



BLOCKCHAIN 101

CREDIT : คุณเพชร, คุณอิว, ทีมงาน
Research,
คุณเลือ, คุณชุม, ทีมงาน GRAPHIC

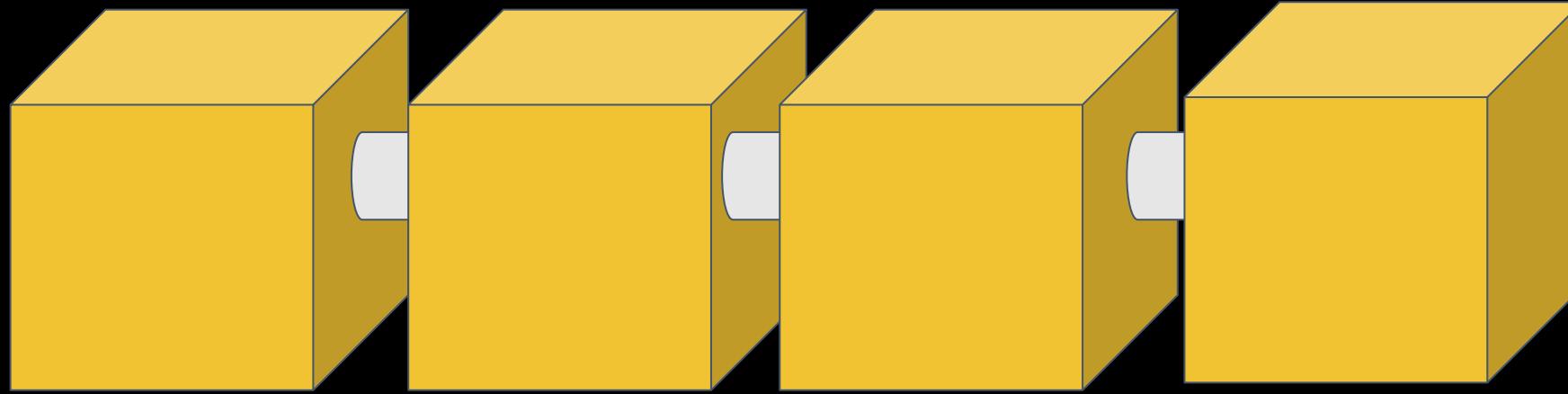


“What the internet did for communications, I think blockchain will do for trusted transactions”

Ginni Rometty CEO of IBM



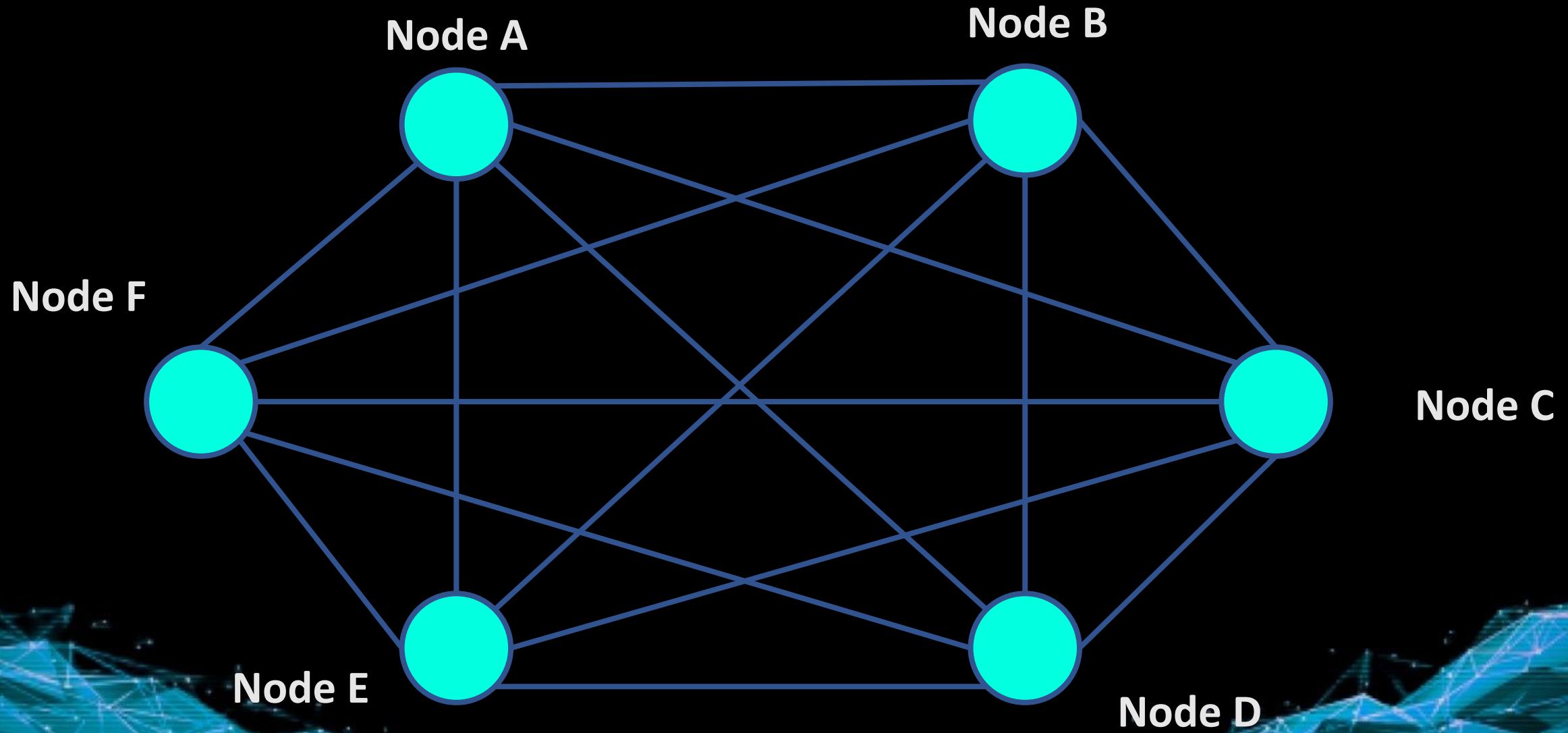
blockchain



BLOCK 1 BLOCK 2 BLOCK 3 BLOCK 4

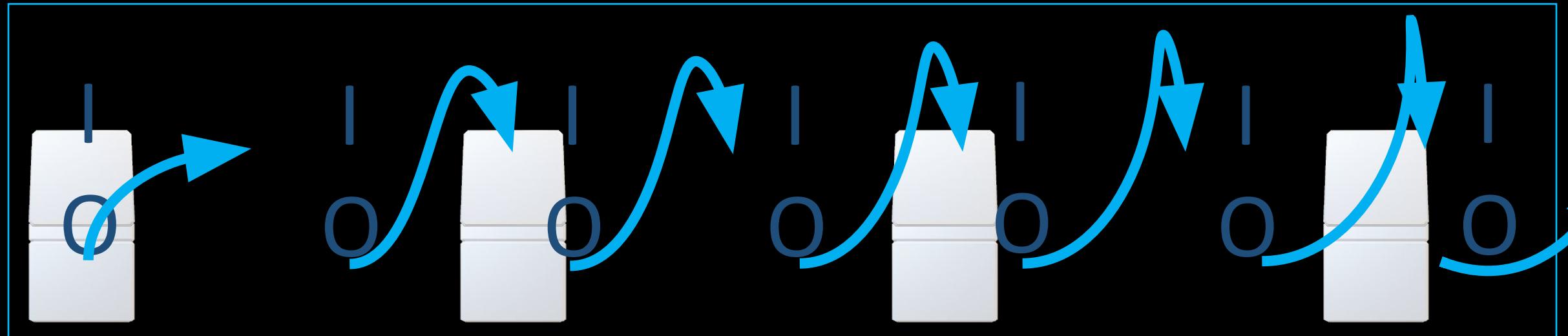


blockchain



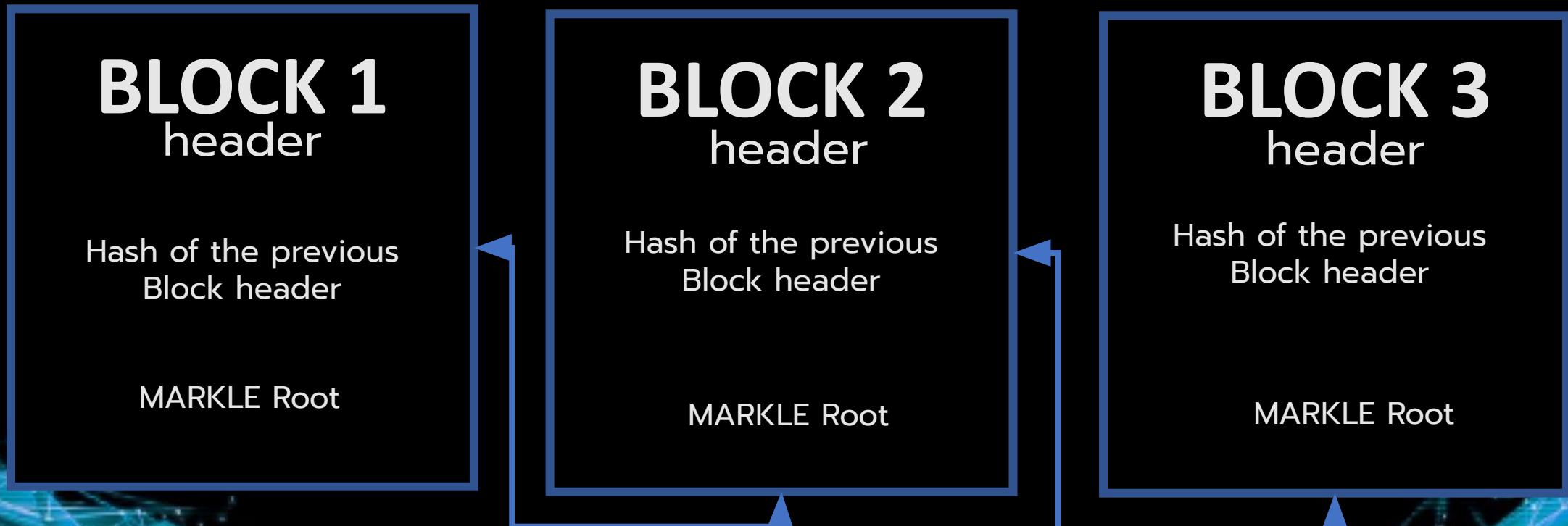


การสร้าง block



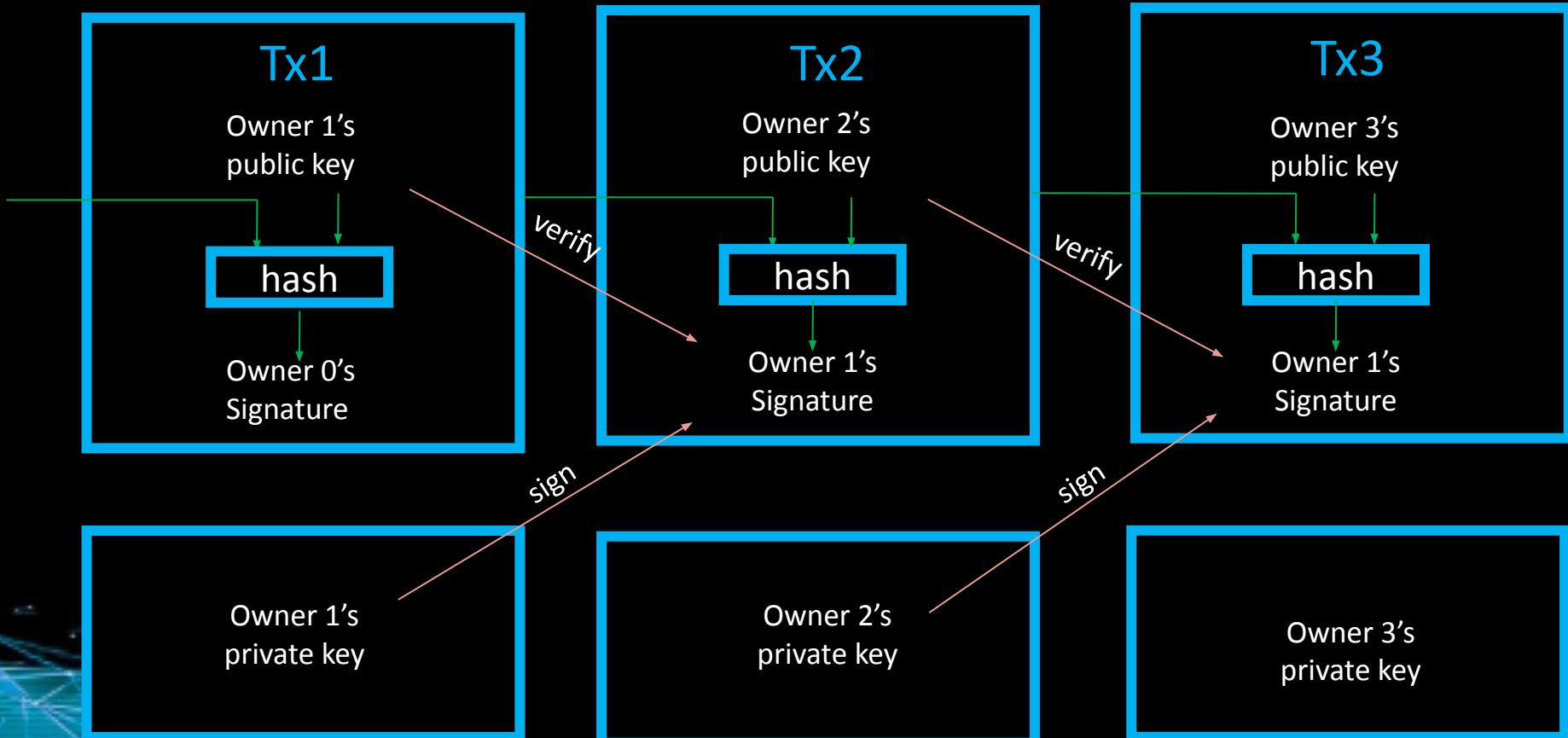
การสร้างblock : block ถูกสร้างมาเพื่อเก็บ transaction หรือธุรกรรมที่เกิดขึ้น (Tx) โดยในแต่ละบล็อกจะประกอบไปด้วยธุรกรรมจำนวนมาก โดยธุรกรรมที่เกิดขึ้นจะเกิดขึ้นได้ จะต้องประกอบด้วย input และ output (output ของคนที่ 1 ก็จะเป็น input ของคนที่ 2)

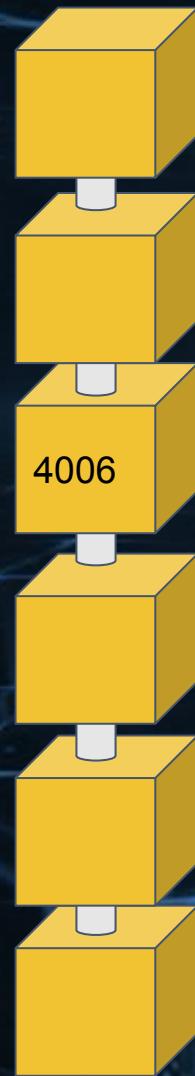
เมื่อผ่านการตรวจสอบความถูกต้องจาก tx เหล่านี้จะไปถูกจัดเก็บอยู่ใน block เมื่อ tx เต็มจะมีการ ปิดล็อก โดยในแต่ละบล็อกจะประกอบไปด้วย Block Header , Hash ของ block ก่อนหน้า และ ข้อมูล tx เป็นองค์ประกอบหลัก โดยค่า Hash ของ block ก่อนหน้าจะเป็นตัวเชื่อมบล็อกเข้าด้วยกันเป็นโซนขึ้นมา





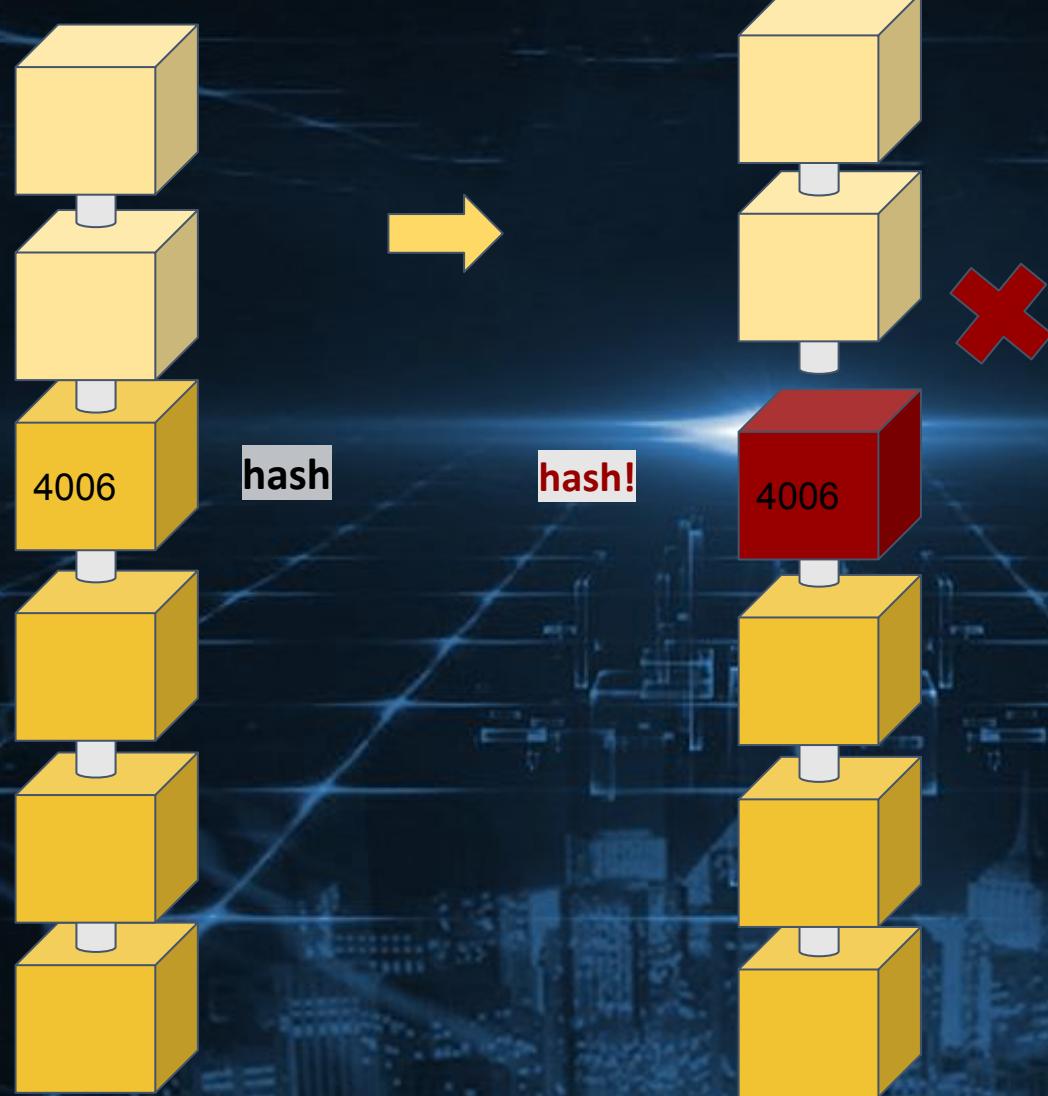
Transactions

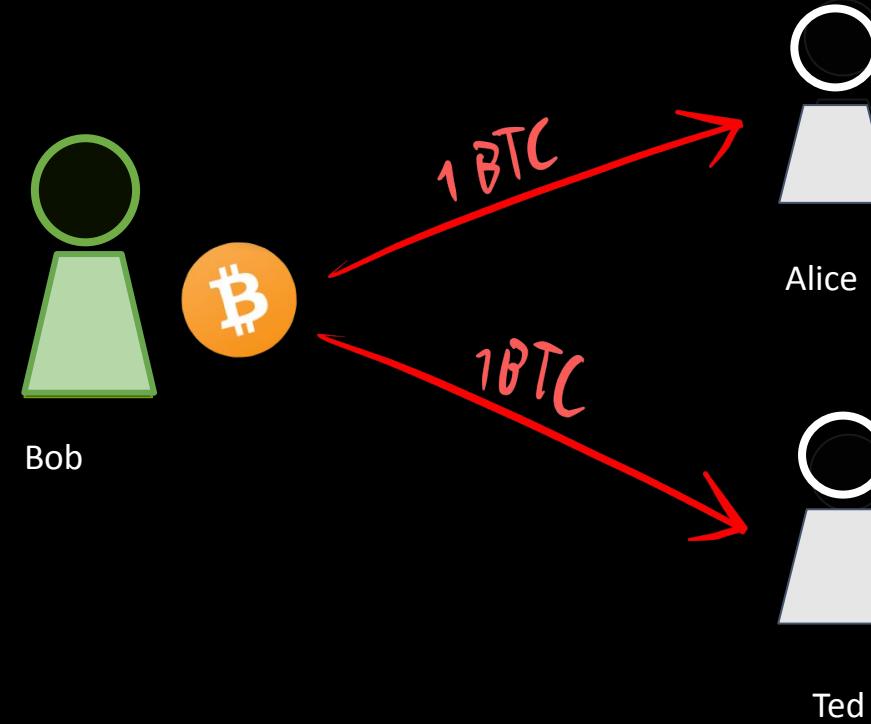


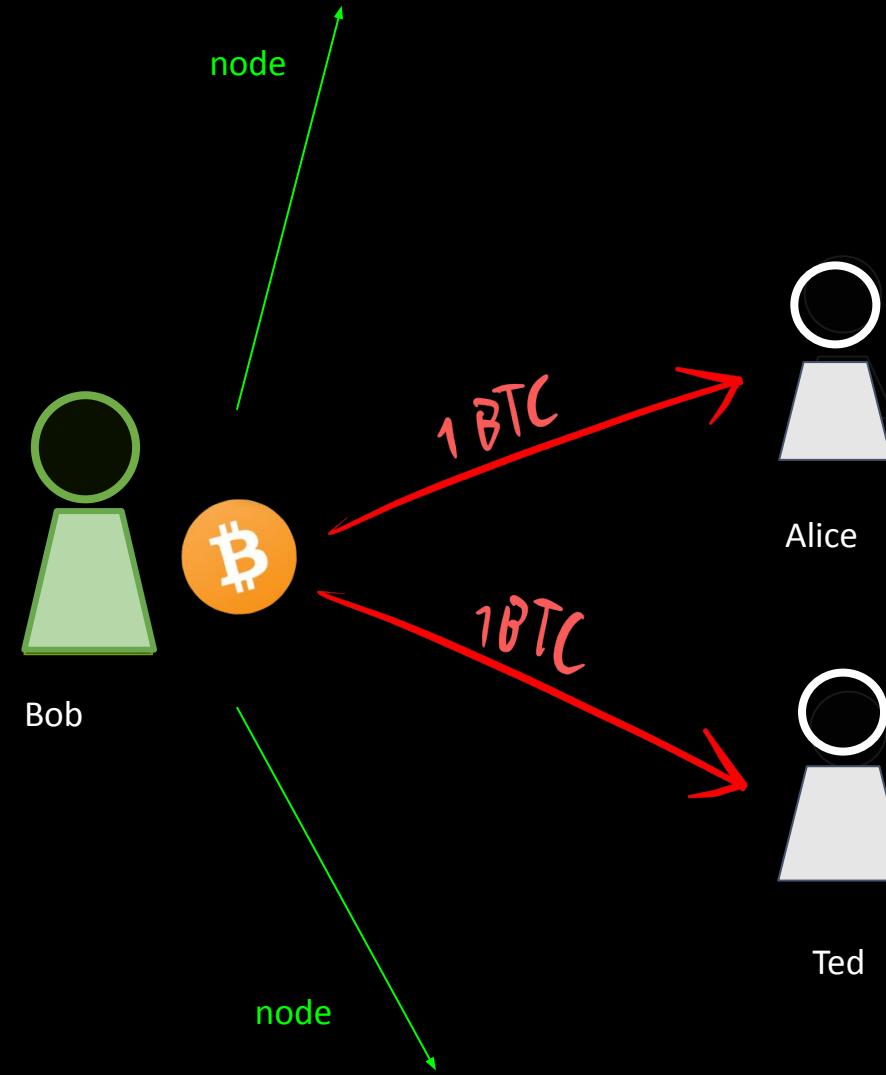


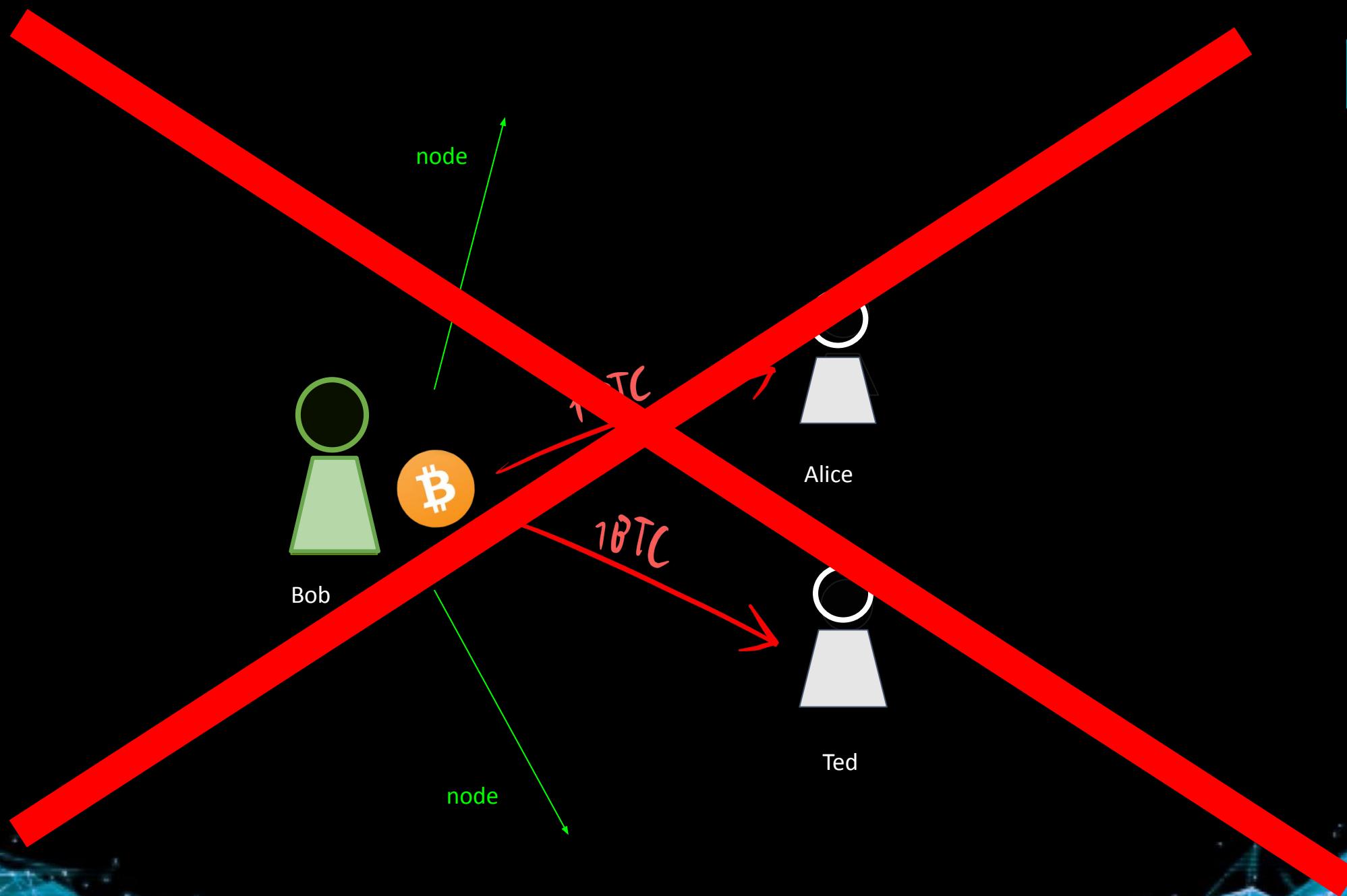
hash













Throughput คืออะไร (Tx/S)

- เป็นจำนวน transaction/request ที่ถูกสร้างขึ้นหรือทำงานได้ในช่วงเวลาการทดสอบหนึ่งๆ ค่าใช้สำหรับบอกว่า ระบบงานมีความสามารถในการจัดการงานจำนวนเท่าไรในแต่ละหนึ่งหน่วยเวลา นั่นเอง

สูตรการคำนวณ

(จำนวน request หรือ transaction)

$$\text{Throughput} = \frac{\text{จำนวน request หรือ transaction}}{\text{จำนวนเวลาการทำงานรวม}}$$



$$\text{Throughput} = \frac{5 \text{ gear}}{1 \text{ sec}}$$

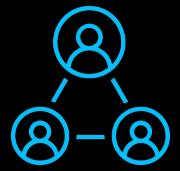
$$10 \text{ gear} \rightarrow 5 \text{ gear} \text{ waiting} \quad \frac{5 \text{ gear}}{1 \text{ sec}}$$

หน่วยที่นิยมใช้สำหรับวัดค่า Throughput นั่นก็คือ
Transaction Per Second (TPS)

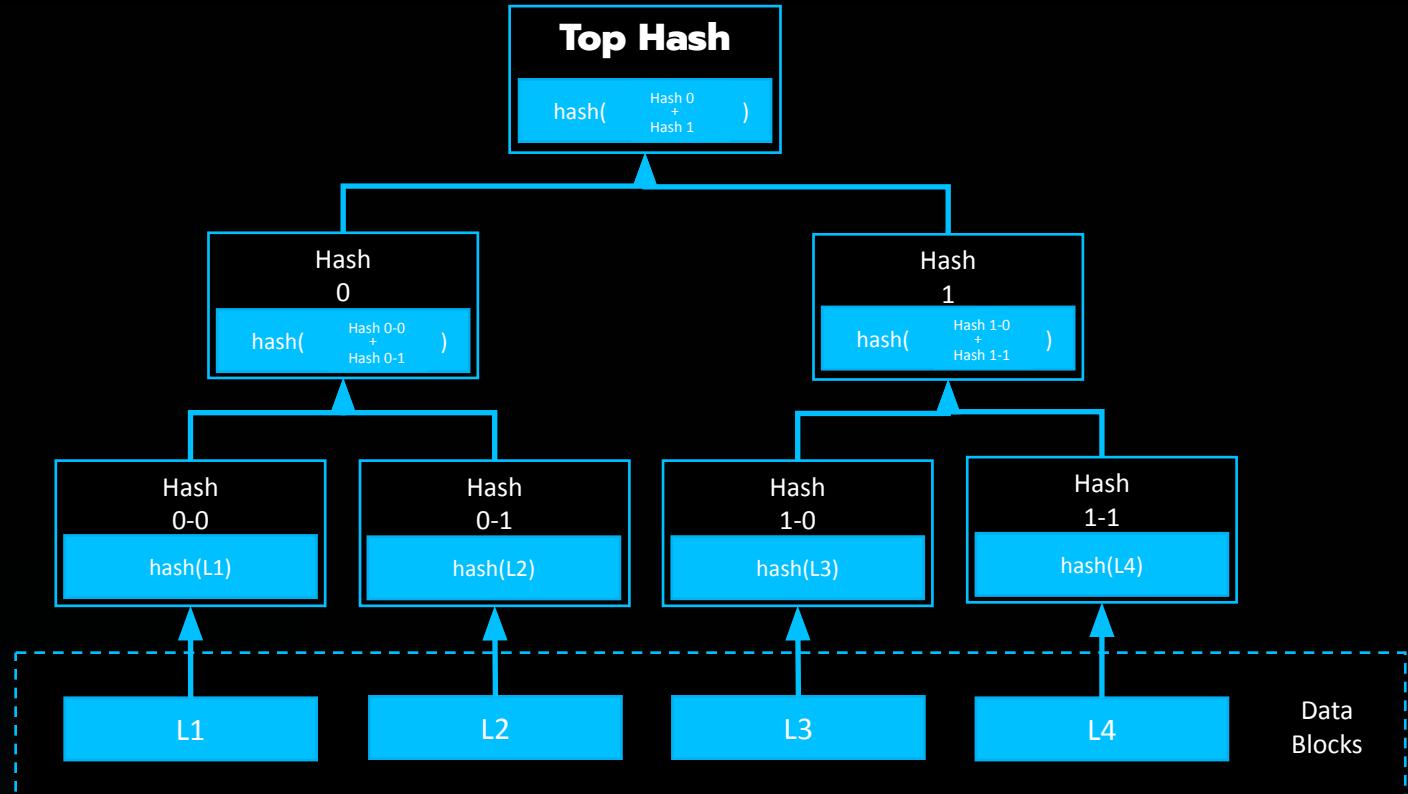
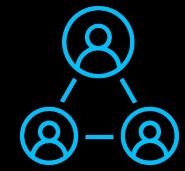


$$\frac{100 \text{ } \text{gear}}{10 \text{ sec}} = \frac{10 \text{ } \text{gear}}{1 \text{ sec}}$$

- เมื่อจำนวน request สูงขึ้นมาเรื่อยๆ ค่าของ Throughput ก็เพิ่มมากขึ้นเช่นกัน เมื่อไรก็ตามที่ จำนวน request และ จำนวนการประมวลผลของระบบการทดสอบเริ่มนั่นแสดงว่า ค่าของ Throughput ของระบบนั้นนีงหรือเสถียรแล้วเช่นกัน
- ซึ่งถ้าการเพิ่มจำนวน request มันทำให้ค่า Throughput ลดลงมา แสดงว่ามีส่วนใดส่วนหนึ่งในระบบงานเกิดปัญหาคอขวดมาแล้ว หรือนั้นคือ เกินขีดความสามารถของระบบในตอนนั้นครับ เช่น เข้าคิวเพื่อรอทำงานนานเกินไป เช่น CPU, database และ network เป็นต้น ส่งผลให้ response time สูงขึ้นมาก จนเกิด timeout

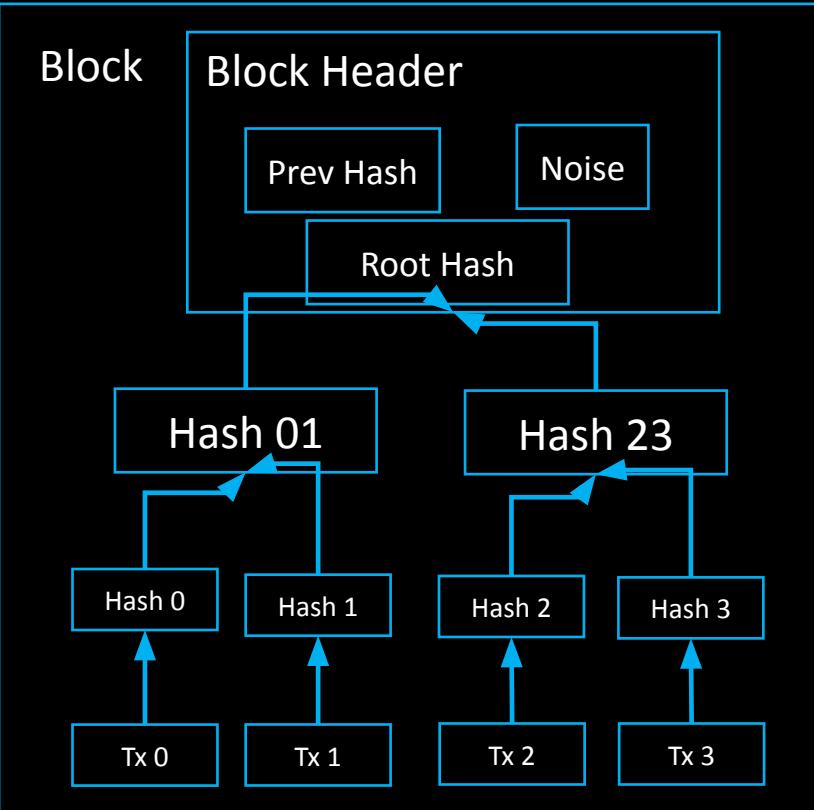


การทำงานของ Merkle tree

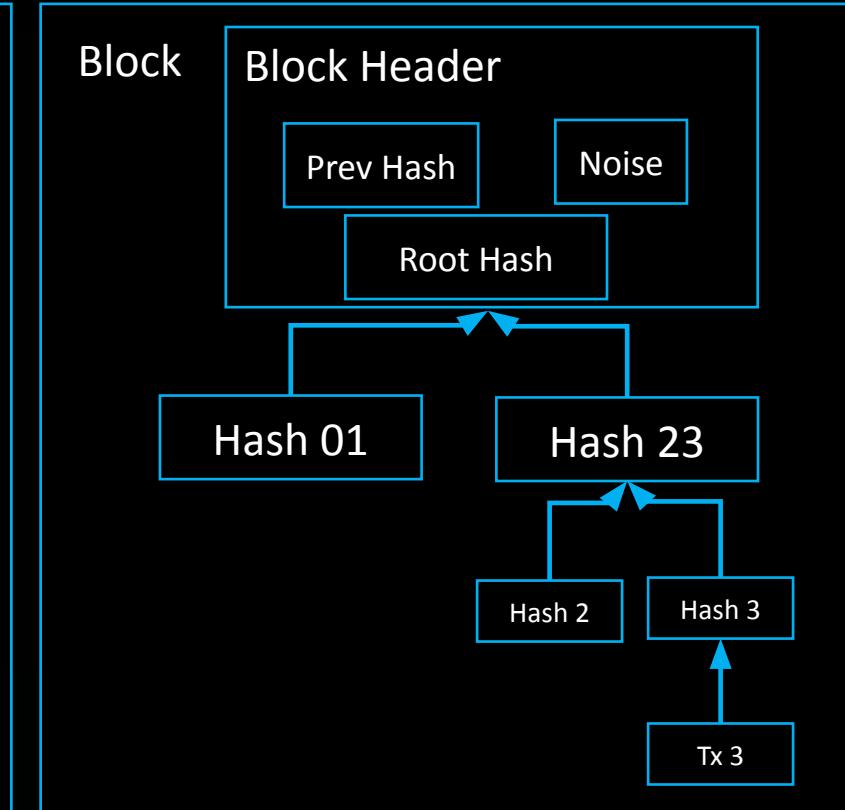




หลักการเก็บข้อมูล



Transactions Hashed in a Merkle tree



After Pruning Tx0-2 from the Block



<https://andersbrownworth.com/blockchain/blockchain>

ลิงค์สำหรับลองเล่น Blockchain

<://andersbrownworth.com/blockchain/blockchain>





Cryptography





INPUT → DIGISET

Turtle

Cryptographic Hash function

DFCD 5895 5465 BAFF 4584
748D HJYU 854H IOKG 458Y

Turtle like
toeatcarrot

Cryptographic Hash function

DFCD 5895 5465 BAFF 4584
OPLI IOKO 748H IOKG 458Y

Turtle like
toeatcarrot

Cryptographic Hash function

DFCD 5895 5465 BAFF 4584
748D POLI POKL IOKG 458Y

Turtle like
toeatcarrot

Cryptographic Hash function

DFCD 5895 5465 BAFF 4584
748D HJYU 854H IOKG IOPK

Turtle like
toeatcarrot

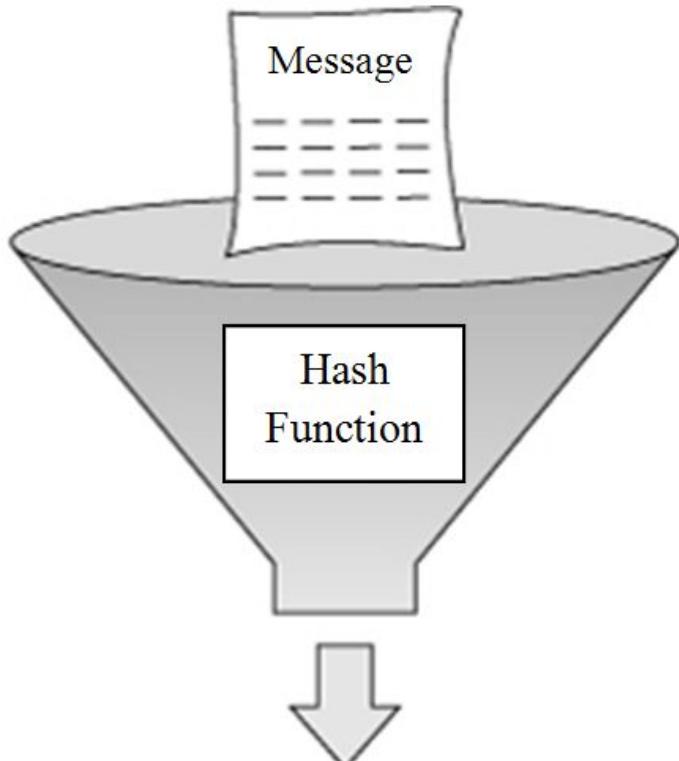
Cryptographic Hash function

IOPL 5895 5465 BAFF 4584
748D IOPK 854H IOKG 7844

พังชั่นการแฮชเข้ารหัส เป็นการเข้ารหัสข้อมูล จาก input ให้มีขนาดเล็กลง เพราะเมื่อเราต้องเก็บข้อมูลชุดเดียวกันในคอมพิวเตอร์ทุกเครื่องการแฮชให้ขนาดของข้อมูลเล็กลงจึงเป็นประโยชน์อย่างมาก



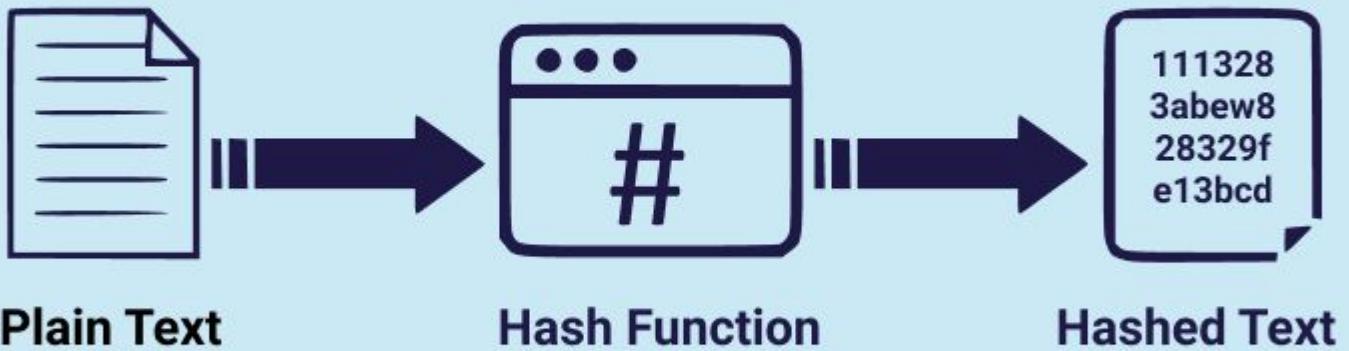
Data of Arbitrary Length

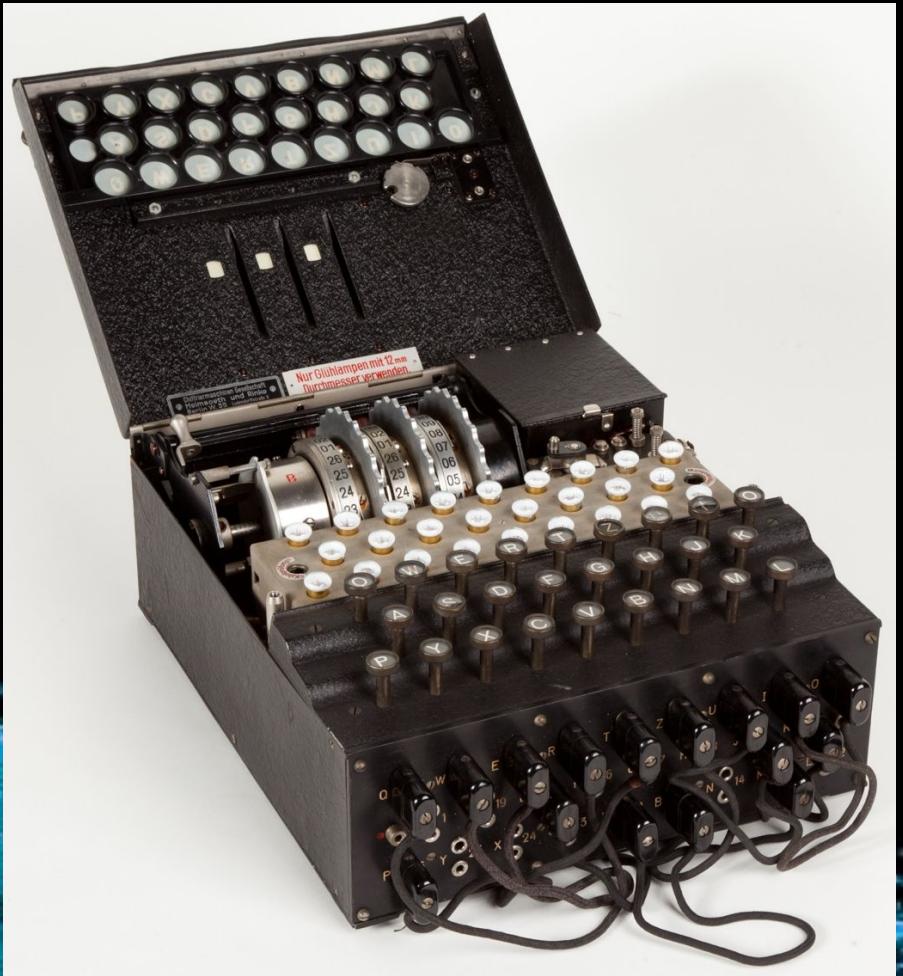


Fixed Length Hash (Digest)



Hashing Algorithm

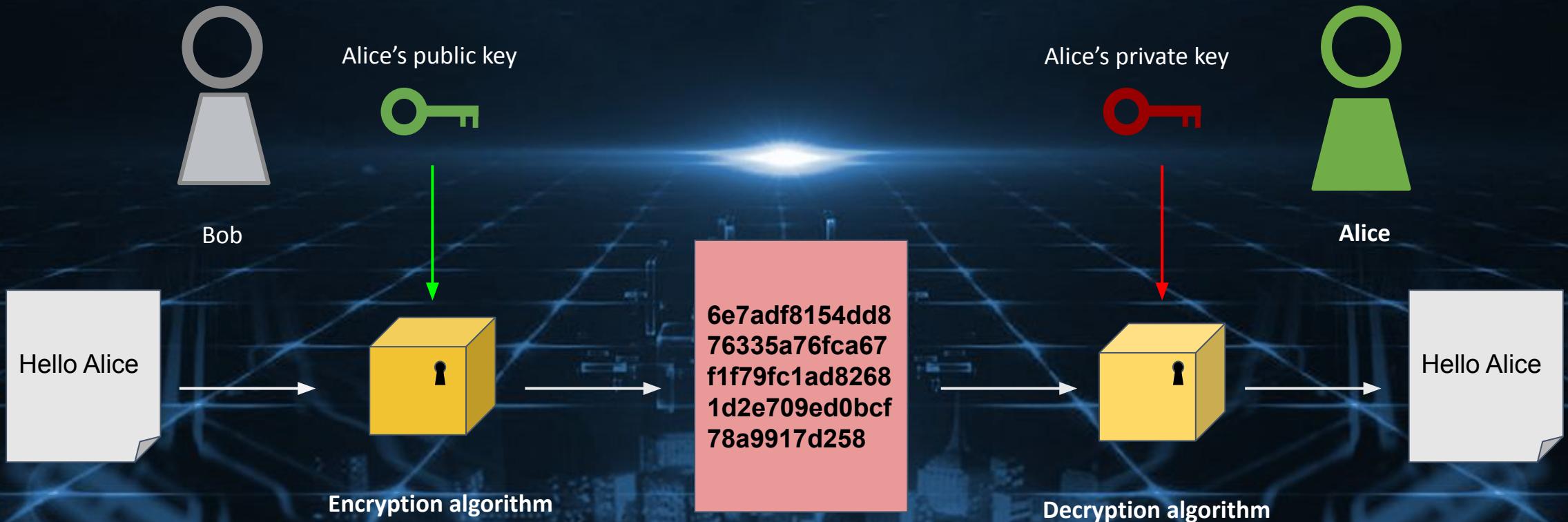




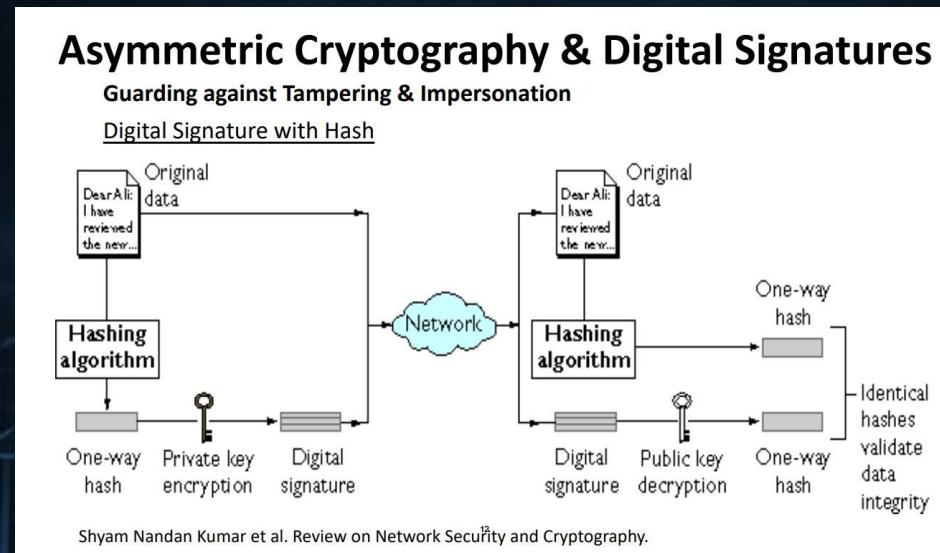
[Enigma machine - Wikipedia](#)



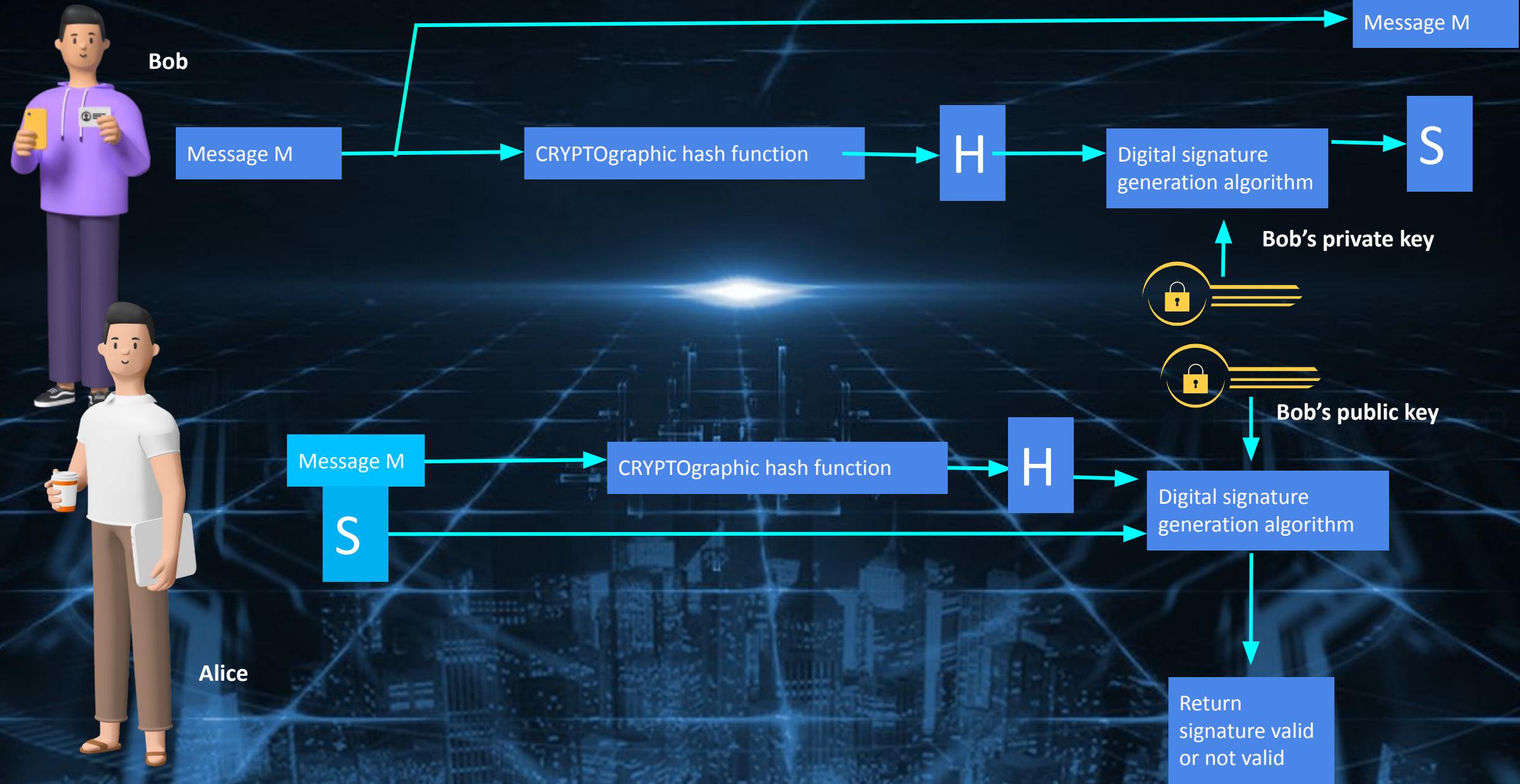
Asymmetric



DIGITAL SIGNATURE WITH HASH



https://ocw.mit.edu/courses/15-s12-blockchain-and-money-fall-2018/3bcae7f65945633fc0ae6b955f36dfb4/MIT15_S12F18_ses4.pdf



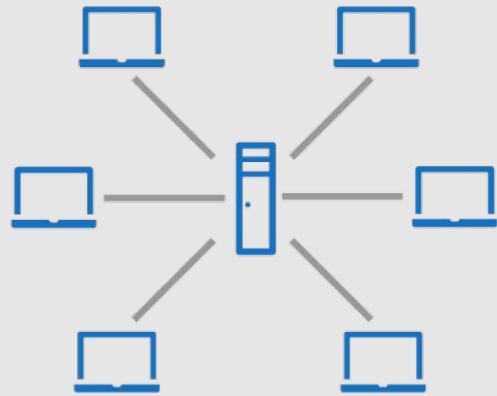


NETWORK

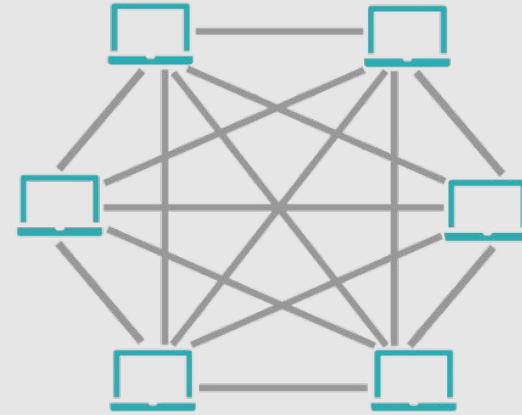




NETWORK ARCHITECTURES



SERVER-BASED

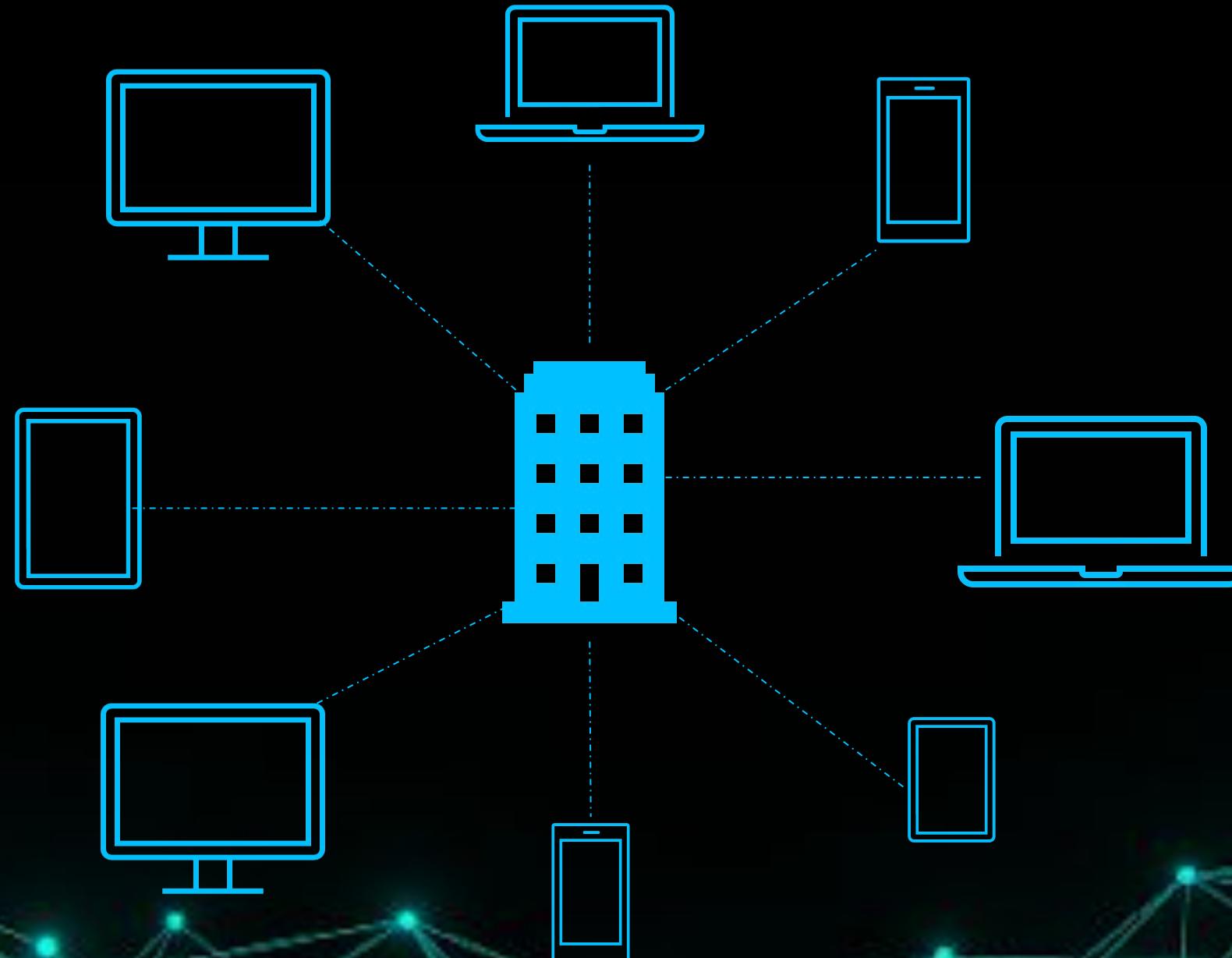


P2P-NETWORK

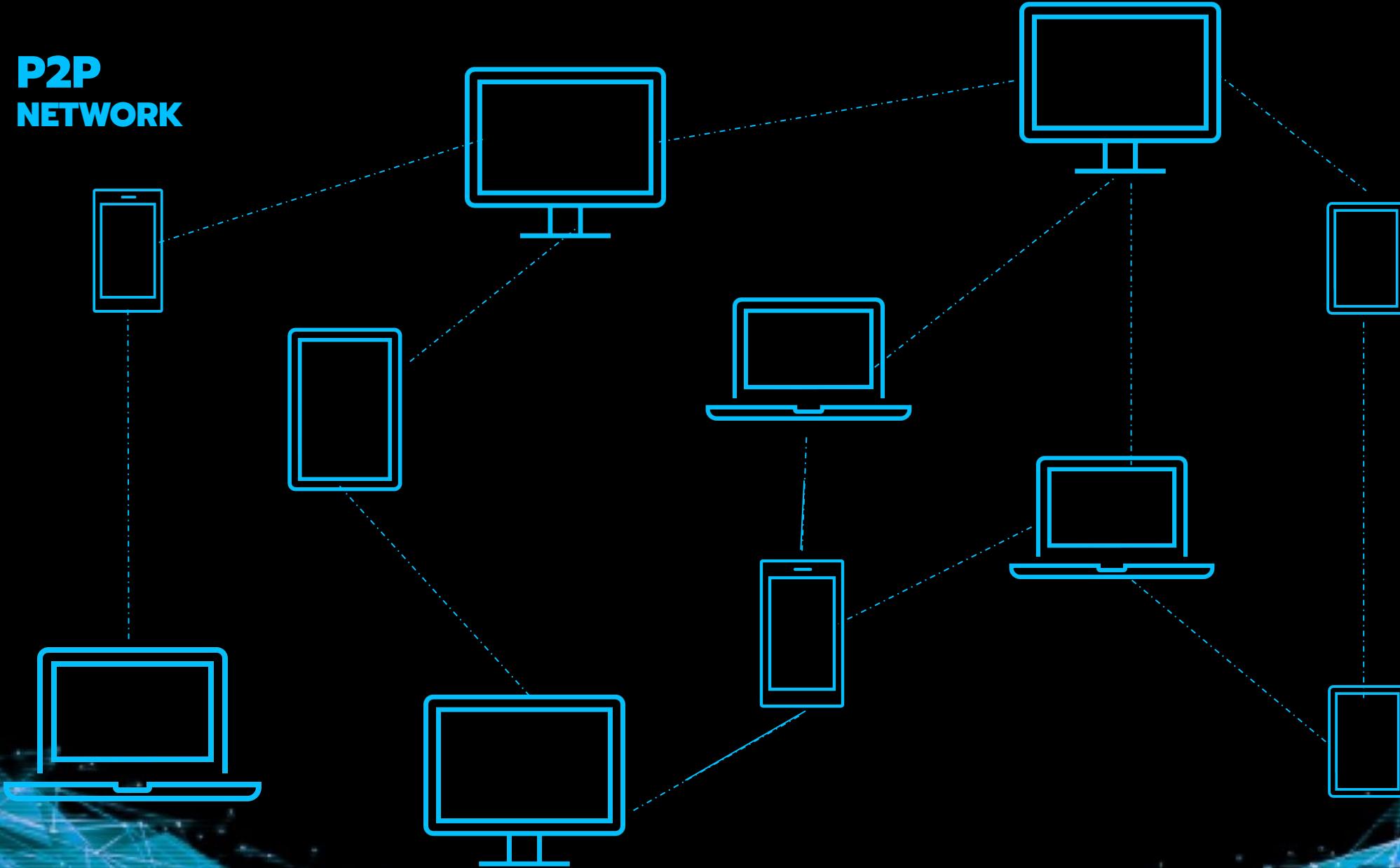
<https://www.linkedin.com/pulse/peer-to-peer-network-loizos-agapiou>

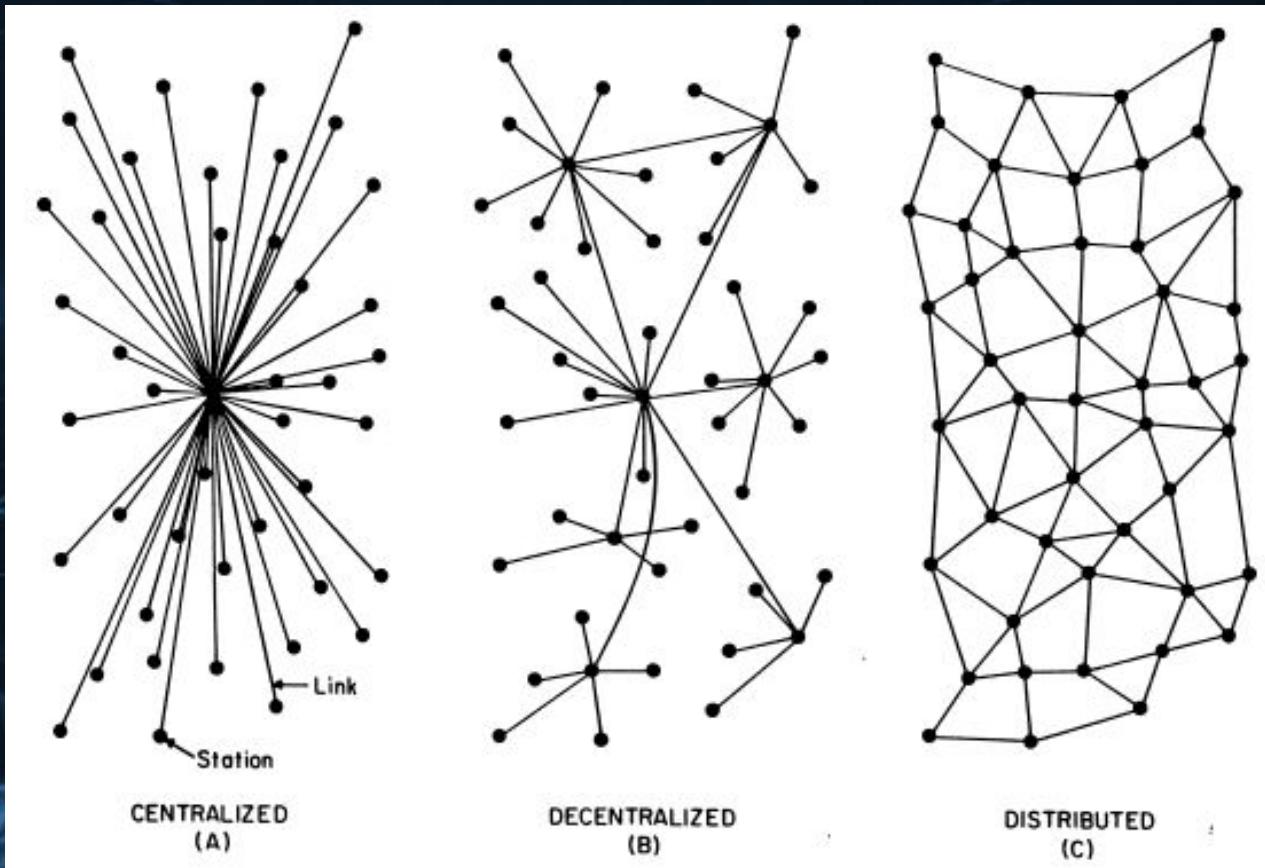


Centralized Network



P2P NETWORK





[On Distributed Communications: I. Introduction to Distributed Communications Networks | RAND](#)



Consensus

(POS, POA, POW)





POW คือเครือข่ายหรือโหนด (Node)

ต้องแข่งกันแก้ไขสมการทางคณิตศาสตร์ เพื่อยืนยันความถูกต้องของธุรกรรม และสร้างบล็อกใหม่ขึ้นบนบล็อกเชน หากมีโหนดใดแก้ไขสมการได้ก่อนและสร้างบล็อกขึ้นมา

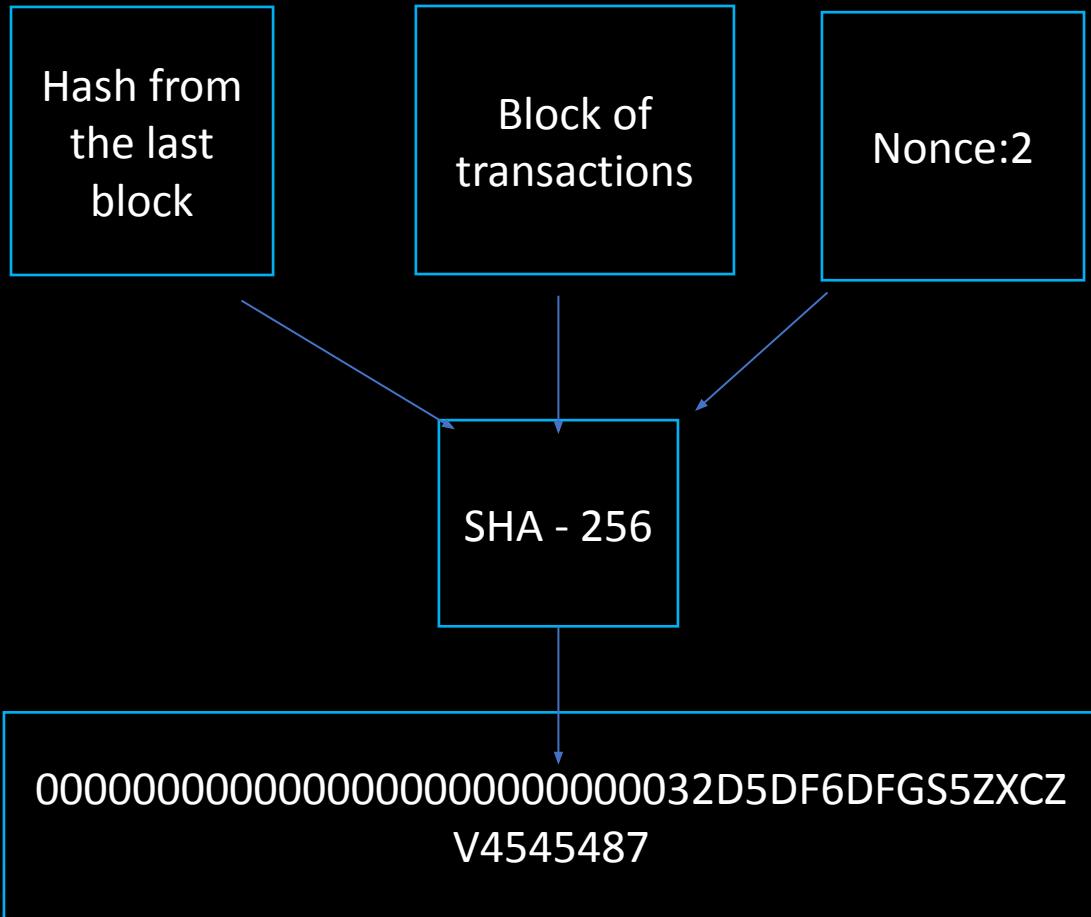
โหนดอื่นๆในเครือข่ายก็จะเข้ามาตรวจสอบความถูกต้องของบล็อกนั้นอีกที ก่อนที่จะส่งขึ้นไปอยู่บนบล็อกเชนแบบถาวร การแยกเครือข่ายสำเร็จจะต้องมีกำลังในการประมวลมากกว่า 51% ของทั้งเครือข่าย ยิ่งเครือข่ายบล็อกเชนใหญ่แค่ไหน โอกาสที่จะถูกโจมตีสำเร็จก็เป็นได้ไปยกขั้นเท่านั้น



PROOF OF WORK



หลักการทำงาน



การจะปิดบล็อกได้จำเป็นจะต้อง แซงบล็อกโดยใช้ SHA 256 เป็นการสุ่มแซงซึ่งเป็นอะไรก็ได้ การแซงเป็นเรื่องที่ทำได้ง่าย และปิดบล็อกได้อย่างรวดเร็ว ทำให้บล็อกไม่มีนั้นเร็วตาม

การทำให้บล็อกไม่โดนปิดเร็วเกินไปโดยใช้ค่าความยากหรือdifficultyในการบอกว่าแซงไหนดีพอ เช่นการสุ่มเลขแล้วทำการแซงบล็อกหากค่าที่ได้มี 0 7ตัวอยู่หน้าสุดถือว่าเลขที่สุ่มนั้นทำให้เกิดแซงที่ดีพอ และค่าความยากยังสามารถใช้ในการพิสูจน์ว่าเราได้ใช้กำลังไฟฟ้าในการประมวลผลหรือสุ่มเลขเพื่อ hashออกมาได้ค่าที่ดีพอ

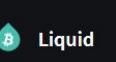
เพื่อเพิ่มความยากในการสุ่มเพื่อให้แต่ละบล็อกจบโดยประมาณ 10 นาที ซึ่งผู้ที่สุ่มเจองจะได้รางวัลเป็นเหรียญ ซึ่งหากบล็อกปิดเร็วเกินไปจำนวนเหรียญที่ถูกผลิตออกมาก็จะมากนั้นเอง





Blockstream Explorer

 Bitcoin

 Liquid



[Dashboard](#) [Blocks](#) [Transactions](#)

Search for block height, hash, transaction, or address





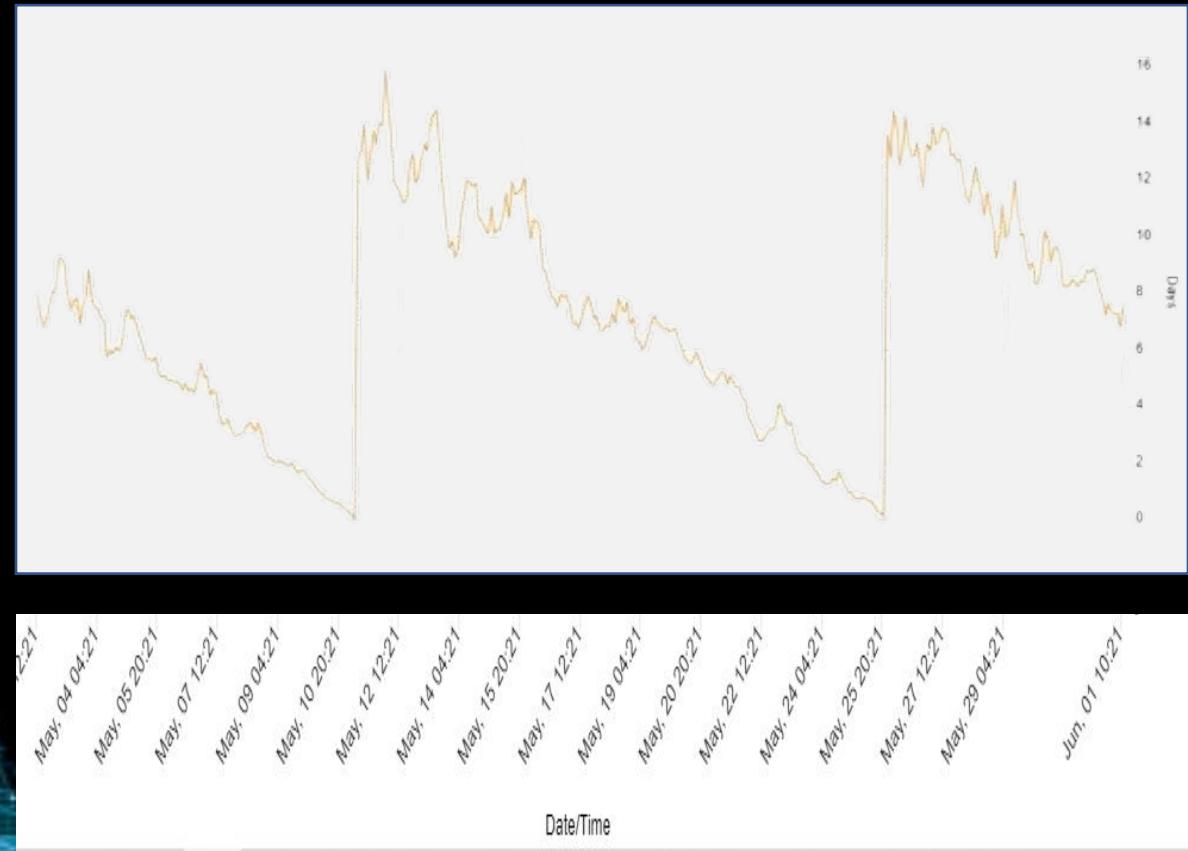
Block 746176

0000000000000000000000000061c7ab749fe77797d45edf8af193efef40ac2e2bd3200 

 PREVIOUS

 DETAILS 

HEIGHT	746176
STATUS	In best chain (1 confirmation)



ค่าความยาก จะมีการปรับค่าความยากอัตโนมัติ จะปรับค่าความยากทุกประมาณ 2 อาทิตย์ หรือประมาณ 2016 บล็อก

โดยจะใช้การดูเมอนิเตอร์ค่าเฉลี่ยของ block time โดยเฉลี่ย 10 นาที หากกำลังบุดเยอะ การสุ่มเจอเลขเร็วหรือการสุ่มใช้น้อยกว่า 10 นาที จะบวกว่าบล็อกนั้นเร็วไป หรือถ้ามากกว่า 10 นาทีบล็อกนั้นก็จะช้าเกินไป

หากมีกำลังบุดเยอะค่าความยากในการกำหนดว่าแข็งให้ดีพอก็จะอยู่ในรูปแบบที่แคบลงเพื่อให้สุ่มหายากขึ้น



51% Attack

Crypto51

About

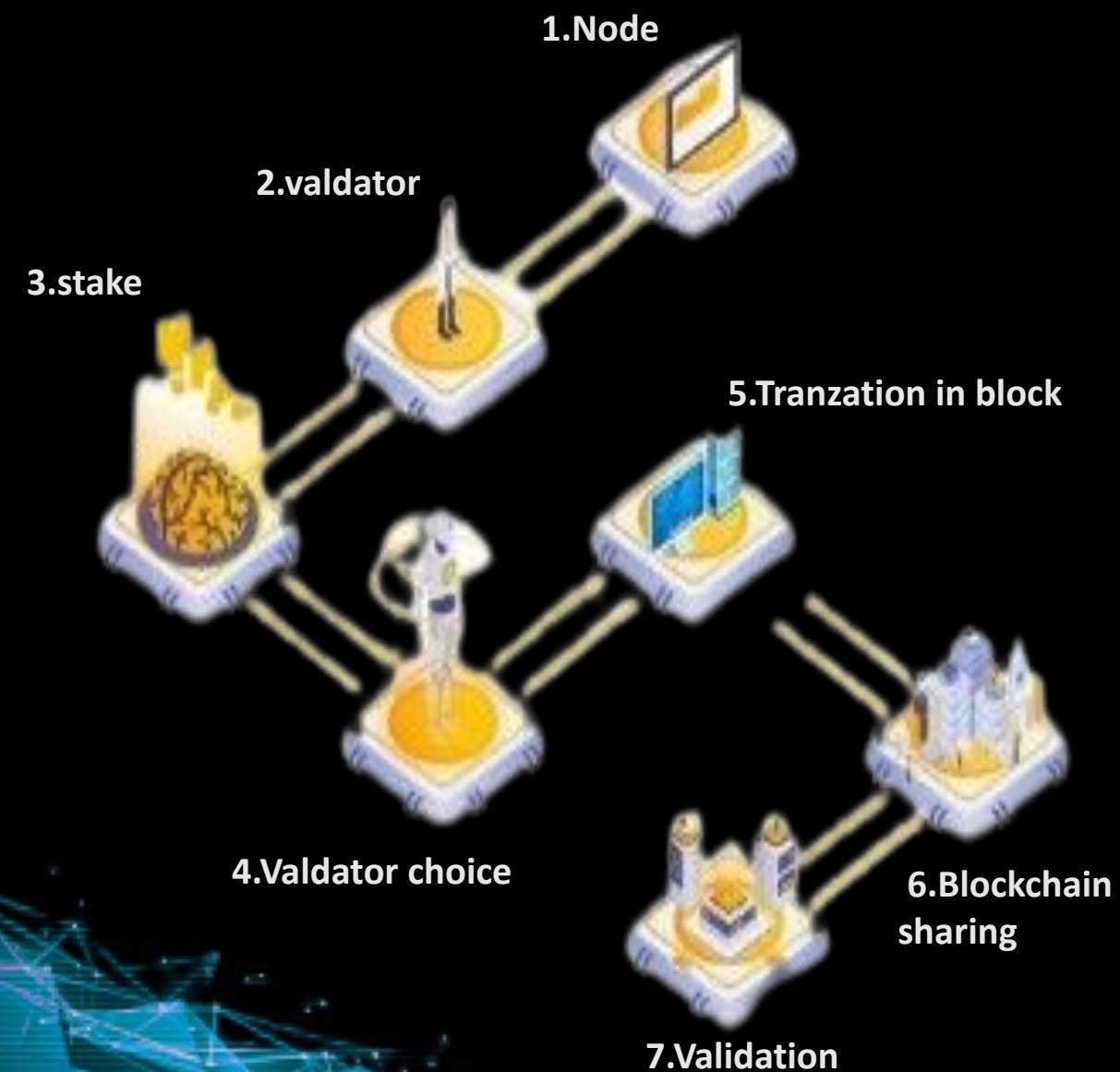
PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

[Learn More](#) [⚡ Tip](#)

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	\$439.07 B	SHA-256	188,792 PH/s	\$854,032	0%
Ethereum	ETH	\$191.22 B	Ethash	903 TH/s	\$901,047	5%
Litecoin	LTC	\$4.04 B	Scrypt	410 TH/s	\$59,825	10%

<https://www.crypto51.app/>



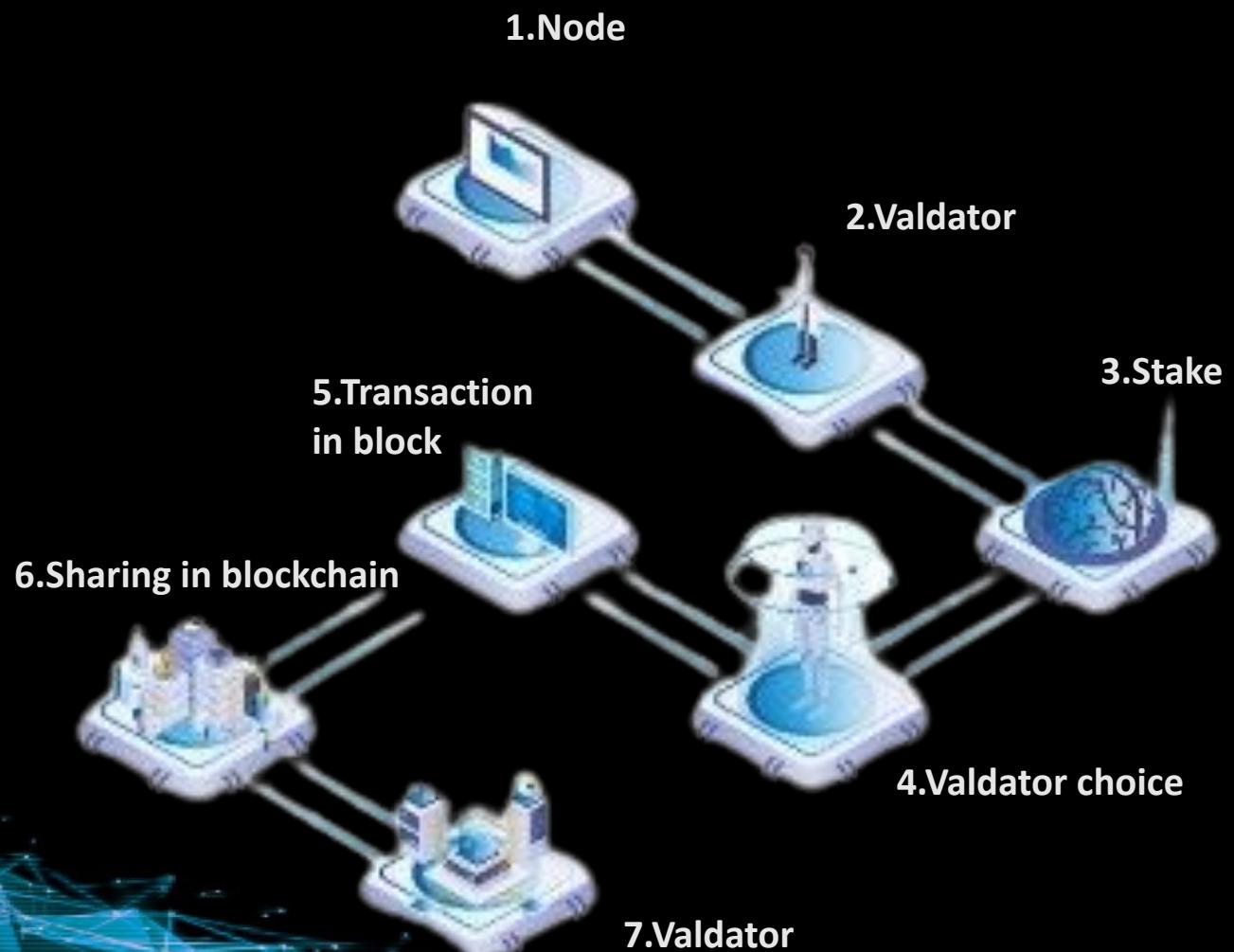
PoS Proof of Stake

PoS แตกต่างจาก PoW เนื่องใน การรับสิทธิ์รับรองธุรกรรม โดยที่สามารถตรวจสอบและยืนยันธุรกรรมได้จะต้องมีการฝากทรัพย์สินขึ้นต่ำไว้กับเครือข่าย

เมื่อฝากทรัพย์สินถึงเกณฑ์ที่แต่ละบล็อกเชนกำหนดและได้รับสิทธิ์ในการยืนยันธุรกรรมแล้ว เมื่อมีธุรกรรมเกิดขึ้น บล็อกเชนจะเลือกโหนดขึ้น

มาให้ทำการยืนยันธุรกรรม โดยเกณฑ์ในการเลือก ก็คือ ต้องเป็นโหนดที่เคยได้รับสิทธิ์มาก่อน หรือเป็นโหนดที่มีจำนวน transaction มากที่สุด แล้วก็จะมีการเลือกโหนดที่มีจำนวน transaction มากที่สุด

หรือบังก์ที่เลือกโหนดที่มีการฝากเหรียญสูง ๆ ก่อน หากโหนดนั้นทำหน้าที่ได้ถูกต้อง ก็จะได้รับรางวัลเป็นเหรียญ



PoA Proof of Authority

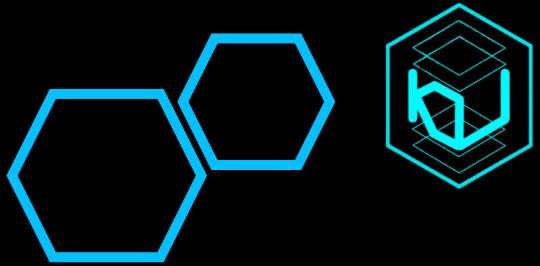
PoA เป็นอันดับต้นแบบอ้างอิงเชื่อเสียง
เป็นการสุ่มโอนด้วยในเครือข่าย โดยโอนด้วยเป็นต้องเปิดเผยตัว
ตนว่าเป็นองค์กรใด เพื่อความสุจริตโปร่งใส
ในการยันธุรกรรมต่างๆเพื่อง่ายต่อการตรวจสอบได้ว่าใครเป็นผู้
ยืนยันธุรกรรม หากมีการธุจริตผู้ที่ยืนยันธุรกรรมก่อธุจริต ก็อาจ
เสียเชื่อเสียงได้ ผู้ที่จะเป็นโหนดให้กับการตรวจสอบแบบ PoA ได้
จำเป็นจะต้องได้การยอมรับจากผู้ที่เป็นโหนดคนอื่นๆ
หรือการปลดกํต้องได้รับความเห็นชอบจากโหนดอื่นๆ เช่นกัน



Impossible Trinity

DECENTRALIZATION





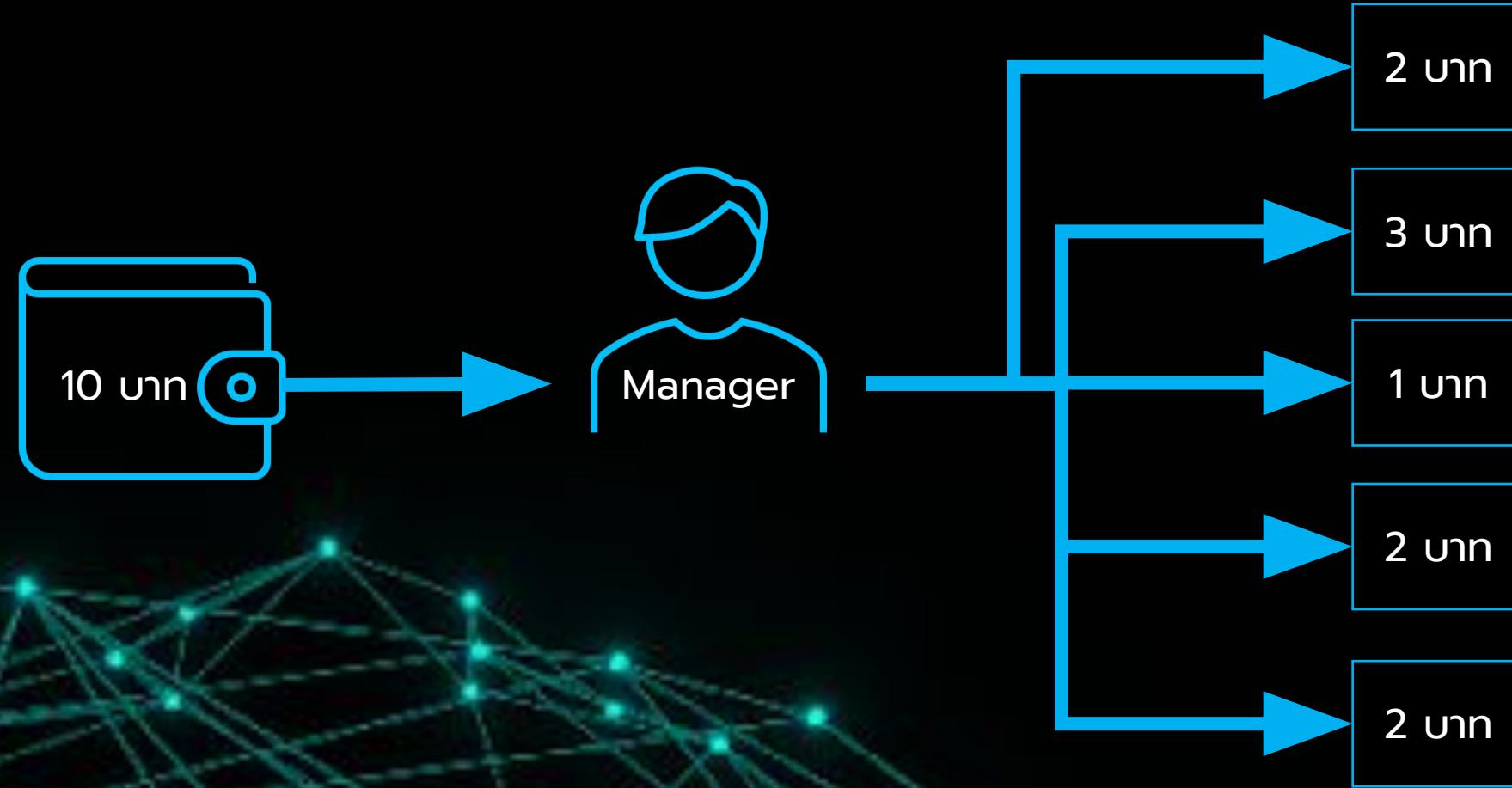
Bank vs Smart contract

- Smart contract คือ คือสัญญาที่ตกลงกันโดยไม่ต้องมีตัวกลางในการดำเนินการ ไม่ต้องเชื่อใจใคร เชื่อใจในระบบ มีความโปร่งใสเราสามารถเห็นได้ตลอดว่าโค้ดจะดำเนินการอย่างไร ตั้งแต่ตอนจบทำให้การโกรังมันเกิดขึ้นได้ยาก



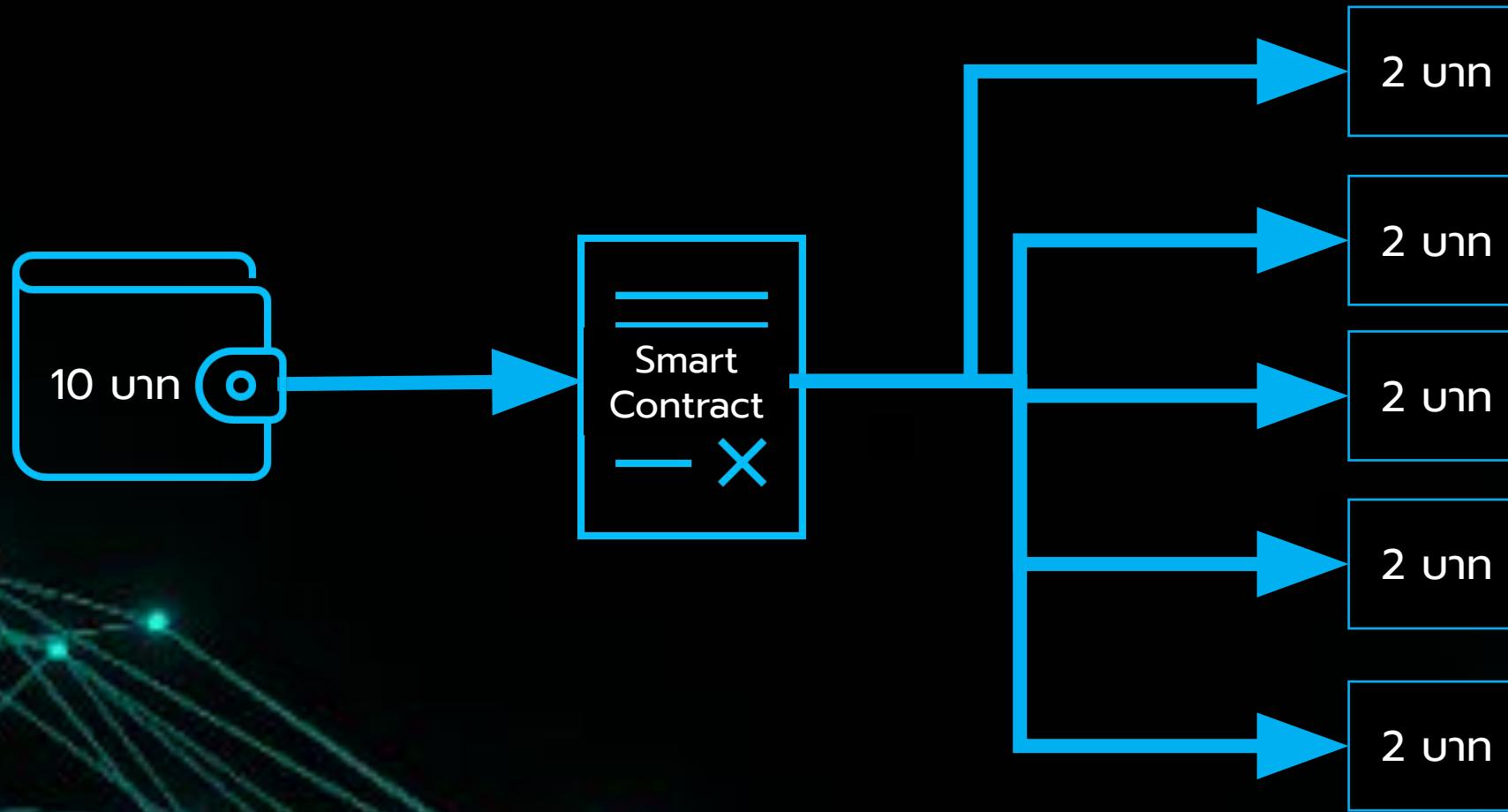


- Smart contract จัดการความผิดพลาดของมุบงย์เนื่องจากถูกดำเนินการโดยเครื่องจักร ตัดเรื่องความรู้สึกของมนุษย์ออกไป เช่น หากร้านค้าร้านหนึ่งได้ tip 10 บาทและมีพนักงาน 5 คนปกติเราจะใช้ ผู้จัดการในการแจกจ่าย tip ให้กับพนักงาน โดยปกติพนักงานทุกคนจะได้คันละ 2 บาท แต่หากผู้จัดการชอบพนักงานคนใดเป็นพิเศษอาจให้คนหนึ่ง 3 บาท อีกคน 1 บาทก็ได้



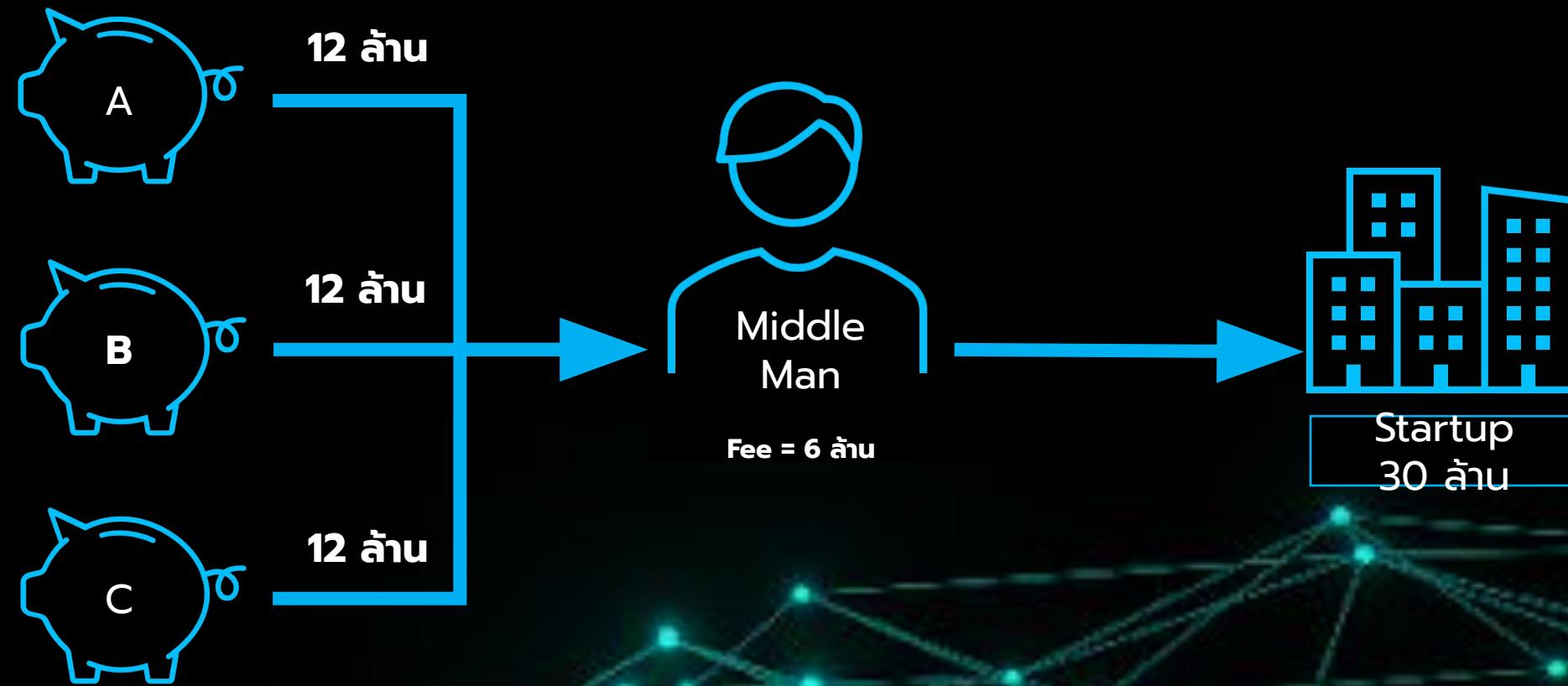


- แต่ถ้าเป็น smart contract ทุกงานทุกคนจะได้เงินเท่ากันตามเงื่อนไขที่เขียนในสัญญา



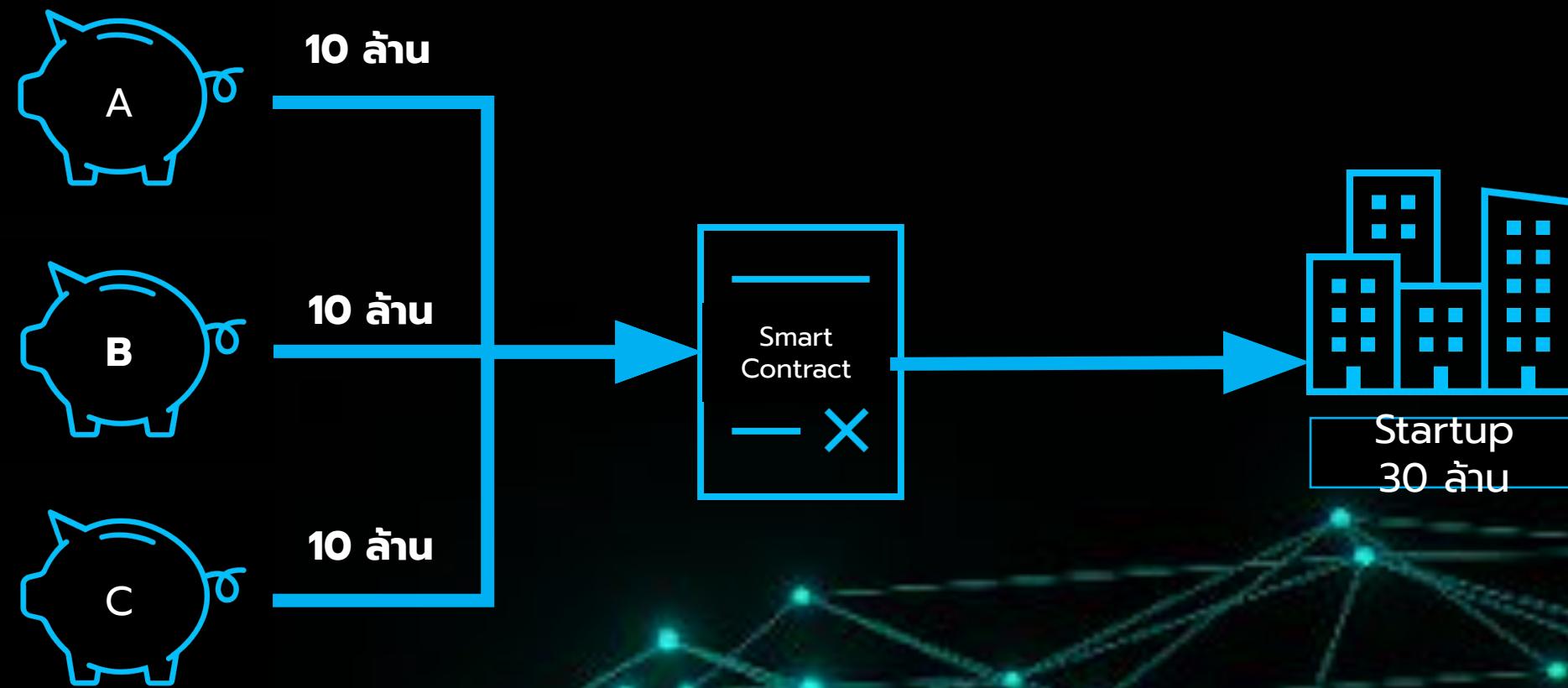


- การมาของ Smart contract ทำให้บทบาทของตัวกลางลดลง โดยการตัดตัวกลางของ Smart contract แต่ยังสามารถยังคงความหน้าเชื้อต่อไว้ได้ ช่วยเพิ่มความสะดวกและความถูกต้องรวดเร็ว ยกตัวอย่างเช่น หาก start up ต้องการระดมทุน 30 ล้านบาทโดยการระดมทุนปกติจำเป็นจะต้องมีตัวกลางในการช่วยดำเนินงาน โดยตัวกลางจะมีการเก็บค่าบริการในการดำเนินการ



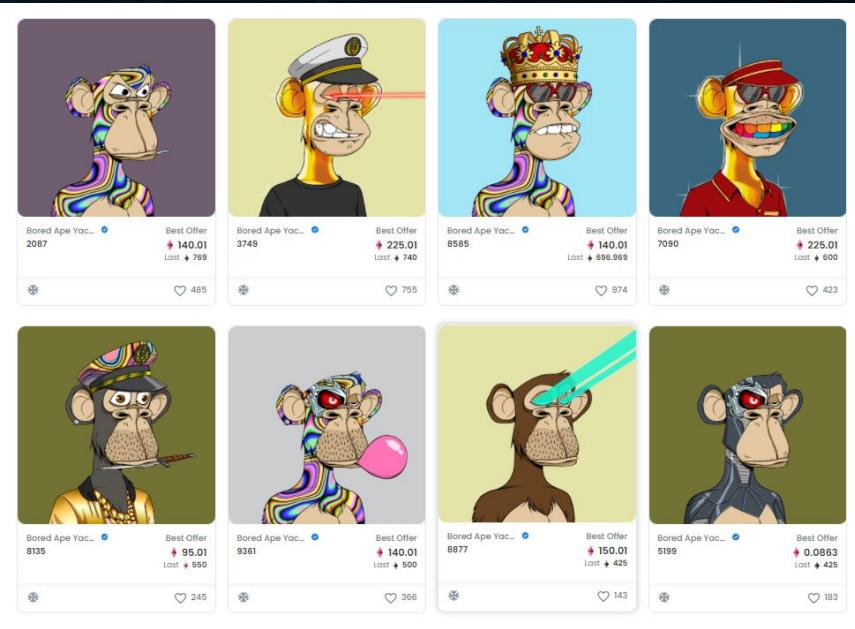


- แต่หากใช้ Smart contract ค่าใช้จ่ายในการดำเนินการจะลดลง โดยมีความเร็วและความถูกต้องเพิ่มขึ้น และถึงแม้สัญญาไม่ถูกต้องหรือระดมทุนได้ไม่ถึงเป้าเงินก็จะถูกส่งคืนบัญชีทันทีและไม่เสียค่าใช้จ่าย



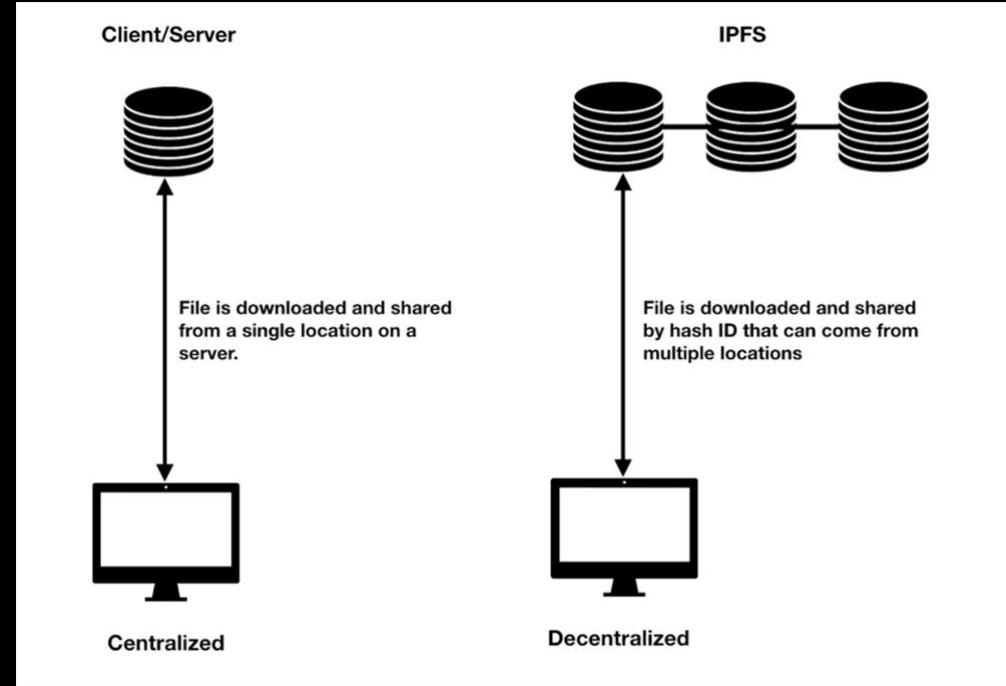


[https://nikopartners.com/blockchain-gaming-and-the-rise-of-axie-infinity/?lang=en#iLightbox\[gallery7770\]/0](https://nikopartners.com/blockchain-gaming-and-the-rise-of-axie-infinity/?lang=en#iLightbox[gallery7770]/0)



<https://forkast.news/headlines/opensea-nft-marketplace-hacked-332-eth/>

<https://otherside.xyz/litepaper?fbclid=IwAR3dp2LNp0i4qCJ7w09S37yLq30x1Z1NGd8LXMSXKfZBMqwJU-RBMcH73hi>



<https://medium.com/0xcode/using-ipfs-for-distributed-file-storage-systems-61226e07a6f>



Bitcoin launched in 2009

- Bitcoin script(no loop)
- UTXO base

Ethereum launched in 2015

- Smart contracts
- Account / Balance mode

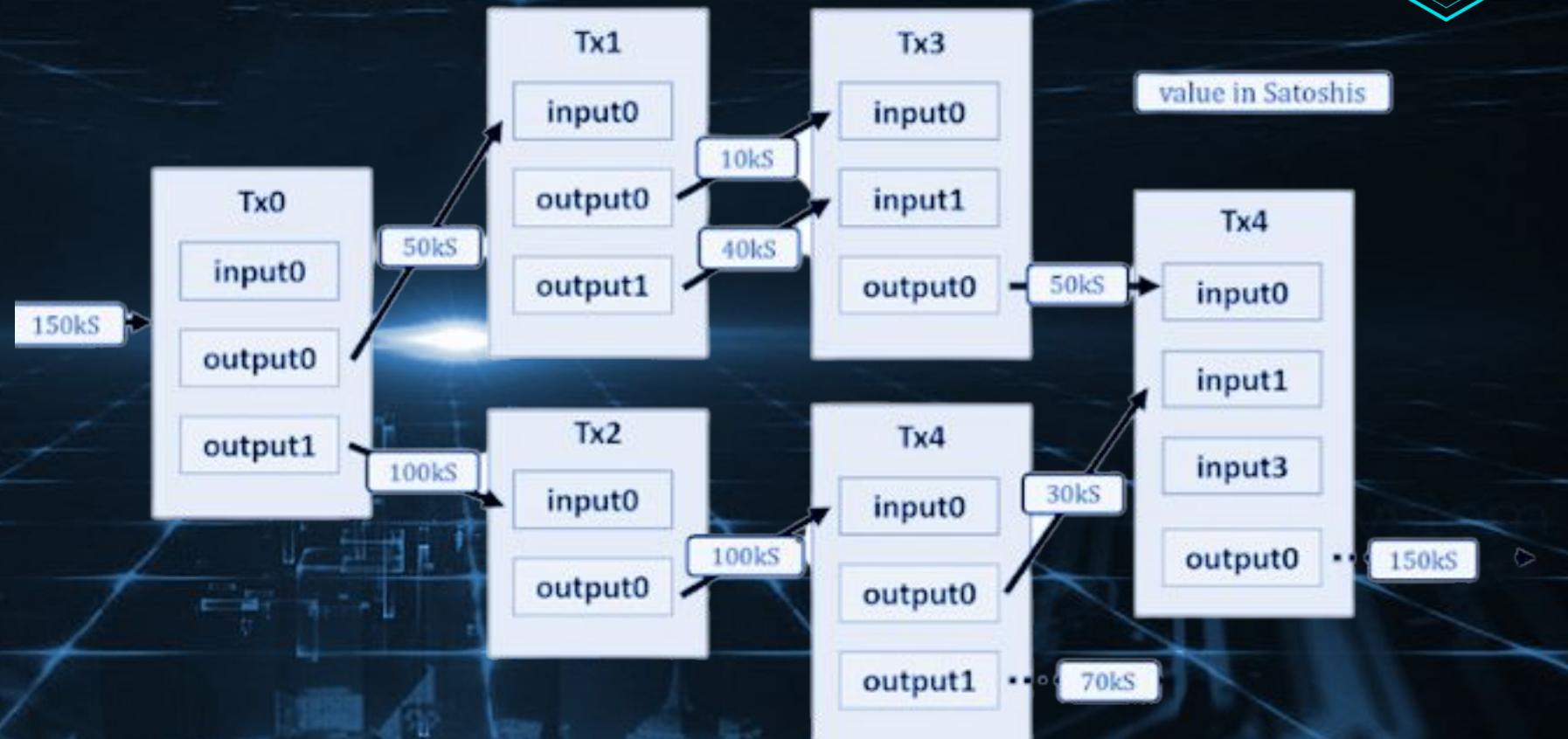






Bitcoin

Bitcoin : UTXO base
Stack-based



https://www.researchgate.net/figure/An-example-of-UTXO-based-transfers-in-Bitcoin_fig6_334434726

<https://bitcoin.org/bitcoin.pdf>



Ethereum

Account base

Smart contracts

Defi, Dao, Gamefi



Account Model Example from Ethereum

Previous State

0x4fabb145d:
30 ETH

0x6grw2356f:
5 ETH

→

Transaction

to:
0x4fabb145d
from:
0x6grw2356f

Value:
3 ETH

Next State

0x4fabb145d:
27 ETH

0x6grw2356f:
8 ETH

BINANCE RESEARCH

<https://research.binance.com/en/projects/ethereum>



ERC20



From [EIP-20 ↗](#):

Methods

```
1 function name() public view returns (string)
2 function symbol() public view returns (string)
3 function decimals() public view returns (uint8)
4 function totalSupply() public view returns (uint256)
5 function balanceOf(address _owner) public view returns (uint256
balance)
6 function transfer(address _to, uint256 _value) public returns (bool
success)
7 function transferFrom(address _from, address _to, uint256 _value)
public returns (bool success)
8 function approve(address _spender, uint256 _value) public returns (bool
success)
9 function allowance(address _owner, address _spender) public view
returns (uint256 remaining)
10
```

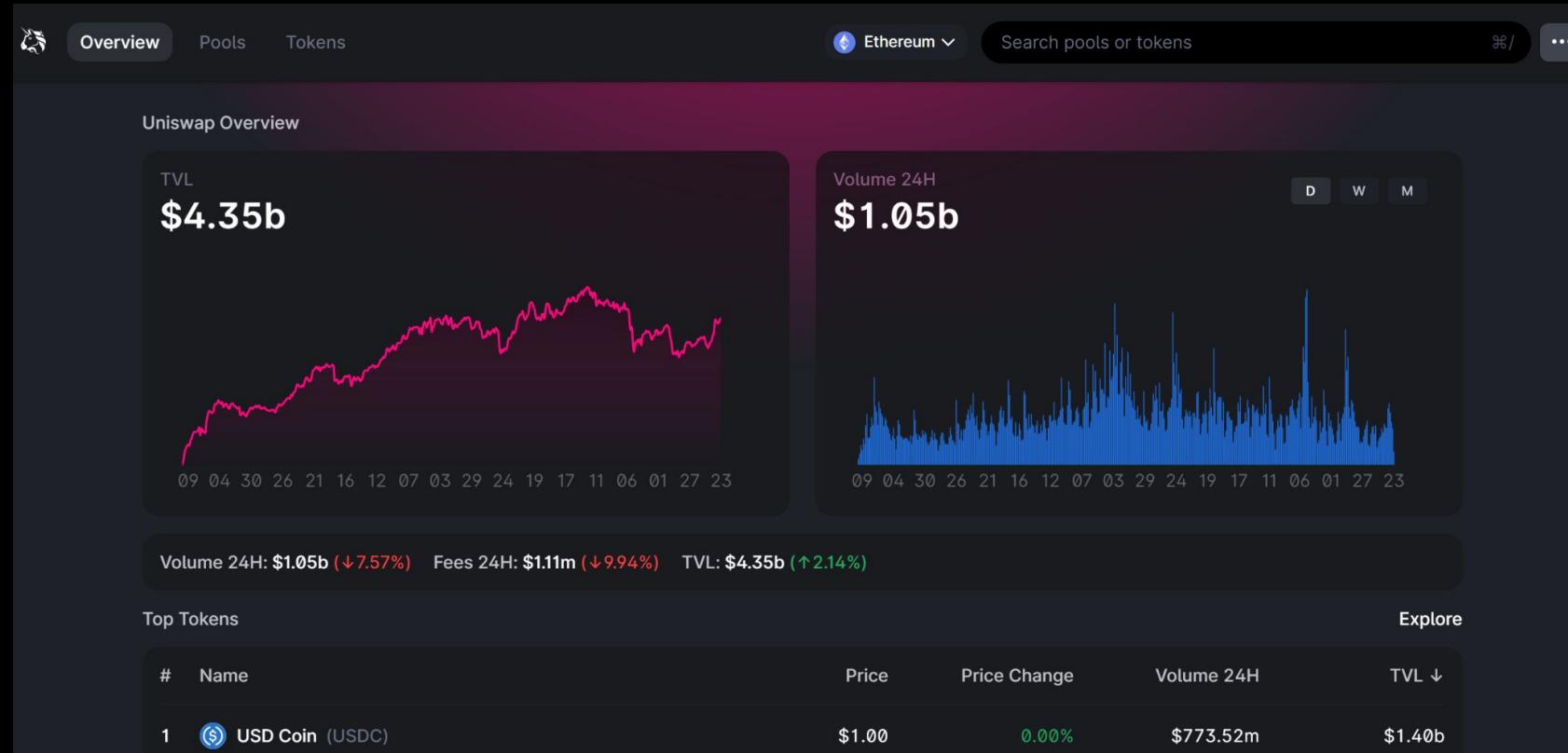
Show less Copy

Events

```
1 event Transfer(address indexed _from, address indexed _to, uint256
_value)
2 event Approval(address indexed _owner, address indexed _spender, uint256
_value)
3
```

Copy

[ERC-20 Token Standard | ethereum.org](#)



<https://info.uniswap.org/#/>



From [EIP-721](#):

Methods

```
1 function balanceOf(address _owner) external view returns (uint256);
2 function ownerOf(uint256 _tokenId) external view returns (address);
3 function safeTransferFrom(address _from, address _to, uint256
4 _tokenId, bytes data) external payable;
5 function safeTransferFrom(address _from, address _to, uint256
6 _tokenId) external payable;
7 function transferFrom(address _from, address _to, uint256 _tokenId)
8 external payable;
9 function approve(address _approved, uint256 _tokenId) external
10 payable;
11 function setApprovalForAll(address _operator, bool _approved)
external;
12 function getApproved(uint256 _tokenId) external view returns
(address);
13 function isApprovedForAll(address _owner, address _operator)
external view returns (bool);
```

Events

```
1 event Transfer(address indexed _from, address indexed _to, uint256
indexed _tokenId);
2 event Approval(address indexed _owner, address indexed _approved,
uint256 indexed _tokenId);
3 event ApprovalForAll(address indexed _owner, address indexed
_operator, bool _approved);
4
```

[ERC-721 Non-Fungible Token Standard | ethereum.org](#)



Image credit: Bored Ape Yacht Club/OpenSea



Image credit: larvalabs.com



Image credit: The Lunacian/Axie Infinity/axie.substack.com

ERC721



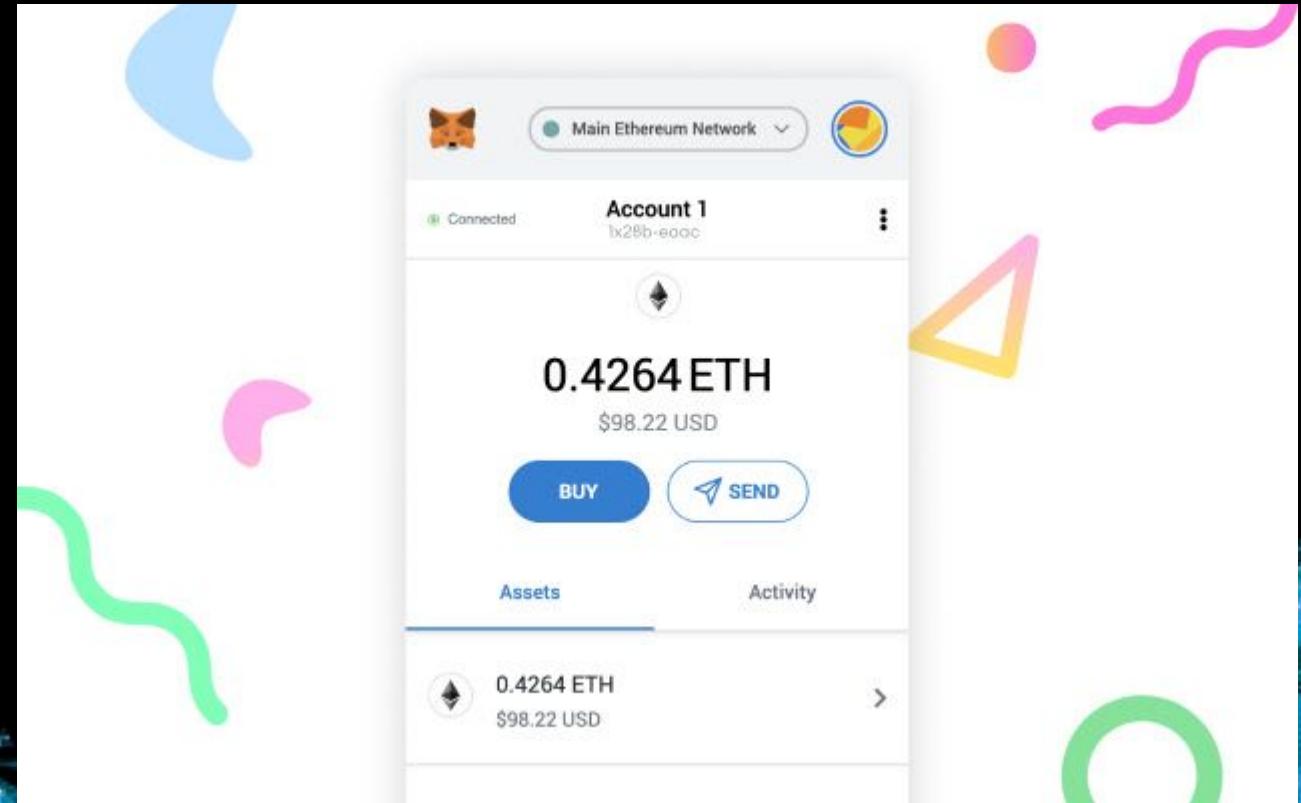
Smartcontract

compile





Cryptocurrency wallet





Subscribe



KUBCS



KU Blockchain Society

Goal: ชุมชน Blockchain อันดับ 1 ในประเทศไทย



Facebook



Twitter



Discord



Instargram



Linktree*