

Key Risk for Blockchain and Digital Assets

Presentation for BFIA 2022

www.bitkub.com



Key Risk for Blockchain and Digital Assets

1 - Blockchain

- Blockchain Technology explained
- Basic infrastructure and communication
- Consensus
- Addresses and Private Key
- Tracking transactions via blockchain explorer
- Smart Contract

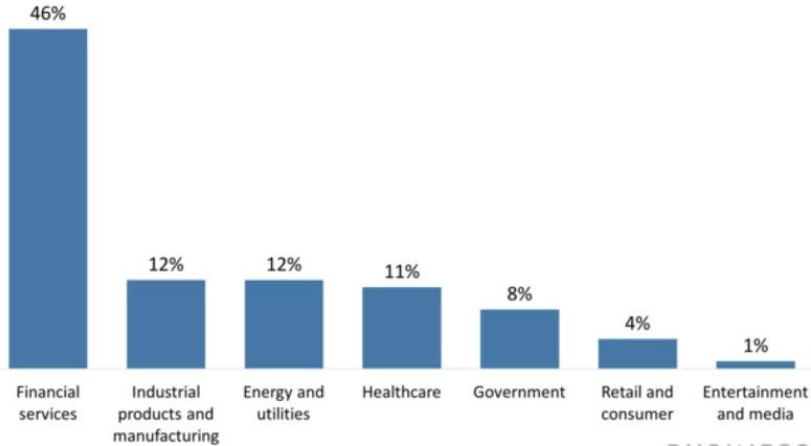
2- Digital Asset

- Custodian and Non-custodial wallets
- Transfers and Recovery of Digital asset
- Difference type of services
- High risk transactions



Blockchain Technology potential use cases

Industries That Global Executives Think Are Most Advanced In Blockchain Development



Note: Percentages don't sum to 100% because industries with less than 1% of votes are excluded.

Source: PwC Global Blockchain survey, n=600, 2018

BUSINESS
INSIDER
INTELLIGENCE



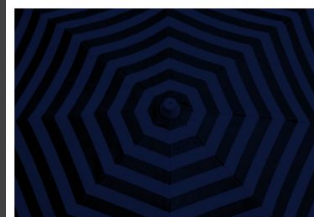
Central Bank Digital Currencies



Digital Identity

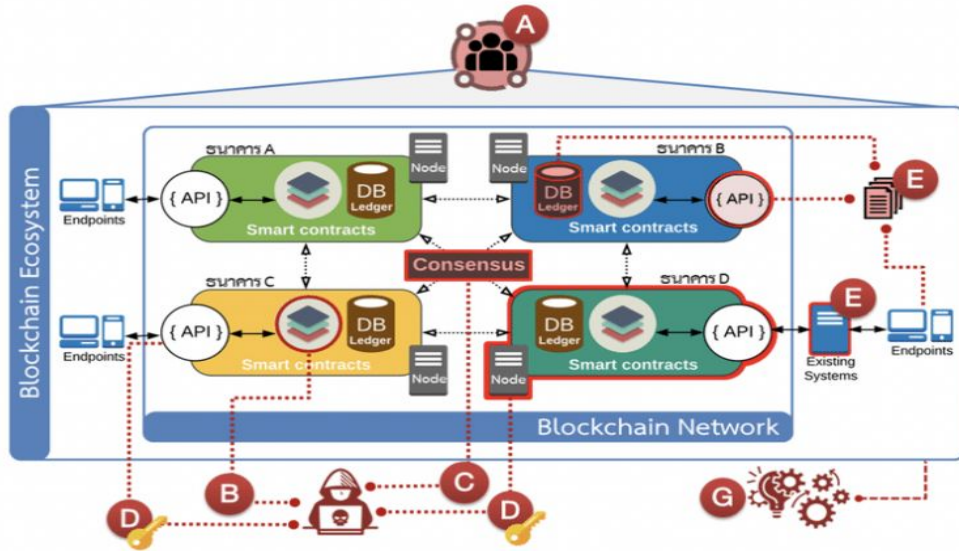


Retail Fashion and Luxury



Insurance

Inherent Risk of Blockchain



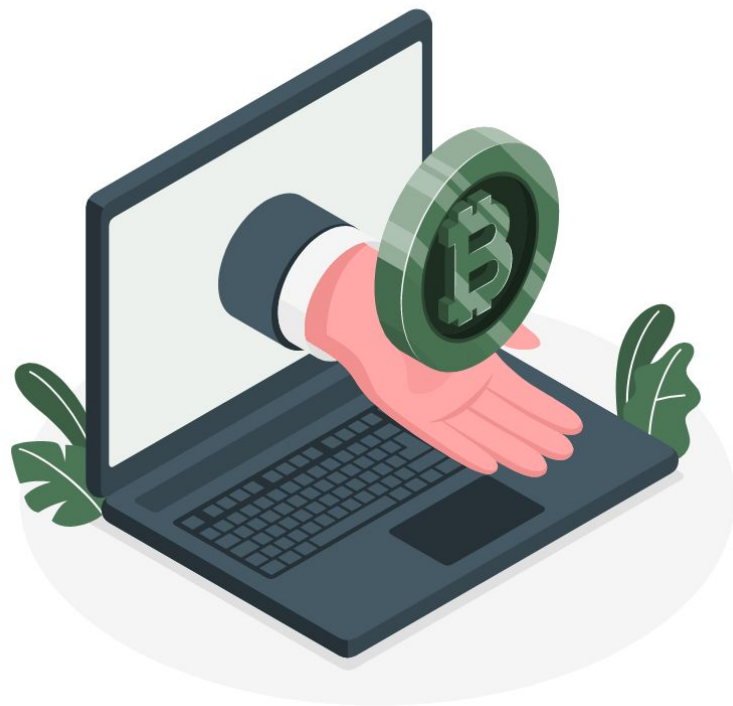
ความเสี่ยงเฉพาะจากการใช้เทคโนโลยี Blockchain

- A การกำกับดูแลเครื่องง่าย Blockchain และสมาชิกในเครื่องง่ายไม่ครอบคลุมเพียงพอ
- B Smart Contract ทำงานไม่ถูกต้องและไม่ปลอดภัย
- C การโจมตีกลไก Consensus
- D การบริหารจัดการกฎเกณฑ์เข้ารหัสที่ไม่รัดกุมเพียงพอ

ความเสี่ยงพื้นฐานด้าน IT และภัยคุกคามทางไซเบอร์

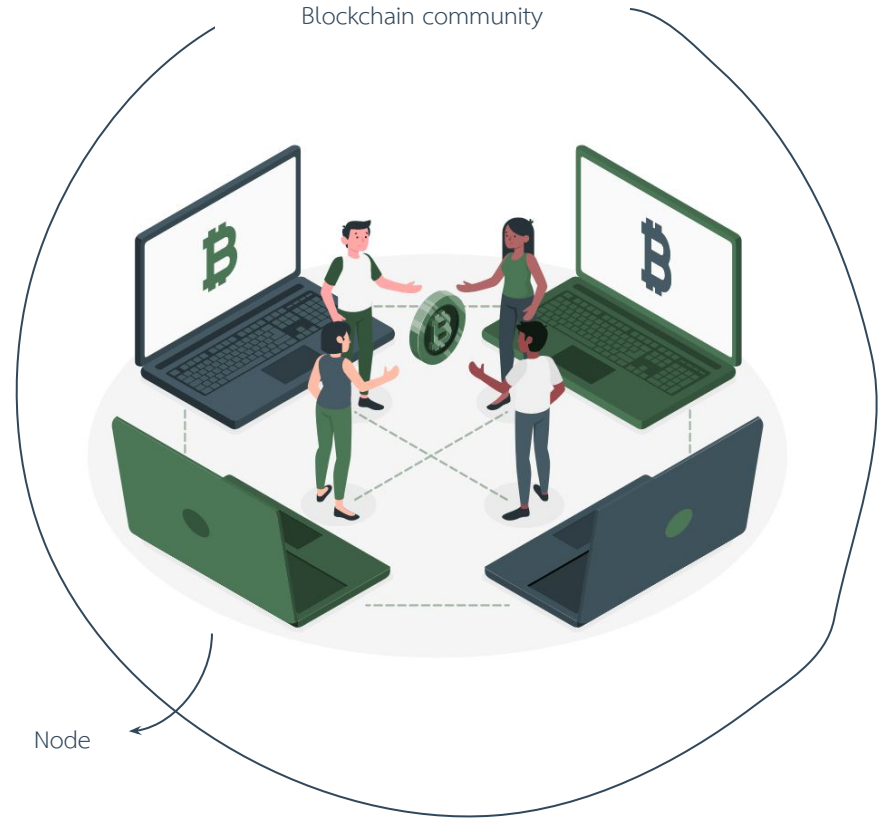
- E ความเสี่ยงจากการเชื่อมต่อระบบโครงสร้างพื้นฐานเดิมกับเครื่องง่าย Blockchain
- F ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยี

Blockchain



How does Blockchain work?

Imagine strangers sitting in a room, each with their own **notebook** and they don't trust each other. Their notebooks can be used to store and send any type of digital property.



How does Blockchain work?



A transfers cryptocurrency to B

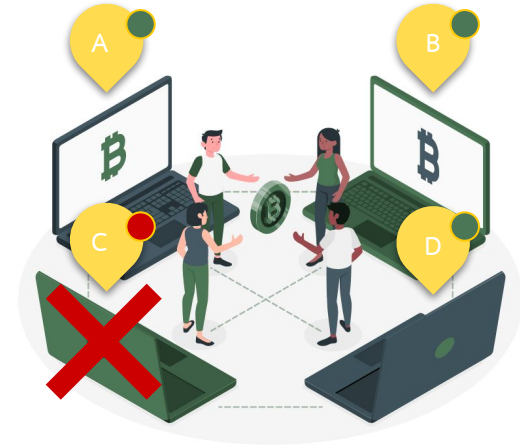


Each of them records a transaction and compare all notebooks to make sure they match.

How does Blockchain work?



A transfers cryptocurrency to B

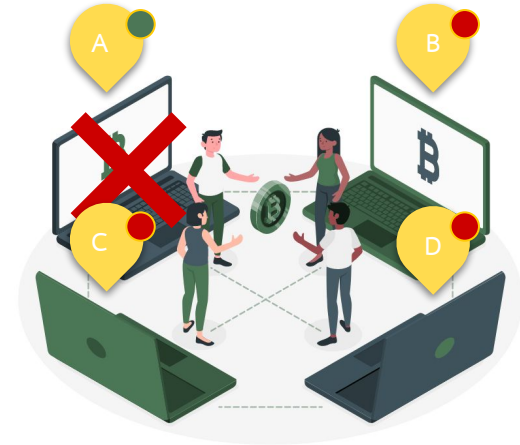


Each of them records a transaction and compare all notebooks to make sure they match. **If a stranger is lying, the others ignore and move on.**

How does Blockchain work?



A transfers cryptocurrency to B



Each of them records a transaction and compare all notebooks to make sure they match. If one blockchain copy is different from all others in the network, the network automatically rejects the transaction that doesn't match the rest.



Consensus algorithm

An agreement or qualification of the strangers to ensure that all strangers in the room can agree on a single source of truth, even if some stranger fail.

Blockchain Consensus

Proof Of Work [POW]



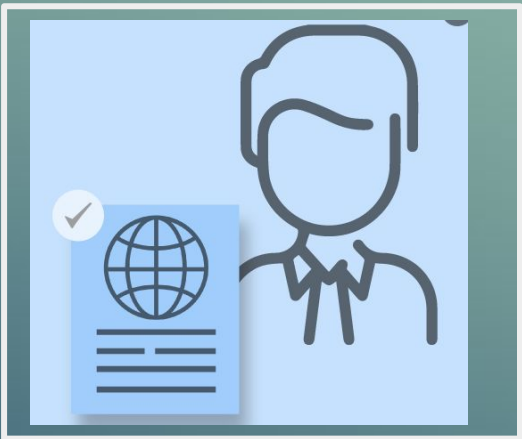
Using powerful computing power to solve math problems

Proof Of Stake [POS]



People with most token

Proof Of Authority [POA]



Selected entity/individual with good reputation



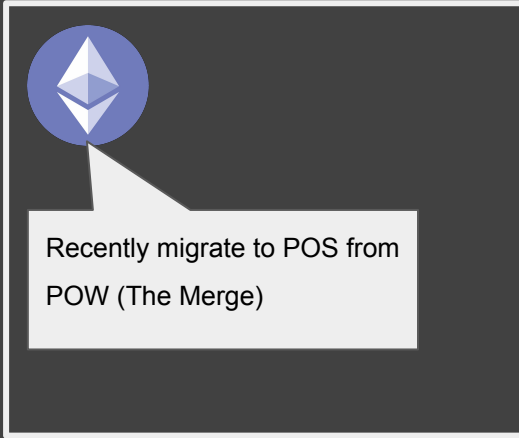
Blockchain Consensus

Proof Of Work [POW]



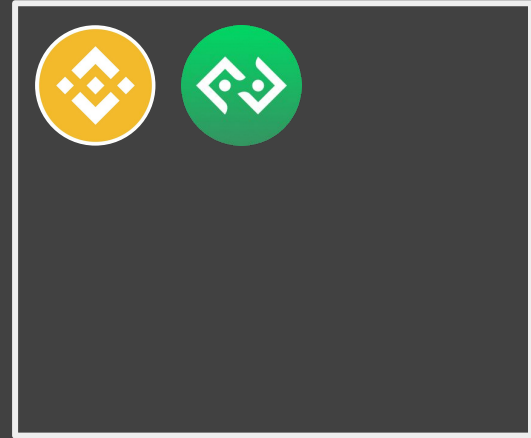
Using powerful computing power to solve math problems

Proof Of Stake [POS]



People with most token

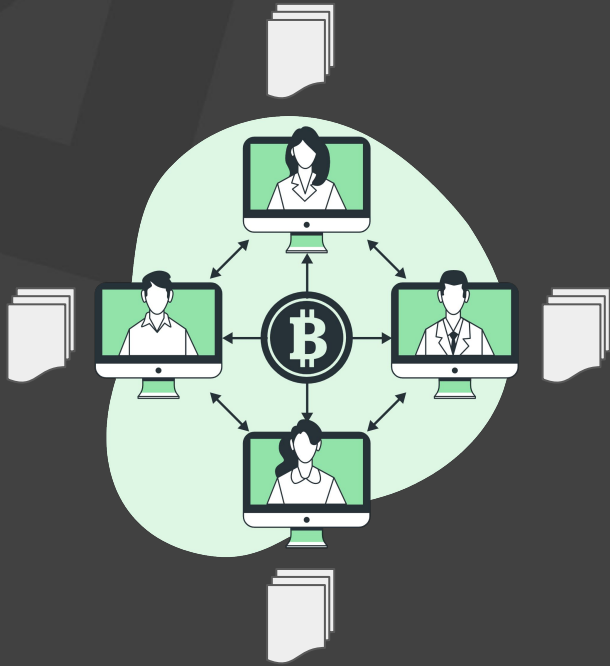
Proof Of Authority [POA]



Selected entity/individual with good reputation

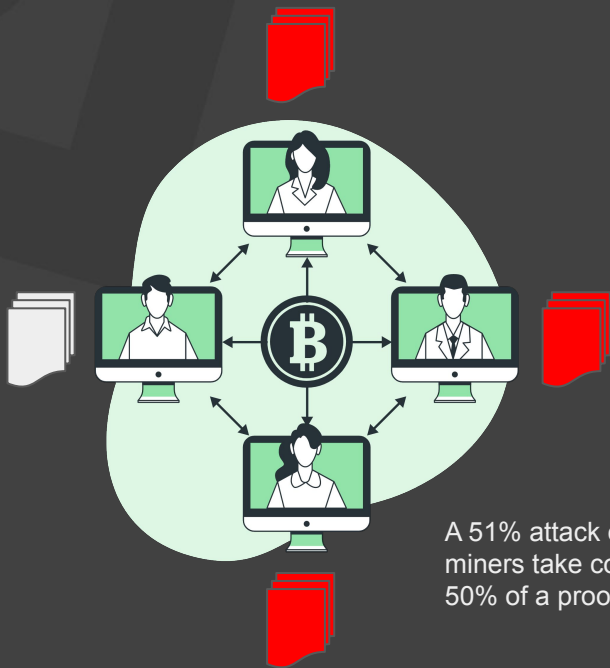
POSA

Blockchain - What could go wrong ?



Blockchain depends on everyone [validator nodes] to maintain information / database. With this decentralized network, if one node was compromise, information can not be manipulated by malicious individuals. Unless ?

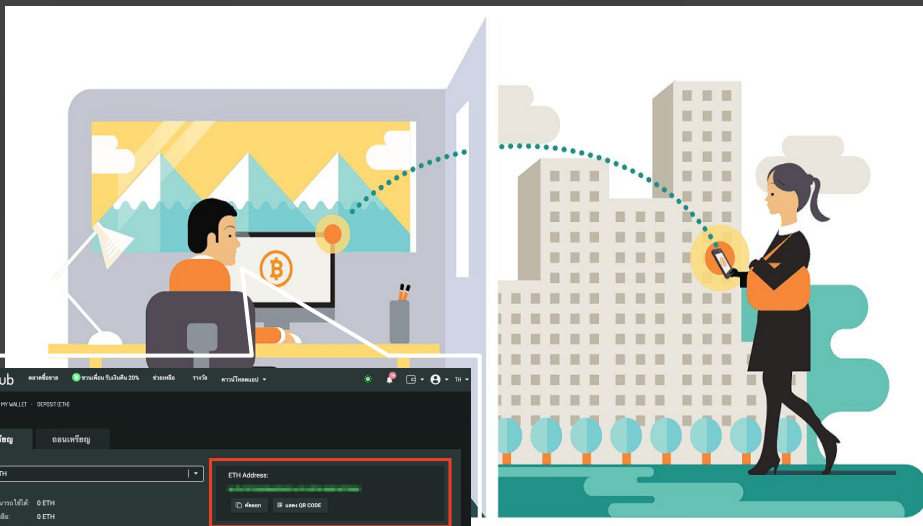
Blockchain - What could go wrong ?



A 51% attack occurs when malicious miners take control of more than 50% of a proof-of-work blockchain.

The screenshot shows a news article in Thai. At the top is the logo for 'BITCOIN SV SATOSHI VISION' with a Bitcoin icon. Below the logo is a yellow and black patterned background with the text 'Bitcoin SV (BSV) ถูกโจมตี 51% attack "ครั้งใหญ่"'. The article title is 'เครือข่าย Bitcoin SV (BSV) ถูกโจมตี 51% attack "ครั้งใหญ่"' and the date is 'สิงหาคม 4, 2021'. The main text states: 'มีรายงานว่า Bitcoin SV (BSV) ประสบกับการโจมตี 51% attack "ครั้งใหญ่" โดยเริ่มตั้งแต่วันที่ 22:45 ของวันอังคาร ส่งผลให้มีการหยุด chain บางถึงสามชั่วโมงครึ่ง'. Below this is a tweet from CoinMetrics.io (@coinmetrics) reporting: 'FARUM has identified a 51% attack today on the BSV network at around 11:45AM EDT. coinmetrics.io/farum/'. A reply from Lucas Nuzzi (@LucasNuzzi) says: 'BSV is going through a massive 51% attack. After an attempted attack yesterday, some serious hashing power was unleashed today at 11:46AM and attackers are succeeding. Over a dozen blocks are being reorg'd & up to 3 versions of the chain being mined simultaneously across pools.' The tweet is dated '2:51 ก่อนเที่ยง - 4 ส.ค. 2021' and has 54 likes and 9 retweets.

เลข Wallet Address มาได้ไง



“โอนมาที่ Address นี้ได้เลย !”

เริ่มต้นจากการใช้วิธีการเข้ารหัสที่เรียกว่า PKI (Public Key Infrastructure)

วิธีการนี้จะมี Key อยู่ 2 อันคือ

1. Public Key เอาไว้ส่งให้ Public เข้ารหัส
2. Private Key ต้องเก็บไว้เป็นความลับ เอาไว้ถอดรหัส



เลข Wallet Address มาได้ไง

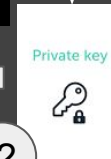


ตอนสร้างกระเป๋าใหม่จะได้มา 2 อย่างคือ

1. Wallet Address
2. Private Key



ต้องเอา Private Key มาถึงจะ Decrypt หรือ เข้าถึงกระเป๋านี้ได้



Encode with Base58

1

Wallet Address:

bc1qqdykm85ycxjqjh5hrkwmefts02mm6ku5rlck3m

Private Key:

E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262

อันนี้ต้องเก็บไว้เป็นความลับ ห้ามแชร์ให้คนอื่น ห้ามหาย

Addresses and Private Key

<https://vanity-eth.tk/>



Address: 0x6d9e0B8870d1e3C91aC71D88C2c12D9B98b27a75

Private key: b1ee578770bdc6916d72ab8dac9bc69e01958cf9bc766aa9567c743bf88f8e3a

Save

Etherscan

Eth: \$1,208.83 (-4.53%) | 18 Gwei

All Filters

Search by Address / Txn Hash / Block / Token / Ens

Home Blockchain Tokens Resources More Sign In

Address 0x6d9e0B8870d1e3C91aC71D88C2c12D9B98b27a75

Buy Exchange Earn Gaming

Sponsored: PEPEBET - Buy a token - place a bet and win cash prizes! Buy PEPEBET token

Overview

Balance: 0 Ether

Ether Value: \$0.00

More Info

My Name Tag: Not Available, login to update

Ad

Advertise your brand here!

Start Today

Transactions Erc20 Token Txns Analytics Comments

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
----------	--------	-------	-----	------	----	-------	---------

There are no matching entries

<https://etherscan.io/>

ถ้าลืม Private Key แล้วทำยังไง ?



BIP 39: Mnemonic code for generating deterministic keys

สามารถใช้คำ 12-24 คำที่ Random ขึ้นมาเพื่อ restore Private Key ได้ โดยคำเหล่านี้มาจาก Word List ที่เป็นไปได้ทั้งหมด 2048 คำ

Setup Phrase

Write down the following words IN ORDER and keep them somewhere safe. You cannot recover your account without them!

1 ankle	2 measure	3 slender
4 stable	5 equal	6 equip
7 arrest	8 fury	9 record
10 skirt	11 recall	12 minimum

- Recovery Phrase เหล่านี้ระบบจะสร้างมาให้
- ต้องเก็บเป็นความลับเหมือน Private Key
- ต้องจดตามลำดับ
- เวลาเอามาใช้ เพื่อกู้ Private Key ต้องใส่ตามลำดับด้วย

Private Key:

```
xprv9s21ZrQH143K42r3nHWHumL2sBrw6MvmkyP5y  
bGd7GgUjCxHw6bo3fvTVRWVaxZLKMZSP82xEavw  
2AEeZfS1LzUQPjiNKWURVrdD2m56sMq
```

<https://iancoleman.io/bip39/>

Addresses and Private Key



<https://cryptoglobally.com/seed-phrase-generator-wallet/>

Coin

ETH - Ethereum

24 Words

GENERATE

Mnemonic Seed Phrase Language

[English](#) [日本語](#) [Español](#) [中文\(简体\)](#) [Français](#) [Italiano](#)

BIP39 Mnemonic Seed Phrase

pull zero burger fatal case float bleak witness crop civil victory next since
child outside nominee crowd blanket unusual garment asthma finger exist
hello

Check Balance

Click this Button Every time you Generate New Seed Phrase.



ETH Balance

0



BNB Balance

0



Matic Balance

0

Public address and Private Key

0x21c108c336E2f1052115883F31A3ea61577798B5, 0x5ab6a4caa033f

There are 2048 words possible

<https://getcoinplate.com/blog/official-bip39-word-list-mnemonic-in-english-verified/>

<https://etherscan.io/>

Addresses and Private Key



- Wallet Address และ Private Key มีลักษณะเหมือน Username และ Password
- ดังนั้นก็มีความเสี่ยงที่ Private Key จะถูกสุ่มเดาด้วยการ Brute Force ได้ -> Very low possibility but not 0%

```
C:\Users\Pedro\Desktop\BITCRACK>start1  
  
C:\Users\Pedro\Desktop\BITCRACK>bitcrack64 -b 32 -t 256 -p 16 -c -u -s 4997CAE96B36C4DEA75E574D60F5D913BCD2D3A8B4D939A67  
FD63A11DBFEEDE3 12QvKQTV2wrwfhfZbAF3PjgANVjAqaPJqH -o out.txt  
Device: GeForce GTX 1080  
Target: 12QvKQTV2wrwfhfZbAF3PjgANVjAqaPJqH  
Compression: both  
Starting at: 4997CAE96B36C4DEA75E574D60F5D913BCD2D3A8B4D939A67FD63A11DBFEEDE3  
Initializing...  
Running  
  
Private key: 4997CAE96B36C4DEA75E574D60F5D913BCD2D3A8B4D939A67FD63A11DBFEEDE3  
Compressed: no  
Public key: EA27E6FB91E29A8F8D7947D04B19B5ABB24EDF8A3E8DCB263B3637F6B0093AB3  
B9224AD2C51D8985CDB2360C02DD472CD3458A194455DFDDAFE4D76934E6B62E  
  
C:\Users\Pedro\Desktop\BITCRACK>
```

ตัวอย่างการใช้โปรแกรมเพื่อเดา Private Key

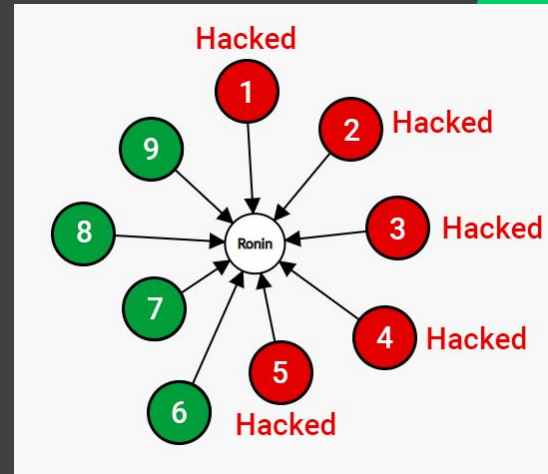




Axie Infinity hack

\$552,025,328 Loss

- Ronin is a side-chain of Ethereum (in which Axie Infinity operates). It's secured by 9 validators and you only needed 5 (+50%) to attack the network
- The attackers got access to the System that operates 4 of the nodes, and found a bug to access another node
- With +50% of the nodes in the hands of the hackers, they stole* all the bridged Ether and USDC

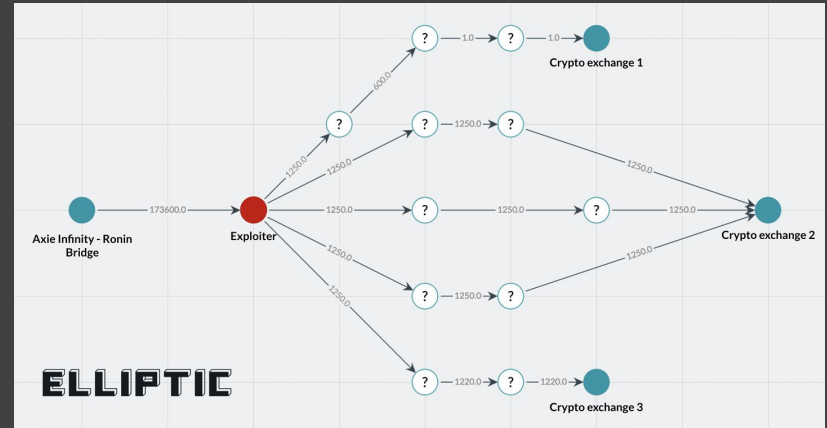


<https://cointelegraph.com/news/the-aftermath-of-axie-infinity-s-650m-ronin-bridge-hack>

*Stole = Create transaction to withdraw asset and signed this transaction with majority number of private keys [consensus]

Lesson Learned

- Server security still a top priority
- Do not allow one entity to control majority nodes



Addresses and Private Key - What could go wrong

- Unauthorized access to where keys are stored [End Point]
- Unauthorized access or Lost access to
 - Private key
 - Recovery seed phrases



Enhanced transaction controls

MPC (Multi-Party Computational)

MPC distributes the Hot Vault's "Private-Key" secrets in an isolated chip-that sets across both cloud servers (SGX) and the customer's owned secure mobile enclaves. The private key doesn't exist and is never reconstructed in one place. This eliminates the possibility for a single point of compromise.

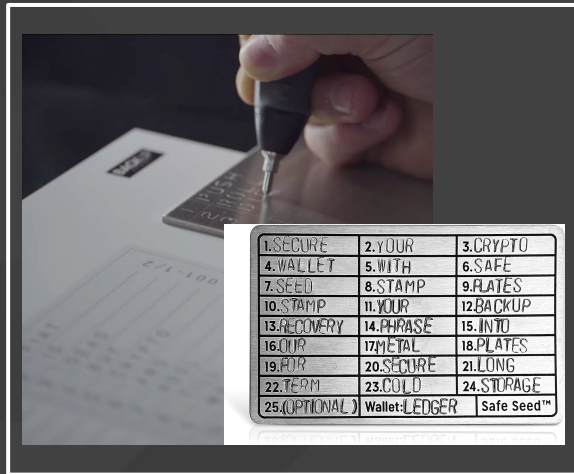
Multi-Keys

Immediately after the User Key is generated, it is shared and split into a number of N shards and distributed among an equal number of different "Key Shard Holders" in a manner that requires M of N key shard holders to come together and reconstitute the key for signing a client initiated transaction.

เก็บ Private Key อย่างไรให้ปลอดภัย



Paper Wallet



Steel Plate



Hardware Wallet

Private Key Management

If a company decides hold digital assets securely how would such company go about doing this

1. No individual can have access to all element used for making transactions
 - a. Hardware Wallet
 - b. Pin code
 - c. Seed Phrases
2. Keeping backup into multiple-location + [1]
 - a. Note - backup can not be all at the same place
 - b. Note - Bank's safes are rare



Ethereum Chain






















Improvement from BTC

- Ethereum was developed to augment and improve on bitcoin, expanding its capabilities.
- Importantly, it was developed to feature prominently “smart contracts:” decentralized, self-executing agreements coded into the blockchain itself.

Ethereum Virtual Machine (EVM) and ERC20

- An Ethereum virtual machine is a software platform, or “virtual computer,” used by developers to create decentralized applications (DApps), as well as to execute and deploy smart contracts on the Ethereum system.
- DApps developed using “Solidity” language
- ERC20 = Token standard

Blockchain on EVM and ERC20 Compatible

#	Name
1	 BNB BNB
2	 Polygon MATIC
3	 Avalanche AVAX
4	 Cronos CRO
5	 OKB OKB
6	 Fantom FTM
7	 IoTeX IOTX
8	 Optimism OP
9	 Harmony ONE
10	 Moonbeam GLMR
11	 Aurora AURORA
12	 Velas VLX
13	 Moonriver MOVR
14	 Telos TLOS
15	 Boba Network BOBA
16	 TomoChain TOMO
17	 xDai STAKE
18	 Ubiquitous UBQ
19	 Evmos EVMOS

Implication of EVM and ERC20 Compatible

Etherscan

Eth: \$1,191.70 (-1.21%) | 17 Dwei

Home Blockchain Tokens Resources More Sign In

Token Holdings 0xF977814e90dA44bFA03b6295A0616a897441aceC | Binance 8

Overview

Net Worth in USD: **\$22,588,013,511.64**

Net Worth in ETH: **18954446.179065**

Total Balance Change (24H): **-1.94%**

Assets in Wallet (1,092): **\$22,588,013,511.64**

NFT Assets (12): -

Liquidity Pool Assets in Wallet (0): -

Assets in Wallet (1,092)

Asset	Symbol	Contract Address	Quantity	Price	Change (24H)	Value	More
Ethereum	ETH	-	1904674.09956718243...	\$1,191.70	-1.21%	\$2,269,800,124.45	More
Binance USD	BUSD	0x4fab0145d64652a948...	1420000000	\$1.002	-0.04%	\$14,228,400,000.00	More
BNB	BNB	0xB8c77482e45F1F44d...	7494452.67762456	\$266.185404	-1.49%	\$1,994,913,912.50	More
Tether USD	USDT	0xdac179582e2e523a2...	700000000	\$1.001	+0.12%	\$700,700,000.00	More
USD Coin	USDC	0xa0b86991c6218b36c1...	289477899.633	\$1.00	-0.07%	\$289,477,699.63	More
SHIBA INU	SHIB	0x95aD61b0a150d7921...	29706554054973	\$0.000009	-1.68%	\$267,358,986.49	More
ChainLink To...	LINK	0x514910771a9ca856af...	35000000	\$6.11	-1.01%	\$213,850,000.00	More
chiliz	CHZ	0x3506424f91d3308446...	900000000	\$0.22423	+1.37%	\$201,807,000.00	More
CocosToken	COCOS	0x0c695f7d555e7518f68...	351392574.166234247...	\$0.462888	+0.13%	\$162,655,405.87	More
Pax Dollar	USDP	0x8e670d67f660d95d5b...	125383576	\$1.001	-0.11%	\$125,508,959.58	More

Show 10 Records

Page 1 of 110

By complying to the same ERC20 standard one address can support multiple tokens

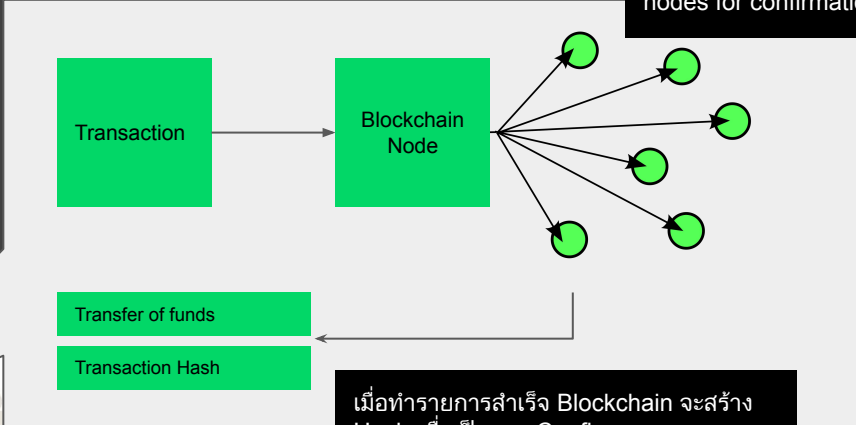
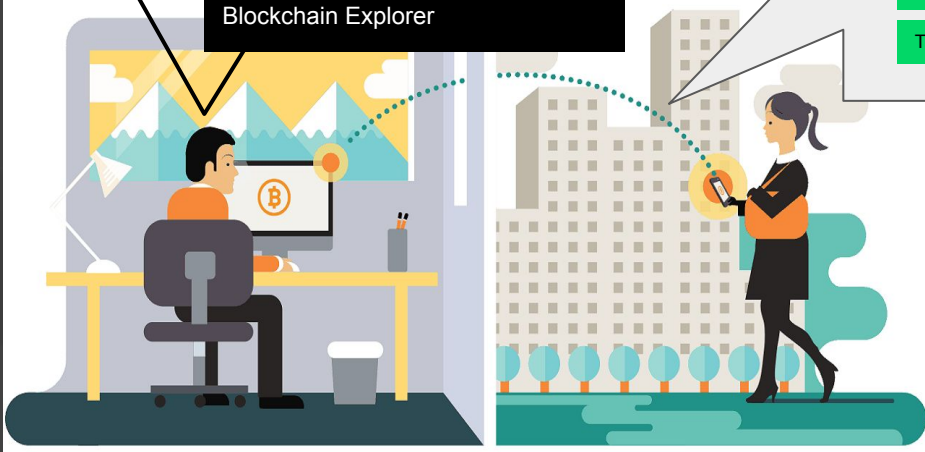
เวลาทำการโอนเหรียญเกิดอะไรขึ้นบ้าง



Hash	Time	Amount (BTC)	Amount (USD)
85156f1d43b86dc267959b709821fc595ec00d6f0...	22:03	1.26903658 BTC	\$50,428.63
174534a3ae55a836d353417929a458501554be9a...	22:03	0.08153844 BTC	\$3,240.15
bbd8baf9d6d43d9a3160e42f3b6862adef085a6a...	22:03	0.00031447 BTC	\$12.50
634c4694a9d39b81be1d7e34d18614e5d17867a31...	22:03	0.00121096 BTC	\$48.12
7201eab5ce862ad71f54abe6e25f47adc0bf95d5bb...	22:03	0.00483416 BTC	\$192.10
94a8ad27258432cf0aae824944cc60b770e14e718...	22:03	0.00892408 BTC	\$354.62

[View All Transactions →](#)

ผู้รับสามารถเข้าไปตรวจสอบรายการ โดย Search หาค่า Hash ใน Blockchain Explorer



เมื่อทำรายการสำเร็จ Blockchain จะสร้าง Hash เพื่อเป็นการ Confirm รายการ Hash นี้เหมือนกับ ID ของรายการ Transfer

Follow blockchain transaction

On public blockchain, it is possible to trace transactions and addresses. However there is limited to no information on who is the owner of this address

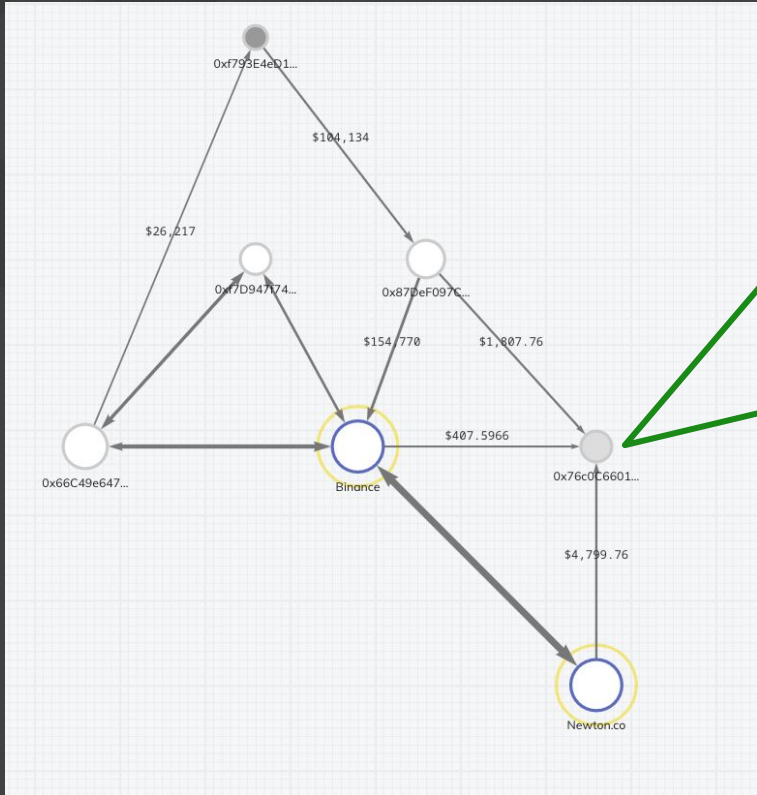
The screenshot shows the Etherscan interface for a specific wallet address. The address is 0x2Db1D8CdF1Abe8C70b531a790CDf2F38aecF652. The wallet's balance is 459.06682775703259024 Ether, with an Ether value of \$560,750.13. The token balance is \$607,193.46. A 'More Info' section shows 'My Name Tag' is not available. Below the wallet overview is a 'BC.GAME' banner with a 'Welcome bonus up to 500 ETH' and a 'PLAY NOW' button. The 'Transactions' section is visible at the bottom, showing a list of transactions with columns for Txn Hash, Method, Block, Age, From, To, Value, and Txn Fee.

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x1d94d5a7cd27336e5...	Transfer	15996302	2 mins ago	0x2db1d8cdf1abe8c70b...	0x760c6601f52b19c8e...	1.53 Ether	0.00027297
0x5395ce4114208f144c...	Transfer	15996291	4 mins ago	0x2db1d8cdf1abe8c70b...	0x18065e5886c5a0a95...	0.0000307 Ether	0.00002704
0xc69d16b87b078c4ab9...	Transfer	15996270	8 mins ago	0x2db1d8cdf1abe8c70b...	0x37beae428524cbe...	2 Ether	0.00003004
0x7b0c028706640d65c...	Transfer	15996253	12 mins ago	0x2db1d8cdf1abe8c70b...	0x64364412a79674d3df...	0.030571 Ether	0.00003142
0x5d1c7640b49be9e169...	Transfer	15996243	14 mins ago	0x2db1d8cdf1abe8c70b...	0x421bf68aa8d382706c...	0.0122 Ether	0.00002725
0xc0f80e2f252620670a...	Transfer	15996228	17 mins ago	0x2db1d8cdf1abe8c70b...	0x71aab0f757430223c4...	0.117075 Ether	0.00008579
0x467a554548b047828e...	Transfer	15996212	20 mins ago	0x2db1d8cdf1abe8c70b...	0x421bf68aa8d382706c...	0.0386 Ether	0.00007151
0x9f0898be3c3207386...	Transfer	15996190	24 mins ago	0x2db1d8cdf1abe8c70b...	0x421bf68aa8d382706c...	0.0855 Ether	0.0000765
0xd46120a637c7b4cd05...	Transfer	15996111	40 mins ago	0x2db1d8cdf1abe8c70b...	0x85381b10f0a1133171...	0.012236 Ether	0.00007598

The screenshot shows the Etherscan interface for another wallet address: 0x760c6601F52Fb19c8E35f5425abBad524A4e7. The balance is 3.192640886197305395 Ether, with an Ether value of \$3,899.81. The token balance is \$113.53. A 'More Info' section shows 'My Name Tag' is not available. Below the wallet overview is a 'Blockscan Chat' banner with a 'Start Chat' button. The 'Transactions' section is visible at the bottom, showing a list of transactions with columns for Txn Hash, Method, Block, Age, From, To, Value, and Txn Fee.

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x1d94d5a7cd27336e5...	Transfer	15996302	3 mins ago	0x2db1d8cdf1abe8c70b...	0x760c6601f52b19c8e...	1.53 Ether	0.00027297
0x4919d543868a6031...	Transfer	15993241	10 hrs 19 mins ago	0x2db1d8cdf1abe8c70b...	0x760c6601f52b19c8e...	1.56 Ether	0.00003091
0x73ac45892be83ea819...	Transfer	15990803	19 hrs 10 mins ago	0x760c6601f52b19c8e...	Tether: USDT Stablecoin	0 Ether	0.00195847
0x7e160d363b1934b6...	Transfer	15990596	19 hrs 11 mins ago	0x760c6601f52b19c8e...	0xeec50ae241c61597a0...	0.27 Ether	0.00061612
0x2202678be2832569a3...	Transfer	15988641	1 day 1 hr ago	0x760c6601f52b19c8e...	0x1143b1366e1366dfb6...	0.04059 Ether	0.00002019
0x4d112c3211f76552e...	Transfer	15988626	1 day 1 hr ago	0x760c6601f52b19c8e...	0x760c6601f52b19c8e...	0.03993472 Ether	0.000037
0xad23959af0b508848...	Transfer	15977403	2 days 15 hrs ago	0x2db1d8cdf1abe8c70b...	0x760c6601f52b19c8e...	0.271 Ether	0.00004673
0xeea193c0e737b442c1...	Transfer	15976577	2 days 18 hrs ago	0x760c6601f52b19c8e...	0xeec50ae241c61597a0...	0.58 Ether	0.00041303
0xc95c61eb17bb50c74...	Transfer	15973687	3 days 3 hrs ago	0x760c6601f52b19c8e...	Tether: USDT Stablecoin	0 Ether	0.00068885

Follow blockchain transaction



The screenshot shows the Etherscan interface for the address **0x76C0C6601F52Fb19c8E35f55425abBad5245A4e7**. The interface includes a search bar, navigation links, and a list of transactions.

Etherscan
Eth: \$1,221.50 (+2.58%) | 13 Days

Address: **0x76C0C6601F52Fb19c8E35f55425abBad5245A4e7**

Sponsored by **BetFury** - Discover BetFury - Leading Crypto Casino [Spin now!](#)

Overview

- Balance: 3.192840886197305395 Ether
- Ether Value: \$3,899.81 (@ \$1,221.50/ETH)
- Token: **\$113.53**

More info

- My Name Tag: Not Available, [login to update](#)

Blockscan Chat | Wallet-to-wallet instant messaging platform. [Start Chat](#)

Transactions | ERC20 Token Txns | Analytics | Comments

17 Latest 25 from a total of 30 transactions

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x1d94d587c227336ef5...	Transfer	15986302	3 mins ago	0x2db1d8cdf1abe8c70b...	0x76c0c660152b19c8e...	1.53 Ether	0.00027287
0x4919d54386ca6ae031...	Transfer	15993241	10 hrs 19 mins ago	0x2db1d8cdf1abe8c70b...	0x76c0c660152b19c8e...	1.56 Ether	0.00030381
0x73ac45892be38a89...	Transfer	15990503	19 hrs 10 mins ago	0x76c0c660152b19c8e...	Tether: USDT Stablecoin	0 Ether	0.00195947
0x7e6160d363c819346...	Transfer	15990596	19 hrs 11 mins ago	0x76c0c660152b19c8e...	0xeeec50ae241c61597a0...	0.27 Ether	0.00061612
0x22d2e78be2832569a3...	Transfer	15988641	1 day 1 hr ago	0x76c0c660152b19c8e...	0x1143b1366e13b6db6...	0.04059 Ether	0.00032019
0x04d112c3211f7d552e...	Transfer	15988626	1 day 1 hr ago	0x7de0970471e10343...	0x76c0c660152b19c8e...	0.03993472 Ether	0.000387
0xad23959af68b508868...	Transfer	15977403	2 days 15 hrs ago	0x2db1d8cdf1abe8c70b...	0x76c0c660152b19c8e...	0.271 Ether	0.00044779
0xe8a1930c6737b4442c1...	Transfer	15976577	2 days 18 hrs ago	0x76c0c660152b19c8e...	0xeeec50ae241c61597a0...	0.58 Ether	0.00041303
0xc95c61eb17bcf50c74...	Transfer	15973687	3 days 3 hrs ago	0x76c0c660152b19c8e...	Tether: USDT Stablecoin	0 Ether	0.00066845



Smart contract

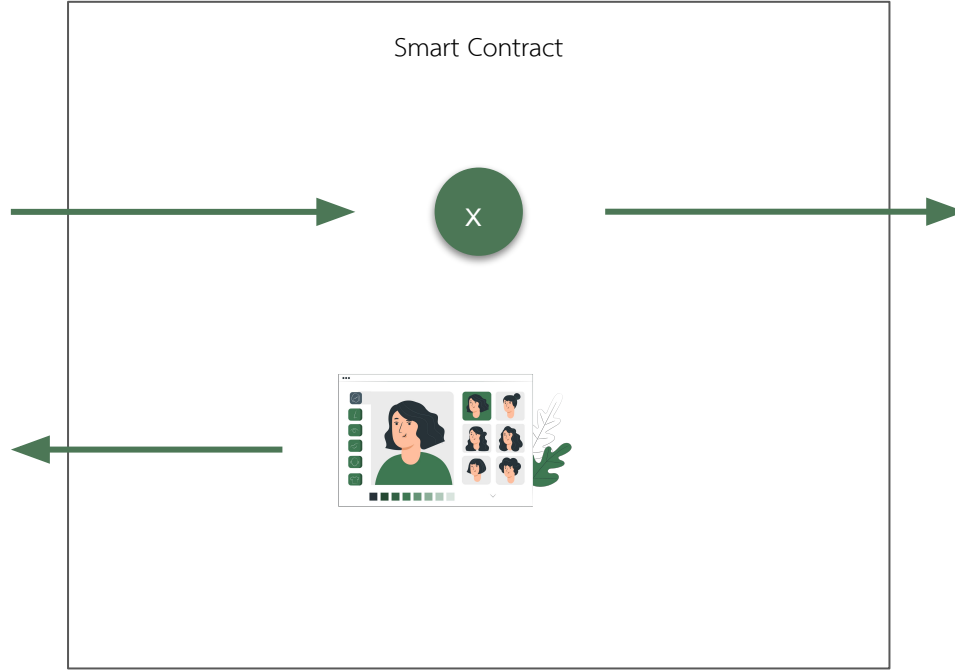
Ethereum uses what's called "Smart Contracts." Those are computer programs that run exactly as promised - without any downtime, censorship, or interference.

All participants in the Smart Contracts can trust that what they agreed on will actually happen - because it happens automatically. For example, if your purchase gets delivered, the seller will automatically be paid.

– *upfolio.com*



Buyer



Seller

Smart Contract Security

Smart Contract is a software developed to be run on blockchain, so it still has the same software security issues

DASP Top 10

1. Reentrancy

2. Access Control

3. Arithmetic

4. Unchecked Low Level Calls

5. Denial of Services

6. Bad Randomness

7. Front Running

8. Time Manipulation

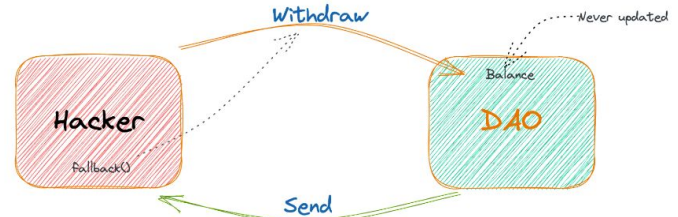
9. Short Addresses

10. Unknown Unknowns

<https://dasp.co/>

Example of Reentrancy attack

\$150m worth of ether (about 3.54 million ETH)



- This entitles the hacker to later call the withdraw() function in The DAO's smart contract.
- When the withdraw() function is eventually called, The DAO's contract sends ETH to the hacker
- Hacker's smart contract intentionally does not have a receive() function
- When it receives ETH from the withdraw request, the hacker's fallback function gets triggered
- This code, immediately upon execution, calls The DAO's smart contract's withdraw() function again

<https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/>

Smart Contract Security



World Invest

16 May at 14:01

วันนี้เราจะมาสรุปเหตุการณ์ของเหรียญ LUNA ให้เข้าใจกันง่าย ๆ ว่าเกิดจากเหตุการณ์ใด ทำให้เหรียญราคาพุ่งมากถึง 100% เราจะมาพูดถึงการทำงานของเหรียญ stable coin อย่าง UST กันก่อนว่าเกี่ยวข้องกับเหรียญ LUNA อย่างไร

โดยเหรียญ UST กับ LUNA มี Algorithm ที่สร้างมูลค่าโดย เมื่อเหรียญ UST มีมูลค่า < 1\$ จะทำการ Burn UST และทำการ Mint LUNA ขึ้นมาเพื่อ ลดจำนวน UST ทำให้ราคาเหรียญ UST กลับไปที่ราคา 1\$ แต่ส่งผลให้เหรียญ LUNA มีจำนวนเพิ่มขึ้นทำให้ ราคาเหรียญ LUNA ลดลง แต่ถ้าราคาเหรียญ UST > 1\$ จะทำการ Mint UST และ Burn LUNA เพื่อเพิ่มจำนวนเหรียญ UST ลดจำนวนเหรียญ LUNA ทำให้ราคา UST ลดลง และราคา LUNA เพิ่มขึ้น นี่คือระบบในการ Peg มูลค่าของ UST

ที่นี่เราจะมาพูดถึงปัจจัยที่ทำให้ราคาของเหรียญ Luna ร่วงกัน

- ปัจจัยที่ 1 เนื่องจากราคาของ BTC เพราะเรารู้กันอยู่แล้วเนื่องจาก market cap ของ BTC ที่ใหญ่มากเมื่อ BTC ราคาตกลงก็ทำให้เหรียญส่วนมากมีราคาลดลงตาม รวมถึง LUNA ด้วยเช่นกัน
 - ปัจจัยที่ 2 เนื่องจากมีการเทขายเหรียญ UST อย่างมาก ในช่วงที่ผ่านมา ทำให้ราคาของ UST ร่วงลงต่ำกว่า 1\$ ทำให้มีการ Mint เหรียญ LUNA ออกมาเป็นจำนวนมาก
- สรุปโดยปัจจัยหลักที่ทำให้เห็นได้ชัดมากที่สุดคือ "การเทขาย" UST ทำให้ราคนั้น หลุด Peg นั้นเอง และเกิดการ Mint เหรียญ LUNA ออกมาเป็นจำนวนมาก

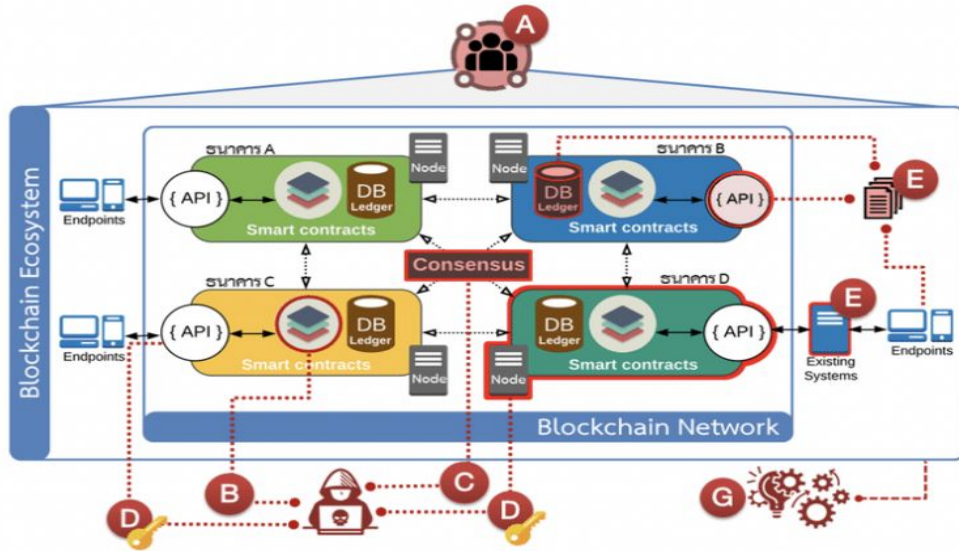
Terra's Algorithmic Market Module



cointelegraph.com

source: Terra Money, Cointelegraph Research

Inherent Risk of Blockchain



ความเสี่ยงเฉพาะจากการใช้เทคโนโลยี Blockchain

- A การกำกับดูแลเครื่องง่าย Blockchain และสมาชิกในเครื่องง่ายไม่ครอบคลุมเพียงพอ
- B Smart Contract ทำงานไม่ถูกต้องและไม่ปลอดภัย
- C การโจมตีกลไก Consensus
- D การบริหารจัดการกฎเกณฑ์เข้ารหัสที่ไม่รัดกุมเพียงพอ

ความเสี่ยงพื้นฐานด้าน IT และภัยคุกคามทางไซเบอร์

- E ความเสี่ยงจากการเชื่อมต่อระบบโครงสร้างพื้นฐานเดิมกับเครื่องง่าย Blockchain
- F ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยี

Digital Assets



Type of Digital Assets

ประเภทของสินทรัพย์ดิจิทัลภายใต้ พรก.สินทรัพย์ดิจิทัล



Digital Assets

Digital Token = สิทธิในการร่วมลงทุน หรือ ได้มาซึ่งสินค้าและบริการ

Cryptocurrency = สื่อกลางในการแลกเปลี่ยนสินค้า/บริการ

NFT

Investment Token

สิทธิในการร่วมลงทุน

Utility Token

สิทธิในการได้มาซึ่งสินค้าและบริการ

- พร้อมใช้
- ไม่พร้อมใช้

SiriHub
TOKEN

DESTINY TOKEN

โทเคนดิจิทัลสภาพคล่องครบถ้วนจำนวน ๒



Popcoin



MVP Coin



Private (ออกโดยภาคเอกชน)

CBDC

(ออกโดยธนาคาร
แห่งประเทศไทย)

Stable Coin

(มีสินทรัพย์หนุนหลัง)

Blank Coin

(ไม่มีสินทรัพย์หนุนหลัง)



Tether (USDT)



ethereum



Bitcoin



Dogecoin



Inthanon-LionRock

NFT Charity : Happy Chana
Bitkub ICON store

NFT Charity : Happy Chana เป็นโครงการ NFT ที่ผูกเพื่อชุมชน:
มอบทุกคู่คุณได้เป็นของขวัญในครั้งเดียวหรือทำ เพื่อส่งเสริมธุรกิจ รายได้จากการจำหน่ายของจะมอบให้
กับชุมชนเป้าหมาย อ.ระ: ๑.๑๐๖๓ #SaveChana

โปรดติดตามรายละเอียดบนช่องทางโซเชียลมีเดีย ได้ที่:
<https://www.facebook.com/bitkubgroup> และ <https://www.facebook.com/bitkubnft>

จำนวน NFT ทั้งหมด: 265 / 300
ราคาต่อชิ้น 10 KUB/ชิ้น

- 1 +
8 KUB / ชิ้น
= 8456 / ชิ้น

ปุ่ม: ซื้อทันที

NFT ในรายชื่อ

NFT	Rarity	จำนวน	โอกาสได้
[SR] Many Happy - ลากทาลงบน เบ็นดี้	SR	10 Supply	3.33 %
[SSR] Smiling Happy - Happy สองอัน	SSR	10 Supply	3.33 %

Non-fungible tokens (NFTs)

(NFTs) are tokens that we can use to represent ownership of unique items. They let us tokenize things like art, collectibles, even real estate. They can only have one official owner at a time and they're secured by the blockchain – no one can modify the record of ownership or copy/paste a new NFT into existence.

– ethereum.org

GON FRIEND FOREVER CARD

THE STORY THAILAND

NFT ภาษีก่อน เลิกร่อง CRM

ความเสี่ยงระหว่างกระเป๋าทั้งสองแบบนี้ ?



“Not your keys not your coin”

ถ้าเราไม่ได้เป็นคนถือ Private Key เราก็ไม่ได้เป็นเจ้าของเหรียญที่แท้จริง

- ถ้าเราเลือกบริหาร Wallet และเก็บ Private key เองก็ปลอดภัยจากการโดนคนอื่นขโมย Key มากกว่าแต่เราก็ต้องมีความเข้าใจใน Technology และ การบริหารจัดการ
- ถ้าเราไม่เชี่ยวชาญเราสามารถเลือกใช้ Custodial Wallets โดยเลือกผู้ให้บริการที่น่าเชื่อถือ

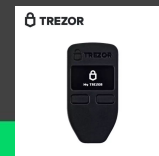
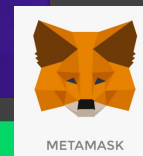
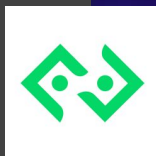
Custodian and Non-custodial wallets



เจ้าของกระเป๋าไม่ได้เป็นผู้ดูแล Private Key ของตัวเอง กระเป๋าถูกสร้างขึ้นโดยการ Support จากบุคคลอื่น มี Third Party ช่วยดูแล Private Key ให้



กระเป๋านี้เจ้าของกระเป๋าเป็นคนดูแล Private Key ของตัวเอง ไม่มีใครมาช่วยเหลือในการบริหารจัดการ



Transfers and Recovery of Digital asset



นายเอ ต้องการโอน ETH ไปให้นายบี

ยอด 1 ETH
Address ปลายทาง: 1234567890



ตอนทำรายการใส่ข้อมูลผิด
Amount 1 ETH
Address: 12345678910



นายบี
Address: 1234567890
Status: ไม่ได้รับเหรียญ

เคสเหรียญไปผิด Address

ใส่ Address ผิดชีวิตเปลี่ยน

แต่ถ้า address นี้ไม่มีเจ้าของ?



นายซี
Address: 12345678910
Status: ได้รับเหรียญมาแบบงงๆ



Transfers and Recovery of Digital asset



According to a recent study by Chainanalysis, around 20% of all Bitcoins are lost and unrecoverable.

<https://www.investopedia.com/news/20-all-btc-lost-unrecoverable-study-shows/>

How to avoid sending to wrong address or mistake

- Test send [small amount]
- Test retrieve
- Check your device for malware

De-Fi Service

What are DeFi Products and Services?



Stable Currencies



Insurance



Financing



Raise Funds



Saving Accounts



Liquidity Mining



Asset Transfers



Staking



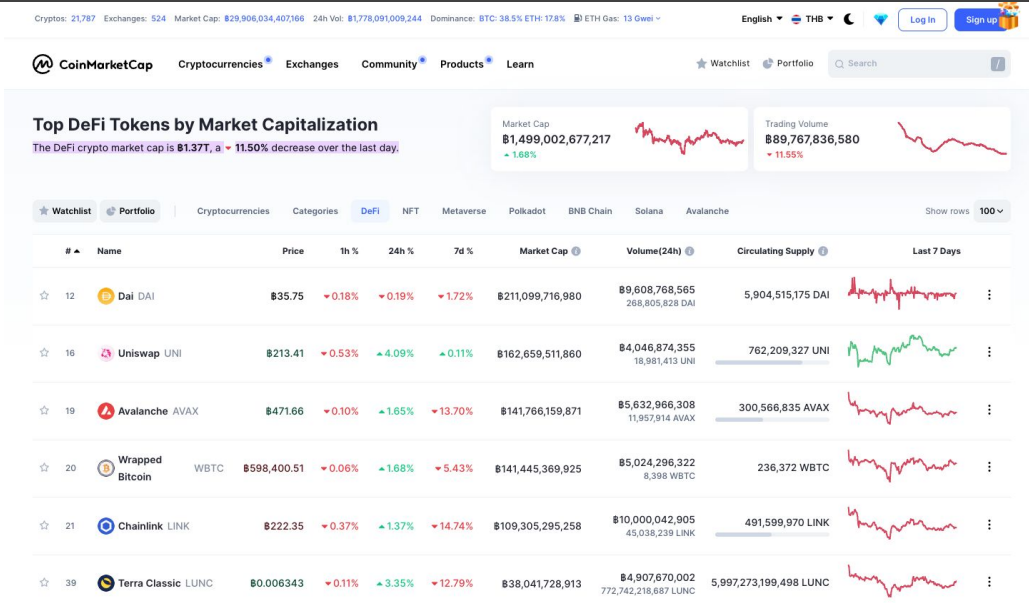
Exchange/Swap



Derivatives



www.brieflyfinance.com



High risk transactions

Due to nature of cryptocurrency, they are used to facilitate high risk transactions as per noted in the table.

As a institution or entity which accept or maintain digital assets you should be aware of where they are coming from and going to.

Wallet address on high risk categories could be identified through various sources such as

- OFAC - <https://sanctionssearch.ofac.treas.gov/>
- Communities
- Commercial sources
- Government agencies and law enforcement

Category or services	Risky when sending	Risky when receiving
Fraud shop	✓	✓
Illicit actor organization	✓	✓
Darknet Market	✓	✓
Mixing	✓	✓
Gambling	✓	✓
P2P exchange	✓	✓
Child abuse	✓	✓
Terrorism financing	✓	✓
Sanctions	✓	✓
High risk exchange	✓	✓
High risk jurisdiction	✓	✓
Protocol privacy	✓	✓

High risk transactions

High profile hackers are targeting digital assets

Business

North Korean Hacker Group Lazarus Targets Japanese Crypto Firms

Lazarus Group has been targeting Japanese firms with phishing links via email and social media.

By Oliver Knight · Oct 17, 2022 at 2:40 p.m. · Updated Oct 17, 2022 at 11:04 p.m.

Crypto

US officials link North Korean Lazarus hackers to \$625M Axie Infinity crypto theft

Carly Page @carlypage_ / 9:53 PM GMT+7 · April 15, 2022

Comment


How the digital assets are stolen are still the same


- Phishing
- Server security
- Endpoint security



Blockchain and Smart Contract Security


<https://www.beakonone.com/home>




[Home](#) [Services](#) [Dashboard](#) [Blog](#) [Contact Us](#) 

Beakon Trust Leaderboard

A blockchain and smart contract security research and consulting group. Collectively group members have extensive experience on development, implementation and audit for major organizations in various industries.


10 Projects are on boarded 





















2 Projects are reviewing 

Smart Contract Audit


We confidently perform review of smart contract using combination of automated and manual audit.


[Request Quote](#)




NAME	SCORING	STATUS	ONBOARD DATE	MORE
1  Redemption V3	 82%	On Boarded	June 23, 2022	→
2  Social Dao	 81%	On Boarded	June 17, 2022	→
3  DiceKingdom	 77%	On Boarded	May 17, 2022	→
4  FansDungeon V1	 81%	On Boarded	February 17, 2022	→
5  Bitkub NFT	 97%	On Boarded	June 20, 2022	→
6  Bitkub Chain Oracle	 93%	On Boarded	April 11, 2022	→
7  Lumi	 87%	On Boarded	February 20, 2022	→
8  We Token	 94%	On Boarded	May 20, 2022	→
9  YES Token	 93%	On Boarded	January 21, 2022	→
10  Yuemmai	 90%	On Boarded	April 19, 2022	→

show Total Results : 10




[Home](#) [Services](#) [Dashboard](#) [Blog](#) [Contact Us](#) 

BLOG




จะเป็น Smart-Contract Auditor...

ก่อนที่จะเริ่มเนื้อหาของ การเริ่มต้นเป็น Smart-Contract Auditor ท่านผู้เขียนต้อง...




สาระที่ Smart-Contract Auditor...

จากสิ่งที่เราได้ศึกษามา ในหัวข้อ การเตรียมตัวเป็น Smart-Contract Auditor นั้น...




Why we should be aware of t...

how they hide malicious code and how they can use malicious code to exploi...




ขอบเขตการทำงานของ Smart-...

จากสิ่งที่เราได้ศึกษามา ในหัวข้อ การเตรียมตัวเป็น Smart-Contract Auditor ใ้...




Applying the Business...

Assuming you are an experienced IT auditor, your past assignment focuse...




คุยกับ Dev #1

การลดค่า Gas ด้วยการใช้...



คุยกับ Dev #2

Public vs External อันไหนใช้ดี...



หนึ่งวันมีแค่ Crypto Wallet อยู่...

ถ้าวันหนึ่ง คุณมีแค่ Crypto Wallet อยู่จะได้ทำอะไร...