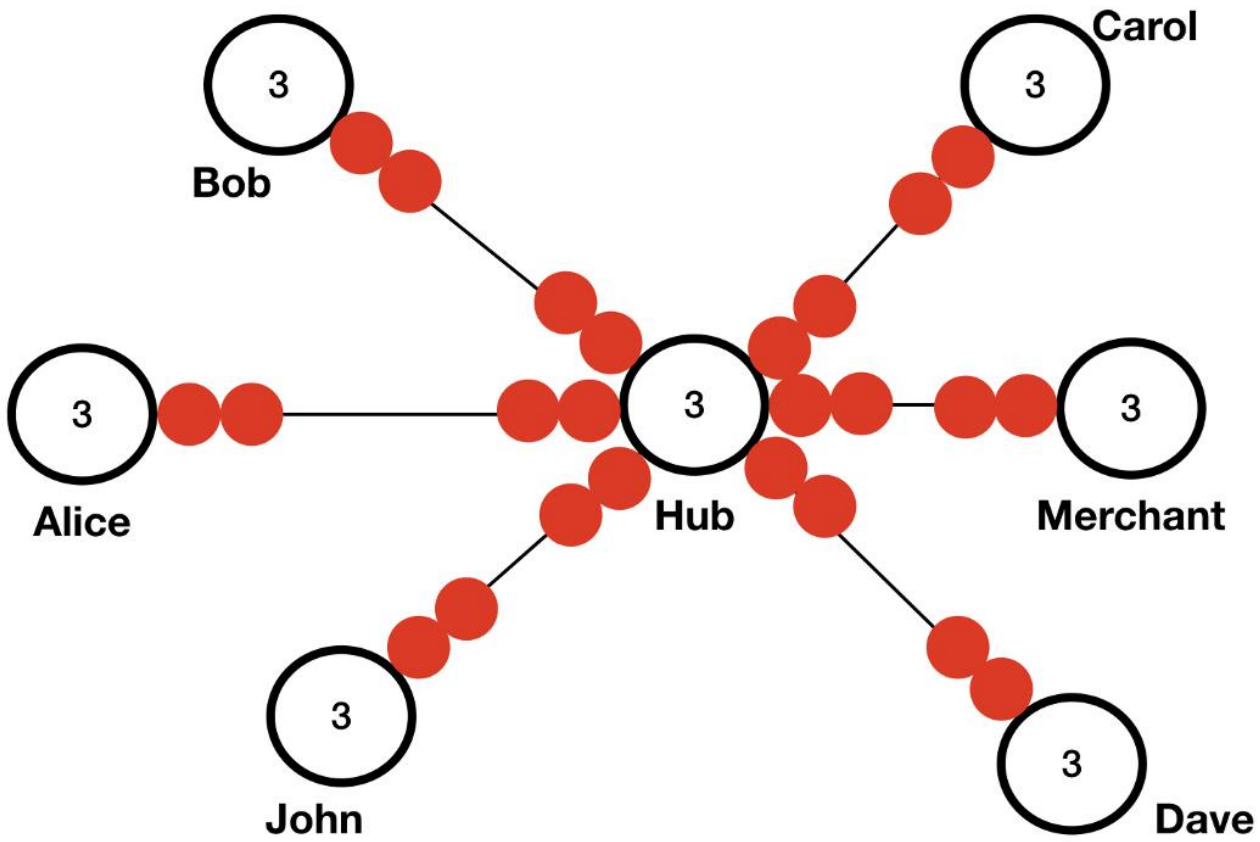
bitcoin taiwan

How about this?



bitcoin taiwan

Hopefully in the future



bitcoin taiwan

Real-Time Lightning Network Statistics

Number of Nodes	Number of Channels	Network Capacity	Node Countdown
8,434 ↑ +4.34%	37,440 ↓ -3.2%	1,036.56 BTC ↓ -3% $8,131,461.35	991,566 0.8%

Nodes with Active Channels	New Nodes (24h)	New Channels (24h)	Channel Countdown
4,285 ↑ +1.25%	18 ↑ +5.88%	248 ↑ +48.50%	962,560 3.7%

Nodes with Public IP	Updated Nodes (24h)	Updated Channels (24h)	Capacity Countdown
3,406	398	29,844	998,963 0.10%

Average Node Capacity	Average Channel Capacity	Layer 1 Capacity Ratio	
0.242 BTC $1,897.65	0.028 BTC $216.92	0.004936%	

比特幣閃電網路：可擴展的 off-chain 即時支付

The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

README.md

⚡閃電網路資源整理 | ⚡Lightning network resources

Powered by Chen Po Wei

Bitcoin Lightning network

https://github.com/cypherpunks-core/Lightning_network_resources_zh

目錄 | Contents

- ⚡ 閃電網路資源整理 | ⚡ Lightning network resources
  - 目錄 | Contents
  - 比特幣資源 | Bitcoin resources
    - 區塊鏈概述 | Blockchain overview
    - 比特幣的基礎知識 | Basic knowledge of Bitcoin
  - ⚡ 閃電網路協議 | Lightning Network Protocol
    - ⚡ 閃電網路概述 | Lightning Network Overview
    - ⚡ 進階閃電網路 ｜ Advanced lightning network
      - 主要論文 | Main paper
      - 摘要 | abstract
      - 演示幻燈片
      - 其他論文與規範 | Other papers and specifications
    - ⚡ 實現 | Implementations
    - ⚡ 閃電網路 app
      - 💰 錢包 | Wallet
        - 💻 桌面界面 | Desktop Interfaces
        - 📱 移動應用程序 | Mobile applications
        - Web界面 | Web Interfaces

iwan

閃電網路白皮書

比特幣閃電網路：可擴展的 off-chain 即時支付

https://github.com/cypherpunks-core/lightning_network_whitepaper_zh

比特幣閃電網路：可擴展的 off-chain 即時支付 | The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

Translator Chen Po Wei

Joseph Poon joseph@lightning.network

Thaddeus Dryja rx@awsomnet.org

二零一五年十一月二十日 草案版本 0.5.9.1

目錄

- 比特幣閃電網路：可擴展的 off-chain 即時支付 | The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments
  - 目錄
  - 摘要 | Abstract
  - 1 比特幣區塊鏈可擴展性問題 | The Bitcoin Blockchain Scalability Problem
  - 2 小額支付通道可以解決可擴展性問題 | A Network of Micropayment Channels Can Solve Scalability
    - 2.1 小額支付通道不要求信託 | Micropayment Channels Do Not Require Trust
    - 2.2 通道網路 | A Network of Channels
  - 3 雙向支付通道 | Bidirectional Payment Channels
    - 3.1 頻道創建中存在的問題

https://github.com/cypherpunks-core/lightning_network_whitepaper_zh

aiwan

閃電的未來

下一代擴展

BTC	ETC	LTC	PayPal	“Next Gen Blockchain”
7 tps	20 tps	56 tps	193 tps	300,000 tps

Bitcoin Lightning

500tps per channel

閃電的未來

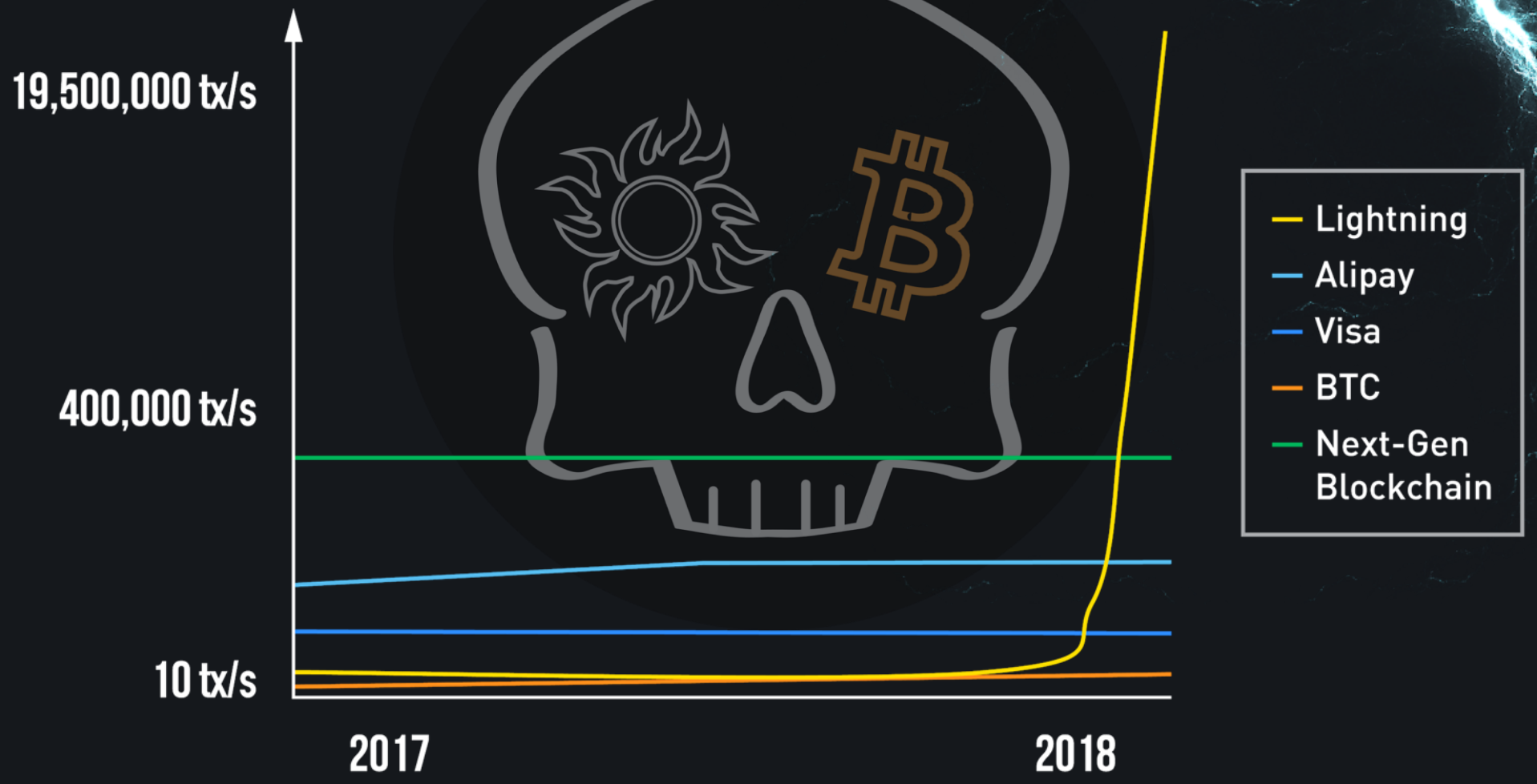
500^{tps} x 39,000

channels

= 19,500,000 tps

Equivalent of 3 TB on-chain blocks

下一代擴展


19,500,000 tx/s
400,000 tx/s
10 tx/s
2017
2018
Lightning
Alipay
Visa
BTC
Next-Gen Blockchain

Real-Time Lightning Network Statistics

Number of Nodes	Number of Channels	Network Capacity	Node Countdown
8,999 ↑ +3.51%	34,340 ↓ -0.4%	942.44 BTC ↓ 0% $12,000,918.66	991,001 0.9%

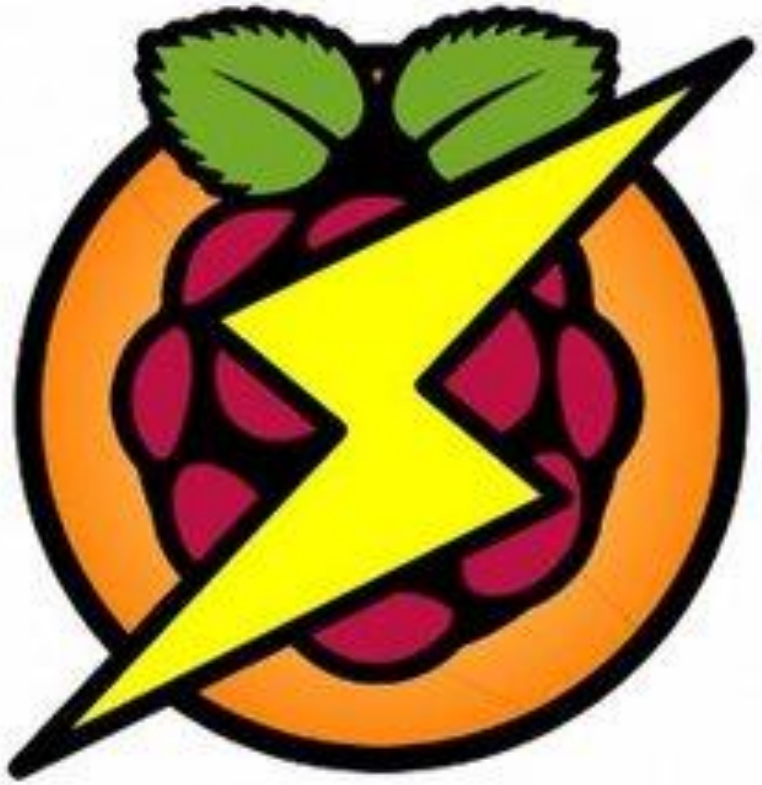
Nodes with Active Channels	New Nodes (24h)	New Channels (24h)	Channel Countdown
4,426 ↑ +1.58%	16 ↑ +45.45%	203 ↑ +52.63%	965,660 3.4%

Nodes with Public IP	Updated Nodes (24h)	Updated Channels (24h)	Capacity Countdown
3,513	332	27,423	999,058 0.09%

Average Node Capacity	Average Channel Capacity	Layer 1 Capacity Ratio	
0.213 BTC $2,711.45	0.027 BTC $349.00	0.004488%	

Lightning Wallet

搭建閃電網路 節點



RaspiBolt

Bitcoin & Lightning Node

en una Raspberry Pi

Asequible! Rápido! Funcional!

van

RaspiBlitz v0.1 fulmo-raspiblitz-main
Bitcoin Fullnode + Lightning Network
load average: 3.65, 2.76, 1.30, CPU 73°C
Free Mem 537M / 927M Free HDD 215G (76%)
Local 192.168.178.49 ▼ 12.0MiB ▲ 19.0MiB
Public 91.65.1.30:8333 Not reachable
Bitcoin v0.16.0 mainnet Sync OK (100.00%)
LND v0.4.2 wallet 220677 sat
2/2 Channels 194092 sat
91.65.1.30:9735

Casastore

PAY WITH CRYPTO SHIPPING & RETURNS HELP VISIT CASA WEBSITE

Casa Node + Casa Gold Membership

$300.00

Description

Here to get a Casa Node?

You can Buy a Casa Node with Gold Membership now over at our new website.

Your Casa Node will ship approximately 2-4 weeks after ordering.

taiwan

閃電網路錢包

tippin.me

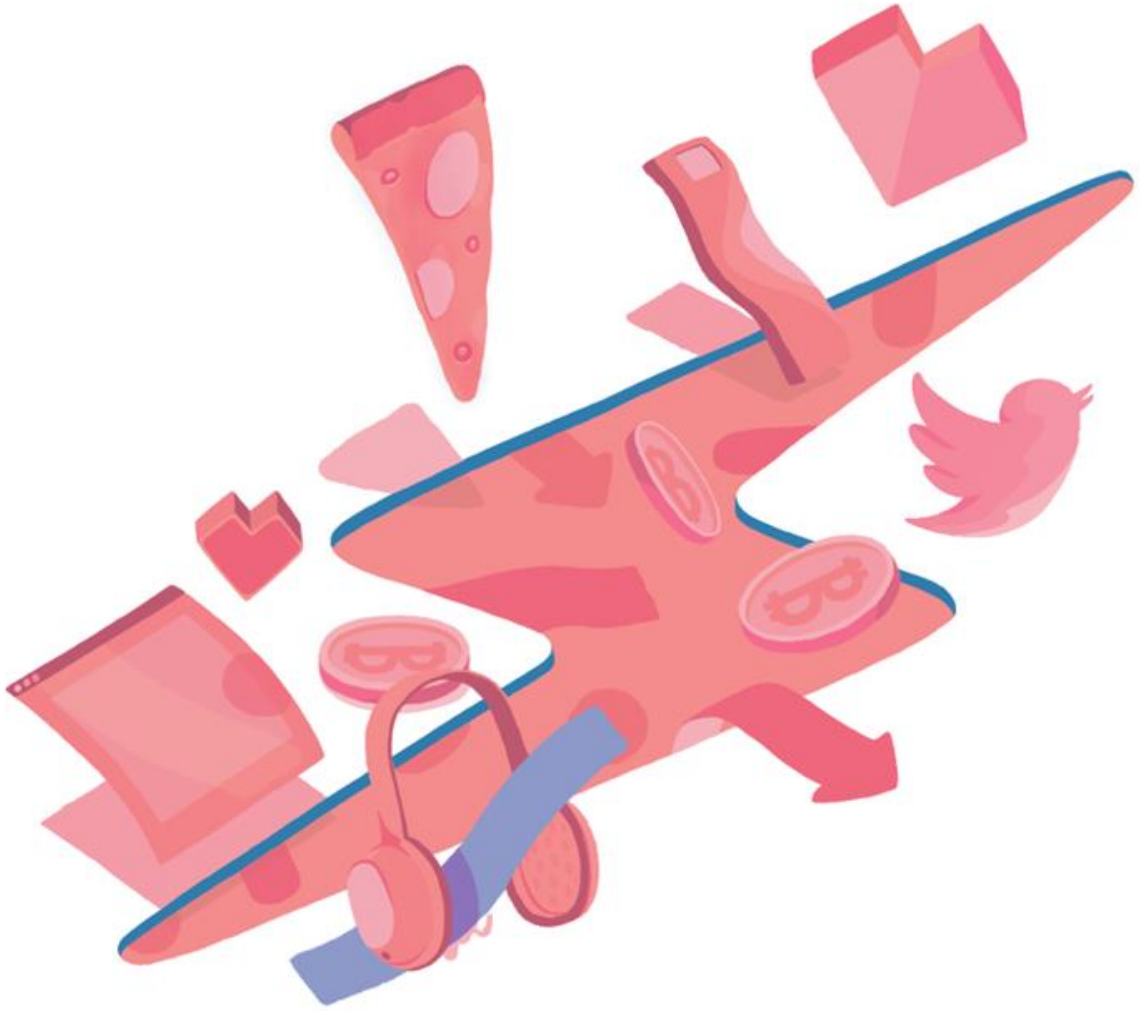
tippin.me beta

Help About Log in

Bitcoin made easy

Receive tips and micropayments anywhere with this Lightning Network Bitcoin wallet.
Sign up with your Twitter account,
cash out anytime.

Create Wallet



tippin.me beta

Help About Log in

Join now

Sign up with Twitter

We'll never post. We'll get user, pic and email.

🚧

This is a beta project, just like the Lightning Network itself, so losing small amounts is a possibility.
Be good and don't play with big amounts!
Send any feedback or bug to support@tippin.me

_Robin_Pan

要授權 tippin.me 使用你的帳戶嗎？

授權應用程式 取消

此應用程式將可以：

- 從您的時間軸上讀取推文。
- 查看你跟隨了哪些人。
- 查看你的電子郵件地址。

將無法：

- 跟隨新的人物。
- 更新您的個人檔案。
- 為你發佈推文。
- 存取你的私人訊息。
- 查看您的 Twitter 密碼。

tippin.me

由 TippinMe

tippin.me

A simple platform to receive micro-payments and tips using Lightning Network

隱私權政策

條款和條件

你隨時可以從「設定」頁面的應用程式標籤中，撤銷任何應用程式的存取權。

如果授權給某個應用程式，你的任何操作仍將根據 Twitter 的服務條款繼續進行。尤其，部分使用資訊將會回傳並與 Twitter 分享。如需詳細資訊，請參閱握門的隱私政策。

tippin.me beta

- ❤️ Browser extension
- 🌍 Your Tippin page
- 🎴 Your web button
- 🌮 Tacos
- 👋 Logout

0

satoshis

$ 0

May 04, 2019	Cash out	-49 sat
May 01, 2019	Cash out	-1 sat
Apr 18, 2019	No message	+50 sat
Apr 18, 2019	Cash out	-9 sat
Apr 18, 2019	Tweet ⚡	+9 sat

Show all transactions

about+

tippin.m

上午10:03 - 2019年5月3日

1 次轉推 8 個喜歡

2 1 8

推你的回覆

Koji Higashi @Coin_and_Peace · 21 小時

In their definition, federated sidechain like Liquid is also considered PoA. While it's fine naming things whatever you want, comparing it with PoW or PoS seems a bit off to me.

翻譯推文

1 3

Koji Higashi @Coin_and_Peace · 21 小時

There are way too many new made-up words and/or tokens to hide the complexity or justify existence of some things...

翻譯推文

3

顯示其他回覆，包括可能含有冒犯內容的回覆 顯示

tippin.m

tippin.me ⚡ get tips lightning fast

tippin.me/

@Coin_and_Peace

⚡ Copy Request

Open a direct channel **with us**.

閃電網路錢包

BlueWallet

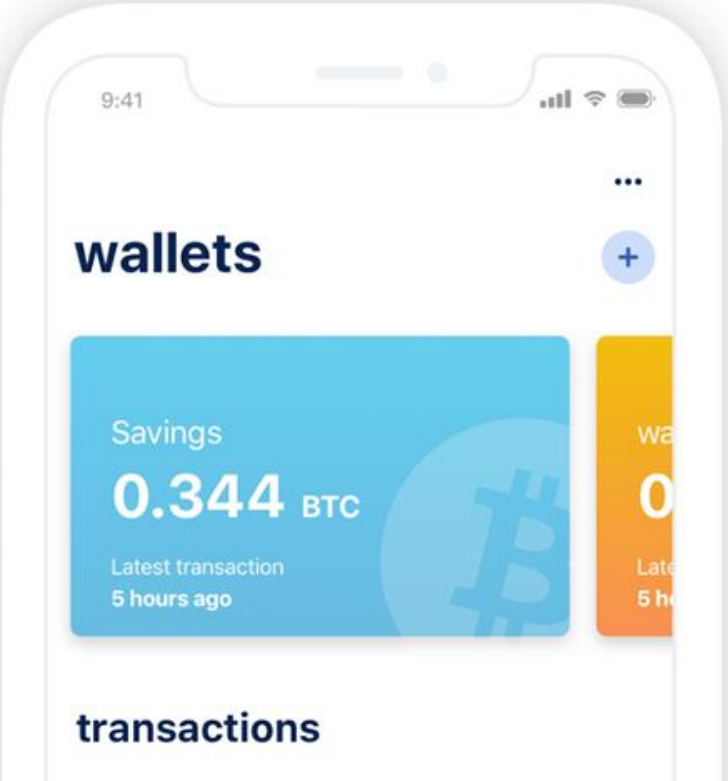
BlueWallet

Features Download Contact Help

A **Bitcoin and Lightning wallet** for iOS and Android

Easy to use and secure

Looking for a desktop wallet? Try out our friends at **Bitlum**



BlueWallet

Wallet types

Previous Next

Bitcoin onchain
0.344 BTC
Latest transaction
5 hours ago

Bitcoin Lightning
300 000 sats
Latest transaction
5 hours ago

Single address
0.344 BTC
Latest transaction
5 hours ago

Bitcoin wallet

The main Bitcoin wallet is easily created from the add wallet screen. It is Segwit compatible and a Hierarchical Deterministic wallet, which means that it generates new receiving addresses every time you tap receive, making it more privacy friendly.

Lightning wallet

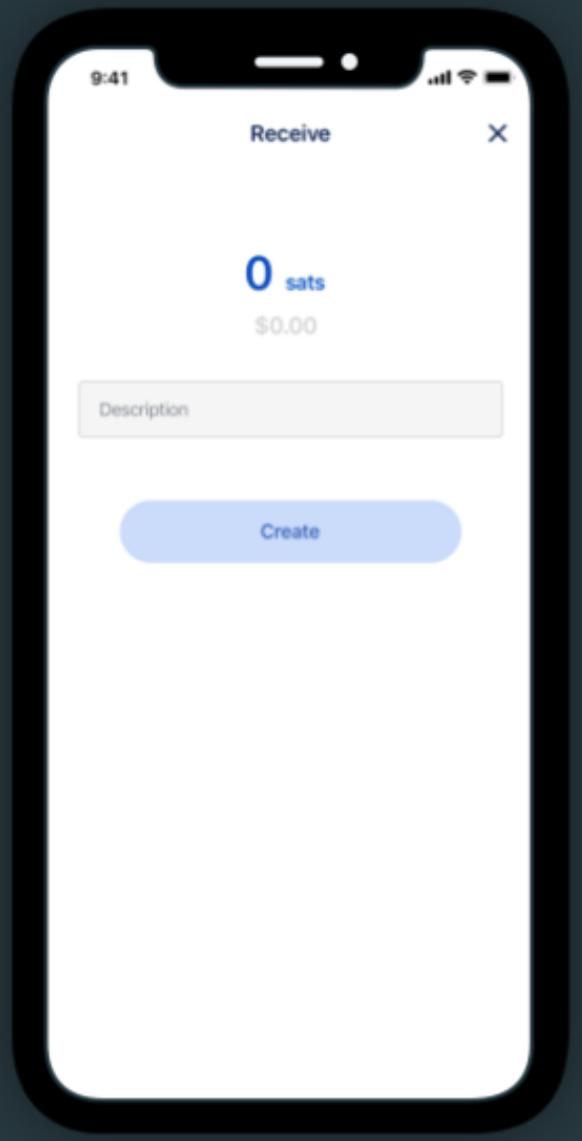
The Bitcoin Lightning wallet can be used on custodial fashion or non-custodial if you run your own node. This wallet provides the ability to receive lightning out of the box and send payments as well. It is powered by our opensource LNDhub solution.

Read more

Single address

The Single address Bitcoin wallet, its a Segwit compatible wallet that always will have the same receiving address. This use case its useful if you want an unique address to receive donations for instance. This wallet also supports RBF.

Features



Refill available

Allows you top up or refill your Lightning wallet with Bitcoin. It requires an on-chain Bitcoin wallet to use it. It needs 3 confirmations to validate the transaction.

Withdraw coming soon

Allows you get your funds back to a Bitcoin on-chain wallet. At the moment Bluewallet redirects you to zigzag.io while the feature is not ready.

Send available

Make payments or send Satoshis after scanning a QR code or having an address. Allows to Scan QR codes, Use screenshots of QR codes or a Lightning addresses. To use requires having funds previously.

Receive available

Recieve payments by generating an invoice. Generates a QR code and an address with expiration time that can be easily shared. Allows to open a direct channel with the node.

Backup/export Key available

Through the wallet options menu you will find the option to backup/export your key. This is a LNDhub key that will only work on services like bluewallet that use LNDhub.

Lightning mobile wallets

Warning: some recent wallets might be scams. Be carefull when experimenting with new wallets.

其它錢包選擇

https://lightningnetworkstores.com/wallets

Name	Open source	Requires own node	Custodial	Mainnet launch date	Web wallet	Mainnet	Testnet
[illegible]	[illegible]	no	no	April 2018	no	android	android
bitcoin lightning wallet	yes	no	no	May 2018	no	android	android
Wallet of Satoshi	no	no	yes	January 2019	no	android iOS	
[illegible]	yes	no	yes	December 2018	no	android iOS	
Bit[illegible]		no	yes	February 2019	yes		
Lig[illegible]		no	no	March 2019	no	android iOS	
Bre[illegible]		no	no	April 2019	no	android	
Mu[illegible]		no	no	May 2019	no	android	
Bit[illegible]		no	yes	March 2019	no	android iOS	
Tippin.me	no	no	yes	December 2018	yes		

How to start

1

Have an on-chain Bitcoin wallet

If you want to refill your wallet with some Satoshis, you need first to have an on-chain Bitcoin wallet with funds

2

Create a Lightning Wallet

Once you have created your Lightning Wallet, you will find the option "manage funds" inside your wallet. This is where you can refill your Lightning Wallet

3

Send an on-chain Transaction

Once you go to the refill option, you will find a list of your available on-chain Wallets. Select your prefered one and send a transaction with the desired amount. Keep the amount low, Lightning is experimental.

4

Start using Lightning

Once you send your transaction, it will require 3 comfirmations before your funds appear on your Lightning wallet. Once it is done, you are welcome to the Lighting experience.

中華電信 4G 下午10:08 82%

搜尋

BlueWallet - Bitcoin wallet

Bluewallet Services, S. R...

打開

評分不足

4+
年齡

新功能

版本記錄

版本 3.9.7

1 週前

v3.9.7

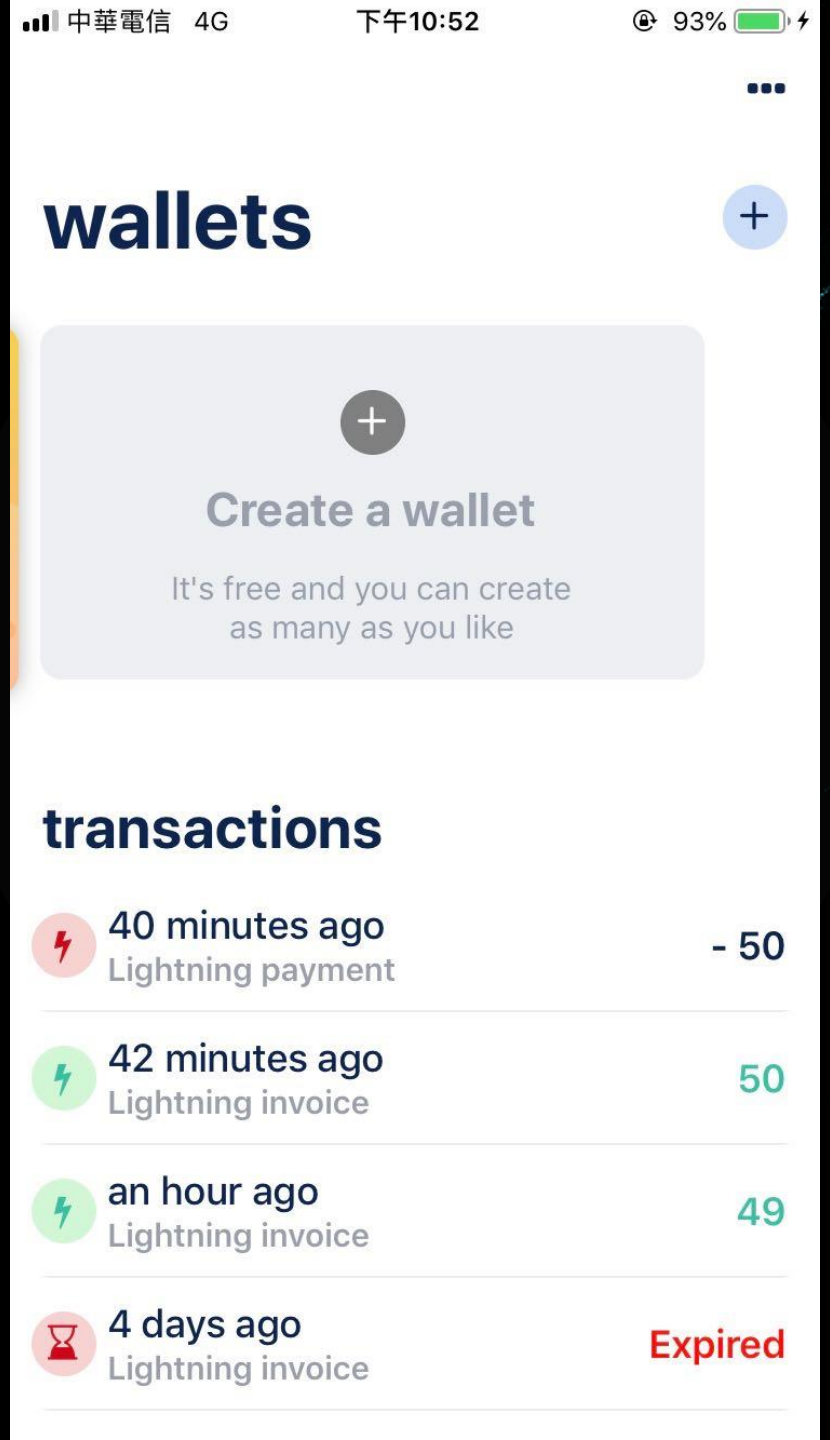
======

* ADD: intermediate step asking user t 更多

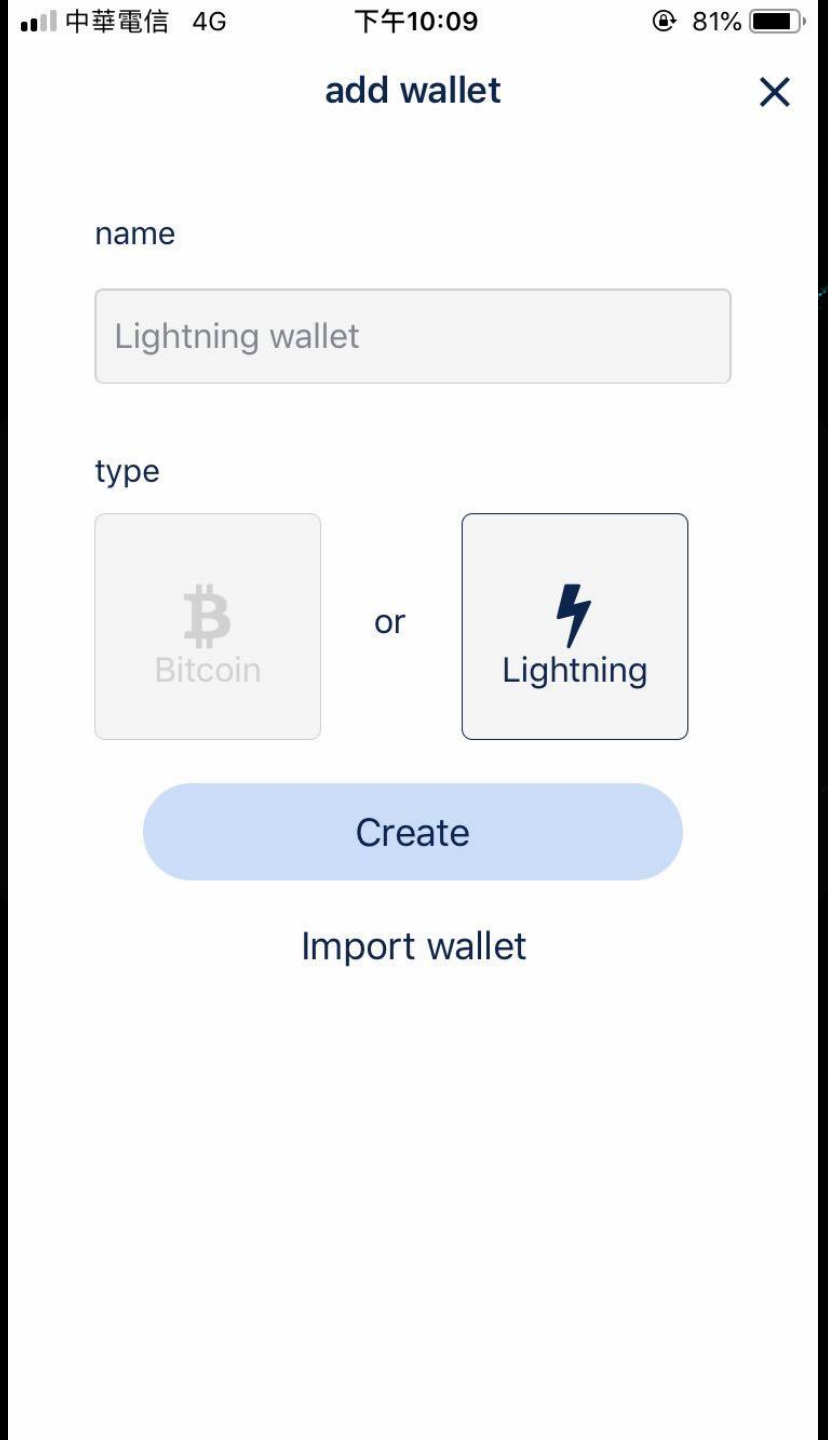
預覽

Today 遊戲 App 更新項目 86 搜尋

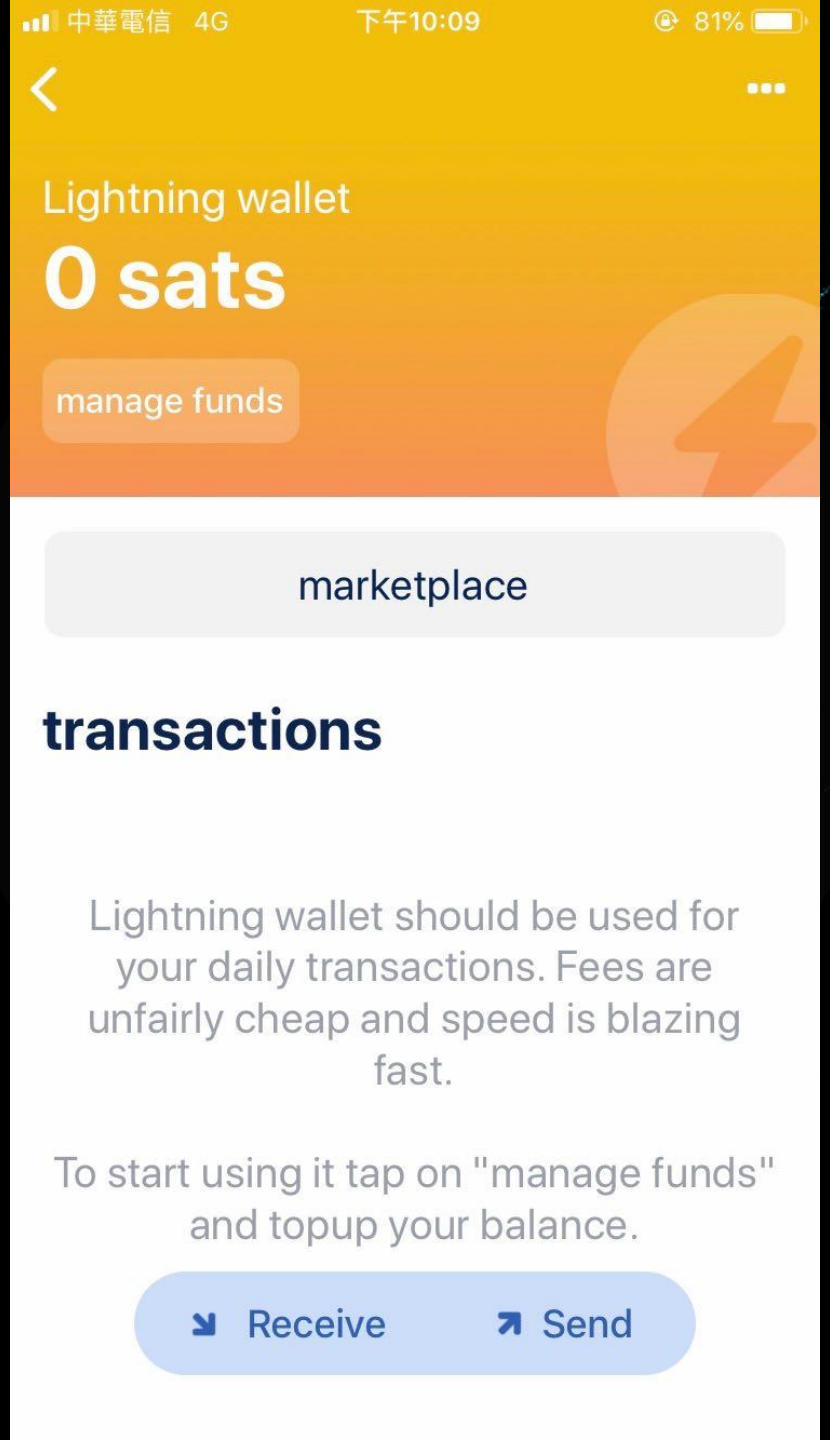
App首頁


中華電信 4G
下午10:52
93%
wallets
Create a wallet
It's free and you can create as many as you like
transactions
40 minutes ago
Lightning payment
- 50
42 minutes ago
Lightning invoice
50
an hour ago
Lightning invoice
49
4 days ago
Lightning invoice
Expired

新增錢包

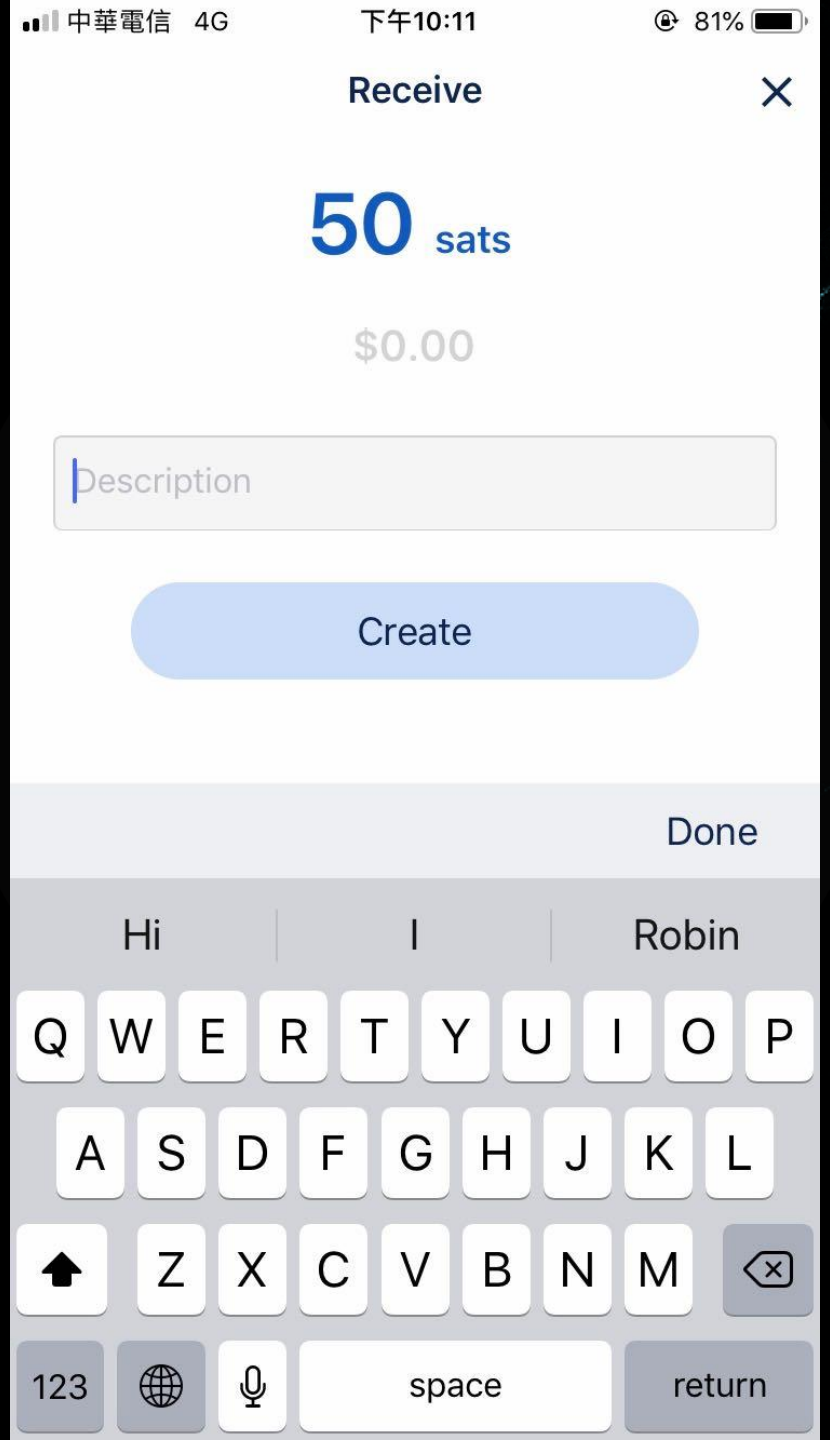

中華電信 4G
下午10:09
81%
add wallet
name
Lightning wallet
type
Bitcoin
or
Lightning
Create
Import wallet

錢包頁面

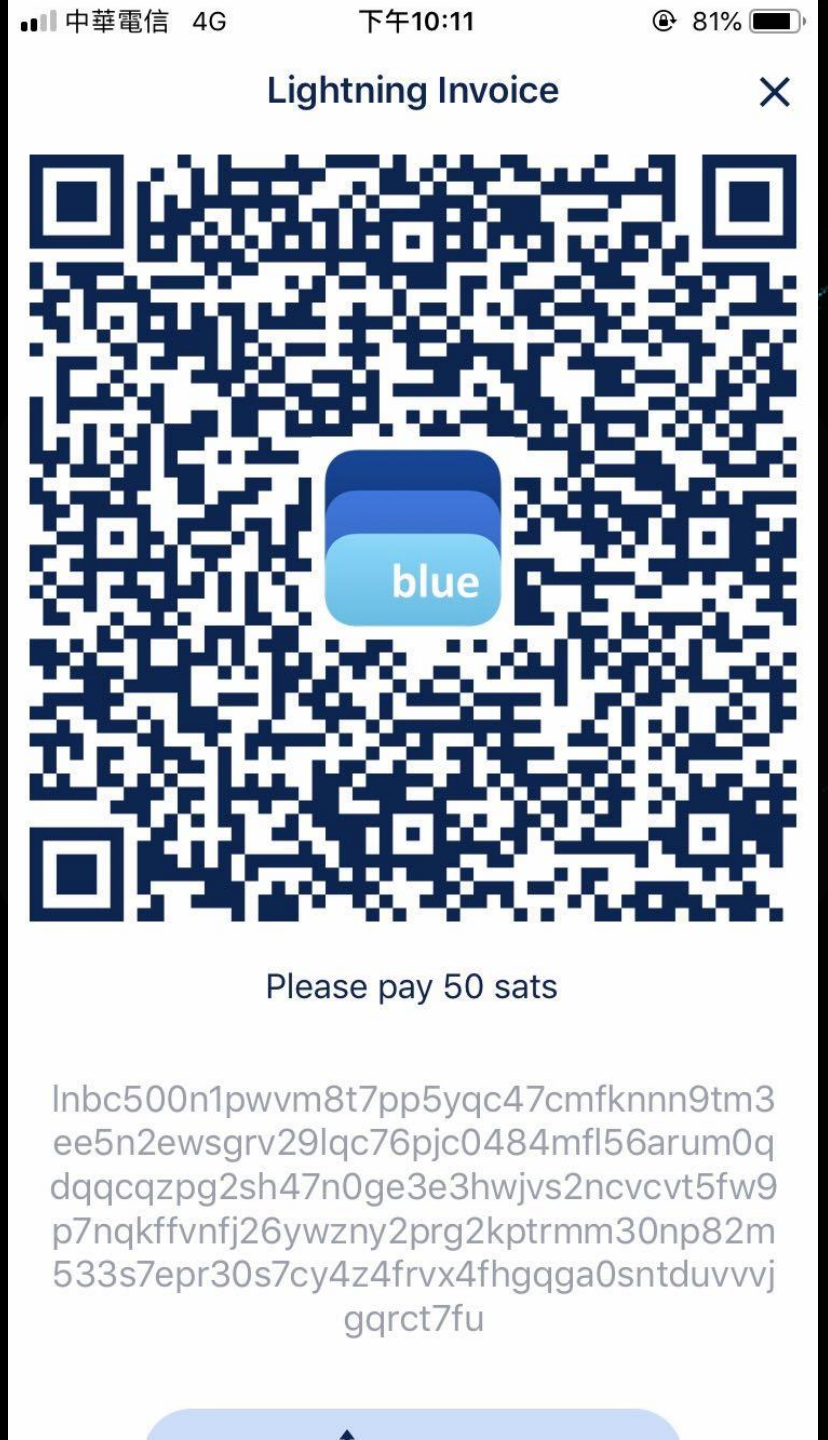

中華電信 4G
下午10:09
81%
Lightning wallet
0 sats
manage funds
marketplace
transactions
Lightning wallet should be used for your daily transactions. Fees are unfairly cheap and speed is blazing fast.
To start using it tap on "manage funds" and topup your balance.
Receive
Send

收款

創建Invoice

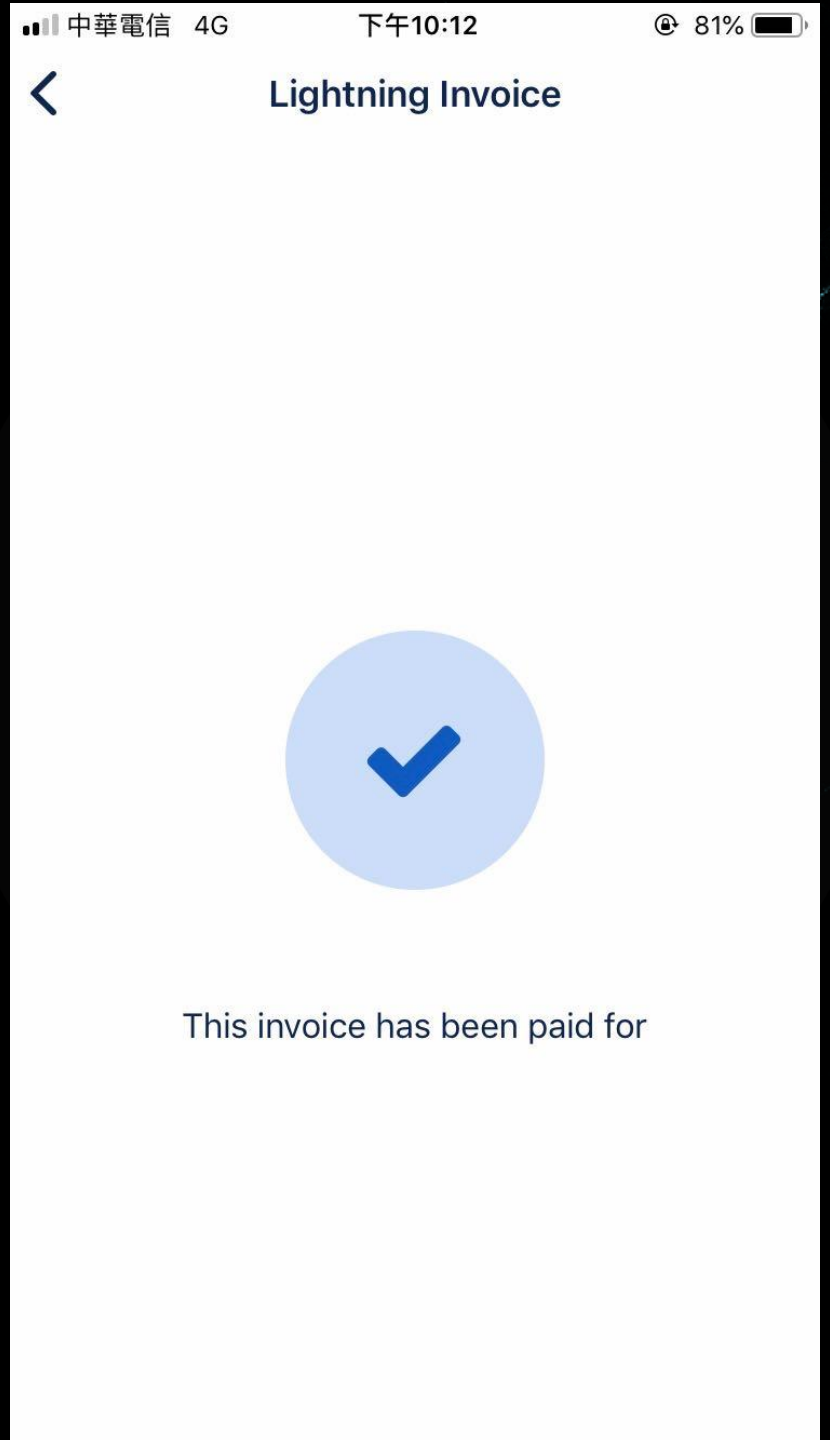


Invoice頁面


中華電信 4G
下午10:11
81%
Lightning Invoice
blue
Please pay 50 sats
lnbc500n1pwvm8t7pp5yqc47cmfknnn9tm3ee5n2ewsgrv29lqc76pjc0484mfl56arum0qdqqcqzpg2sh47n0ge3e3hwjvs2ncvcvt5fw9p7nqkffvnfj26ywzny2prg2kptrmm30np82m533s7epr30s7cy4z4frvx4fhgqga0sntduvvvjgqrct7fu

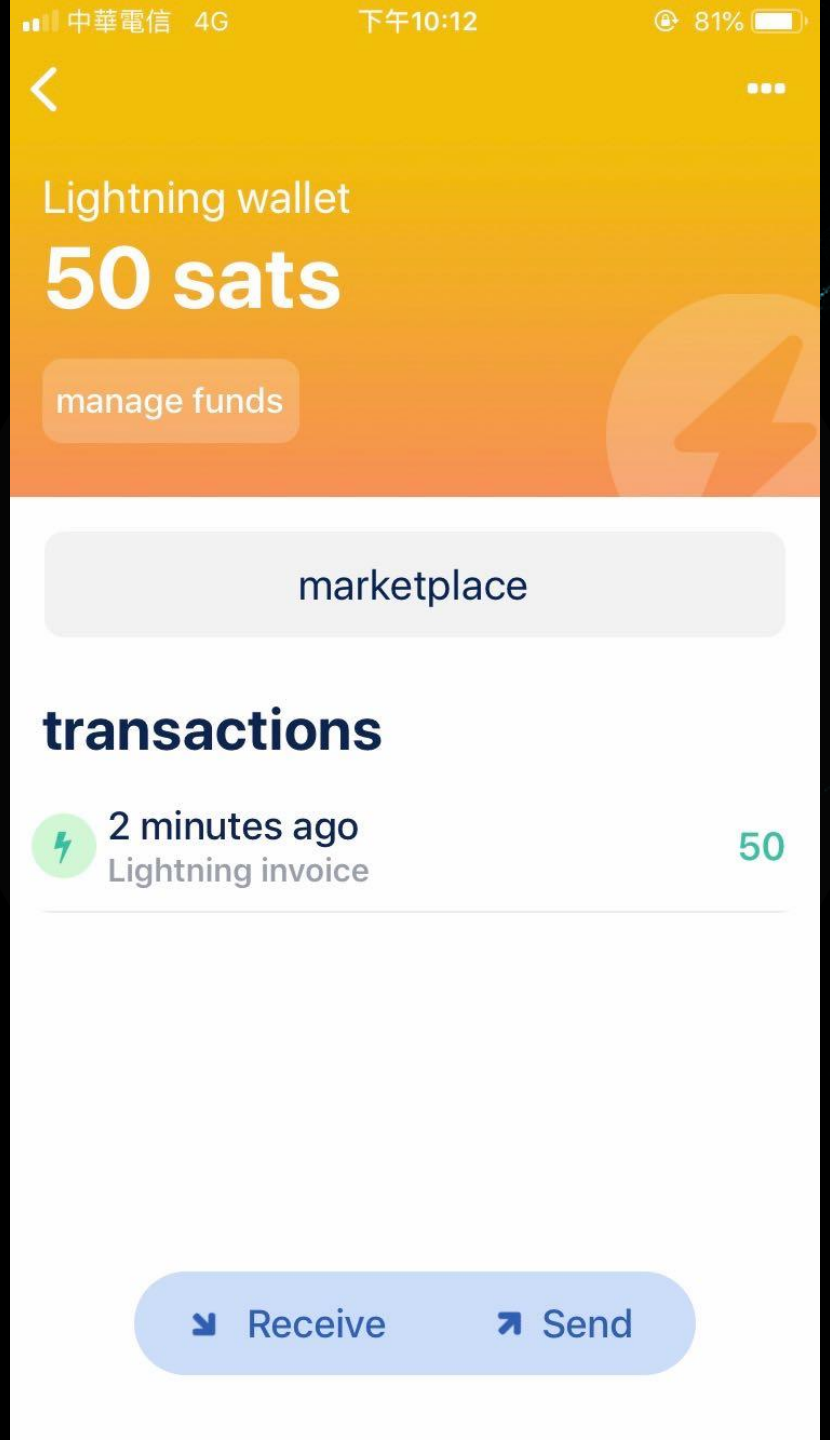
收款成功

Invoice頁面跳轉

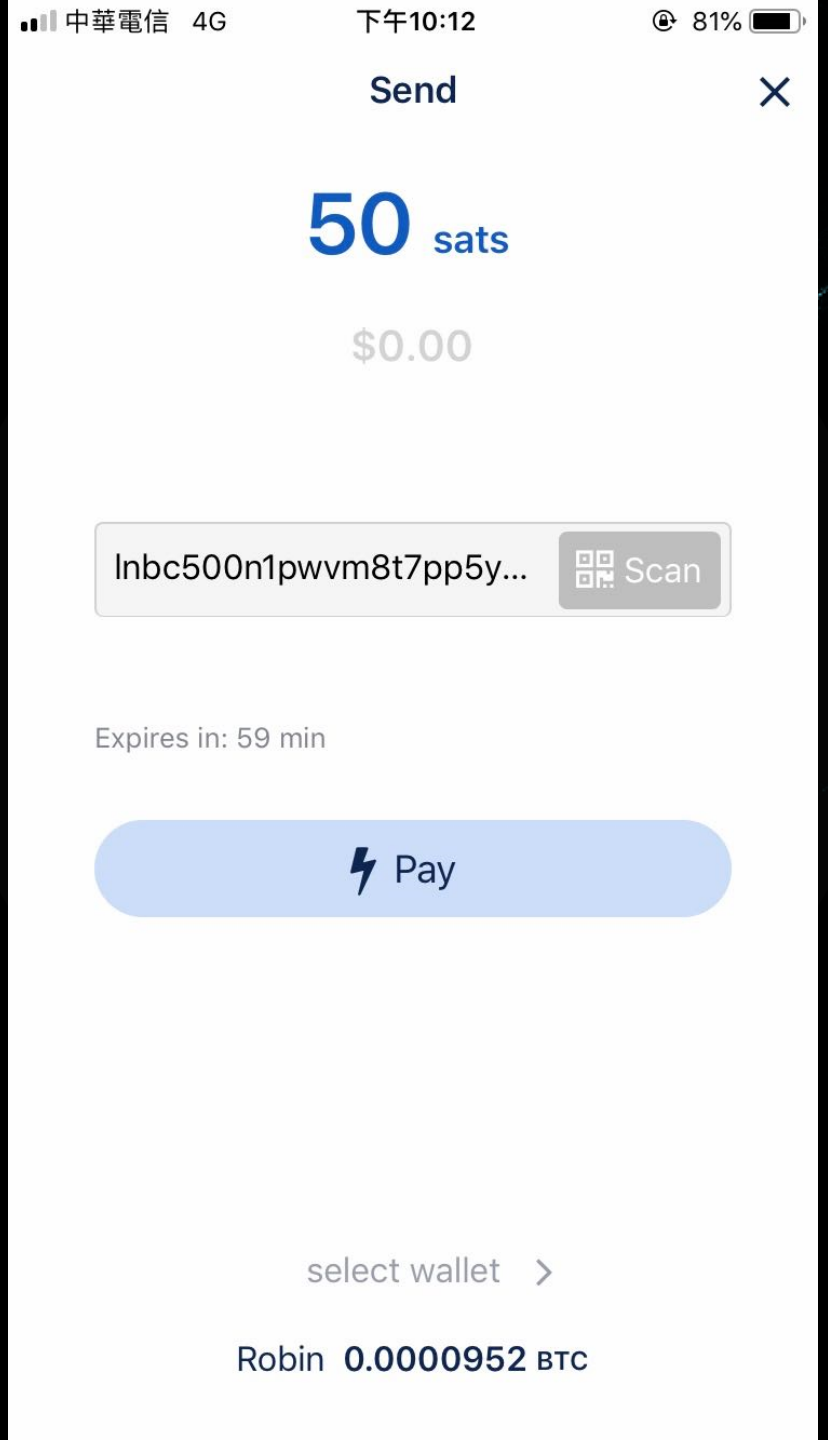


錢包頁面

收到 50 sat

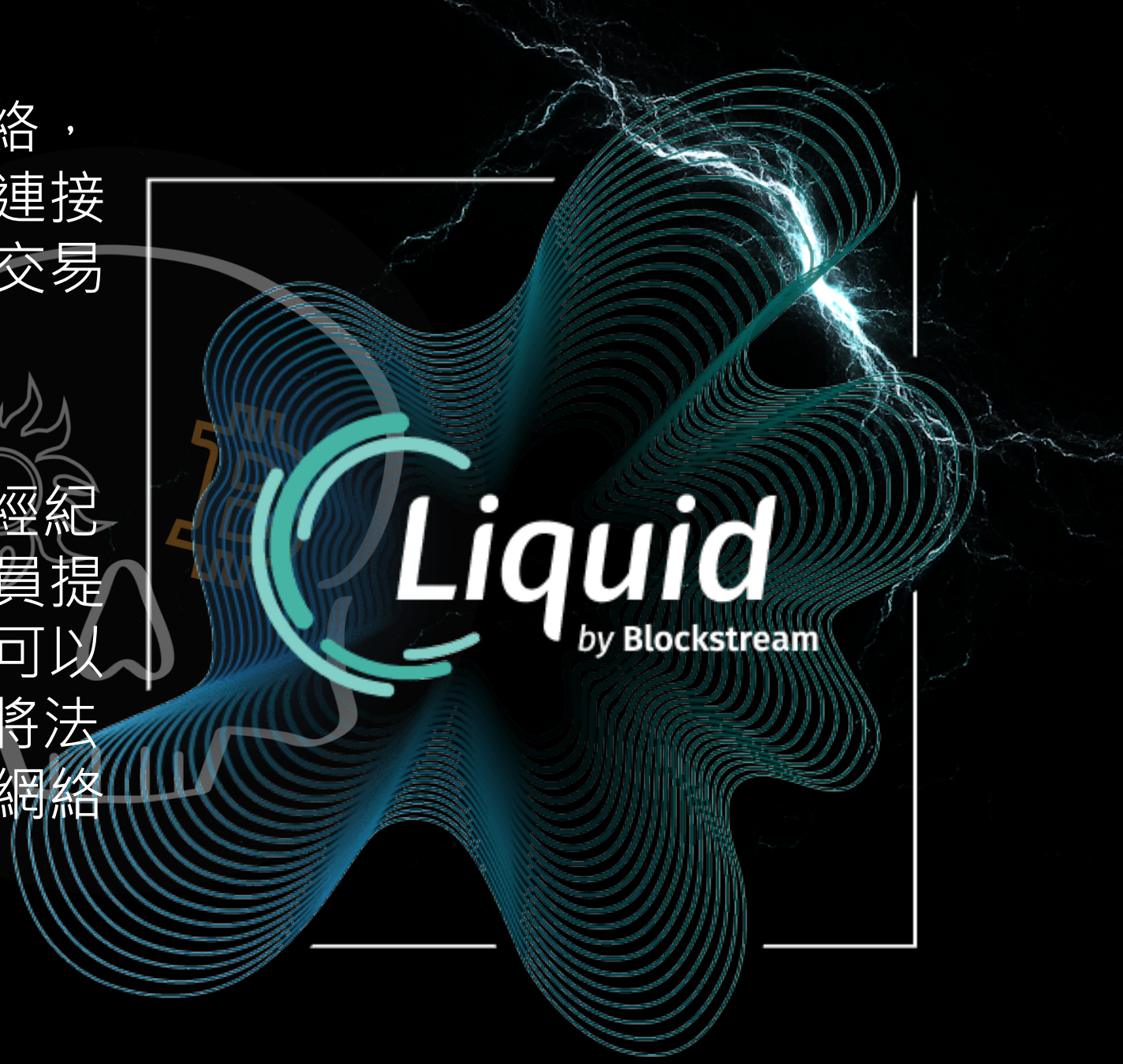


發送交易


中華電信 4G
下午10:12
81%
Send
50 sats
$0.00
lnbc500n1pwvm8t7pp5y...
Scan
Expires in: 59 min
Pay
select wallet
Robin 0.0000952 BTC

Liquid是一個交易所間的清算網絡，將全球的加密貨幣交易所和機構連接起來，提供更快更私密的比特幣交易以及數字資產發行服務。

Liquid網絡是一個面向交易所、經紀商和造市商的區塊鏈，為網絡成員提供快速保密的比特幣交易。用戶可以通過Liquid的已發行資產技術，將法幣、證券，甚至其他加密貨幣在網絡上進行代幣化。

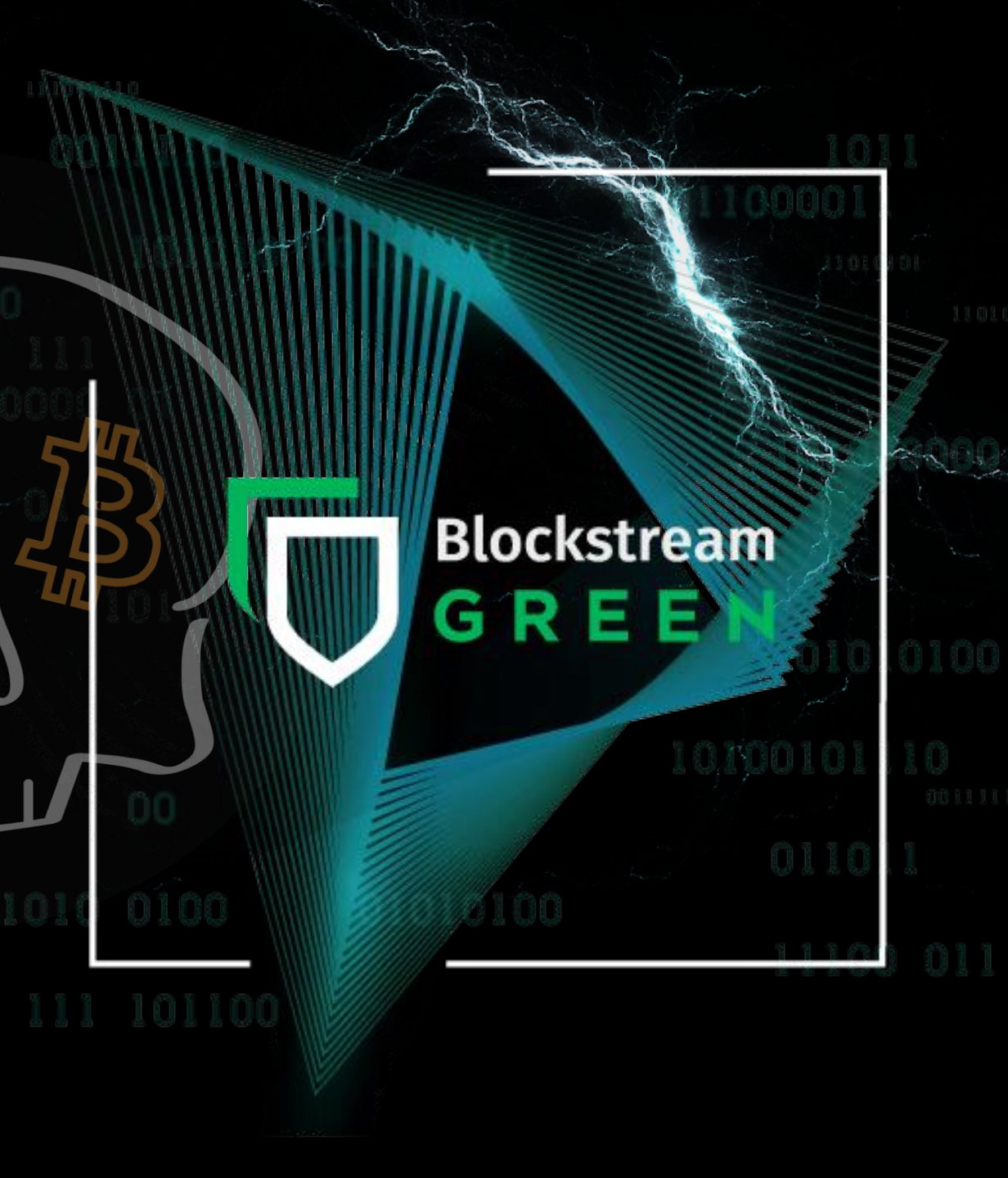


Liquid Network 和閃電網路的設計不同

	Liquid Network	Lightning Network
交易確認時間	2 分鐘	立刻
交易手續費	較高（根據交易量）	低
抵押比特幣資產	需經過 102 確認次數，才可雙向錨定	開創通道
贖回比特幣資產	經過節點（Federation）確認	關閉通道
信任機制	聯邦信任機制（Federation）	交易雙方
是否可發行代幣	O	X
多重簽名	O	X
支援智能合約	O	X

https://www.blocktempo.com/blockstream-explained-liquid-network-in-cypherpunks-taiwan/

創新多重簽名模型使用雙私鑰 - 一個由用戶持有，另一個由我們的服務器持有。這允許我們強制執行雙因素身份驗證來保護您的資金，而時間智能合約保證用戶始終保持對其硬幣的完全控制。



9:41
Blockstream
GREEN
Bitcoin
Create New Wallet
Restore a Green Wallet
A wallet is detected on this device
Log In

區塊鏈隱私資源

Blockchain privacy resources

比特幣 隱私問題

- Bitcoin Address 隨機生成
  - Address 餘額 是公開檢視
  - 足夠的 交易足跡 可以知道 真實身分
    - 實名制交易所
    - 付款的過程
    - ISP的監聽
- Bitcoin 交易廣播 未加密 容易被防火牆封鎖

區塊鏈隱私資源 | Blockchain privacy resources

Powered by Chen Po Wei

https://github.com/cypherpunks-core/Schnorr_Signature_Resources_zh

目錄 | Contents

- 區塊鏈隱私資源 | Blockchain privacy resources
  - 目錄 | Contents
  - 概觀 | Overview
  - 背景 | Background
  - 機密交易 | Confidential Transactions
  - 零知識證明 | Zero Knowledge Proofs
  - 環簽名 | Ring Signatures
  - MimbleWimble
  - 蒲公英 | Dandelion
  - 防彈 | Bulletproofs
  - 其他文章 | Other articles

https://github.com/cypherpunks-core/Schnorr_Signature_Resources_zh

Schnorr簽名資源

Schnorr Signature Resources

多簽地址 問題

- 創造一個多簽交易 容量很大
  - 相對 高的手續費
  - 使得 多簽技術難以推廣
- 多簽應用
  - Green address 一個 以第三方擔保的方式 過濾 雙花攻擊
  - 交易所的 資金保管
  - 閃電網路的 通道搭建

Schnorr簽名資源 | Schnorr Signature Resources

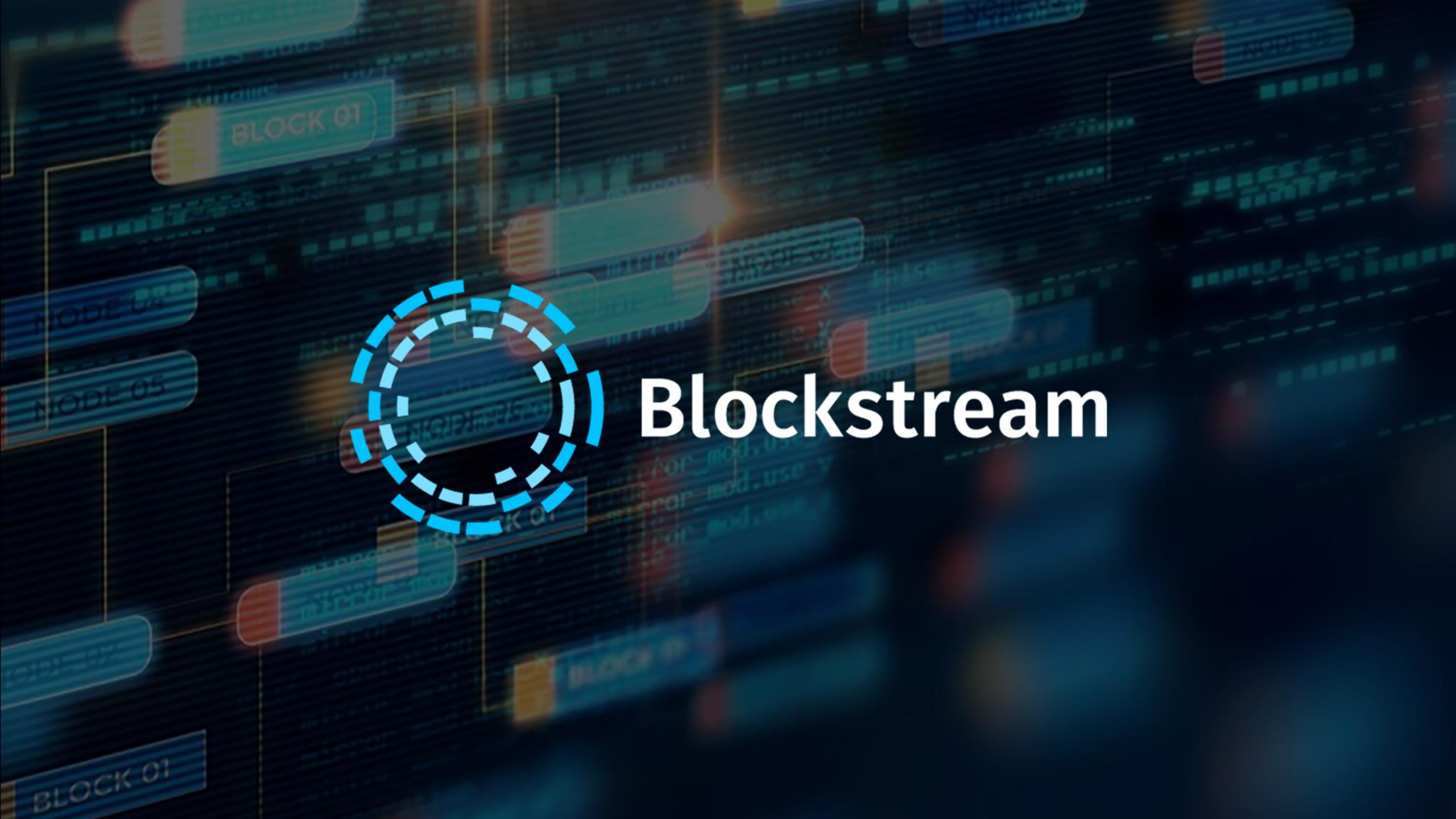
Powered by Chen Po Wei

Schnorr

Schnorr Signatures 是一個聚合多個簽名演算法，主要為了減少m-n多簽名的size，不管有多少個使用者，都可以用一個簽名來解決，從而減少區塊的大小。另外一方面這也縮短了簽名校驗的時間，因為多簽名情況下，只需要驗證一個簽名就可以。同時也可以一定程度解決匿名性，多簽名中隱藏了單個使用者的資訊。由於專利的問題，這個演算法並沒有標準實現（目前專利保護已經到期），有可能多語言之間互通還有些挑戰。Schnorr Signatures也是一種橢圓簽名演算法，不能解決量子計算攻擊。https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/ by 三眼世界

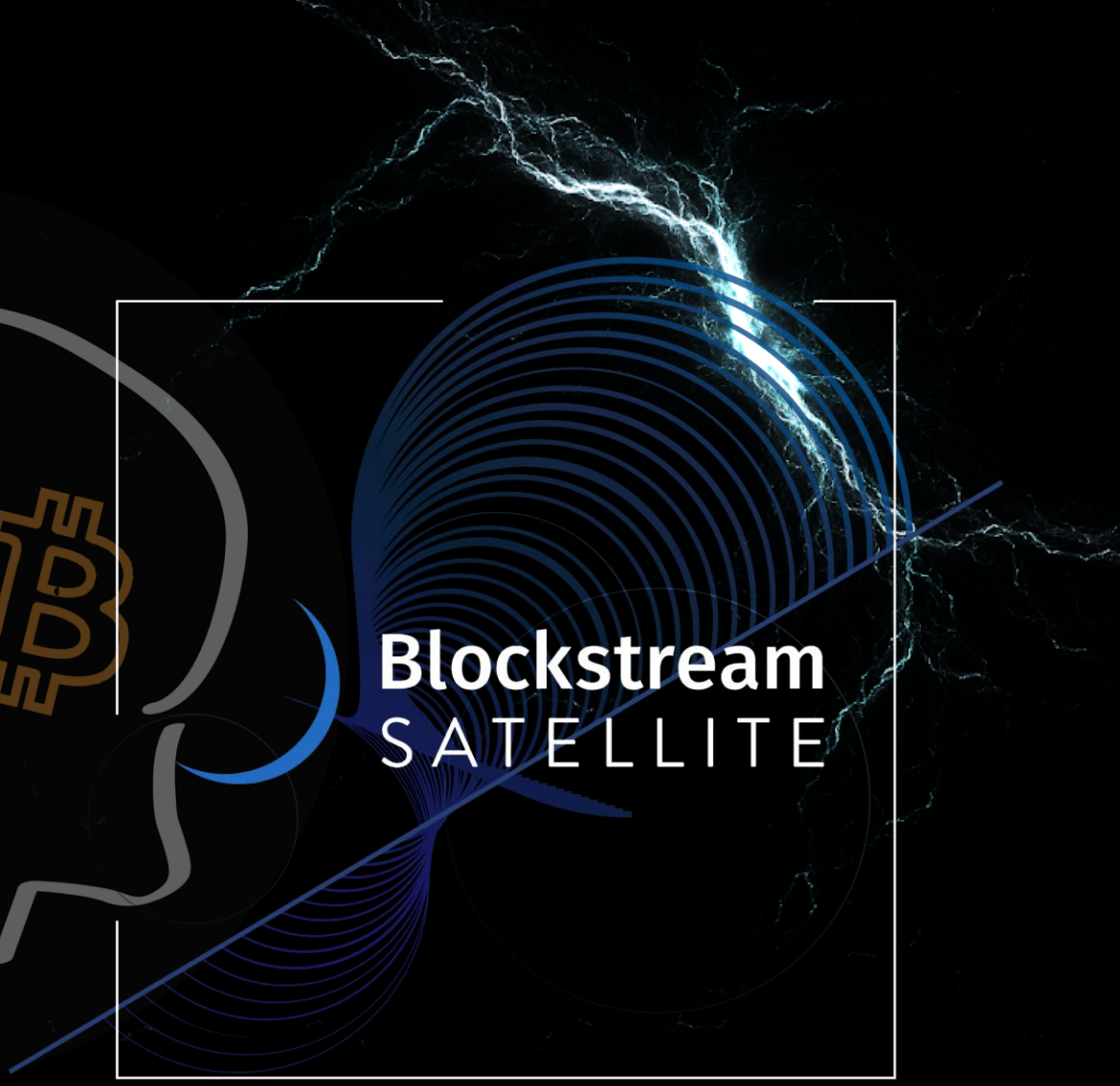
2008年專利過後的區塊鏈新專案不少使用Schnorr Signature簽名，例如monero, corda, hyperledger iroha, chain等。

Crazy Project


Blockstream

Blockstream
SATELLITE
API

Blockstream衛星網絡24小時不間斷地免費將比特幣區塊鏈廣播到全世界，保護網絡不受干擾，讓世界上的每一個人都有機會使用比特幣。



為什麼使用衛星？

- 無需上網： Blockstream衛星將比特幣區塊鏈廣播至整個地球，減少比特幣對網路的依賴。現在世界上的每一個人都有機會使用比特幣。
- 大量成本節約： 去除了成本這個障礙後，人們可以不花一分錢即可接收區塊，讓更多人能夠用上比特幣並參與到比特幣網路中來。
- 網路穩定性： Blockstream衛星提供了新的接收比特幣區塊鏈的方法，並且這個方法不會受連接故障的影響。這保護了用戶不受網路波動的影響，防止任何全節點被孤立或隔離。

工作原理

1. Blockstream衛星在地面的站點被稱為「基站（teleport）」，它們參與比特幣網路並將區塊傳送至地球同步衛星。
2. 在35,786公里（22,236英里）高空軌道運行的地球同步衛星接收來自Blockstream衛星基站的訊號，並將其廣播到地球的大部分地區。
3. 只要你在覆蓋區域內，擁有一個小型衛星天線和一個便宜的USB接收器即可接收這些區塊並保證他們的節點一直保持同步。
4. 此外，每個Blockstream衛星基站也可以從世界上的其他基站接收區塊，保證基站不會被孤立。
5. 整個Blockstream衛星網路在地球周圍形成一個環，以確保比特幣網絡具有完全冗餘。

Satellite Project 衛星計畫

目標：在台灣發射比特幣交易到TELSTAR 18V衛星 Goal: Launch Bitcoin transactions in Taiwan to TELSTAR 18V satellite

衛星計畫 材料

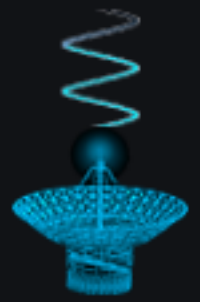
- [x] 筆電-一台裝有Linux筆電 ，最好有i5 ，硬碟要求 裝的下220GB全節點(最低要求3G修剪過的節點): https://amzn.to/2x6G86r
- [ ] 至少46公分（18英寸）衛星天線: https://amzn.to/2wBtPzK
- [ ] 軟體定義的無線電接口(Software Defined Radio Interface): https://amzn.to/2g8Nu2O
- [ ] Linear Polarization (線性極化) PLL LNB: https://amzn.to/2w0Zk4C
- [ ] LNB 安裝支架: https://amzn.to/2xgotXU
- [ ] LNB 電源: https://amzn.to/2KUGouq
- [ ] 同軸電纜: https://amzn.to/2w7N4xQ
- [ ] F連接器到SMA同軸適配器（F Connector to SMA Coax Adapter）: https://amzn.to/2gajpAh
- [x] 用於調整配件的螺絲起子和鉗子
- [ ] (選則)3英尺，衛星三腳架: https://amzn.to/2w81RZm

Blockstream satellite

API data transmission architecture

衛星網絡覆蓋範圍

mapbox
© Mapbox © OpenStreetMap Improve this map © DigitalGlobe



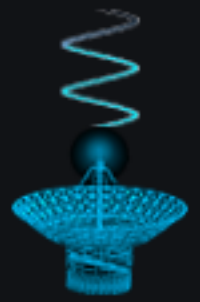
GALAXY 18

北美洲

經度：123W

頻率：12022.85 MHz

極性：水平



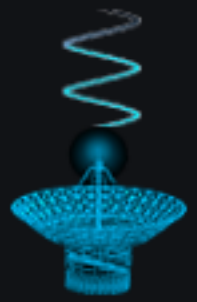
EUTELSAT 113

南美洲

經度：113W

頻率：12026.15 MHz

極性：垂直



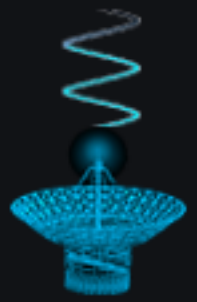
TELSTAR 11N

非洲

經度：37.5W

頻率：11476.75 MHz

極性：水平



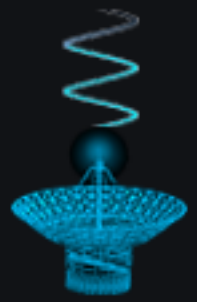
TELSTAR 11N

歐洲

經度：37.5W

頻率：11504.02 MHz

極性：垂直



TELSTAR 18V

Asia

Long: 138E

Freq: 4057.5Mhz

Pol: Horizontal

衛星計畫

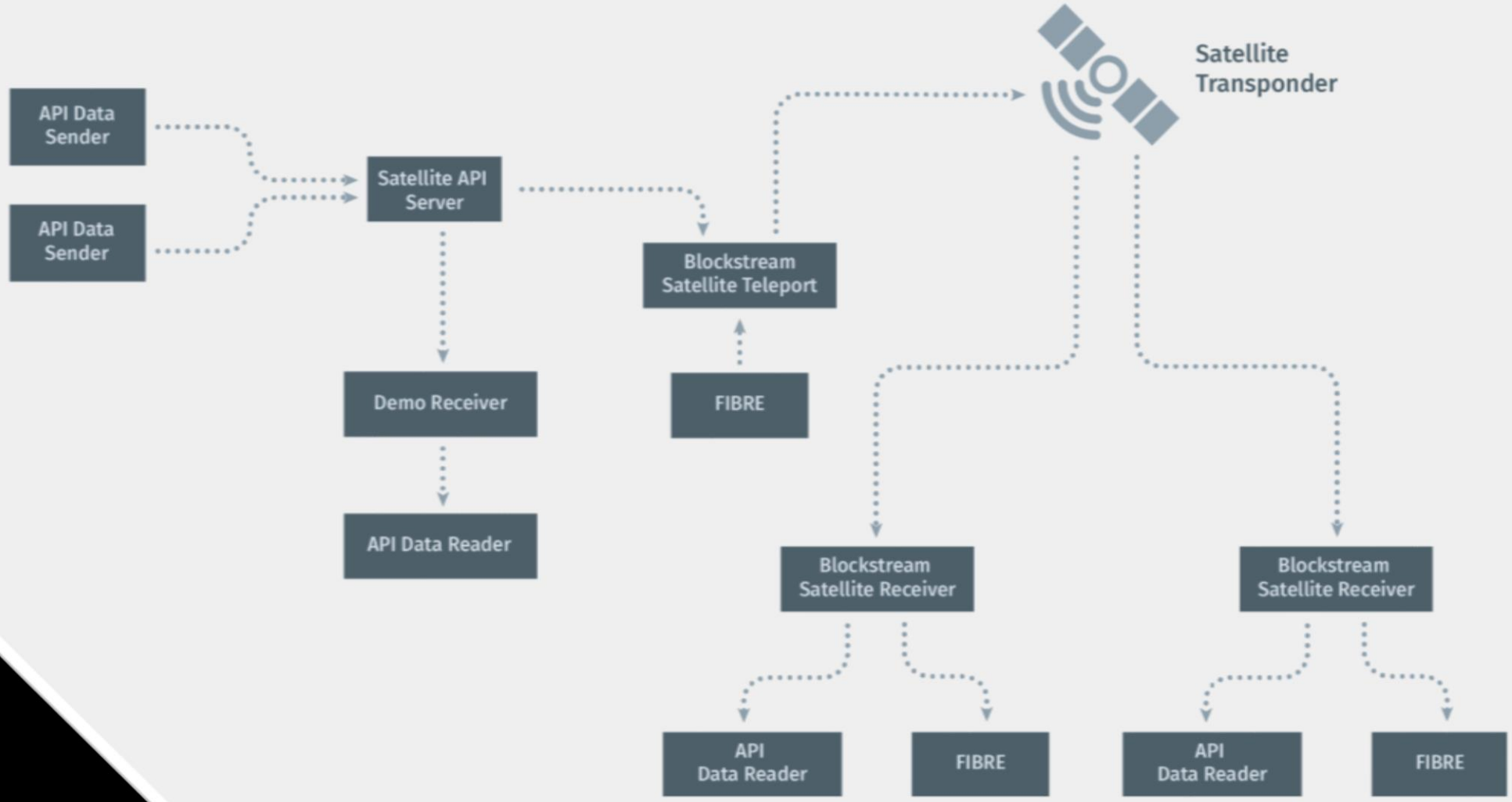
Blockstream Satellite Stories: Japan
Here, the radio waves are amplified
and the frequency is downconverted,

Blockstream Satellite Stories: Japan
The received data is sent
through this white cable

Blockstream Satellite Stories: Japan
15V
In the near future, we will be able
to receive data in Japan from a satellite,

Blockstream satellite

API data transmission architecture



AsiaSat 6/Thaicom 7
Thaicom 4
AsiaSat 4
ChinaSat 6A
JCSAT 4B
LaoSat 1
JCSAT 3A
Vinasat 2
Vinasat 1A
Apstar 6
JCSAT 2A
Telstar 18
Express AT2
Sky Muster 1 (NBN-Co 1A)
Apstar 9
Superbird C2
Sky Muster 2 (NBN-Co 1B)
Optus D2
JCSAT 1B
JCSAT 2B
Optus D3
方位角：145°
高度：55°
25°2'1" N
121°31'52" E

goTenna

goTenna

GOTENNA MESH

Clips onto your backpack for the next adventure.

GOTENNA PRO

Equips every operator with tactical-grade mesh radio communications.

GOTENNA PRO X

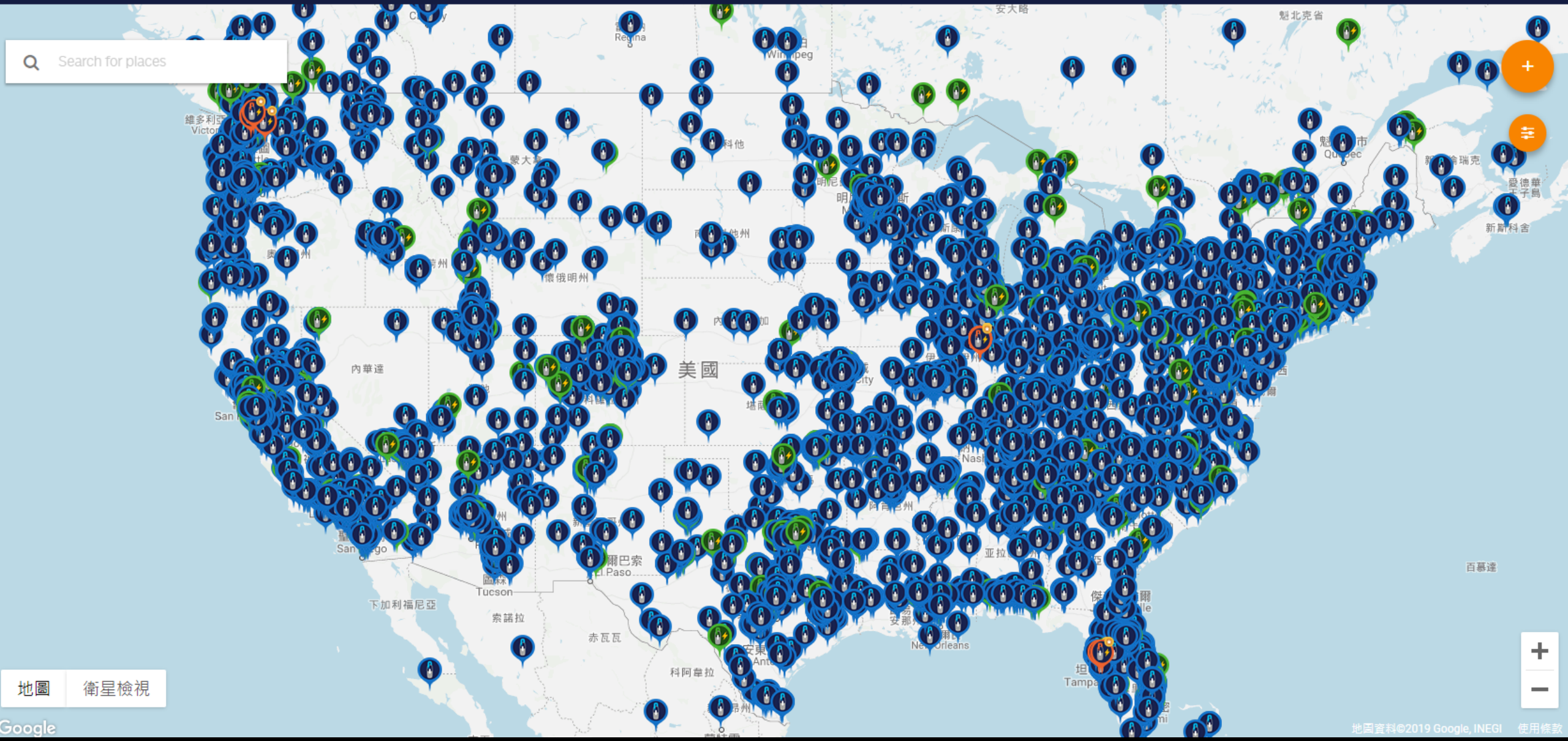
Integrates with custom and third-party apps such as ATAK.

Network Map

This map is not live, all nodes are self-reported.

We respect your privacy & do not track your goTenna Mesh device.
Add & discover nodes to connect with others in the mesh network!

#Imeshyou Share Discussions



武吉英達
TAMAN
BUKIT INDAH
金海灣
DANGA BAY
KOTA MASAI
巴西古當
Pasir Gudang
三巴旺公園
Sembawang Park
TANJUNG PUTERI
Sungei Buloh
Wetland Reserve
Admiralty Rd
三巴旺
SEMBAWANG
SIMPANG
Kranji Way
林厝港
LIM CHU KANG
義順
YISHUN
SLE
BKE
Mandai Rd
SUNGEI KADUT
Punggol Waterway Park
實里達
SELETAR
盛港
SENGKANG
Lim Chu Kang Rd
蔡厝港
CHOA CHU
KANG
KJE
BUKIT PANJANG
KPE
白沙公園
Pasir Ris
Loyang Ave
BUKIT BATOK
中央集水區
自然保護區
CENTRAL WATER
CATCHMENT
新加坡
Singapore
巴耶利峇
PAYA LEBAR
TAMPINES
Jln Bahar
PIE
JURONG WEST
裕廊
JURONG EAST
AYE
TOA PAYOH
CHANGI
章宜
武吉知馬
BUKIT TIMAH
NOVENA
BEDOK
Kilin Ave
文禮
BOON LAY
金文泰
CLEMENTI
新加坡植物園
Singapore
Botanic
Gardens
KALLANG
Upper East Coast Rd
ECP
East Coast
Park
Tanah Merah Coast Rd
Jln Buroh
女王鎮
QUEENSTOWN
市中心
DOWNTOWN
CORE
紅山
BUKIT MERAH
W Coast Hwy
MCE
Malaysia
Singapore

論文研討

比特幣 分岔、絲綢之路事件、Mt.Gox交易所事件 對比特幣帶來的影響

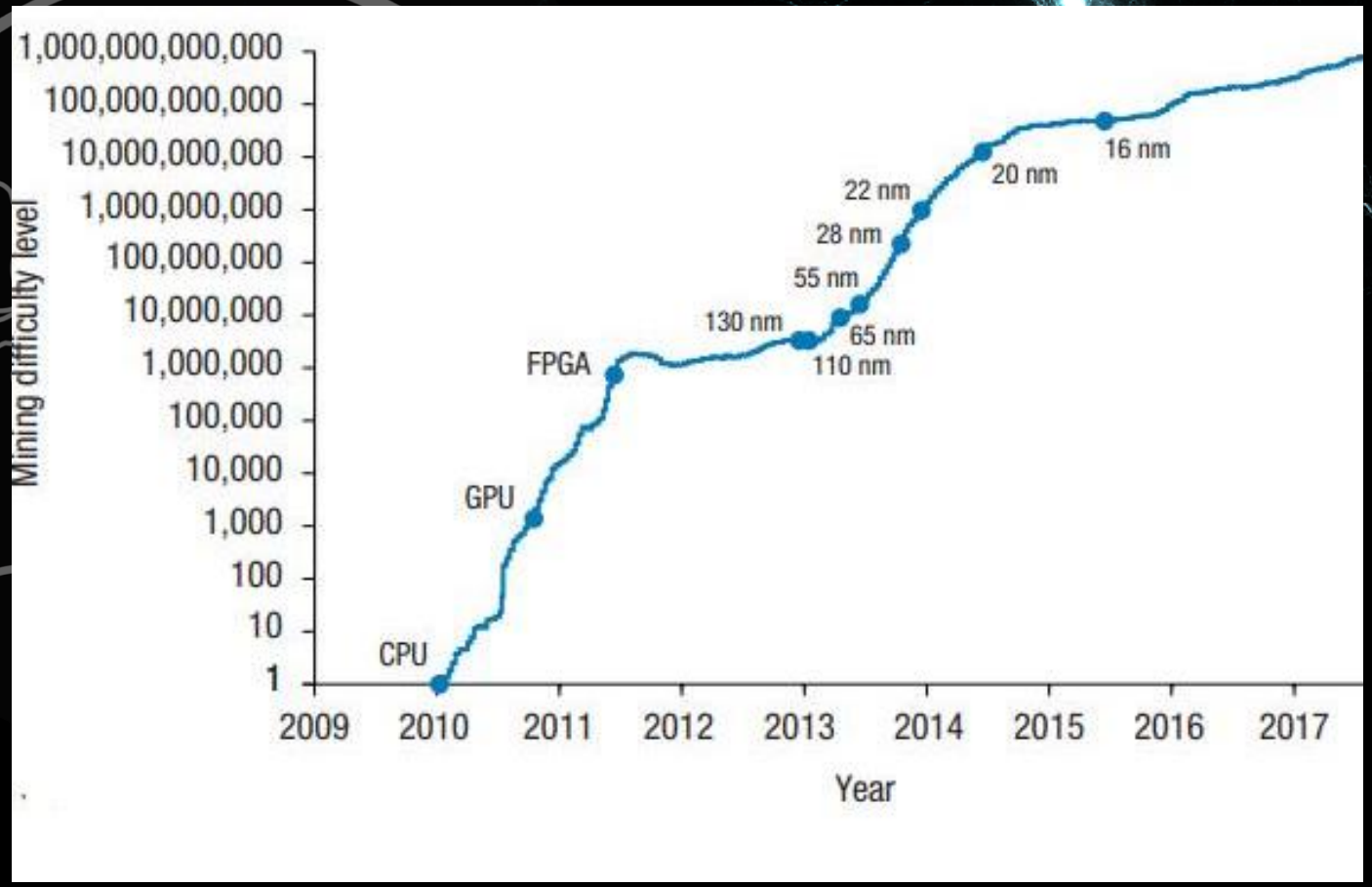
- Fraser, John Gregor, and Ahmed Bouridane. "Have the security flaws surrounding BITCOIN effected the currency's value?." Emerging Security Technologies (EST), 2017 Seventh International Conference on. IEEE, 2017.
- http://ieeexplore.ieee.org/document/8090398/

TABLE I. RESULTS GATHERED

Dates	Highest Value ($)	Lowest Value ($)	Value change against USD ($)	Proposed Reason for drop in value	Category	Score
10/04/13 15/04/13	230.00	68.00	-162.00	A fork in the Bitcoin Blockchain [8] [13][27]	Flaw in the Bitcoin Protocol	70.43
04/12/13 19/12/13	1230.68	553.48	-677.20	The closure of Silk Road [8][17][18]	Flaw or Breech of a Bitcoin Service	55.02
02/02/14 17/02/14	945.00	279.11	-665.89	The collapse of Mt. Gox [8] [14][19]	Flaw or Breech of a Bitcoin Service	70.46
05/03/14 11/04/14	666.62	383.17	-283.45	Chinese Government Intervention [8] [15] [9]	Other Factor	42.52
19/06/16 23/06/16	769.99	600.22	-169.77	Brexit [20][21][22]	Other Factor	22.05
29/07/16 02/08/16	657.41	503.46	-153.95	Breach of Bitfinex [22][23][24]	Flaw or Breech of a Bitcoin Service	23.42
05/01/17 13/01/17	1118.53	787.59	-330.94	Chinese regulation fears [21][25][26]	Other Factor	29.59

比特幣礦機的演進

- Taylor, Michael Bedford. "The Evolution of Bitcoin Hardware." Computer 50.9 (2017): 58-66. http://ieeexplore.ieee.org/document/8048662/



量子計算器對比特幣造成的威脅

[1]. Tessler, Louis, and Tim Byrnes. "Bitcoin and quantum computing." arXiv preprint arXiv:1711.04235 (2017).

https://arxiv.org/abs/1711.04235

[2]. Jogenfors, Jonathan. "Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics." arXiv preprint arXiv:1604.01383 (2016).

https://arxiv.org/abs/1604.01383

以貝葉斯神經網路 做價格預測

- An Empirical Study on Modeling and Prediction of Bitcoin Prices with Bayesian Neural Networks Based on Blockchain Information

  http://ieeexplore.ieee.org/document/8125674/?source=MyXploreApp

DATA FOR THE EMPIRICAL STUDY

Data category	Data
Response var.	prices or log prices of Bitcoin(USD), vol. or log vol. of Bitcoin(USD)
Blockchain information	Trading vol.(USD,CNY), avg. block size, transactions/block, median confirm. time, hash rate, difficulty, cost % of trans., miners' rev., confirmed trans., total num. of uniq. Bitcoin
Macro economic development	S& P500, Eurostoxx, DOW30, NASDAQ, Crude oil, SSE, Gold, VIX, Nikkei225, FTSE100
Global currency ratio(/USD)	GBP, JPY, CHF, CNY, EUR

分析 DarkLaunder, Bitlaunder and CoinMixer三個平臺的洗錢服務

- de Balthasar, Thibault, and Julio Hernandez-Castro. "An Analysis of Bitcoin Laundry Services." Nordic Conference on Secure IT Systems. Springer, Cham, 2017.
- https://link.springer.com/ch…/10.1007%2F978-3-319-70290-2_18

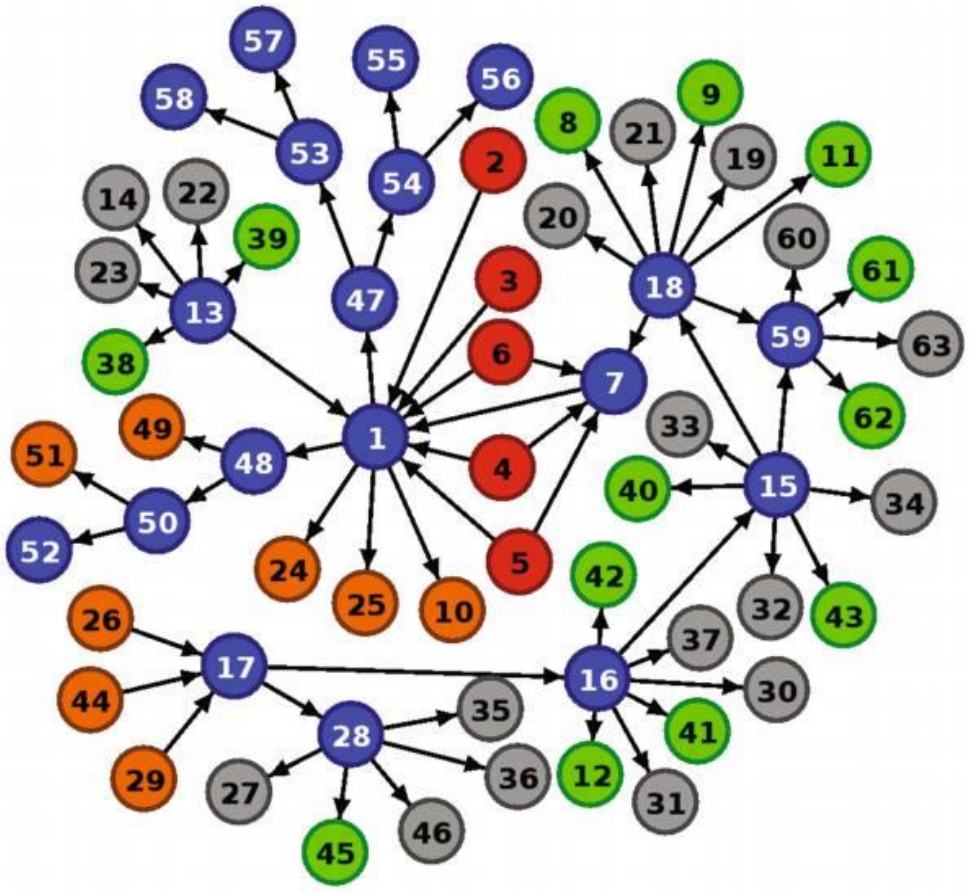


Fig. 8. Darklaunder workflow

比特幣在第一個四年使用的場景、頻率、量，物件包括交易所、賭場，各種是占率比較。

- Lischke, Matthias, and Benjamin Fabian. "Analyzing the bitcoin network: The first four years." Future Internet 8.1 (2016): 7.
- http://www.mdpi.com/1999-5903/8/1/7/htm

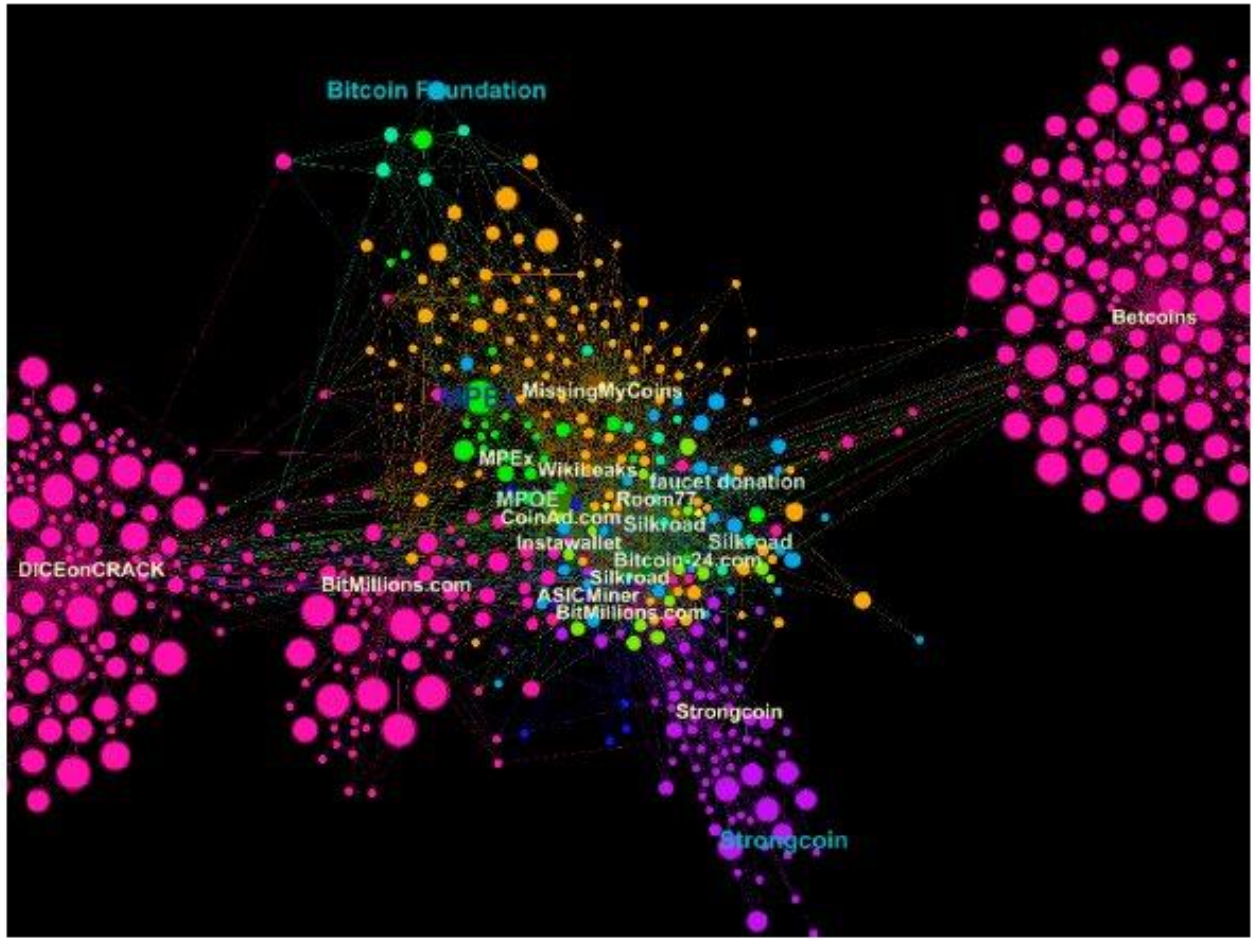
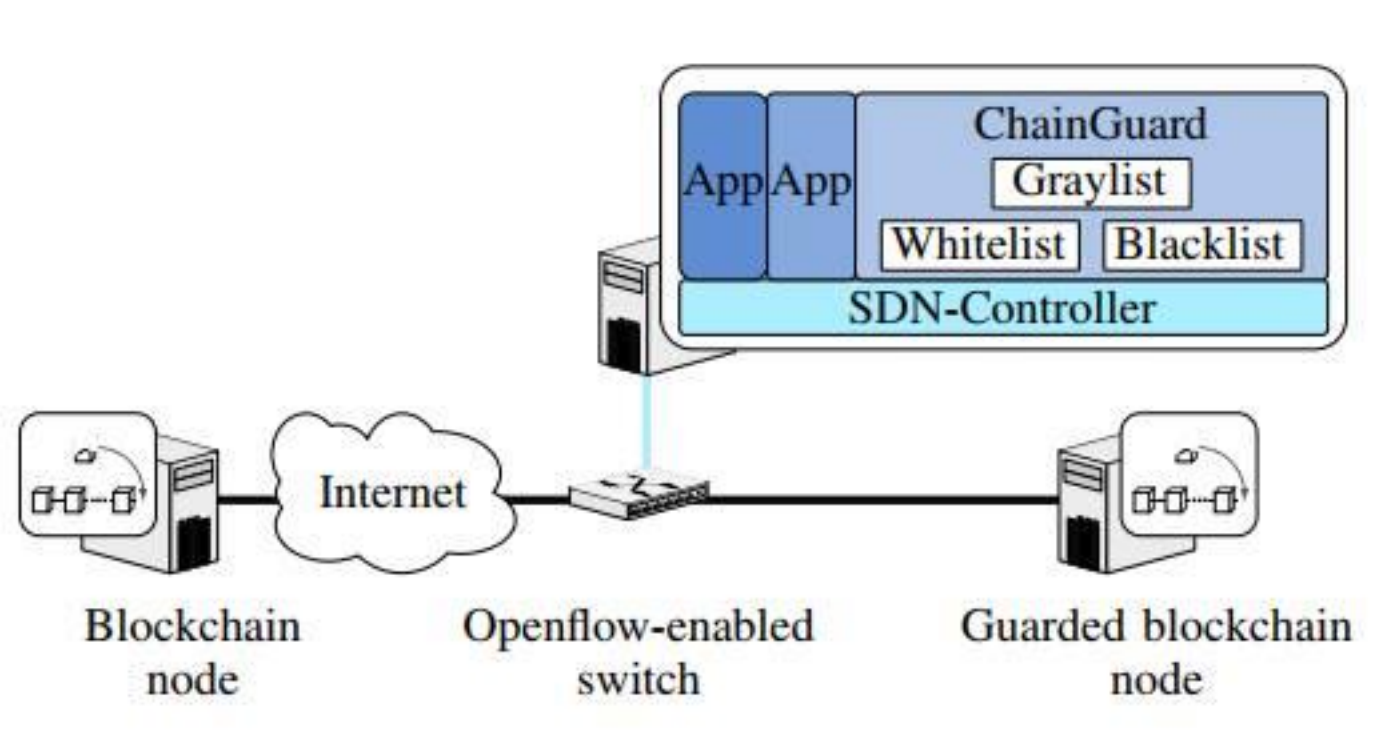


Figure 38. Visualization of the Transaction Value in the Bitcoin Network.

整理Bitcoin勒索軟體的勒索價格、用的網路是否TOR、加密方法...等

- The state of ransomware. Trends and mitigation techniques
- http://ieeexplore.ieee.org/document/8110056/

VaultCrypt: in BTC, the price depen
ds on the number of encrypted files
TeslaCrypt: $500 equivalent in BTC, doubled every
60 hours
NanoLocker: 0.25 BTC
Linux.Cryptor: 1 BTC
Simplelocker: MoneXy, Qiwi
OSX/KeRanger-A: 1 BTC
WannaCry: $300/600 in BTC
Petya: $300/600 in BTC
NotPetya: n/a
Cerber: 0.045/0.090 BTC
Spora: depends on the number of encrypted files
Serpent: 0.025/0.075 BTC

以區塊鏈的方式 同步 防火牆規則

- ChainGuard - 使用SDN和OpenFlow的區塊鏈應用程式的防火牆
- http://ieeexplore.ieee.org/document/8169748/