E-SAN THAILAND CODING & AI ACADEMY

โครงการวิจัยโมเดลระบบนิเวศการเรียนรู้ที่บูรณาการ CODING & AI สำหรับเยาวชน

Model of Learning Ecosystem Platform integrate with Coding & AI for Youth

โครงการย่อยที่ 2

การพัฒนาเยาวชนเพื่อเข้าสู่วิชาชีพขั้นสูงด้าน Coding & AI

ร่วมกับ Coding **Entrepreneur & Partnership: Blockchain & Fintech**

ชื่อหัวข้อ เจาะลึกทางเทคนิคของ Blockchain

ผศ. ดร.ปรมะ แขวงเมือง

หัวหน้าโครงการย่อยที่ 2

Outline

การพัฒนาเยาวชนเพื่อเข้าสู่วิชาชีพขั้นสูงด้าน Coding & AI **ร่วมกับ** Coding **Entrepreneur & Partnership: Blockchain & Fintech**

Chapter 3: เจาะลึกทางเทคนิคของ Blockchain

หัวข้อ 3.1 เจาะลึกทางเทคนิคของ Blockchain

- บท 1: Node คืออะไร ?
- บท 2: Miner คืออะไร ?
- บท 3: Consensus คืออะไร ?

หัวข้อ 3.2 สรุปการทำงานของ Blockchain

- บท 4: Tokenomics ของ Bitcoin
- บท 5: Public Key และ Private Key คืออะไร ?
- บท 6: สรุปการทำงานพื้นฐานของ Bitcoin

หัวข้อ 3.3 สามเหลี่ยมของ Blockchain

- บท 7: ความสามารถในการรองรับผู้ใช้งานสำคัญอย่างไร
- บท 8: การรองรับผู้ใช้งาน, ความกระจายศูนย์, และความแข็งแกร่งของระบบ
- บท 9: ปัญหาของระบบ Blockchain

หัวข้อ 3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

- บท 10: ขนาดและเวลาปิดของ Blockchain
- บท 11: การเพิ่มการรองรับผู้ใช้งานจำนวนมากแบบแนวนอน
- บท 12: การเพิ่มการรองรับผู้ใช้งานจำนวนมากแบบแนวตั้ง

03

3.1 เจาะลึกทางเทคนิคของ Blockchain

Node คืออะไร ?

- Node คือคอมพิวเตอร์ที่มีส่วนร่วมในการจัดเก็บชุดของข้อมูลบน Blockchain เพื่อเพิ่ม Decentralization (ความกระจายศูนย์) ให้แก่ Blockchain นั้น ๆ หรือเรียกอีกอย่างได้ว่า "Distributed Ledger"
- ยิ่งมีจำนวน Node มากก็จะยิ่งเพิ่ม Decentralization (ความกระจายศูนย์) ให้กับ Blockchain นั้น ๆ และจะยิ่งยากต่อการแทรกแทรงหรือบิดเบือนข้อมูลบน Blockchain

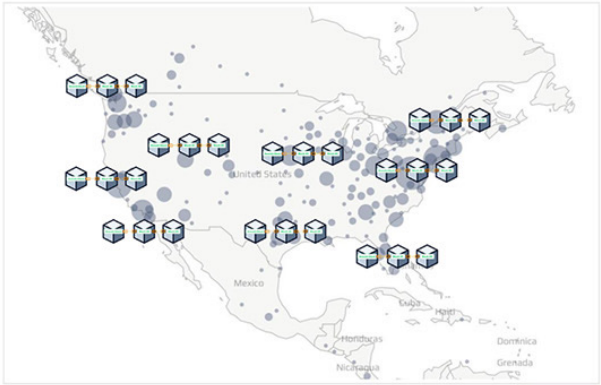
REACHABLE BITCOIN NODES
Updated: Mon Oct 9 11:17:22 2023 +07

16494 NODES CHARTS

IPv4: -5.1% / IPv6: -2.4% / .onion: +1.3%

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

RANK	COUNTRY	NODES
1	n/a	10507 (63.70%)
2	United States	1526 (9.25%)
3	Germany	1244 (7.54%)
4	France	416 (2.52%)
5	Netherlands	328 (1.99%)
6	Canada	260 (1.58%)
7	Finland	229 (1.39%)
8	United Kingdom	178 (1.08%)
9	Russian Federation	168 (1.02%)
10	Switzerland	147 (0.89%)

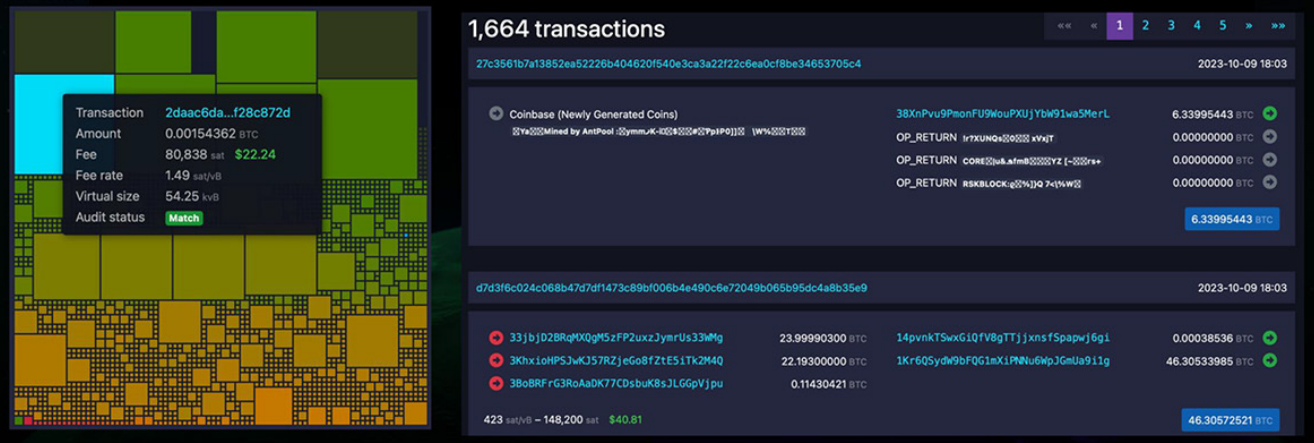


Map shows concentration of reachable Bitcoin nodes found in countries around the world. LIVE MAP

3.1 เจาะลึกทางเทคนิคของ Blockchain

Node คืออะไร ?

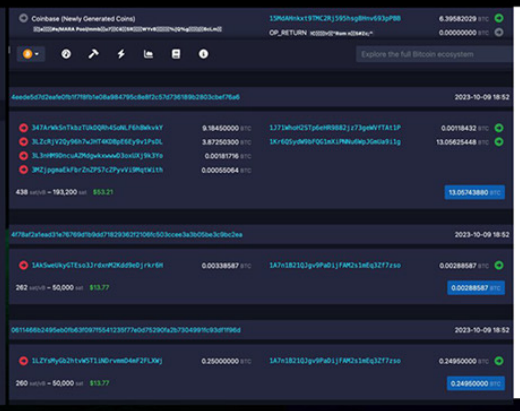
- Node ของ Cryptocurrency นั้นแบ่งแยกออกมาได้หลากหลายประเภท และจะมีข้อดี-เสีย ที่แตกต่างกันไป
- POW (Proof of Work - Bitcoin)
  - Full Node : จัดเก็บข้อมูลฉบับเต็มของ Blockchain เช่น Bitcoin
  - Miner Node : จัดเก็บข้อมูลฉบับเต็มของ Blockchain และเข้าร่วมการแข่งขันเพื่อสรุปข้อมูลและเพิ่ม Block ใหม่ สู่เครือข่าย Blockchain
  - Light Node (SPV Client) : จัดเก็บข้อมูลเพียงแค่บางส่วน เพื่อให้ไม่ใช้ Requirement ในการ Run Node ที่มากจนเกินไป และสามารถทำได้ง่าย

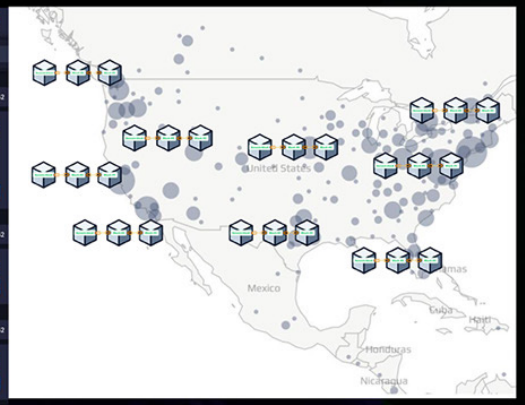


3.1 เจาะลึกทางเทคนิคของ Blockchain

Miner คืออะไร ?

- Miner คือคอมพิวเตอร์ที่พยายามแข่งขันผ่าน Consensus เพื่อเป็นผู้ที่ได้รับหน้าที่สรุปบัญชี และยืนยันธุรกรรมที่รอยืนยันใน Mempool เข้าสู่ Blockchain ใน Block ถัดไป
- เมื่อเกิดธุรกรรมขึ้น เหล่า Miner Node จะมีการจัดเรียงธุรกรรมต่าง ๆ เหล่านั้นไว้ใน Mempool ของตนเองและจะดำเนินการทำธุรกรรมที่จ่ายค่าธรรมเนียมสูงก่อน จากนั้นค่อยไล่ตามลำดับ
- Miner จะแข่งขันกันตาม Consensus Machanism เพื่อหาผู้ชนะและได้รับหน้าที่สรุปบัญชีใน Mempool ของเขาและส่งข้อมูลทุก ๆ อย่างไปยัง Node ที่กระจายตัวกันอยู่รอบโลกได้นำไปบรรจุเป็น Block ใหม่ของระบบ Blockchain ถือเป็นการยืนยันธุรกรรม

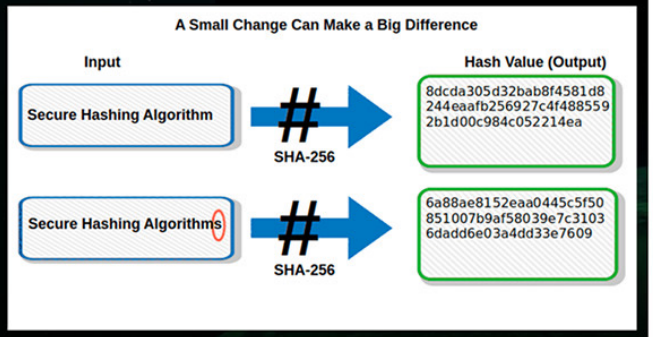


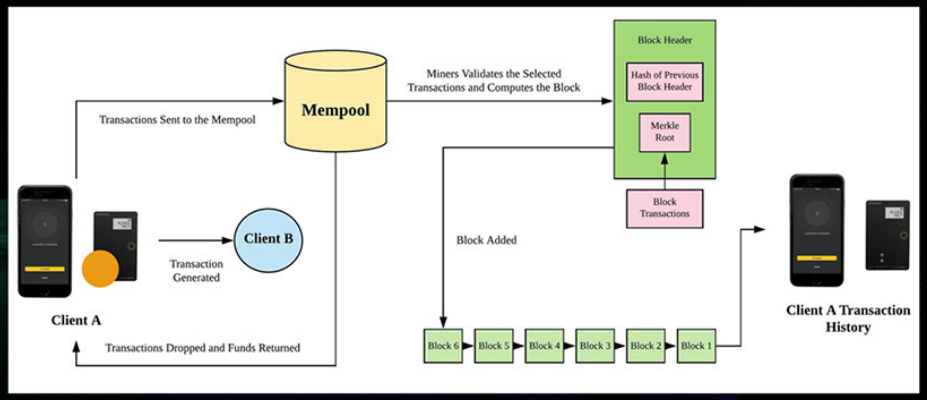


3.1 เจาะลึกทางเทคนิคของ Blockchain

Miner คืออะไร ?

- ใน Consensus Proof of Work ของ Bitcoin เหล่า Miner จะทำการ Hash (SHA-256) และหา Nonce เพื่อให้ตรงตามเป้าที่ Difficulty กำหนด
- โดยเฉลี่ยแล้ว ทุก Block จะมี Miner ที่ชนะตามเวลาที่ Blocktime กำหนดไว้ โดยจะสามารถปรับเปลี่ยนได้ตาม Difficulty ของระบบ
- เมื่อมี Miner ที่สามารถชนะการแข่งขันได้สำเร็จ Miner นั้นจะทำการสรุปบัญชีโดยอ้างอิงจาก Mempool ของเขาและส่งข้อมูลทุก ๆ อย่าง ไปยัง Node ที่กระจายตัวกันอยู่รอบโลกได้นำไปบรรจุเป็น Block ใหม่ของระบบ Blockchain ถือเป็นการยืนยันธุรกรรม
- Miner ที่ชนะการแข่งขันทางคณิตศาสตร์จะได้รับ Block Reward (รางวัล) โดยแบ่งเป็นสองส่วนคือ Block Subsidy และ Fees
- เนื่องจากการแข่งขันที่สูงมากในปัจจุบัน จึงได้มีการรวมกันเพื่อเป็น Mining Pools เพื่อโอกาสในการได้รับ Block Reward ที่มากขึ้น

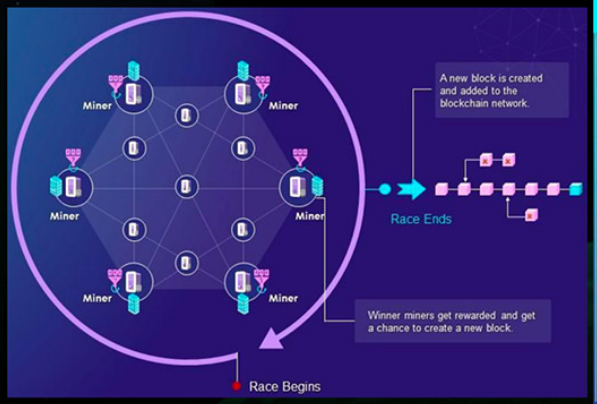




3.1 เจาะลึกทางเทคนิคของ Blockchain

Consensus คืออะไร ?

- Consensus คือวิธีที่ใช้ในการแข่งขันกันของ Miner เพื่อหาผู้ชนะ และได้รับสิทธิในการสรุปข้อมูลต่าง ๆ ใน Mempool และบรรจุเพิ่มเป็น Block ใหม่สู่ระบบ Blockchain โดย Consensus นั้นมีหลากหลาย เช่น Proof of Work และ Proof of Stake
- Consensus เกิดขึ้นเพื่อเป็นกลไกหลักในการทำงานของ Blockchain ป้องกันไม่ให้มีใครคนใดมีสิทธิพิเศษเหนือคนอื่น และทำให้ไม่สามารถรับรู้และโจมตีผู้ที่จะเป็นผู้สรุปบัญชีได้ ถือเป็นกลไกสำคัญที่ทำให้เกิด Decentralization และ Security ของ Blockchain
- Bitcoin ใช้งาน Proof of Work เป็น Consensus ในขณะที่ Ethereum ใช้ Proof of Stake เป็น Consensus

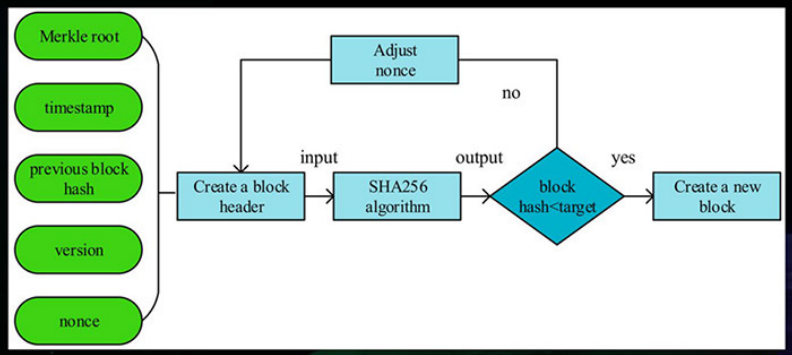


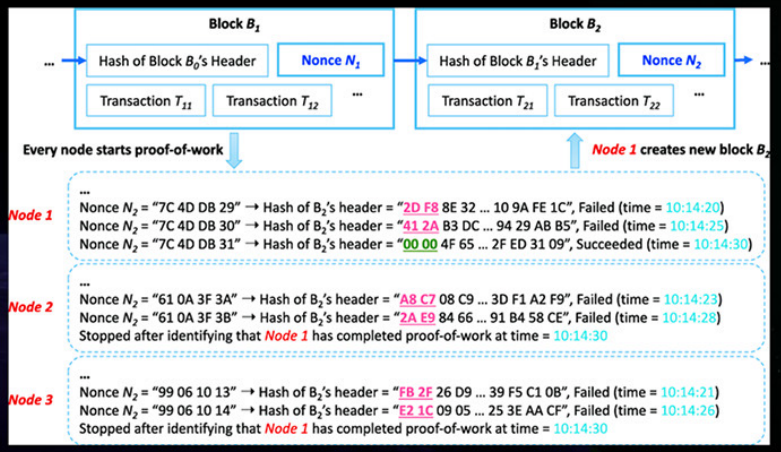
Proof of Work	Comparison Parameter	Proof of Stake
Miners' **computing power** determines the block creation probability.	Block Creation Probability	Validators' **proportion** of **stake** determines the block creation probability.
Miners solve a complex **mathematical problem**, and whosoever solves the problem first is the winner.	Winner Selection	The consensus **algorithm** selects a winner validator based on their **stake size**.
The winner miner is rewarded in terms of **cryptocurrency coins** for successfully creating a new block.	Reward	Winner validators get rewarded in terms of **transaction fees** on successfully creating a new block.
The **low** transaction speed of 64 transactions per second. ↓	Transaction Speed	The **high** transaction speed of 100,000 transactions per second. ↑
Low energy efficiency. ↓	Energy Efficiency	Relatively **higher** energy efficiency. ↑
Costly as specialized equipment are required. ↓	Cost	**Less costly** as no specialized equipment is required. ↑
Offers **more reliability** as security is proven. ↑	Reliability	Since consensus algorithm is new, so relatively **unreliable**. ↓

3.1 เจาะลึกทางเทคนิคของ Blockchain

Consensus คืออะไร ?

- Consensus แบบ Proof of Work (Bitcoin) คือการที่ทุก ๆ Miner จะต้องทำการสุ่ม Nonce เพื่อนำไปรวมกับ Data ต่าง ๆ ใน Mempool แล้วนำไปผ่านการ Hash ด้วย Algorithm SHA-256 จนผลลัพท์ออกมาน้อยกว่า Difficulty ที่กำหนดไว้ ณ เวลานั้น
- ถ้าหากผลลัพท์การสุ่มออกมาไม่ถูกต้อง Miner นั้น ๆ ก็จะทำการสุ่มไปเรื่อย ๆ แข่งกันทุก ๆ Miner รอบโลก
- ถ้าหากผลลัพท์ออกมาถูกต้อง Miner นั้น ๆ จะทำการสรุปบัญชีและเพิ่ม Block เข้าสู่ระบบ Blockchain และ Miner อื่น ๆ ก็จะหยุดการแข่งขันเพื่อไปแข่งขันต่อใน Block ถัด ๆ ไปแทน

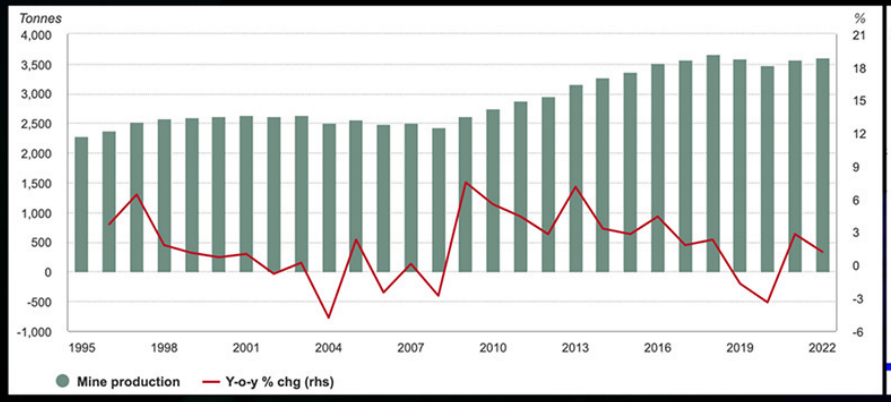


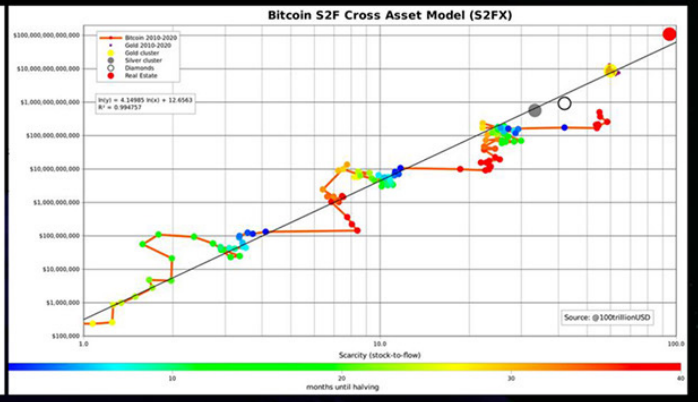


3.2 เจาะลึกทางเทคนิคของ Blockchain ตอนที่ 2

Tokenomics ของ Bitcoin

- Bitcoin จะต้องมีการออกแบบ Tokenomics ที่ดีเพื่อให้สามารถทำหน้าที่ของ Salability across Space, Scale, Time ได้เป็นอย่างดี สิ่งสำคัญคือการควบคุม Supply และ Inflation Rate ของเหรียญ และการออกแบบกลไกให้ครอบคลุมเพื่อให้ไม่ต้องมีการเปลี่ยนแปลงนโยบายใด ๆ เลยในภายหลัง
- ความตั้งใจของ Bitcoin คือต้องการให้สามารถเป็นได้ทั้ง Medium of Exchange ที่ดีและเป็น Store of Value ได้ดั่งทองคำดิจิทัล
- การเป็น Store of Value ที่ดีนั้นจะสามารถพิจารณาได้จาก Inflation Rate และ Stock to Flow Ratio (Existing Supply / New Production)
- ทองคำมี Supply Inflation Rate ต่อปีที่เฉลี่ยประมาณ 2%
- Bitcoin มี Inflation Rate ต่อปีประมาณ 1.8% และจะเหลือเพียง 0.88% ในการ Halving ครั้งที่ 4

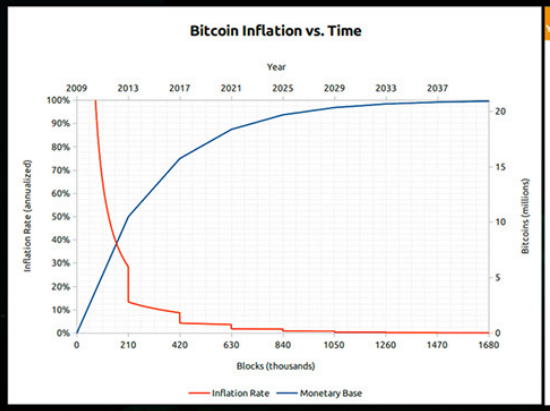




3.2 เจาะลึกทางเทคนิคของ Blockchain ตอนที่ 2

Tokenomics ของ Bitcoin

- Tokenomics ของ Bitcoin ถูกควบคุมด้วยหลายสิ่งหลัก ๆ เช่น Limited Supply, Halving, Transaction Fees, Automatic Difficulty Adjustment
- Bitcoin มี Limited Supply อยู่ที่ 21,000,000 Bitcoin และจัดมีการ Halving ทุก ๆ 210,000 Blocks (ประมาณ 4 ปี) เพื่อลด Block Subsidy ลงครึ่งหนึ่ง เพื่อให้ Bitcoin มีอัตราการเฟ้อที่ลดลงไปเรื่อย ๆ โดยคาดหวังว่าเมื่อเวลาผ่านไป ราคา Bitcoin จะสูงมากพอที่จำทำให้เหล่า Miner สามารถแข่งขันกันได้ต่อไป
- ในช่วงแรก Bitcoin ต้องมี Block Subsidy ที่สูงเพื่อเป็น Incentive ให้เกิด Miner จำนวนมากและสร้างความแข็งแกร่งให้กับระบบ

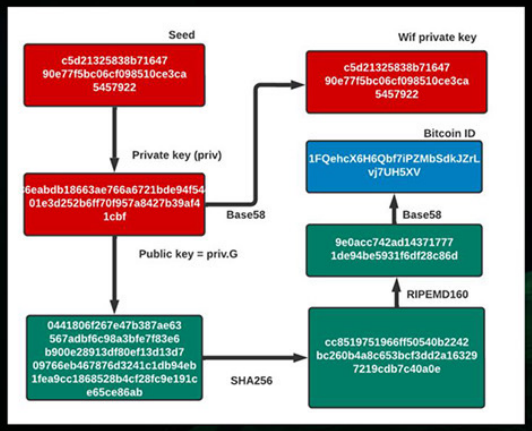


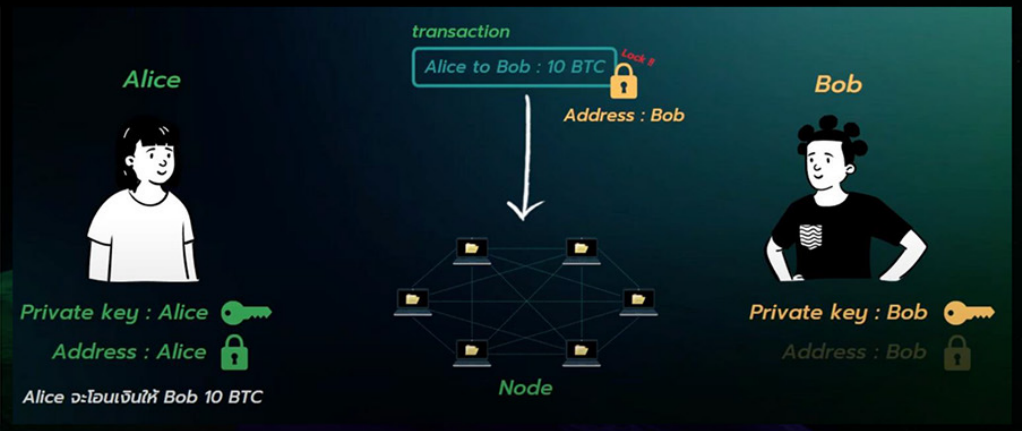
Halving Year (Estimated)	Block Number	Block Reward	BTC Circulating Supply	Circulating Supply Percentage
2009	0	50.00000000	10,500,000.00000000	0%
2012	210,000	25.00000000	15,750,000.00000000	50.00000006%
2016	420,000	12.50000000	18,375,000.00000000	75.00000008%
2020	630,000	6.25000000	19,687,500.00000000	87.50000010%
2024	840,000	3.12500000	20,343,750.00000000	93.75000010%
2028	1,050,000	1.56250000	20,671,875.00000000	96.87500011%
2032	1,260,000	0.78125000	20,835,937.50000000	98.43750011%
2036	1,470,000	0.39062500	20,917,968.75000000	99.21875011%
2040	1,680,000	0.19531250	20,958,984.37500000	99.60937511%
2044	1,890,000	0.09765625	20,979,492.18750000	99.80468761%
2048	2,100,000	0.04882812	20,989,746.09270000	99.90234386%
2052	2,310,000	0.02441406	20,994,873.04530000	99.95117186%
2056	2,520,000	0.01220703	20,997,436.52160000	99.97558604%
2060	2,730,000	0.00610351	20,998,718.25870000	99.98779307%
2064	2,940,000	0.00305175	20,999,359.12620000	99.99389658%
2068	3,150,000	0.00152587	20,999,679.55890000	99.99694833%
2072	3,360,000	0.00076293	20,999,839.77420000	99.99847420%
2076	3,570,000	0.00038146	20,999,919.88080000	99.99923713%
2080	3,780,000	0.00019073	20,999,959.93410000	99.99961859%
2084	3,990,000	0.00009536	20,999,979.96970000	99.99980932%
2088	4,200,000	0.00004768	20,999,989.97250000	99.99990468%
2092	4,410,000	0.00002384	20,999,994.97890000	99.99995236%
2096	4,620,000	0.00001192	20,999,997.48210000	99.99997620%
2100	4,830,000	0.00000596	20,999,998.73370000	99.99998812%
2104	5,040,000	0.00000298	20,999,999.35950000	99.99999408%
2108	5,250,000	0.00000149	20,999,999.67240000	99.99999706%
2112	5,460,000	0.00000074	20,999,999.82780000	99.99999855%
2116	5,670,000	0.00000037	20,999,999.90550000	99.99999929%
2120	5,880,000	0.00000018	20,999,999.94330000	99.99999966%
2124	6,090,000	0.00000009	20,999,999.96220000	99.99999984%
2128	6,300,000	0.00000004	20,999,999.97060000	99.99999993%
2132	6,510,000	0.00000002	20,999,999.97480000	99.99999997%
2136	6,720,000	0.00000001	20,999,999.97690000	99.99999999%
2140	6,930,000	0.00000000	20,999,999.97690000	100.00000000%

3.2 เจาะลึกทางเทคนิคของ Blockchain ตอนที่ 2

Public Key และ Private Key คืออะไร ?

- Private Key และ Public Key คือส่วนสำคัญในการทำธุรกรรมต่าง ๆ บน Bitcoin ผ่านกระบวนการ Asymetric Cryptography
- Private Key เปรียบเสมือนกุญแจลับที่เอาไว้ใช้เพื่อยืนยันความเป็นเจ้าของในธุรกรรมต่าง ๆ , Public Key เปรียบเสมือนเลขบัญชี
- Private Key และ Public Key จะถูกสร้างด้วย Application Wallet ต่าง ๆ โดย จะเริ่มจากการสุ่ม Private Key โดยมีความเป็นไปได้อยู่ที่ 10^77 และนำไปสร้าง Public Key ผ่าน ECDSA ซึ่งไม่สามารถทำการคำนวนกลับย้อนหลังได้ และจากนั้นก็จะผ่านกระบวนการต่าง ๆ กลายเป็น Address ให้ง่ายต่อการใช้

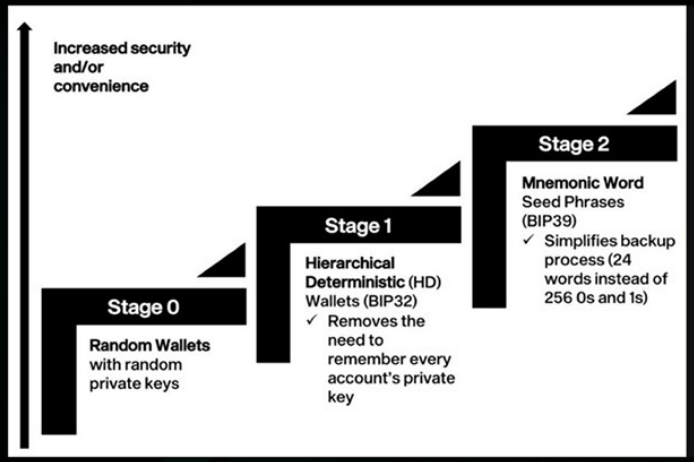


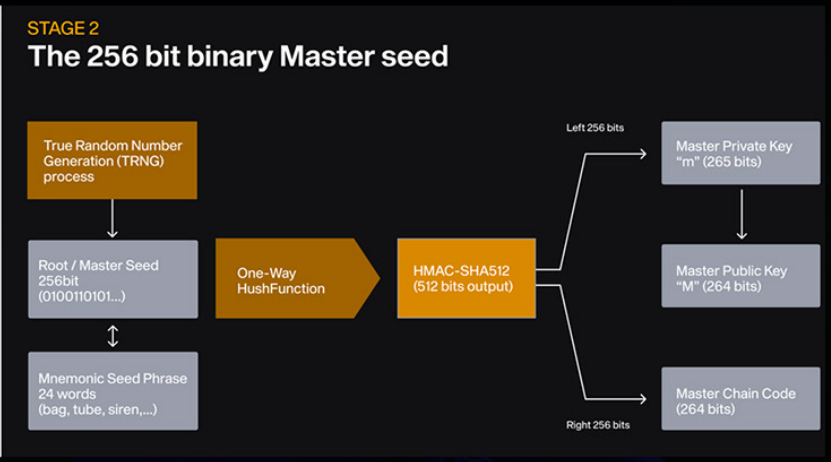


3.2 เจาะลึกทางเทคนิคของ Blockchain ตอนที่ 2

Public Key และ Private Key คืออะไร ?

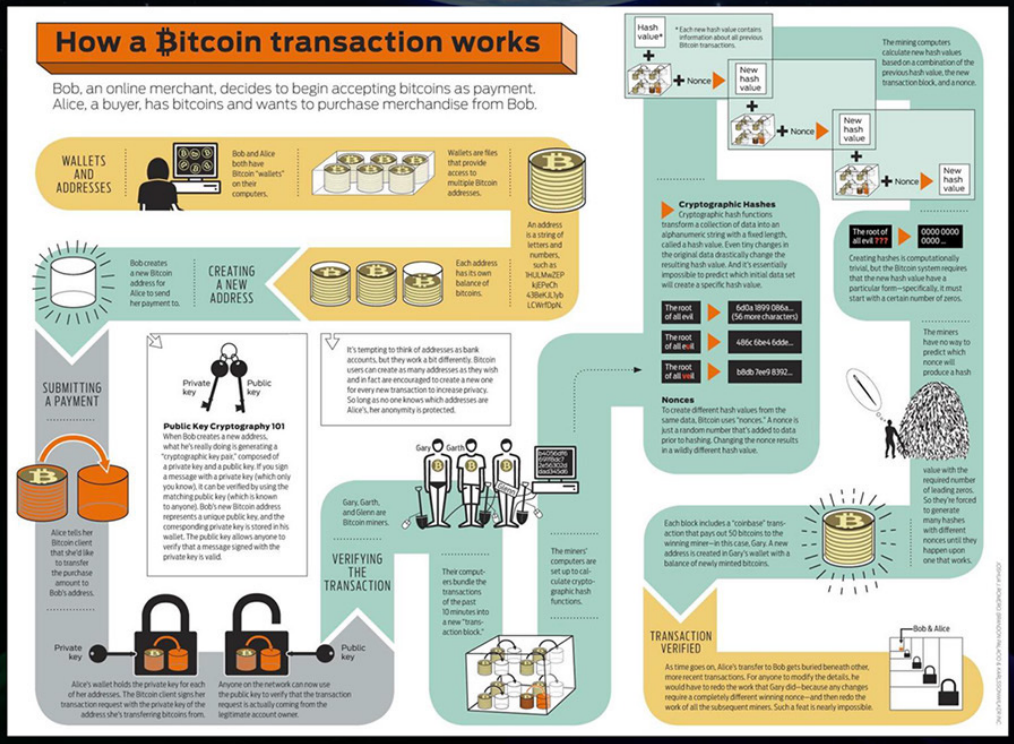
- ผู้ใช้งานสามารถที่จะมีกี่ Private Key ก็ได้ตามที่ต้องการ และไม่จำเป็นต้องมีการ KYC ใด ๆ จึงทำให้มีความ Privacy สูงมาก และเนื่องจากแต่ละคนอาจมีการใช้งาน Private Key จำนวนมาก จึงมีการคิดค้น Seed ขึ้นซึ่งเปรียบเสมือนพวงกุญแจเพื่อความสะดวกต่อการใช้งาน (BIP-32) หรือเรียกว่า Hierarchical-deterministic (HD) wallet
- การใช้งาน Hierarchical-deterministic (HD) เป็น Format หรือจดจำยากจึงมีการพัฒนามาเป็น BIP-39 (Mnemonic Pharses) ที่ใช้งานในปัจจุบัน





3.2 เจาะลึกทางเทคนิคของ Blockchain ตอนที่ 2

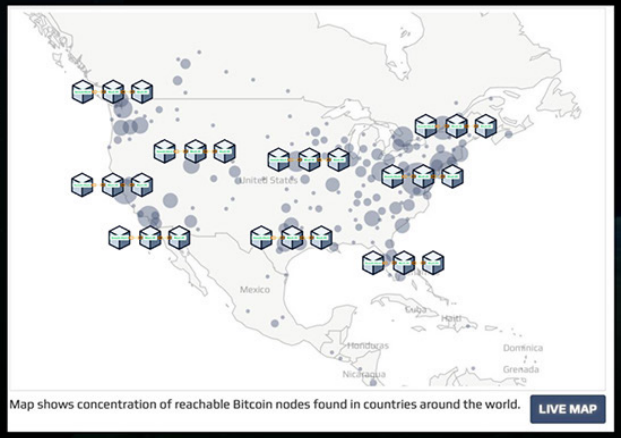
สรุปการทำงานพื้นฐานของ Bitcoin

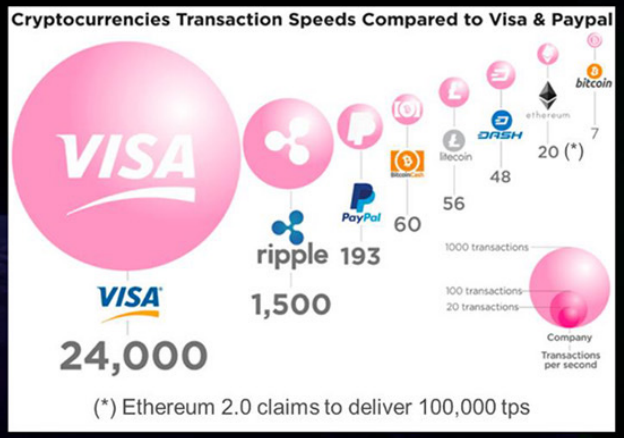


3.3 สามเหลี่ยมของ Blockchain

ความสามารถในการรองรับผู้ใช้งานสำคัญอย่างไร

- ปัญหาในเรื่องของ Scalability บน Blockchain นั้นเกิดขึ้นมาอย่างต่อเนื่อง เนื่องจากข้อจำกัดทางโครงสร้าง
- เนื่องจาก Blocksize ของ Bitcoin นั้นมีขนาดเพียงแค่ 1 Mb / Block (10 Minute) ซึ่งทำให้สามารถทำธุรกรรมได้จำกัดมาก ตามมาด้วยการที่ Blockchain แน่นง่ายและค่า Fees ที่สูงมากจนเป็นปัญหาในการทำธุรกรรม
- เดือน August ของปี 2017 Bitcoin ได้มีการ Upgrade ที่เกิดจากความเห็นร่วมกันของเหล่าผู้รัน Node คือการอัพเกรด Segwit (Segregated Witness) เป็นการอัพเกรดที่ช่วยเรื่อง Scalability ของ Bitcoin ได้ในระดับหนึ่ง (approx. 1,500 to 2,000 transactions)

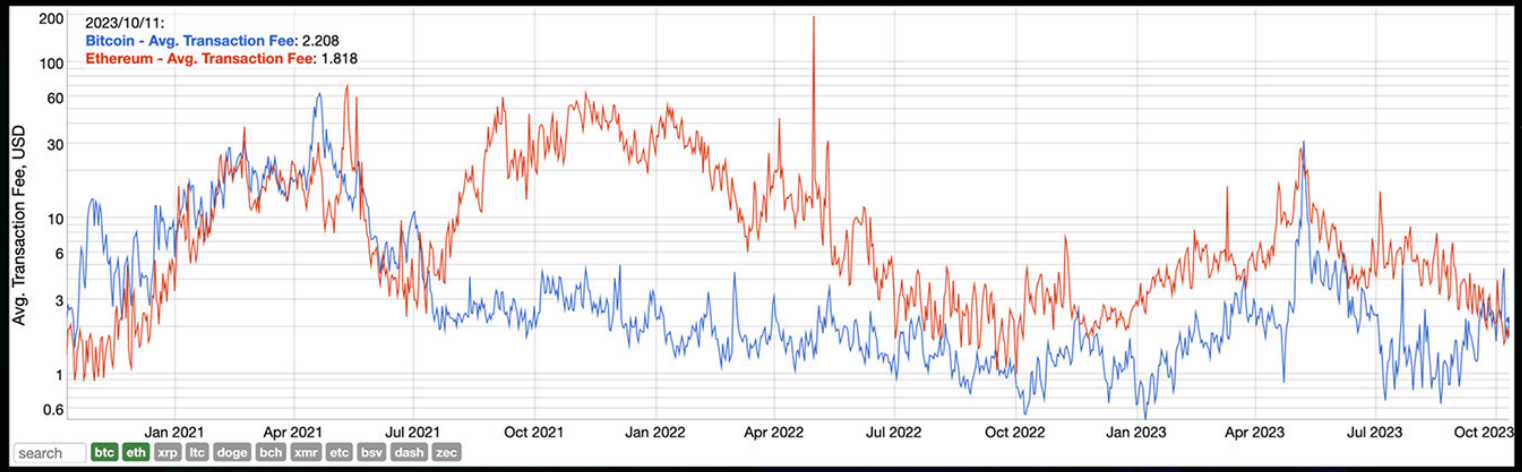




3.3 สามเหลี่ยมของ Blockchain

ความสามารถในการรองรับผู้ใช้งานสำคัญอย่างไร

- ด้วยการใช้งานที่แตกต่างกันอย่างชัดเจนของ Bitcoin และ Ethereum ซึ่งทางฝั่งของ Ethreum นั้นจะเป็นการใช้งานในรูปแบบของ Smart Contract ซึ่งจะมีขนาดที่ใหญ่กว่าธุรกรรมทั่วไปบน Bitcoin มาก ๆ และปัญหาในเรื่องของ Scalability ก็เป็นปัญหาใหญ่ของ Ethereum เช่นกัน
- ทางฝั่งของ Ethereum ก็ประสบปัญหา Network แน่นและส่งผลให้ค่าธรรมเนียม (Fees) สูงขึ้นจนไม่สามารถใช้งานทั่วไปได้เช่นกัน โดยในช่วงปี 2022 ที่มีผู้คนเข้ามาใช้งาน Ethereum จำนวนมาก เคยมีค่า Fees ที่ขึ้นไปสูงถึงเกือบ $200 ต่อธุรกรรม



3.3 สามเหลี่ยมของ Blockchain

การรองรับผู้ใช้งาน, ความกระจายศูนย์, และความแข็งแกร่งของระบบ

- Blockchain Trilemma เป็นแนวคิดโดย Vitalik Buterin ที่บ่งบอกไว้ว่าไม่มี Blockchain ใดที่ตอบโจทย์คุณสมบัติทั้ง 3 ข้อนี้ได้อย่างสมบูรณ์ คือ Scalability, Decentralization, และ Security ซึ่งโดยปกติแล้วการเติบโตของ Scalability จะสวนทางกันกับ Decentralization และ Security
- ในฝั่งของ Cryptocurrency ที่สร้างเพื่อเป็น Medium of Payment Blockchain ของ Bitcoin (BTC) โฟกัสไปที่ Decentraization และ Security จึงทำให้มีปัญหาเรื่อง Scalability และก็มีเหรียญอื่น ๆ พยายามมาแก้ เช่น Bitcoin Cash โดยแลกกันกับความ Decentraization และ Security

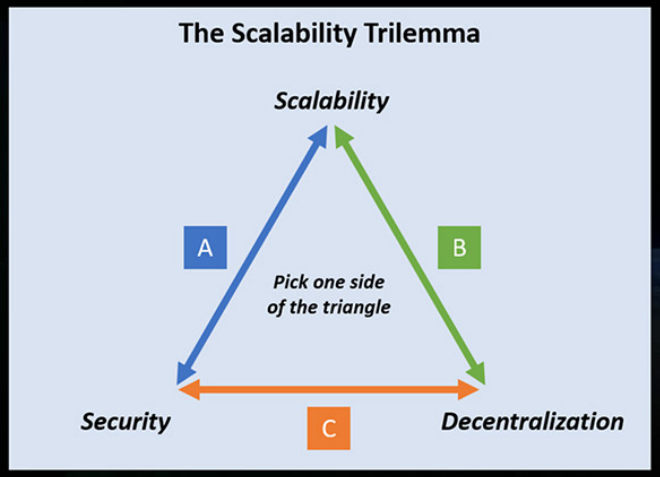


Table 1: Comparison of Bitcoin Private, Bitcoin, Bitcoin Cash, and Bitcoin Gold.

	Bitcoin	Bitcoin Cash	Bitcoin Gold
Total Supply	21 million	21 million	21 million
Privacy	x	x	x
Block Time	10 min	10 min	2.5 min
Block Size	1 MB	8 MB	1 MB
PoW Algorithm	SHA256	SHA256	Equihash
Difficulty Adjustment	2 Weeks	2 Weeks	Every Block
Closed Premine	x	x	Yes
Community-Driven	x	x	x
Governance	x	x	x

3.3 สามเหลี่ยมของ Blockchain

การรองรับผู้ใช้งาน, ความกระจายศูนย์, และความแข็งแกร่งของระบบ

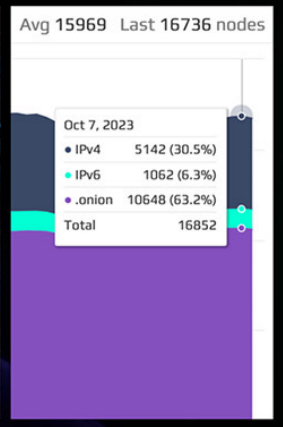
- Bitcoin มี Block Size ที่เล็กมาก ดังนั้น Requirement ที่น้อยมากในการรัน Node จึงใช้ต้นทุนต่ำมาก ๆ ในการรัน Node ส่งผลให้มีจำนวน Node มากมายอยู่รอบโลก และเพิ่มความ Decentralization และ Security ของ Bitcoin
- ในขณะเดียวกัน Bitcoin Cash ที่ตั้งใจจะขยาย Blocksize ให้ใหญ่ขึ้นเพื่อรองรับการใช้งาน ก็ทำให้มี Requirement สูงขึ้นในการรัน Node และตามมาด้วย Decentralization และ Security ที่ลดน้อยลง
- เช่นกันกับกลุ่ม Smart Contract เช่น Ethreum (ETH) และกลุ่ม ETH Killer เช่น Solana (SOL), Cardano (ADA)

Bitcoin Full Node Setup

You will need:

- Raspberry Pi 4 (4GB Memory, at least 32GB micro SD storage)
- Official Rpi Power brick
- Ethernet cord (optional but recommended)
- Minimum 1TB external drive (for storing the blockchain)
- Non metered internet connection

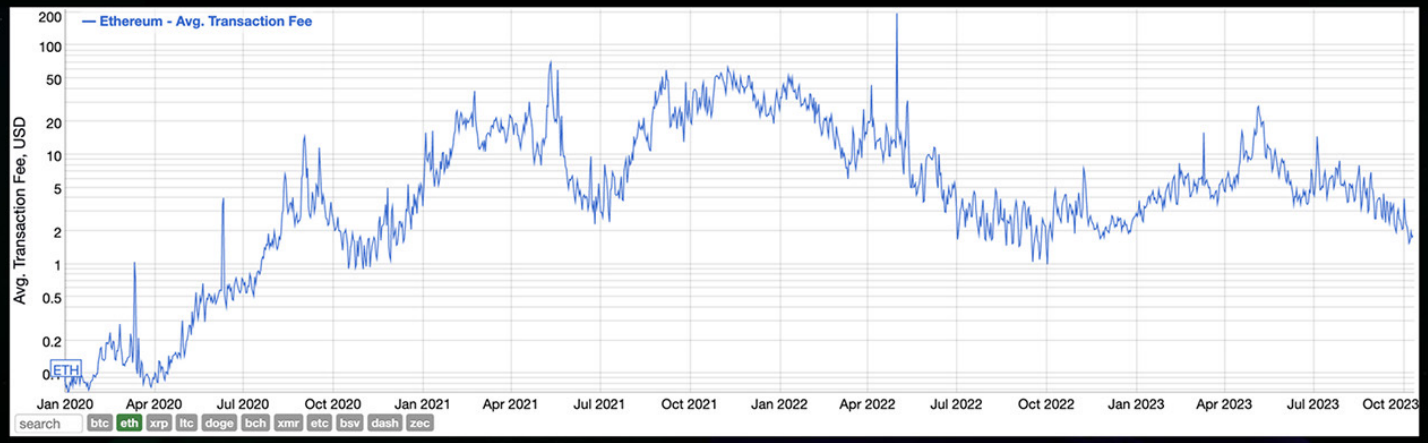
Link parts needed



3.3 สามเหลี่ยมของ Blockchain

การรองรับผู้ใช้งาน, ความกระจายศูนย์, และความแข็งแกร่งของระบบ ตอนที่ 2

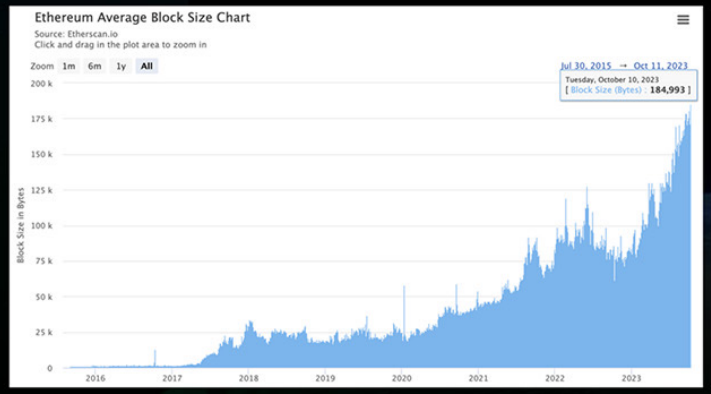
- ทางฝั่งของ Smart Contract Platform ก็มีหลักการเกี่ยวกับ Blockchain Trillema ในรูปแบบเดียวกัน และเนื่องจากความซับซ้อนของ Smart Contract จะทำใช้พื้นที่ต่าง ๆ บน Blockchain มากกว่าการทำธุรกรรมแบบ Medium of Payment มาก จึงทำให้เห็นปัญหาในเรื่องของ Scalability อย่างชัดเจนมาก ๆ เช่น ค่า Fees บน Ethereum Blockchain ที่เคยขึ้นไปเกือบ $200 / Transaction ในช่วงกลางปี 2022
- ทางฝั่งโปรเจคที่ตั้งใจแก้ไขปัญหาเรื่องนี้จึงเกิดขึ้น เป็นเหล่าโปรเจค Etheruem Killer เช่น Cardano (ADA), Solana (SOL) ที่ตั้งใจแก้ไขปัญหานี้ด้วยการเพิ่มขนาดของ Block Size และลดระยะเวลาปิด Block เพื่อให้ Process ธุรกรรมได้รวดเร็ว

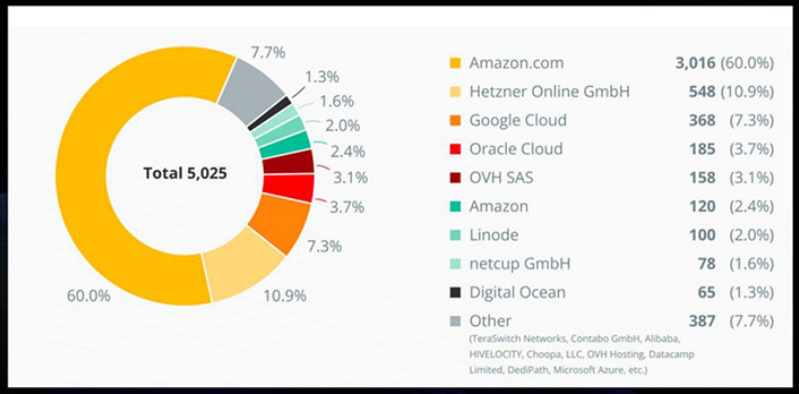


3.3 สามเหลี่ยมของ Blockchain

การรองรับผู้ใช้งาน, ความกระจายศูนย์, และความแข็งแกร่งของระบบ ตอนที่ 2

- ทางฝั่งของ Smart Contract Platform อันดับ 1 อย่าง Ethereum มี Blocksize โดยเฉลี่ยอยู่ที่ 0.184 MB ในปัจจุบัน โดยมี BlockTime เฉลี่ยที่ 12 วินาที (9.2 MB / 10 Minutes)
- ETH Archive Node : Fast CPU with 4+ cores, 16 GB+ of RAM, Geth takes ~13.5 TB, and Erigon takes up ~2 TB, 25 MBit/s bandwidth
- ปัจจุบัน Ethereum มีจำนวน Full Node อยู่ประมาณ 5,025 Node ซึ่งส่วนใหญ่เป็นการใช้งานบน Cloud จึงกลายเป็นคำถามในเรื่องของ Decentralization และ Security ว่าถ้าหากเหล่าผู้ให้บริการ Cloud ต่าง ๆ เหล่านี้เกิดข้อขัดข้องขึ้นจะส่งผลกระทบต่อความแข็งแรงของระบบไหม

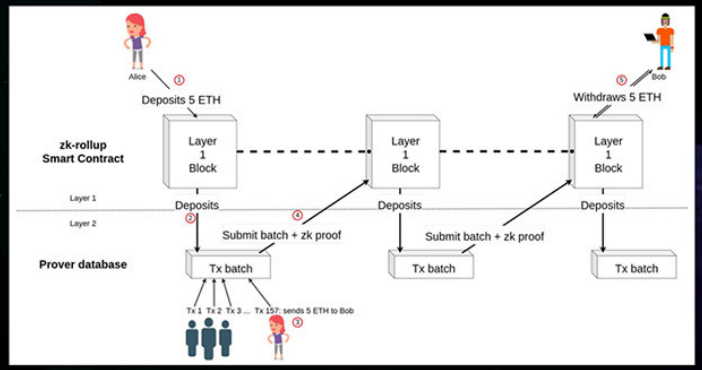


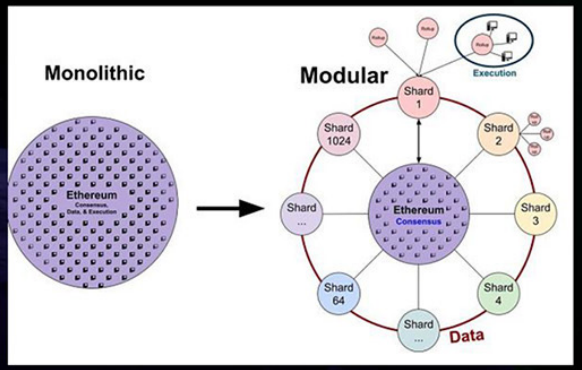


3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

การขยายการรองรับผู้ใช้งานคืออะไร

- Scalability คือ ความสามารถในการรองรับผู้ใช้งาน สามารถวัดได้ด้วย TPS (Transaction per Second) และเป็นหนึ่งในปัญหาที่ใหญ่ที่สุดของ Blockchain อย่าง Bitcoin และ Ethereum ในปัจจุบัน
- การพยายามในการขยาย Scalability เรียกว่า Scaling Solution ซึ่งจะต้องคำนึงถึงหลากหลายปัจจัยทางโครงสร้างของ Blockchain คร่าว ๆ คือ
  - Execution Layer Scaling : การขยาย Scalability ในส่วนของการประมวลผลธุรกรรมต่าง ๆ
  - Data Availability Scaling : การขยาย Scalability ในส่วนของการจัดเก็บข้อมูล (Storage)
  - Consensus Scaling : การขยาย Scalability ในส่วนของ Consensus
- โดยมากในปัจจุบันจะให้ความสำคัญไปที่ส่วนของ Execution Layer Scaling และ Data Availability Scaling

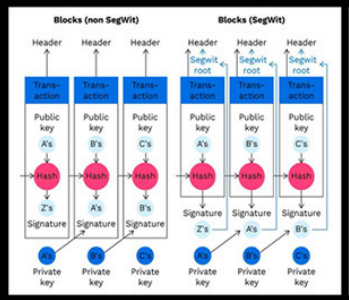


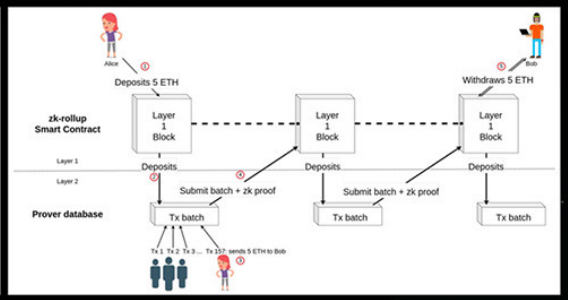


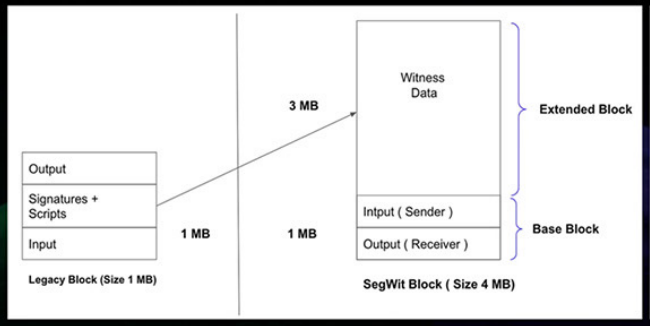
3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

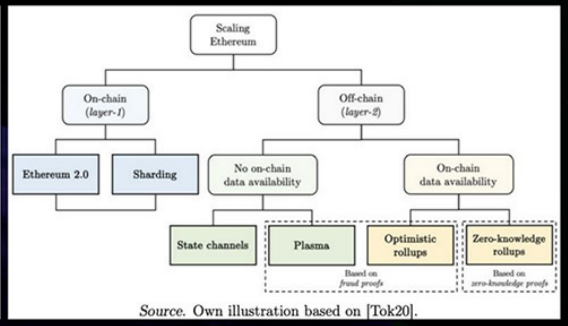
การขยายการรองรับผู้ใช้งานคืออะไร

- Scaling Solution ซึ่งในปัจจุบันมีความพยายามหลากหลายรูปแบบมาก ๆ ที่แตกต่างกันและยังไม่มีข้อสรุปที่ชัดเจน แบ่งย่อยออกเป็น 2 วิธีหลัก ๆ คร่าว ๆ
  - Layer 1 Scaling Solution (On-Chain Scaling)
    - Hardfork
    - New Blockchain project
    - Bitcoin Segregated Witness
    - Sharding
  - Layer 2 Scaling Solution (Off-Chain Scaling)
    - State Channel
    - Sidechain
    - Plasma
    - Rollups
    - Validium









Source. Own illustration based on [Tok20].

3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

การเพิ่มการรองรับผู้ใช้งานจำนวนมากแบบ On-Chain

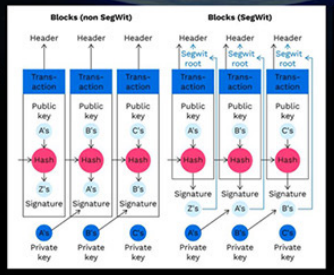
- Scaling Solution แบบ On-chain คือการพยายามเพิ่มความสามารถในการรองรับผู้ใช้งานจำนวนมากด้วยการพัฒนาโครงสร้างบน Blockchain เดิมโดยที่ Execution Layer และ Data Availability ยังจัดเก็บบน Chain เดิม แบ่งคร่าว ๆ เป็นวิธีต่าง ๆ ดังนี้
  - Layer 1 Scaling Solution (On-Chain Scaling)
    - Block size & Block time Adjustment (Hardfork)
    - New Blockchain Project

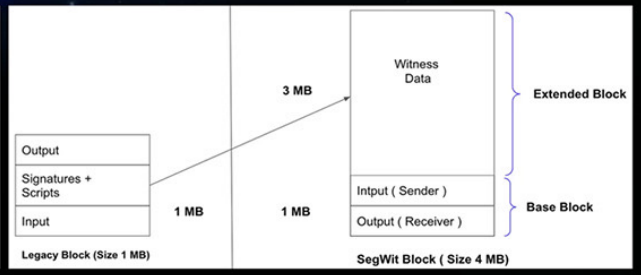
Benchmark/ Coins	Solana	Ethereum	Cardano	Avalanche	Polkadot	Algorand
Transaction Throughput	50,000 - 65,000 tps	15-30 tps	250 tps	4,500 tps	1,000 tps	1,100 tps
Transaction Fee	$0.00025	~$4 - $21	0.4 ADA ~ $0.77	0.001 AVAX ~ $0.63	0.0157 DOT ~ $0.64	$0.002
Consensus Mechanism	Proof of Stake	Proof of Work	Ouroboros Proof of Stake	Proof of Stake	Nominated Proof of Stake	Pure Proof of Stake

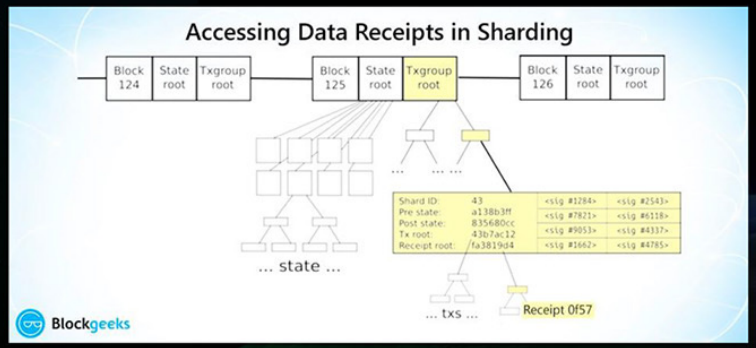
3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

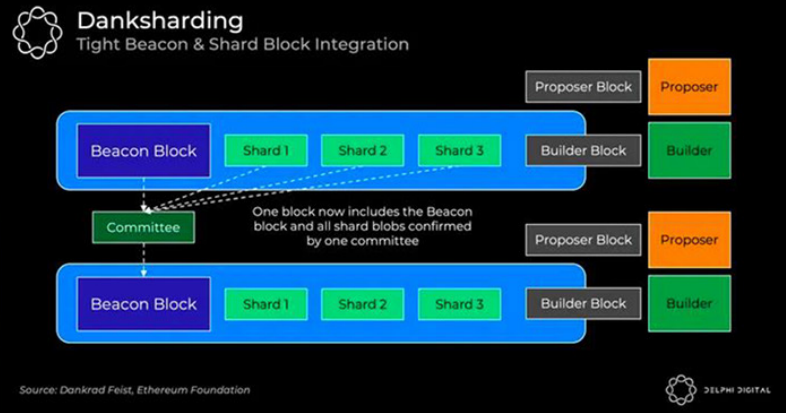
การเพิ่มการรองรับผู้ใช้งานจำนวนมากแบบ On-Chain

- Layer 1 Scaling Solution (On-Chain Scaling)
  - Bitcoin Segregated Witness
  - Sharding





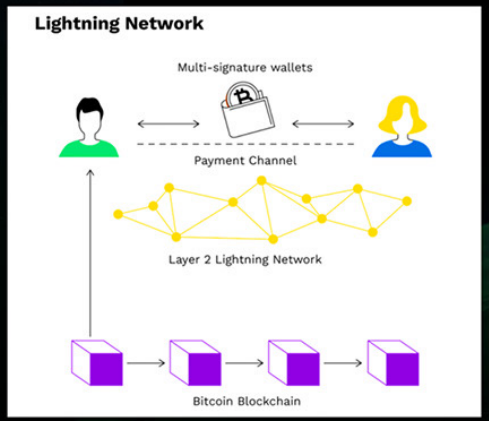


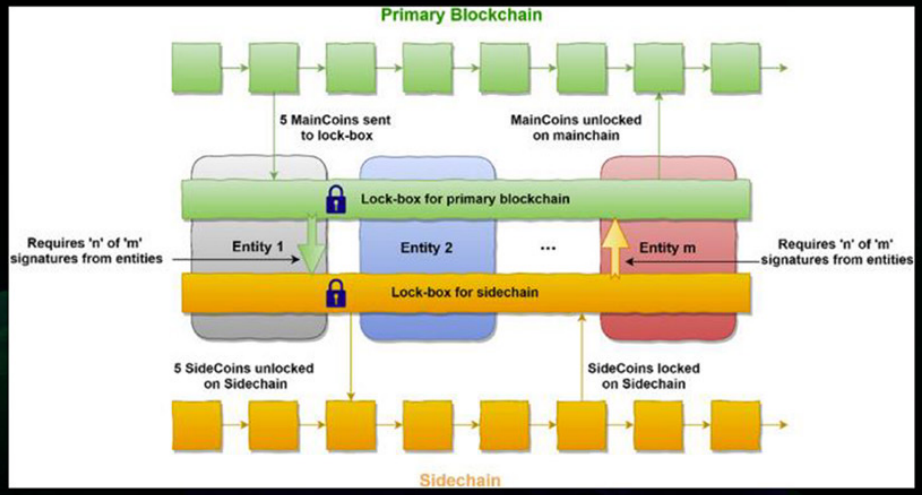


3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

การเพิ่มการรองรับผู้ใช้งานจำนวนมากแบบ Off-Chain

- Scaling Solution แบบ Off-Chain คือการขยาย Scalability ด้วยการใช้ Protocol อื่น ๆ มาทำงานร่วมกับ Main Chain นั้น ๆ โดยไม่ได้จัดการทุก ๆ อย่างอยู่บน Main Chain นั้น ๆ เพื่อขยายประสิทธิภาพหรือแบ่งเบาการทำงานบน Main Chain แบ่งคร่าว ๆ เป็นวิธีต่าง ๆ ดังนี้
- Layer 2 Scaling Solution (Off-Chain Scaling)
  - State Channel เช่น Bitcoin Lightning Network
  - Sidechains เช่น Polygon, XDAI
  - Plasma เช่น OMG Network

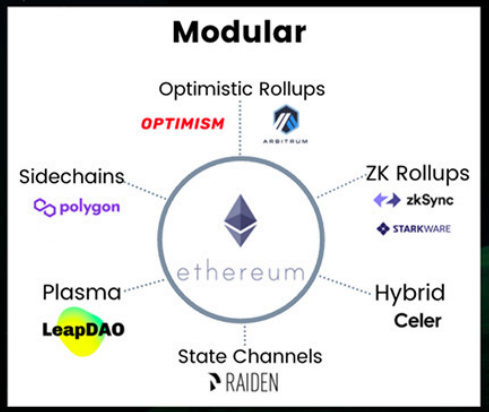


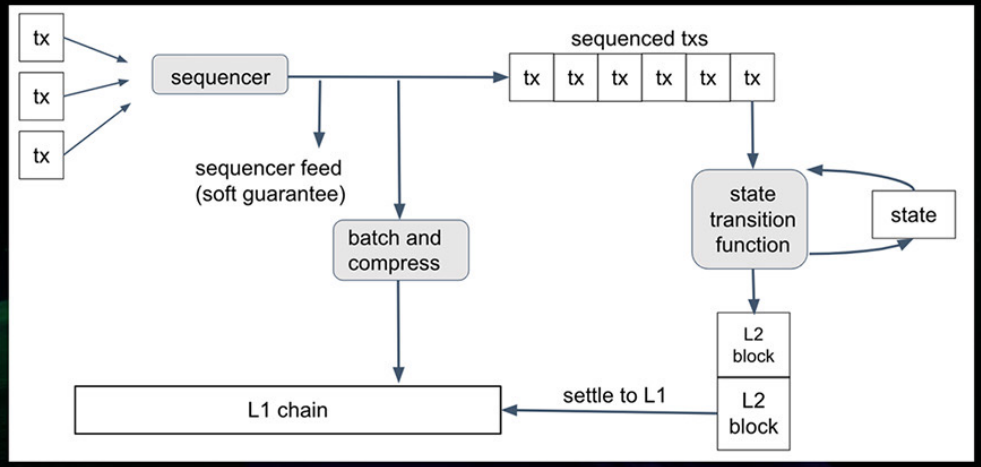


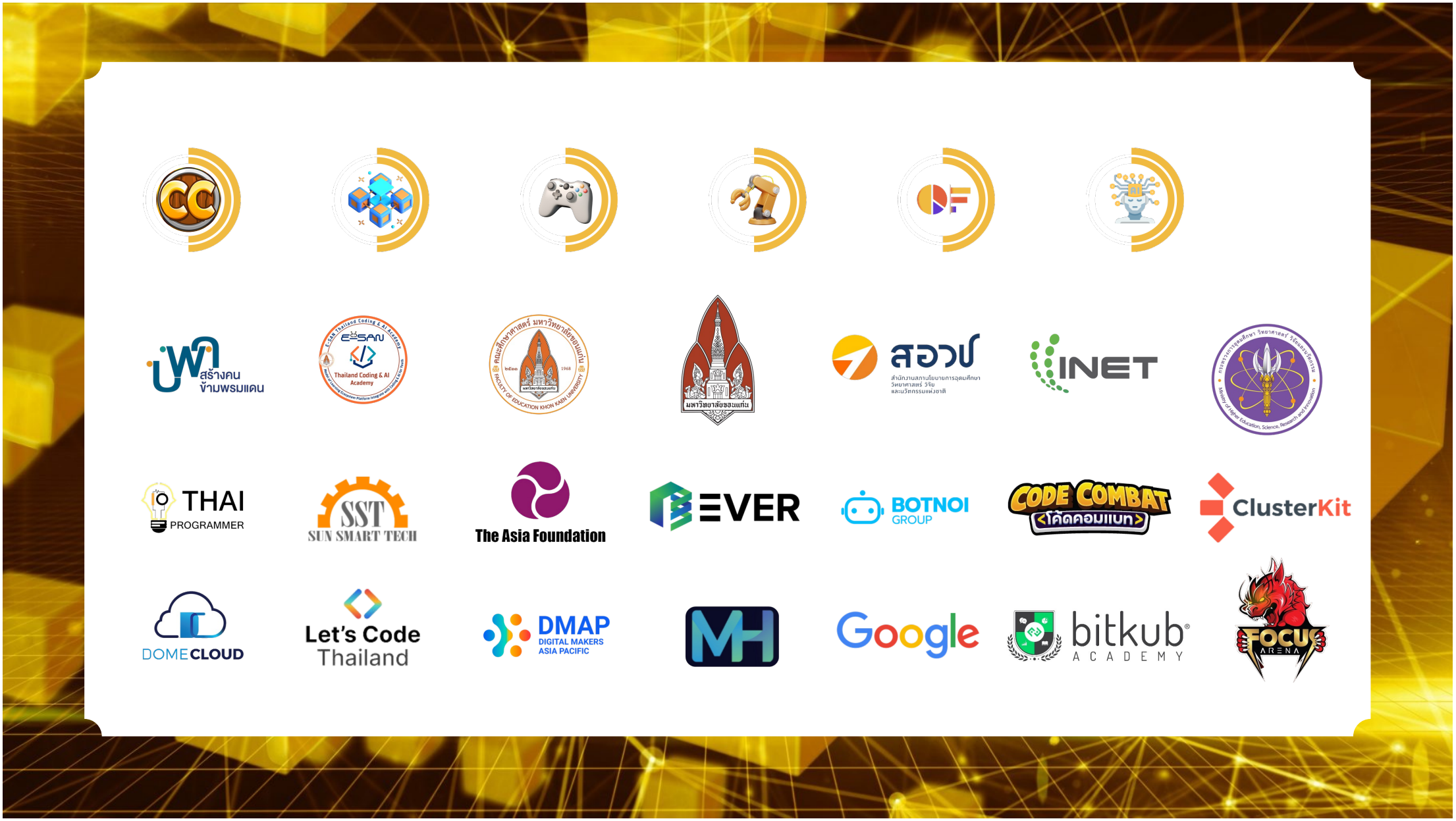
3.4 การรองรับผู้ใช้งานจำนวนมากของ Blockchain ตอนที่ 1

การเพิ่มการรองรับผู้ใช้งานจำนวนมากแบบ Off-Chain

- Layer 2 Scaling Solution (Off-Chain Scaling)
  - Rollups คือ Layer 2 Scaling Solution ที่มีการพัฒนาและ Active ที่สุดในปัจจุบัน แบ่งเป็นอีก 2 เทคโนโลยีคร่าว ๆ คือ
    - Optimistic Rollups เช่น Optimism (OP), Arbitrum (ARB)
    - Zero-Knowledge Rollups เช่น ZKSync, Scroll
  - Validium เช่น ImmutableX






สร้างคน
ข้ามพรมแดน
Thailand Coding & AI Academy
สอวช
INET
THAI
PROGRAMMER
SST
SUN SMART TECH
The Asia Foundation
EVER
BOTNOI
GROUP
CODE COMBAT
ClusterKit
DOMECLOUD
Let's Code
Thailand
DMAP
DIGITAL MAKERS
ASIA PACIFIC
Google
bitkub
ACADEMY
FOCUS
ARENA