Key Risk for Blockchain and Digital Assets

Presentation for BFIIA 2022

bitkub

www.bitkub.com

Key Risk for Blockchain and Digital Assets

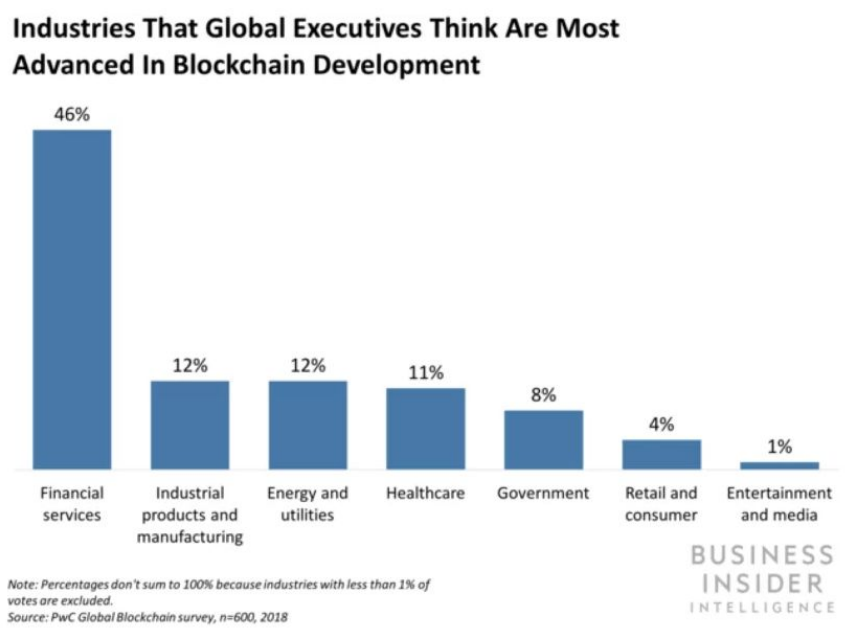
1 - Blockchain

- 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



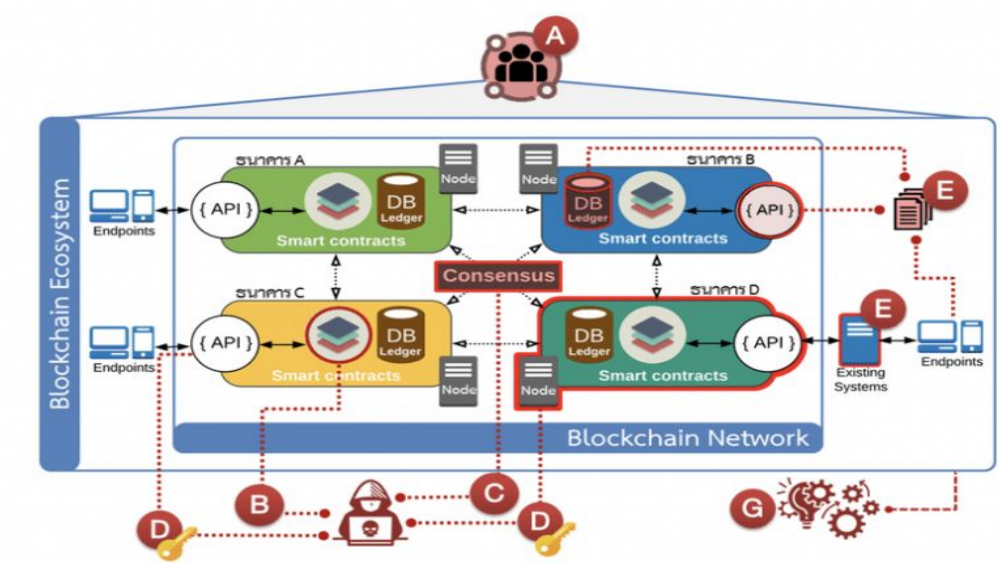
Central Bank Digital Currencies

Digital Identity

Retail Fashion and Luxury

Insurance

Inherent Risk of Blockchain



ความเสี่ยงเฉพาะจากการใช้เทคโนโลยี Blockchain

- A การกำกับดูแลเครือข่าย Blockchain และสมาชิกในเครือข่ายไม่ครอบคลุมเพียงพอ
- B Smart Contract ทำงานไม่ถูกต้องและไม่ปลอดภัย
- C การโจมตีกลไก Consensus
- D การบริหารจัดการกุญแจเข้ารหัสที่ไม่รัดกุมเพียงพอ

ความเสี่ยงพื้นฐานด้าน IT และภัยคุกคามทางไซเบอร์

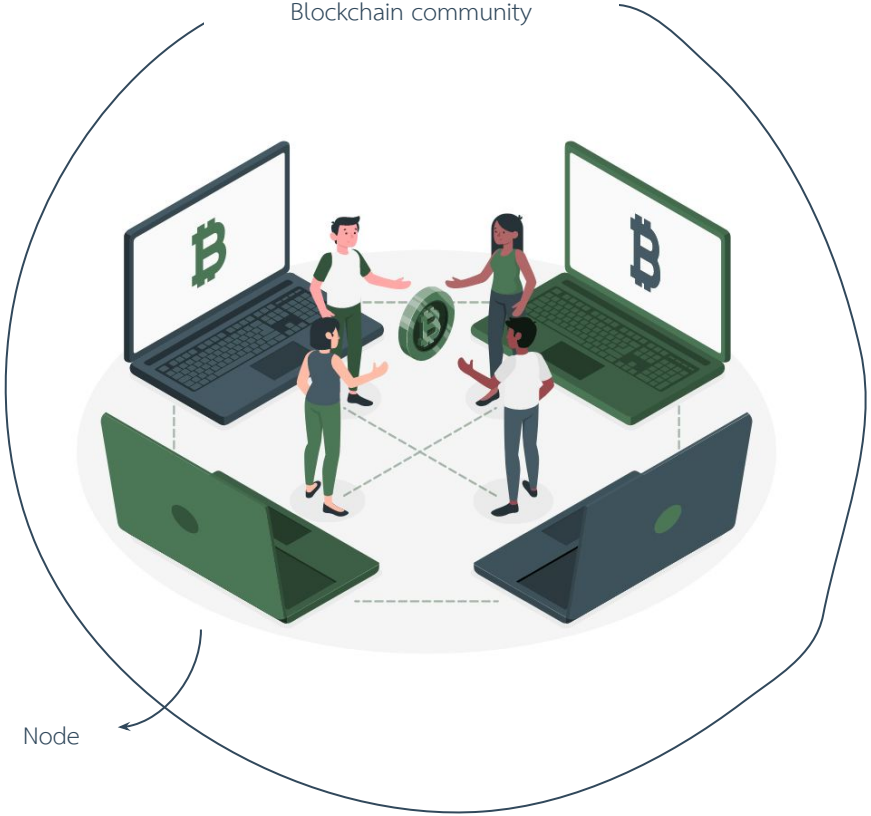
- E ความเสี่ยงจากการเชื่อมต่อระบบโครงสร้างพื้นฐานเดิมกับเครือข่าย Blockchain
- F ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยี

https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2564/ThaiPDF/25640101.pdf

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.



CASE#1

How does **Blockchain** work?

A transfers cryptocurrency to B

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

CASE#2

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.

CASE#3

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

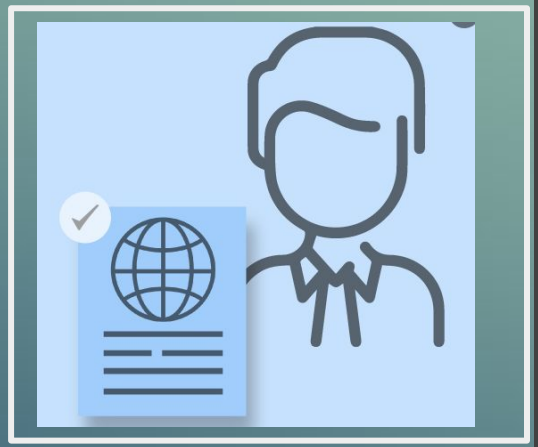
Proof Of Work [POW]

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

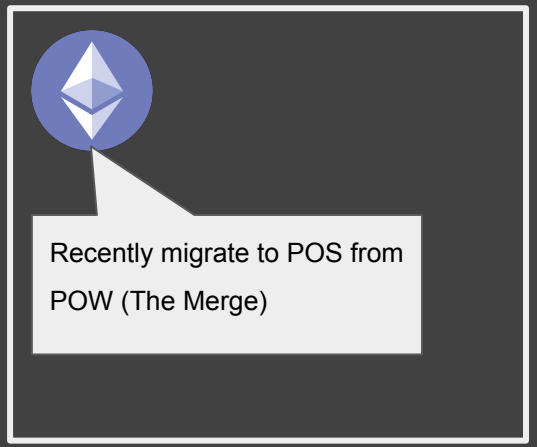
POSA

Blockchain Consensus

Proof Of Work [POW]

Using powerful computing power to solve math problems

Proof Of Stake [POS]



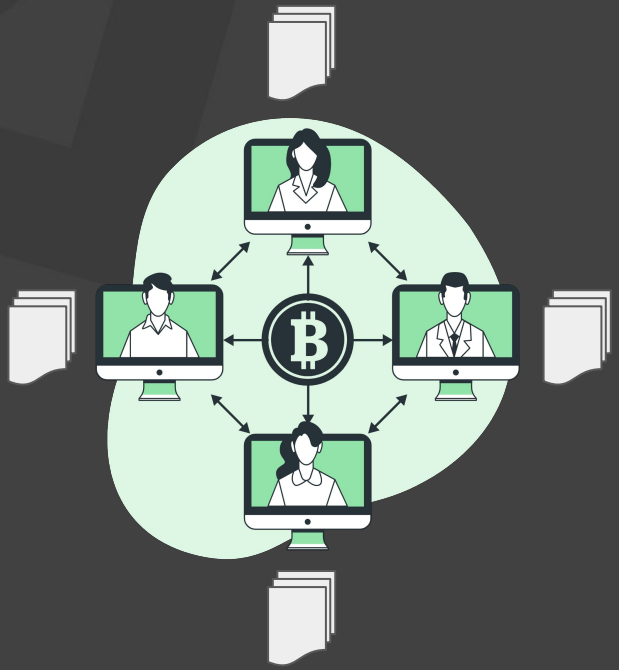
People with most token

Proof Of Authority [POA]

Selected entity/individual with good reputation

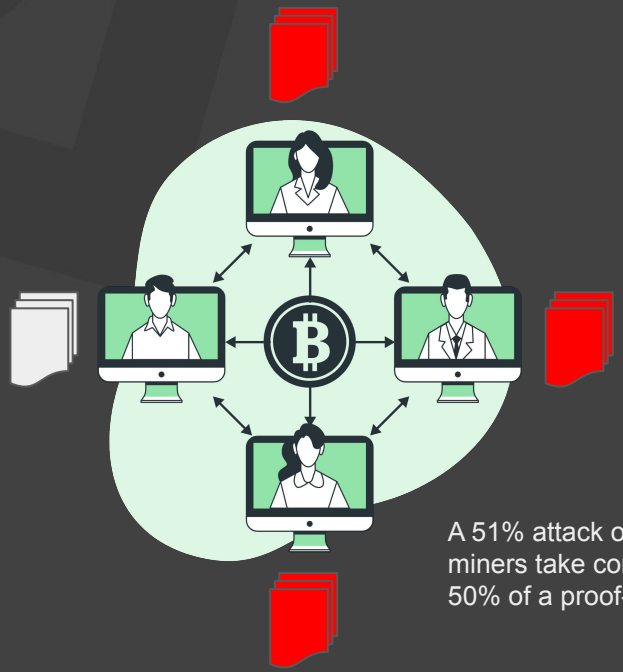
POSA

Blockchain - What could go wrong ?

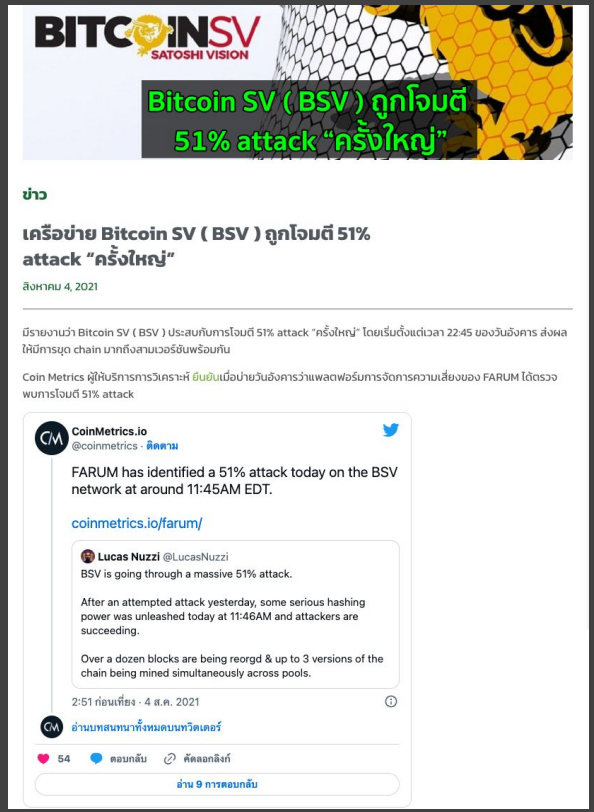


Blockchain depends on everyone [validator nodes] to maintain information / database. With this decentralized network, if one node was compromise, information can not be manipulated by malicious individuals. Unless ?

Blockchain - What could go wrong ?

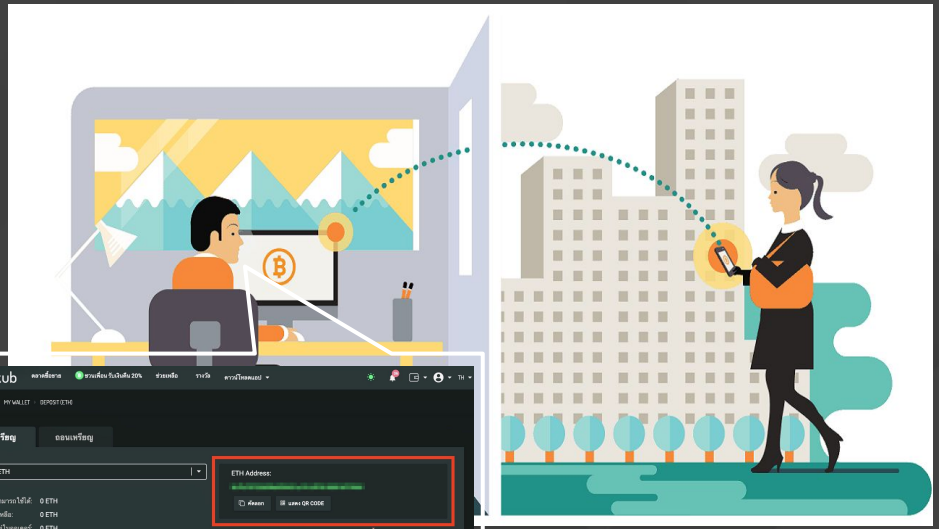


A 51% attack occurs when malicious miners take control of more than 50% of a proof-of-work blockchain.



https://bitcoinaddict.org/2021/08/04/breaking-bsv-reportedly-suffers-massive-51-attack/

เลข Wallet Address มาได้ไง



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

Public key

Private key

2

Encode with Base58

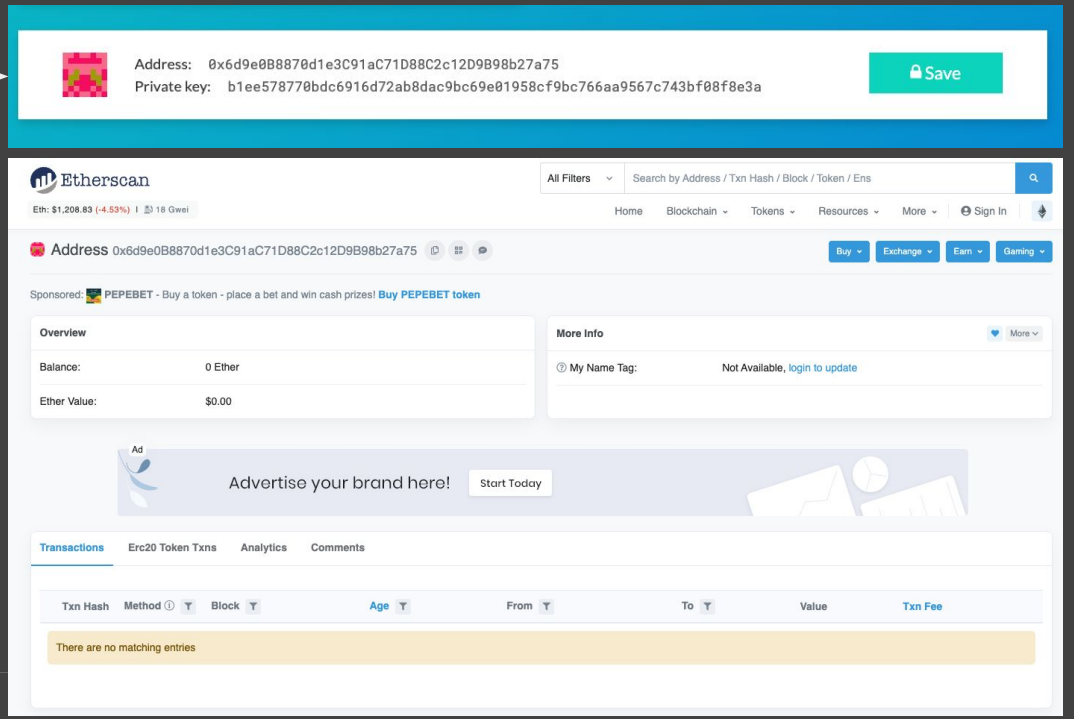
1 **Wallet Address:**
bc1qqdykm85ycxjqjh5hrkwmewts02mm6ku5rlck3m

Private Key:
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262

อันนี้ต้องเก็บไว้เป็นความลับ ห้ามแชร์ให้คนอื่น ห้ามหาย

Addresses and Private Key

https://vanity-eth.tk/



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

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

Private Key:

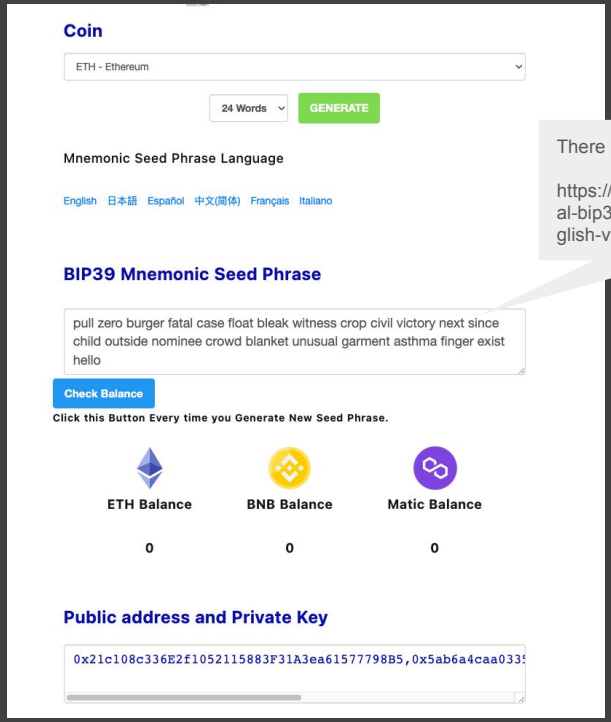
xprv9s21ZrQH143K42r3nHWHumL2sBrw6MvmkyP5y
bGd7GgUjCxHw6bo3fvTVRWVaxZLKMZSP82xEavw
2AEeZfS1LzUQPjiNKWURVrdD2m56sMq

https://iancoleman.io/bip39/

https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

Addresses and Private Key

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



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

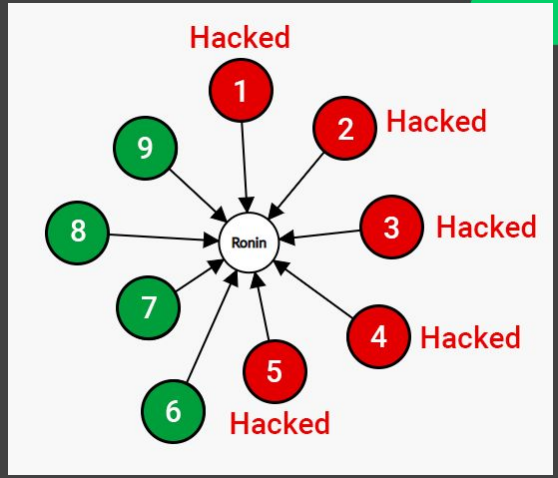
- Ronin is a side-chain of Ethereum (in which Axie Infinity operates). It's secured by 9 validators and you only needed 5 (+50%) to attack the network
- The attackers got access to the System that operates 4 of the nodes, and found a bug to access another node
- With +50% of the nodes in the hands of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

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

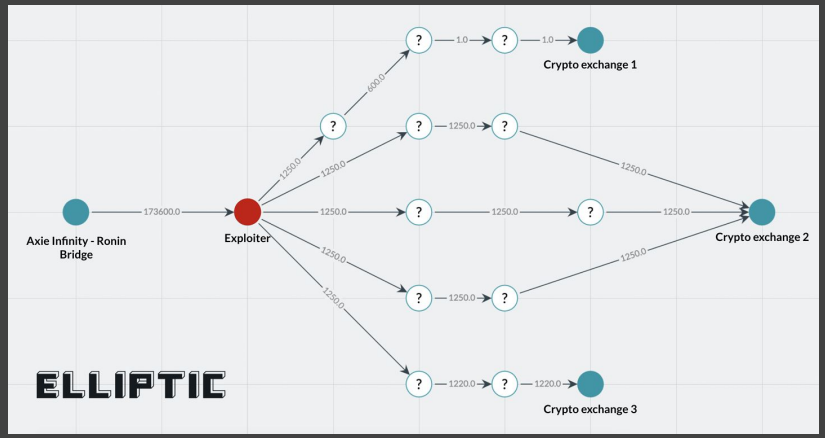
Lesson Learned

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

https://rattibha.com/thread/1508852842685153282



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



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.

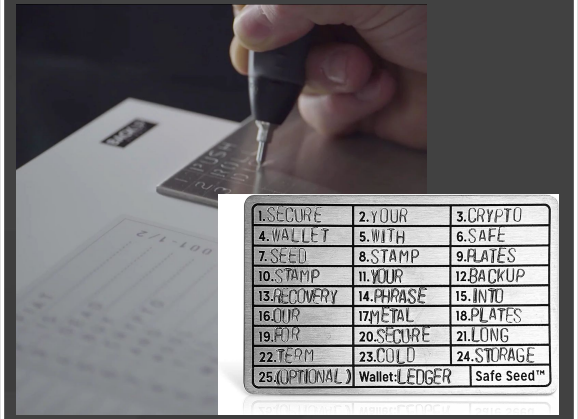
Multi-Keys

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

bitkub

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.

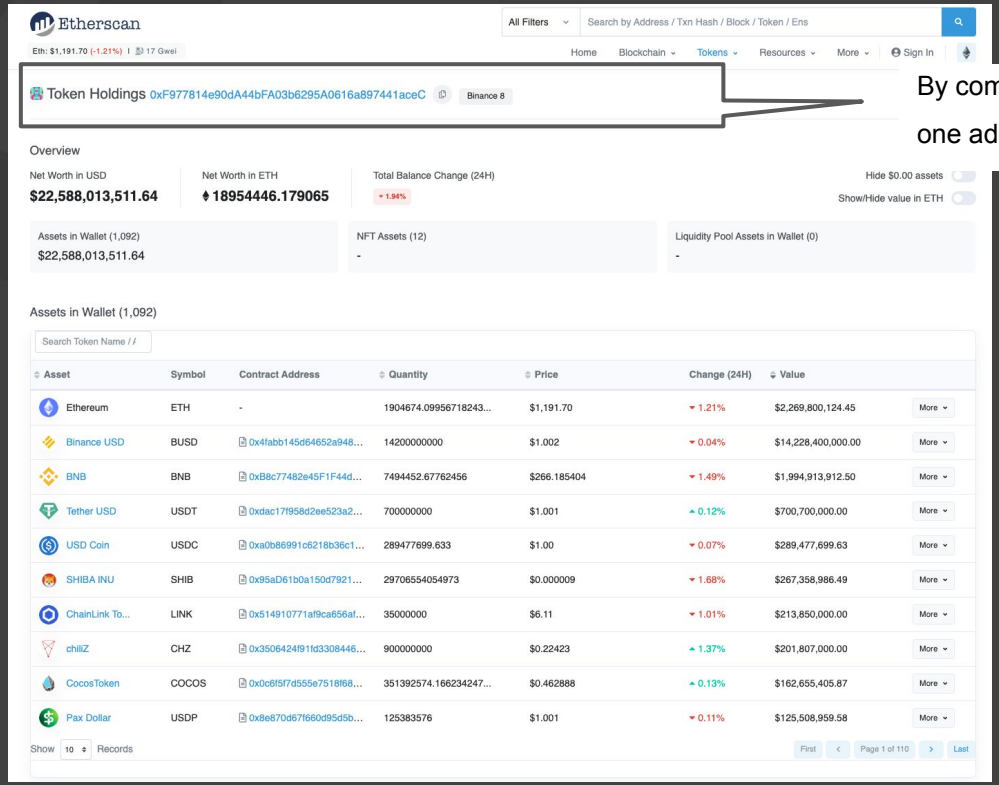
Ethereum Virtual Machine (EVM) and ERC20

- 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	Ubiq UBQ
19	Evmos EVMOS

Implication of EVM and ERC20 Compatible



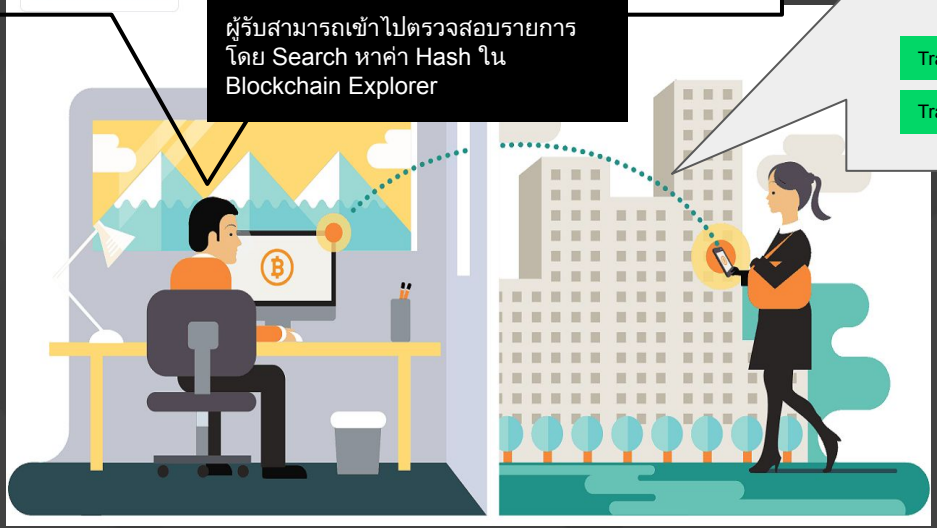
By complying to the same ERC20 standard one address can support multiple tokens

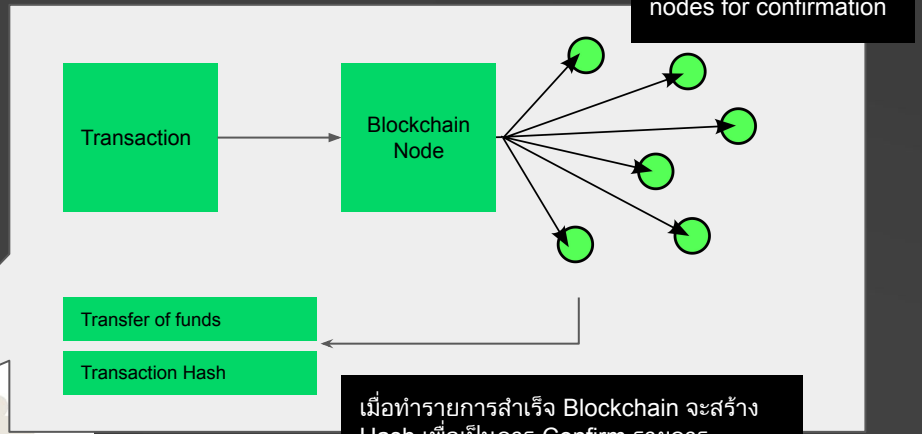
เวลาทำการโอนเหรียญเกิดอะไรขึ้นบ้าง

Hash	Time	Amount (BTC)	Amount (USD)
85156f1d43b86dc267959b709821fc595ec00d6f0...	22:03	1.26903658 BTC	$50,428.63
174534a3ae55a836d353417929a458501554be9a...	22:03	0.08153844 BTC	$3,240.15
bbd8baf9d6d43d9a3160e42f3b6862adeff085a6a...	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



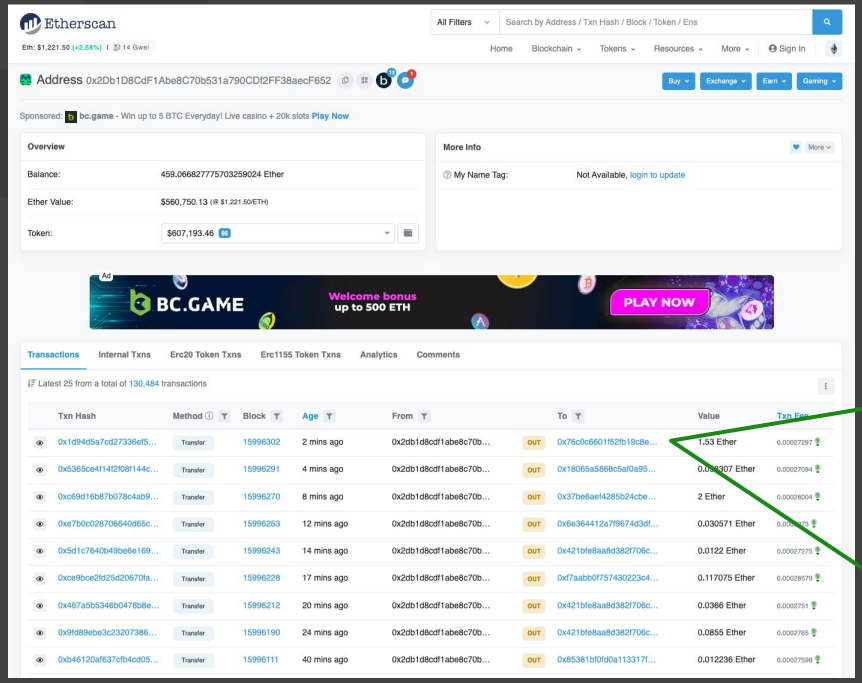


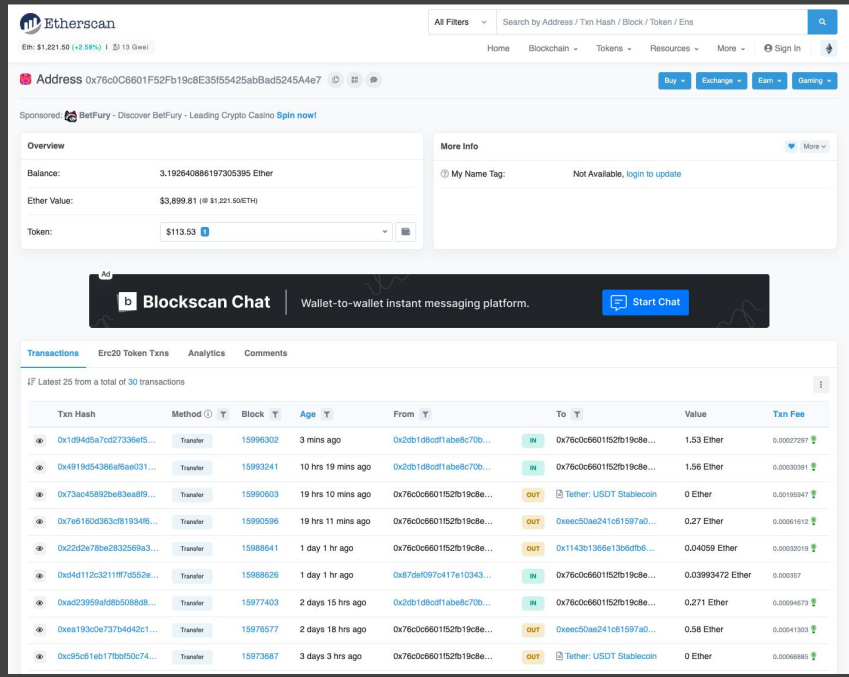
เมื่อทำรายการสำเร็จ Blockchain จะสร้าง Hash เพื่อเป็นการ Confirm รายการ

Hash นี้เหมือนกับ ID ของรายการ Transfer

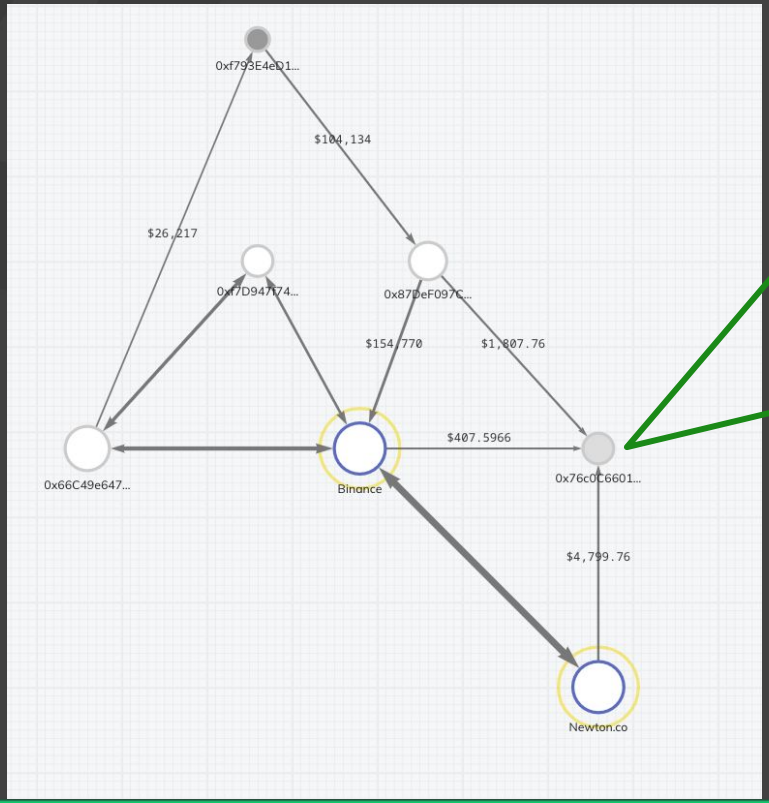
Follow blockchain transaction

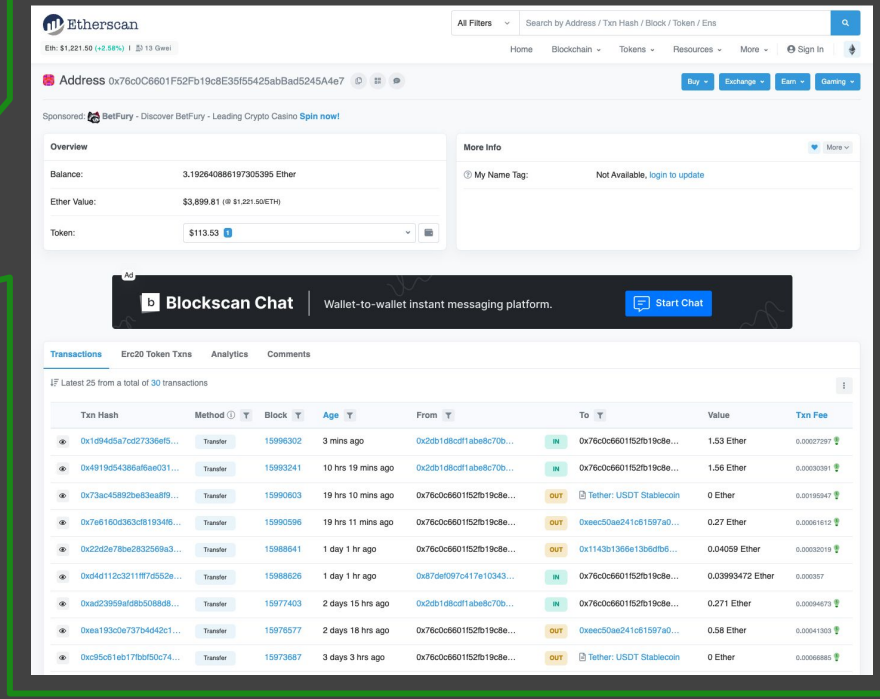
On public blockchain, it is possible to to trace transactions and addresses. However there is limited to no information on who is the owner of this address





Follow blockchain transaction



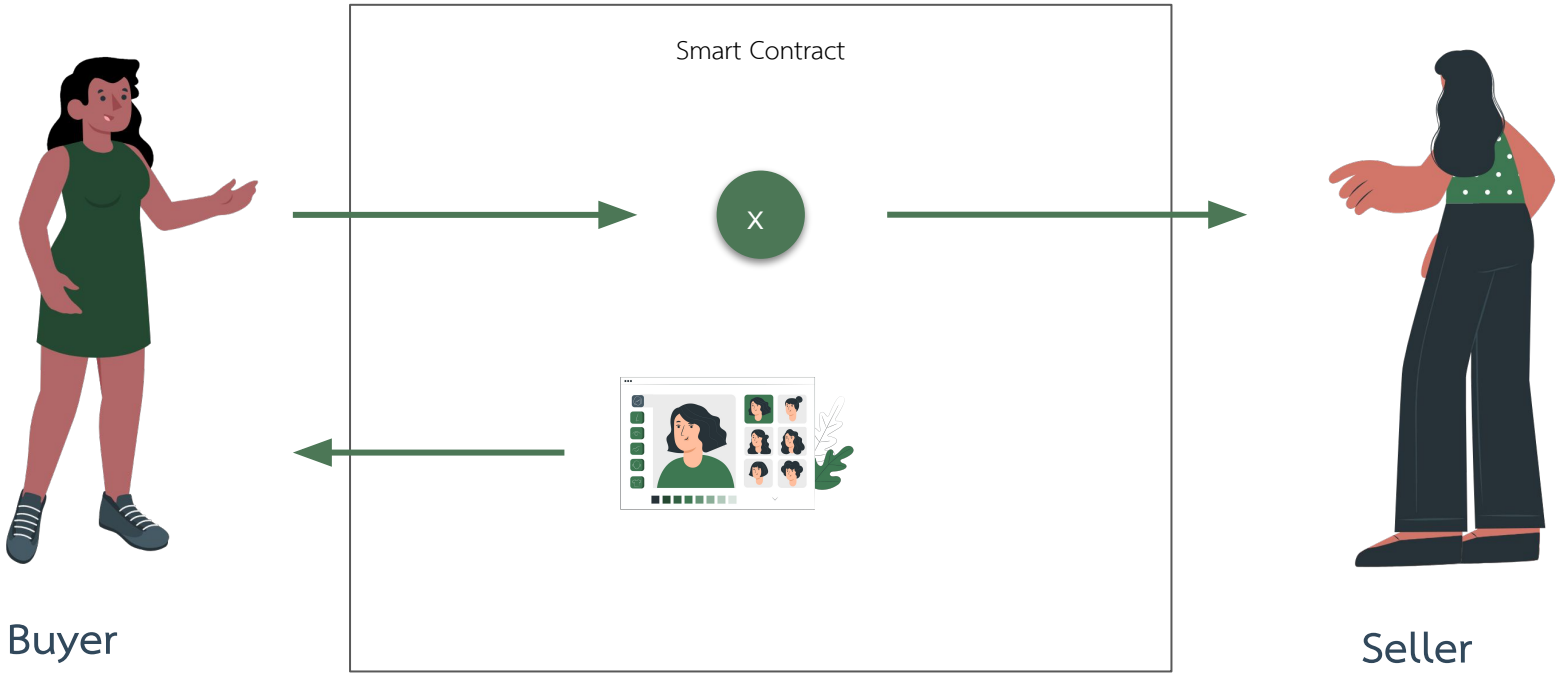


Smart contract

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*


Smart Contract
X
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

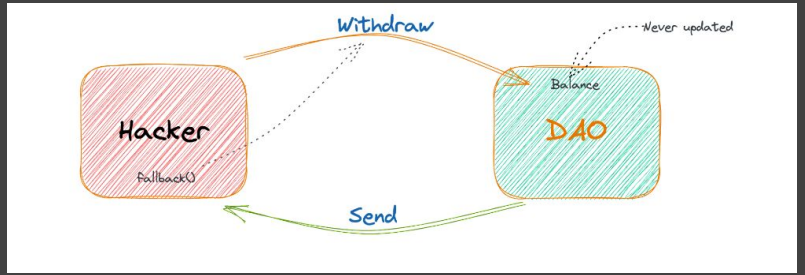
DASP Top 10

1. Reentrancy	6. Bad Randomness
2. Access Control	7.Front Running
3. Arithmetic	8. Time Manipulation
4. Unchecked Low Level Calls	9. Short Addresses
5. Denial of Services	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 ให้เข้าใจกันง่ายๆว่าเกิดจากเหตุการณ์ใด ทำให้เหรียญราคาร่วงมากถึง 100% เราจะมาพูดถึงการทำงานกันของเหรียญ stable coin อย่าง UST กันก่อนว่าเกี่ยวข้องกับเหรียญ LUNA อย่างไร

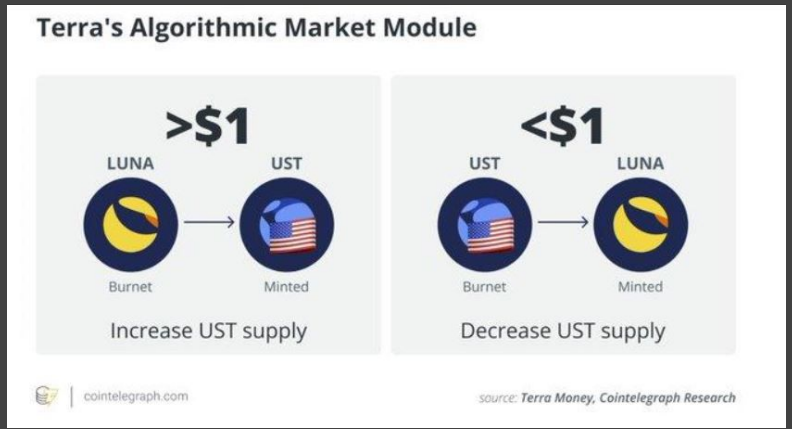
โดยเหรียญ UST กับ LUNA มี Algorithm ที่สร้างมูลค่าโดย เมื่อเหรียญ UST มีมูลค่า < 1$ จะทำการ Burn UST และทำการ Mint LUNA ขึ้นมาเพื่อ ลดจำนวน UST ทำให้ราคาเหรียญ UST กลับไปที่ราคา 1$ แต่ส่งผลให้เหรียญ LUNA มีจำนวนเพิ่มขึ้นทำให้ ราคาเหรียญ LUNA ลดลง แต่ถ้าราคาเหรียญ UST > 1$ จะทำการ Mint UST และ Burn LUNA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

ทีนี้เราก็จะมาพูดถึงปัจจัยที่ทำให้ราคาของเหรียญ Luna ร่วงกัน

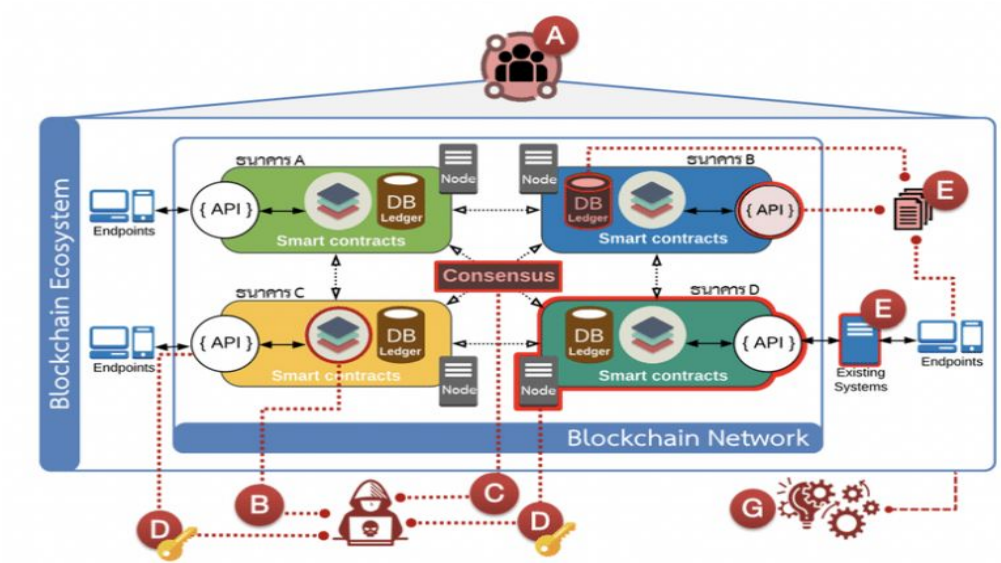
- ปัจจัยที่ 1 เนื่องจากราคาของ BTC เพราะเราก็รู้กันอยู่แล้วเนื่องจาก market cap ของ BTC ที่ใหญ่มากเมื่อ BTC ราคาลดลงก็ทำให้เหรียญส่วนมากมีราคาลดลงตาม รวมถึง LUNA ด้วยเช่นกัน
- ปัจจัยที่ 2 เนื่องจากมีการเทขายเหรียญ UST อย่างมากในช่วงที่ผ่านมา ทำให้ราคาของ UST ร่วงลงต่ำกว่า 1$ ทำให้มีการ Mint เหรียญ LUNA ออกมาเป็นจำนวนมาก

สรุปโดยปัจจัยหลักที่ทำให้เห็นได้ชัดมากที่สุดคือ "การเทขาย" UST ทำให้ราคานั้น หลุด Peg นั้นเอง และเกิดการ Mint เหรียญ LUNA ออกมาเป็นจำนวนมาก

.



Inherent Risk of Blockchain



ความเสี่ยงเฉพาะจากการใช้เทคโนโลยี Blockchain

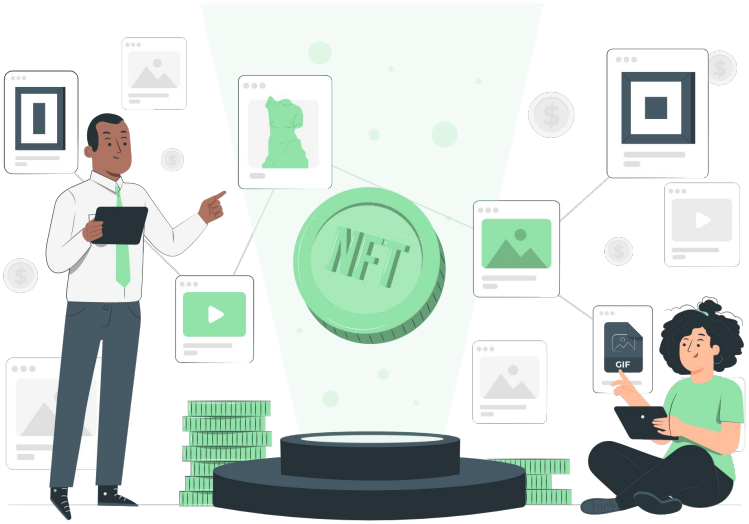
- A การกำกับดูแลเครือข่าย Blockchain และสมาชิกในเครือข่ายไม่ครอบคลุมเพียงพอ
- B Smart Contract ทำงานไม่ถูกต้องและไม่ปลอดภัย
- C การโจมตีกลไก Consensus
- D การบริหารจัดการกุญแจเข้ารหัสที่ไม่รัดกุมเพียงพอ

ความเสี่ยงพื้นฐานด้าน IT และภัยคุกคามทางไซเบอร์

- E ความเสี่ยงจากการเชื่อมต่อระบบโครงสร้างพื้นฐานเดิมกับเครือข่าย Blockchain
- F ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยี

https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2564/ThaiPDF/25640101.pdf

Digital Assets



Type of Digital Assets

ประเภทของสินทรัพย์ดิจิทัลภายใต้ พรก.สินทรัพย์ดิจิทัล

SET

Digital Assets

Digital Token = สิทธิ์ในการร่วมลงทุน หรือ ได้มาซึ่งสินค้าบริการ		Cryptocurrency = สื่อกลางในการแลกเปลี่ยนสินค้า/บริการ			NFT
Investment Token สิทธิในการร่วมลงทุน	**Utility Token** สิทธิในการได้มาซึ่งสินค้าและบริการ	**Private** (ออกโดยภาคเอกชน)		**CBDC** (ออกโดยธนาคารแห่งประเทศนั้นๆ)	
		Stable Coin (มีสินทรัพย์หนุนหลัง)	**Blank Coin** (ไม่มีสินทรัพย์หนุนหลัง)		
	• พร้อมใช้ • ไม่พร้อมใช้	Tether (USDT)	ethereum Bitcoin Dogecoin	UBIN Inthanon-LionRock	

SiriHub TOKEN

DESTINY TOKEN

Popcoin

MVP Coin

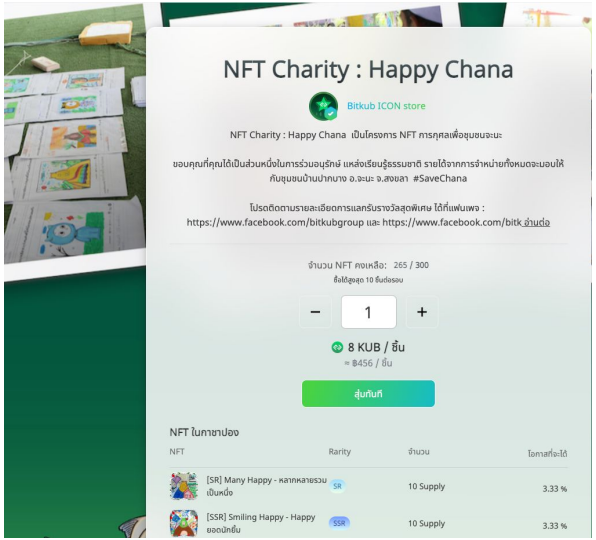
JFIN COIN

Non-fungible tokens (NFTs)

(NFTs) are tokens that we can use to represent ownership of unique items. They let us tokenise 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*

https://www.bitkubnft.com/gashapon/278



ความเสี่ยงระหว่างกระเป๋าทั้งสองแบบนี้ ?

bitkub

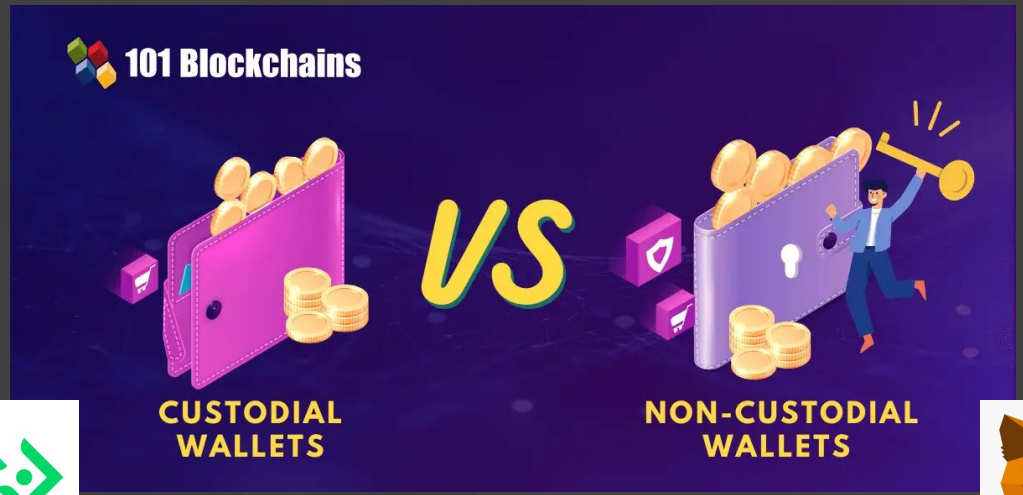
“Not your keys not your coin”

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

METAMASK

TREZOR

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

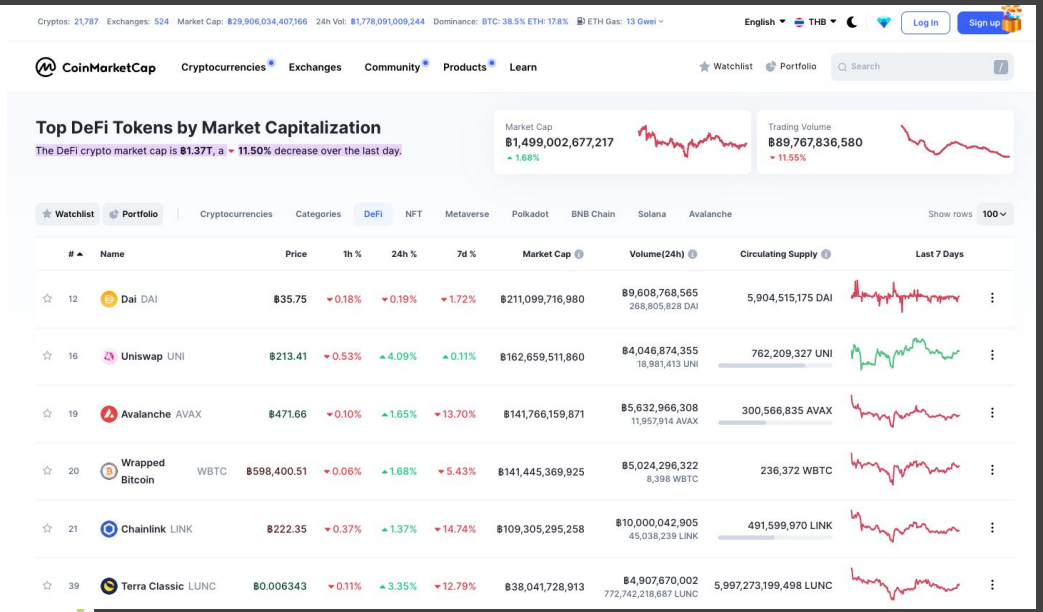
- Test send [small amount]
- Test retrieve
- Check your device for malware

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