



ราชบัณฑิตยสภา

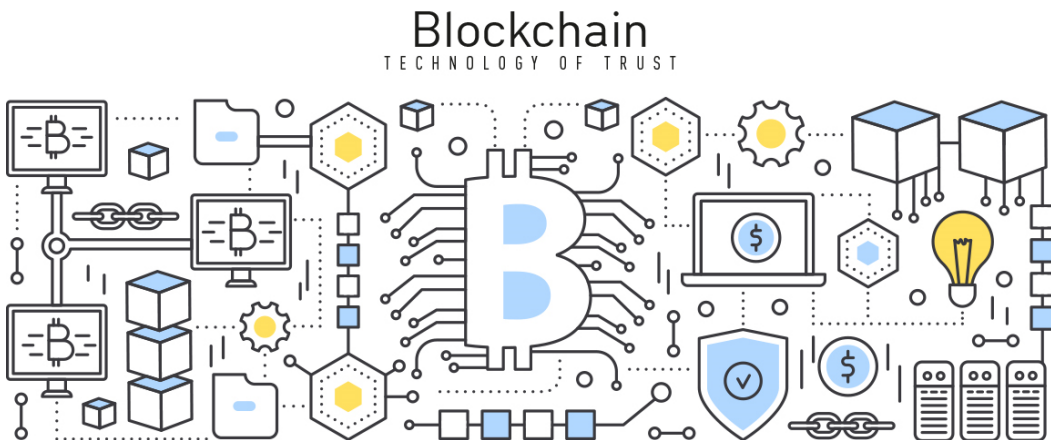
The Royal Society of Thailand



บล็อกเชน: เทคโนโลยีที่เปลี่ยนโลก

Blockchain: A Disruptive Technology

Technology of Trust



๑ กันยายน ๒๕๖๔

ศ.ดร.ธนารักษ์ วีระมั่นคง ราชบัณฑิต

และ อาจารย์ สถาบันเทคโนโลยีนานาชาติสิรินธร

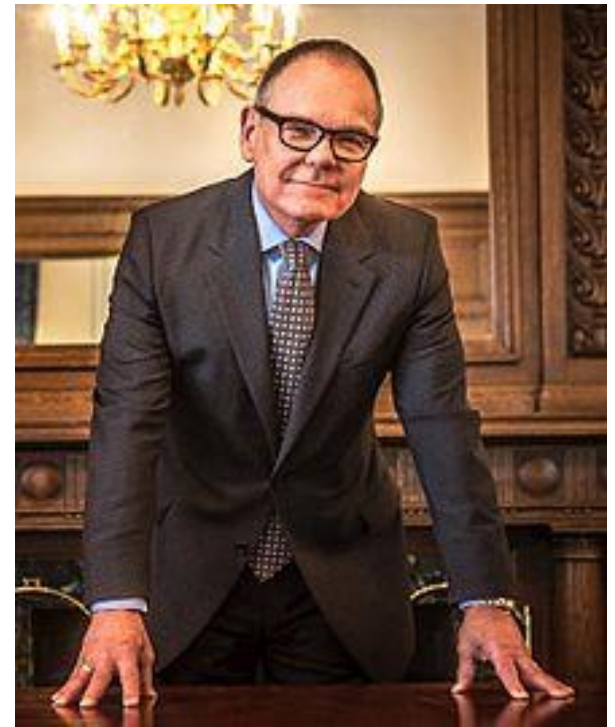
มหาวิทยาลัยธรรมศาสตร์

หัวข้อที่จะบรรยาย

- ความสำคัญของบล็อกเชน (Why Blockchain is Important)
- ทฤษฎีพื้นฐานของบล็อกเชน (Blockchain Fundamentals)
- การใช้งานในปัจจุบันของเทคโนโลยีบล็อกเชน (Blockchain Applications)
 - เงินดิจิทัลหรือคริปโตเคอร์เรนซี (Cryptocurrency)
 - สัญญาอัจฉริยะหรือสมาร์ตคอนแทร็กต์ (Smart Contract)
- การใช้งานบล็อกเชนที่จะปฏิวัติเศรษฐกิจโลก (Economy Disruption)

เว็บที่นำไปอ่านและเข้าใจง่าย: https://nuuneoi.com/blog/blog.php?read_id=900

ความสำคัญของบล็อกเชนภายใน ๗ นาที



Don Tapscott CM (เกิด ๑ มิถุนายน ค.ศ. ๑๙๔๗) เป็นผู้บริหารธุรกิจ นักเขียน ที่ปรึกษา และวิทยากรชาวแคนาดา ซึ่งเชี่ยวชาญด้านกลยุทธ์ทางธุรกิจ การเปลี่ยนแปลงองค์กร และบทบาทของเทคโนโลยีในธุรกิจและสังคม เขาเป็นซีอีโอของ Tapscott Group และผู้ร่วมก่อตั้งและประธานบริหารของสถาบันวิจัยบล็อกเชน เขาเขียนหนังสือขายดี 'Blockchain Revolution'

Understand blockchain in under 7 minutes: Don Tapscott with Lloyds Bank
Mar 22, 2018
<https://www.youtube.com/watch?v=isuAPyuqS7Y>

บล็อกเชนคืออะไร ทำอะไรได้บ้าง นอกจากคริปโทเคอร์เรนซีหรือบิทคอยน์



Blockchain คืออะไร บล็อกเชนทำอะไรได้บ้าง นอกจากแค่ cryptocurrency /bitcoin | DGTH

Nov 17, 2018

<https://www.youtube.com/watch?v=2oaLjzx6tZY>

แรงจูงใจของบล็อกเชน: การรักษาความปลอดภัยบัญชีแยกประเภทสาธารณะ

Motivation of Blockchain: Securing Public Ledger

เปลี่ยนจากส่วนกลางไป เป็น
ทุกคนเห็นบัญชีนี้ แต่จ่ายเพื่ออะไรไม่ระบุ

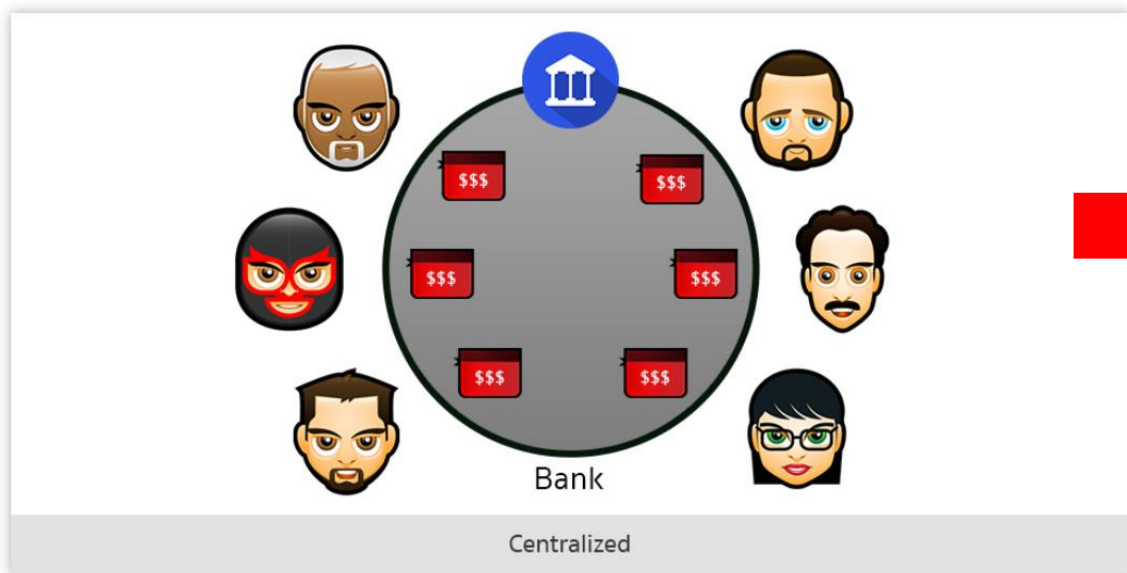
ระบบธนาคาร เมื่อทุกอย่างรวมอยู่ที่เดียว

ธนาคารคือระบบที่ข้อมูลทุกอย่างอยู่ร่วมกันตรงกลาง เห็นม่ว่าตอนเราจะเปิดบัญชีเราก็ต้องเดินไปเปิดที่ธนาคาร เวลาเราจะฝากเงินก็ต้องทำกับธนาคารแล้วอดเงินก็จะขึ้นในบัญชีของเราซึ่งก็อยู่กับธนาคารอีกเช่นกัน ตอนโอนเงินคนที่โยกเงินออกและเข้าให้ก็เป็นธนาคาร ดังนั้นทุกอย่าง 100% จะทำผ่านธนาคารทั้งสิ้น และเราจะเรียกระบบแบบนี้ว่า **ระบบรวมศูนย์กลาง (Centralized)** หรือระบบที่รวมทุกอย่างไว้ในที่เดียว

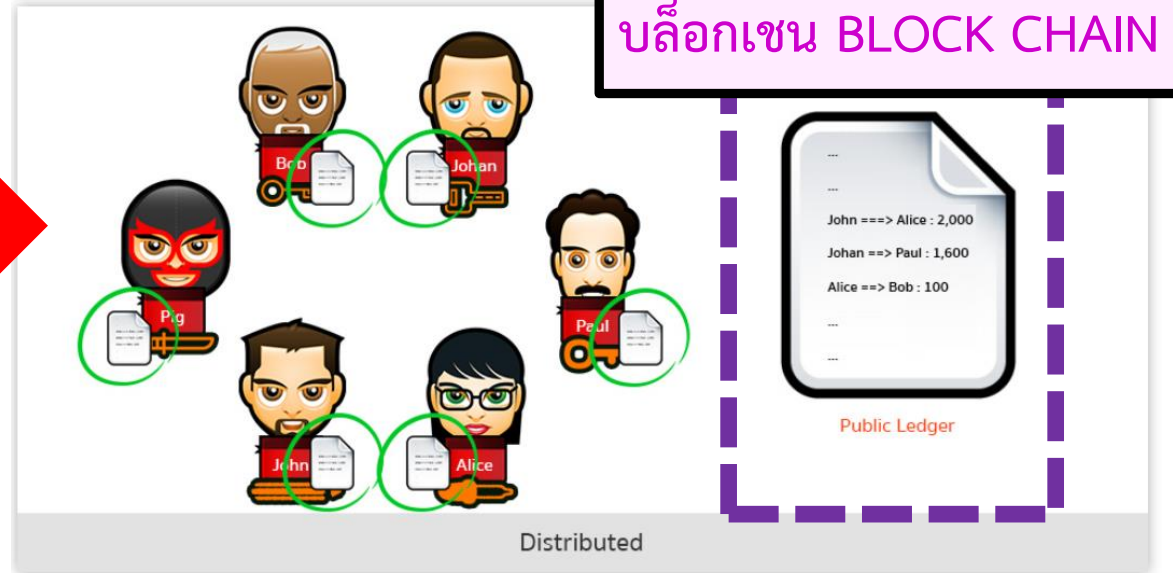
สถานะที่ทุกคนเห็นบัญชีทุกคน แต่ทำให้ไม่มีคนใดคนหนึ่งเข้าไปแก้ไขโดยพลการไม่บอกคนอื่นได้

Public Ledger อยู่ใน "มือทุกคน"

เนื่องจากว่าระบบที่เรากำลังอธิบายอยู่นี้เป็นระบบแบบกระจาย ไม่มีคนตรงกลางนะ ระบบทั้งหมดก็มีกันอยู่แค่ 6 คนนั่นแหละ มันก็ไม่มีคนกลางถือ Public Ledger ให้หรอก แล้วจะฝากไว้ที่ไหนได้ล่ะ? ... ดังนั้นไม่ต้องแปลกใจ จะเป็นแบบไหนไปไม่ได้เลยนอกจาก **ทุกคนจะต้องถือไว้คนละถือปี่จ่า**



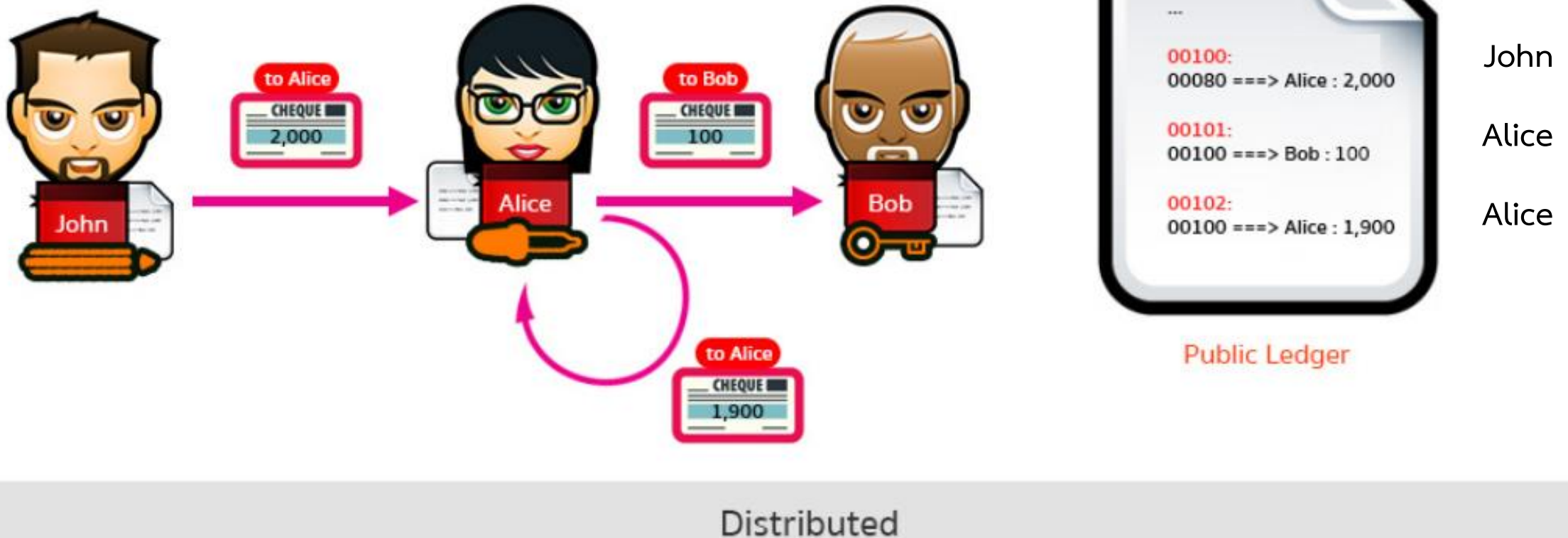
https://nuuneoi.com/blog/blog.php?read_id=900



https://nuuneoi.com/blog/blog.php?read_id=900

การส่งเงินผ่านการเขียนเช็ค

เมื่อ John ส่งเงินผ่านการเขียนเช็คให้ Alice ทุกคนจะรู้ว่า Alice มี Cheque ราคา ๒,๐๐๐ บาทที่ใช้งานได้ อยู่นะ และจะมีแค่ Alice คนเดียวที่ใช้งานมันได้เพราะการที่เช็คเขียนว่า "To Alice" นั่นคือการบอกว่า "คนที่ถือกุญแจของสมุด Alice เท่านั้นที่มีสิทธิ์ใช้งาน Cheque ใบนี้ได้" ซึ่งก็มีแค่เจ้าของสมุดบัญชี Alice คนเดียวที่ถือไว้ ก็เป็นไปตามนี้ครับ



บล็อกเชนคืออะไร

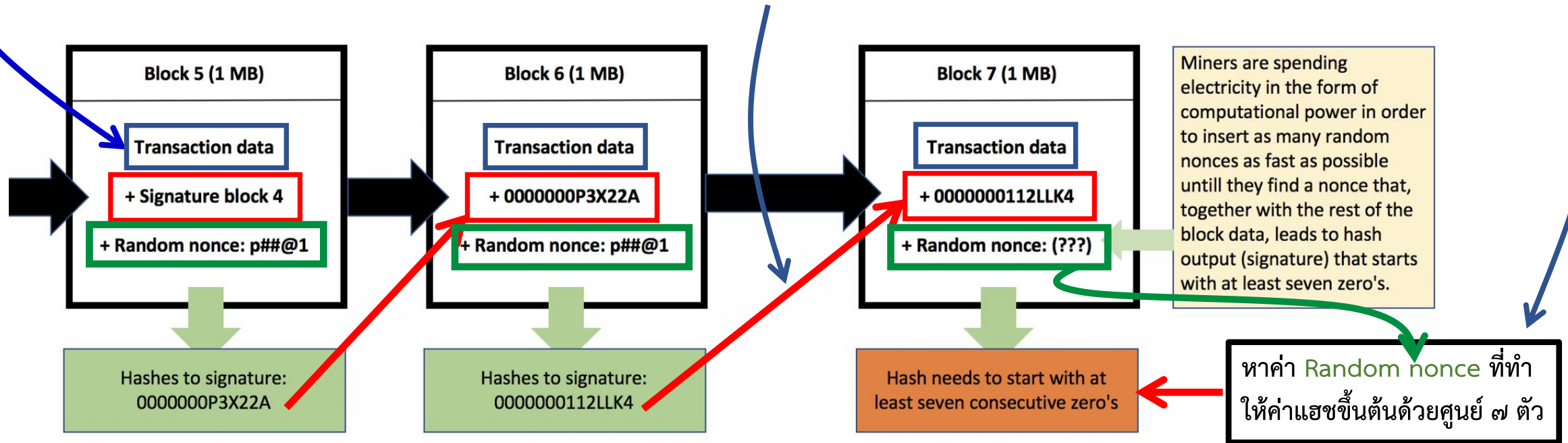
- เทคโนโลยีการจัดเก็บข้อมูลแบบ Shared Database หรือที่รู้จักกันในชื่อ Distributed Ledger Technology (DLT) โดยเป็นรูปแบบการบันทึกข้อมูลที่รับประกันความปลอดภัย ว่าข้อมูลที่บันทึกไปก่อนหน้านี้ไม่สามารถที่จะแก้ไขหรือเปลี่ยนแปลงได้ ซึ่งผู้ใช้งานทุกคนจะได้เห็นข้อมูลชุดเดียวกันทั้งหมด โดยใช้หลักการ Cryptography และความสามารถของ Distributed Computing เพื่อสร้างกลไกความน่าเชื่อถือ
(<https://www.tfac.or.th/Article/Detail/135089>)
- รูปแบบการเก็บข้อมูล (Ledger) แบบหนึ่งของระบบที่ไม่มีศูนย์กลางแต่เชื่อถือได้โง่งยาก
(https://nuuneoi.com/blog/blog.php?read_id=900)
- เทคโนโลยีที่ใช้ในการทำธุรกรรมโดยไม่ต้องผ่านบุคคลที่สามหรือไม่ต้องผ่านคนกลาง
(<https://siambc.com/what-is-blockchain>)

บล็อกเชนคืออะไร

- ต้นแฮช (Hash) หรือที่รู้จักกันในชื่อ Merkle Tree โครงสร้างข้อมูลนี้ได้รับการจดสิทธิบัตรโดย Ralph Merkle ในปีค.ศ. ๑๙๗๙ และถูกนำมาประยุกต์เพื่อตรวจสอบและจัดการข้อมูลระหว่างระบบคอมพิวเตอร์ ในเครือข่ายคอมพิวเตอร์แบบเพียร์ทูเพียร์ Peer-to-Peer (P2P)
(<https://bitblockthai.com/about-blockchain>)
- การเก็บข้อมูลแบบหนึ่งที่เก็บเป็นส่วนๆ และนำมาร้อยต่อกันเรื่อยๆ เหมือนโซ่คล้องกัน (Chain) โดยมีวิธีเข้ารหัสทางคอมพิวเตอร์เพื่อความปลอดภัย ที่ทำให้รู้ว่าข้อมูลถูกเก็บ ณ เวลาใด มีการแก้ไขหรือเปล่า โดยข้อมูลทั้งหมดจะส่งและกระจายเก็บไว้ในคอมพิวเตอร์ทุกเครื่องที่อยู่ในเครือข่าย
(<https://www.efinancethai.com/MoneyStrategist/MoneyStrategistMain.aspx?id=ZHNzbVhubGcyeU09>)
- ระบบที่ทำให้การโอนบิทคอยน์เกิดขึ้นได้ ไม่เหมือนกับสกุลเงินทั่วไปอย่างเช่น ดอลลาร์ หรือ ยูโร ที่สามารถเก็บและใช้ได้แบบรูปธรรม แต่บิทคอยน์นั้นเป็นเงินดิจิทัลที่อยู่ในโลกดิจิทัลและถูกเก็บอยู่ในบัญชีที่มีการกระจายศูนย์ที่เรียกว่า "บล็อกเชน"
(<https://support.bitkub.com/hc/th/articles/360004165832>)

๔ ขั้นตอนการทำงานของบล็อกเชน

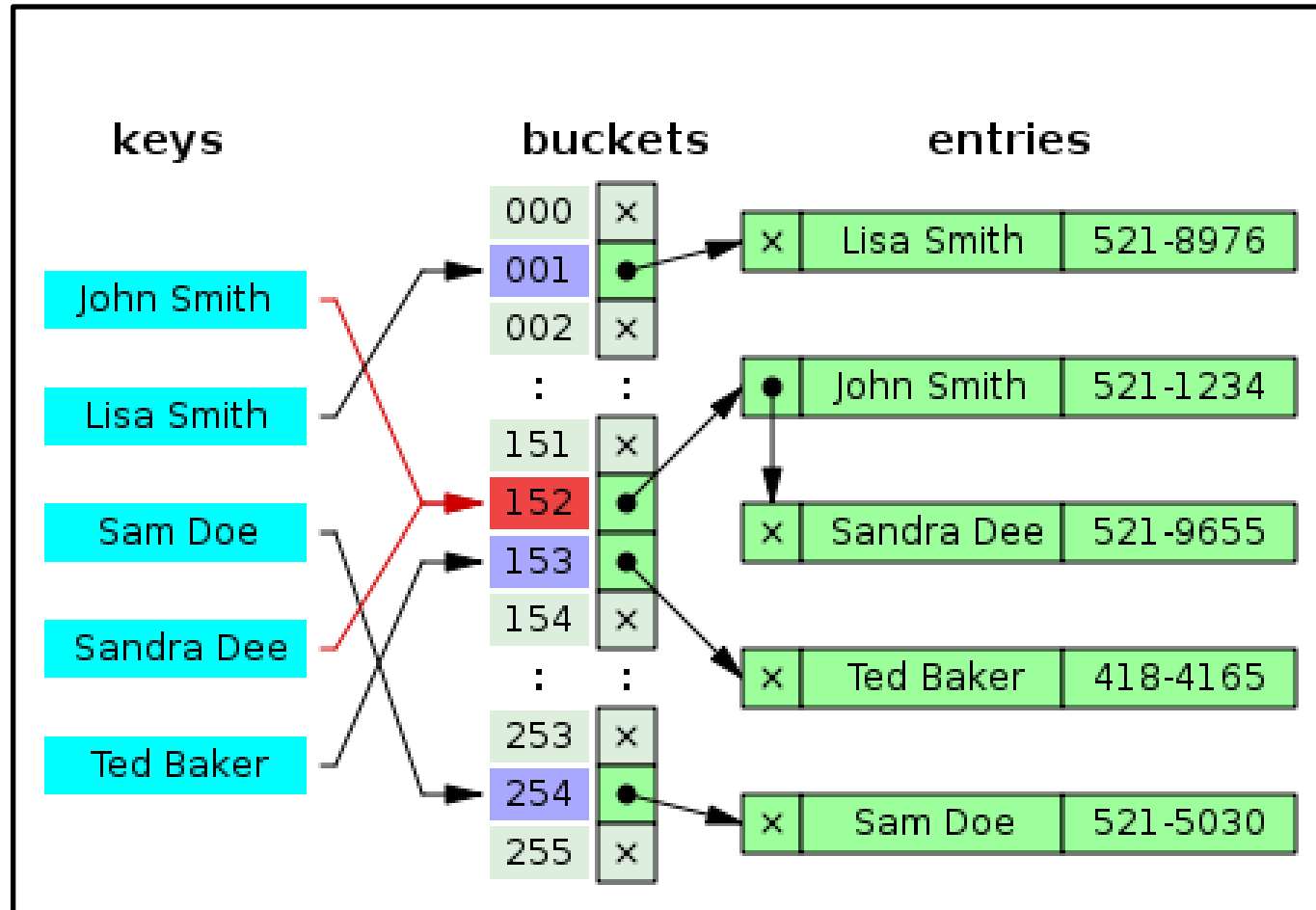
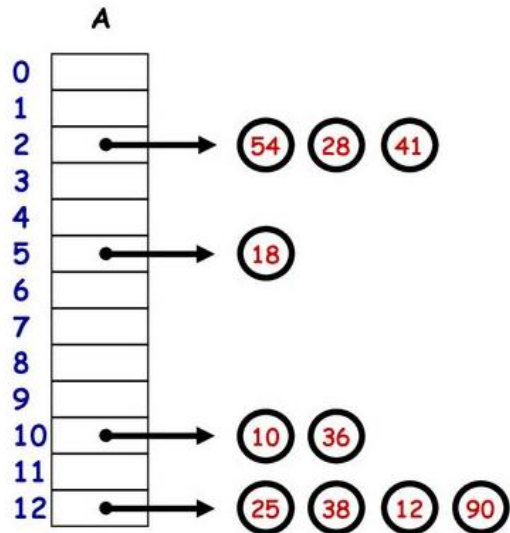
๑. สร้าง**บล็อกข้อมูล**ทรานแซคชั่น (Transaction data)
๒. เผยแพร่ข้อมูลที่เข้ารหัสสู่เครือข่าย (Broadcasting in the network) เพื่อหา**นักขุดตรวจสอบข้อมูลทรานแซคชั่น และหาค่าที่ใช้ครั้งเดียว** (Nonce)
๓. การตรวจสอบข้อมูลและการขุดหาค่าที่ใช้ครั้งเดียวมาสร้าง**ลายเซ็น/แฮช**ซึ่งมีคุณสมบัติตามกำหนด (เช่น ขึ้นต้นด้วยศูนย์ ๗ ตัว) (Finding nonce to create an eligible signature, e.g., starting with 7 zero's)
๔. การต่อบล็อกเป็นห่วงโซ่โดยใช้ค่าแฮชเป็นตัวเชื่อมโยง (Chaining the blocks with hash)



แนวคิดฟังก์ชันแฮชอย่างง่าย (Concepts of Simple Hash Table)

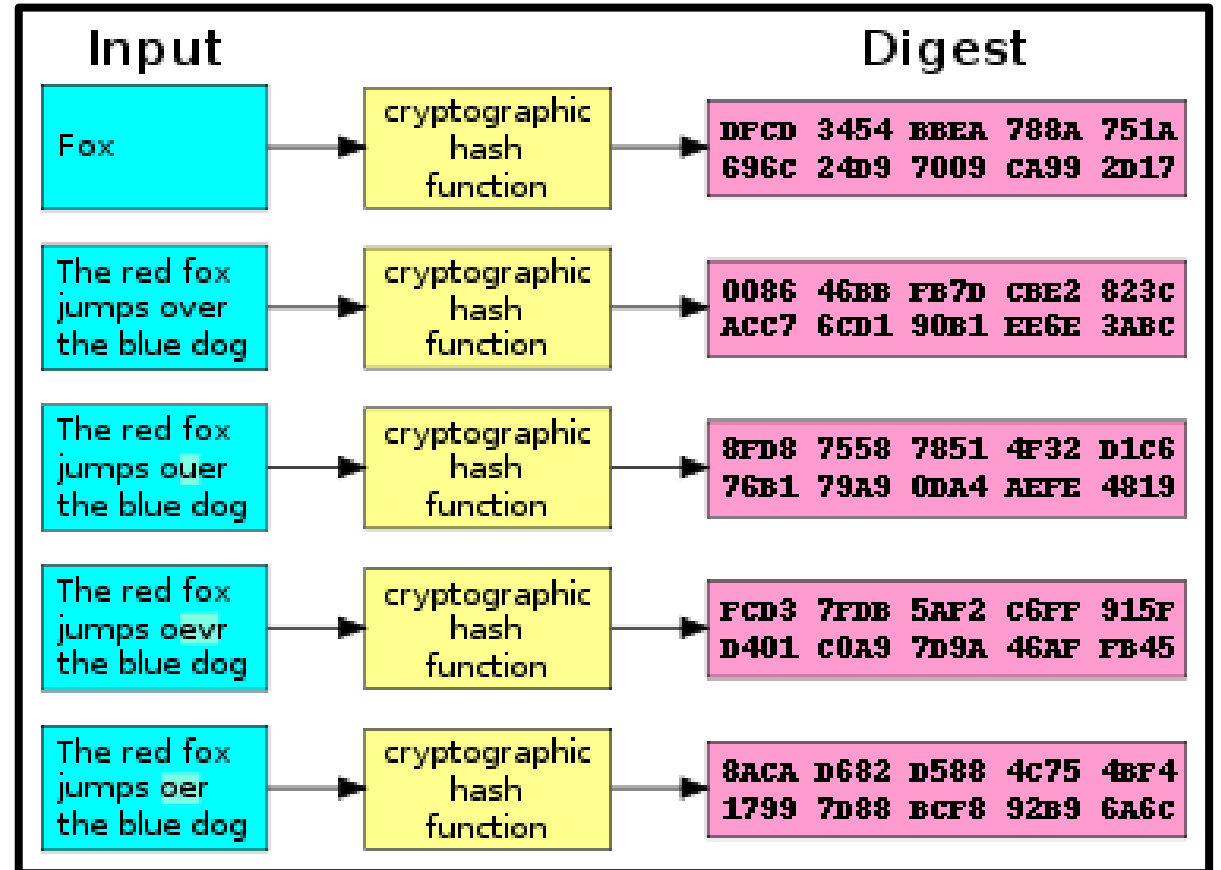
A Hash Table with Chaining

A hash table with size $m = 13$,
 $h(k) = k \bmod 13$,
Store keys: 18, 41, 90, 12, 36, 28, 54, 38, 25, 10



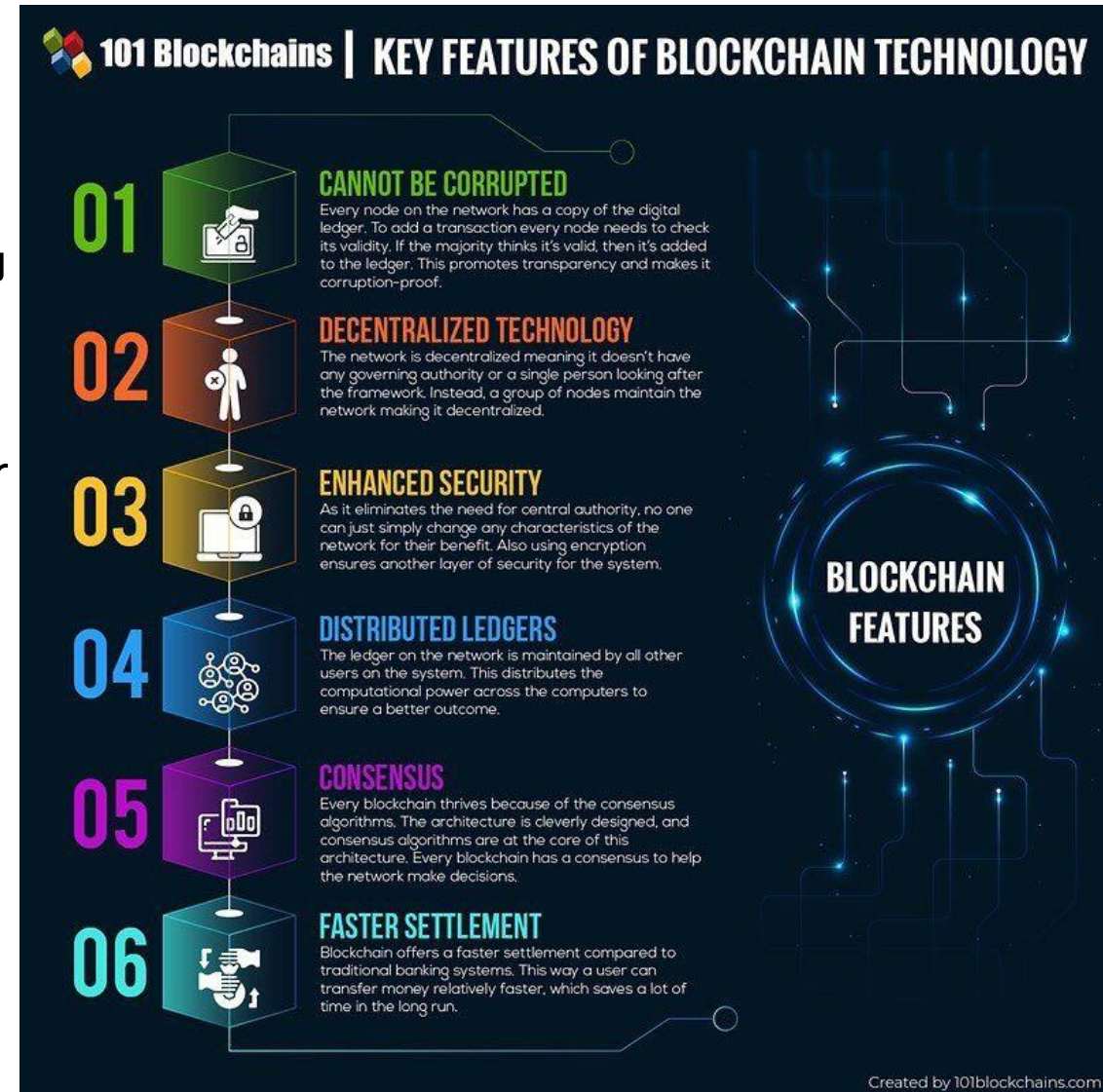
ฟังก์ชันแฮชเข้ารหัส (Cryptographic hash function)

- กลุ่มของฟังก์ชันแฮชที่มีคุณสมบัติพิเศษที่ทำให้เหมาะกับการประยุกต์ใช้ในวิทยาการเข้ารหัสลับ
- ฟังก์ชันแฮชเชิงรหัสลับเป็นขั้นตอนวิธีทางคณิตศาสตร์ที่แปลงข้อมูลที่มีขนาดต่าง ๆ ให้เป็นสตริงฐานสองที่มีขนาดคงที่ เรียกว่า ค่าแฮช และมักถูกออกแบบให้เป็นฟังก์ชันทางเดียว
- นั่นคือฟังก์ชันที่ไม่สามารถหาค่าย้อนกลับได้ วิธีการเดียวในการสร้างข้อมูลนำเข้กลับมาจากฟังก์ชันแฮชเชิงรหัสลับในอุดมคติคือการค้นหารูปแบบที่เป็นไปได้ทั้งหมด (brute-force search) ของข้อมูลนำเข้เพื่อตรวจสอบว่าค่าใดให้ผลลัพธ์ที่ตรงกับค่าที่ต้องการ หรือใช้ตารางรุ้ง (rainbow table) ของค่าแฮชที่มีการคำนวณไว้ก่อนแล้ว



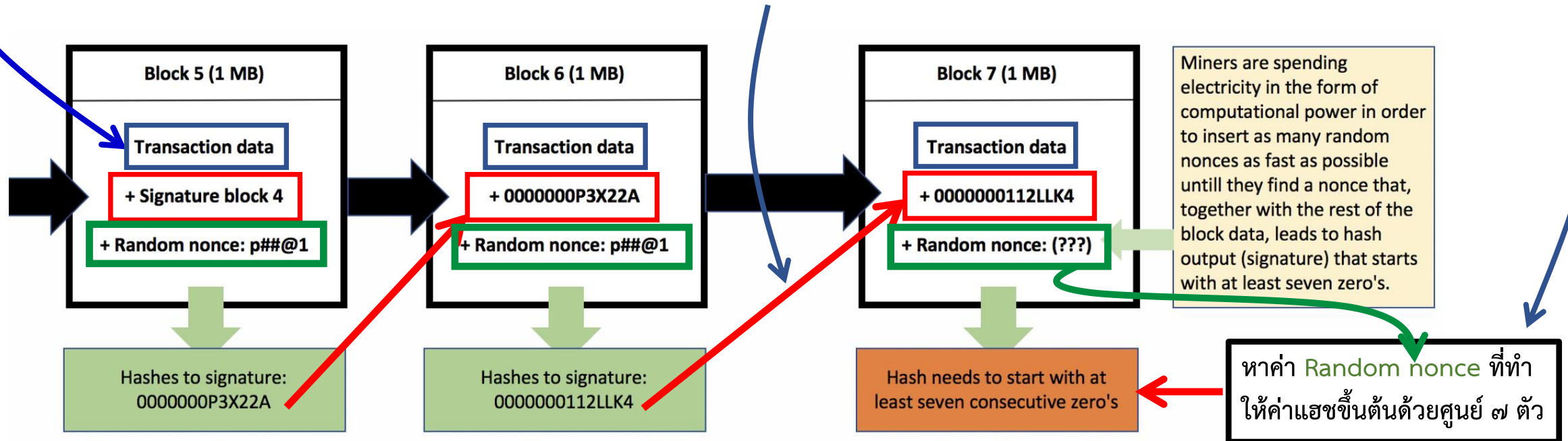
ลักษณะของบล็อกเชน

- ความไม่เปลี่ยนแปลง (Immutability)
 - การเก็บข้อมูลอย่างถาวรเขียนข้อมูลเพิ่มอย่างเดียวไม่มีการลบ
- การกระจายอำนาจ (Decentralized)
 - ไม่มีคนกลาง ไม่มีใครเป็นเจ้าของข้อมูล สำเนา Peer-to-Peer
 - การขยายความปลอดภัย (Enhanced Security)
 - บัญชีแยกประเภทแบบกระจาย (Distributed Ledgers)
- ฉันทามติ (Consensus)
 - การพิสูจน์ด้วยการทำงาน (Proof of Work – PoW)
 - การพิสูจน์ว่ามีส่วนได้ส่วนเสีย (Proof of Stake – PoS)
- การชำระบัญชีที่เร็วขึ้น (Faster Settlement)
 - การสรุปการรับจ่ายเงินได้ทันที



๔ ขั้นตอนการทำงานของบล็อกเชน

๑. สร้าง**บล็อกข้อมูล**ทรานแซคชั่น (Transaction data)
๒. เผยแพร่ข้อมูลที่เข้ารหัสสู่เครือข่าย (Broadcasting in the network) เพื่อหา**นักขุดตรวจสอบข้อมูลทรานแซคชั่น และหาค่าที่ใช้ครั้งเดียว** (Nonce)
๓. การตรวจสอบข้อมูลและการขุดหาค่าที่ใช้ครั้งเดียวมาสร้าง**ลายเซ็น/แฮช**ซึ่งมีคุณสมบัติตามกำหนด (เช่น ขึ้นต้นด้วยศูนย์ ๗ ตัว) (Finding nonce to create an eligible signature, e.g., starting with 7 zero's)
๔. การต่อบล็อกเป็นห่วงโซ่โดยใช้ค่าแฮชเป็นตัวเชื่อมโยง (Chaining the blocks with hash)



ฉันทามติ (Consensus)

- การพิสูจน์ด้วยการทำงาน (Proof of Work – PoW)
 - บิทคอยน์ (Bitcoin)
- การพิสูจน์ด้วยการมีส่วนได้ส่วนเสีย (Proof of Stake – PoS)
 - อีเธอร์เลียม (Ethereum) ตั้งแต่ ธค. 2563
- PoW และ PoS แตกต่างกันในกระบวนการตรวจสอบบล็อกและการเลือกผู้ตรวจสอบหรือนักขุด
 - ระบบ PoW เลือกผู้ตรวจสอบจากผู้ใช้ที่แก้สมการทางคณิตศาสตร์เร็วที่สุดในระบบ
 - ส่วน PoS จะสุ่มเลือกผู้ตรวจสอบจากเหรียญที่วางค้ำประกันไว้
- อย่างไรก็ตาม ผลเสียที่อาจตามมาในทั้งสองระบบคือการรวมศูนย์อำนาจเมื่อเวลาล่วงผ่านไป
 - โดยนักขุดอาจรวมตัวกันสร้าง Mining Pool ในระบบ PoW เพื่อแบ่งรางวัลกัน หรือ
 - ผู้ตรวจสอบอาจถูกสุ่มเลือกซ้ำในระบบ PoS เมื่อวางสินทรัพย์ค้ำไว้ไว้นานมาก และมีประวัติการทำงานที่ดีอย่างต่อเนื่อง

<https://www.bitkub.com/blog/proof-of-work-proof-of-stake-2a5ed294dca3>

The infographic is titled "Blockgeeks" and compares "Proof of Work" (PoW) and "Proof of Stake" (PoS). It is divided into two columns. The PoW column features a blue miner icon, a pickaxe, and two red carts filled with coal. The PoS column features a red person icon and a grey tablet with a circular interface. Text descriptions explain the processes: PoW requires solving a difficult puzzle, while PoS chooses a block creator based on stake. It also details the requirements for adding a malicious block: PoW requires more than 51% of the network's computing power, while PoS requires owning 51% of the cryptocurrency. Finally, it notes that PoW rewards the first miner to solve the puzzle, while PoS has no reward for block creation, relying on transaction fees.

Blockgeeks

Proof of Work vs. **Proof of Stake**

To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.

There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

The first miner to solve the puzzle is given a reward for their work.

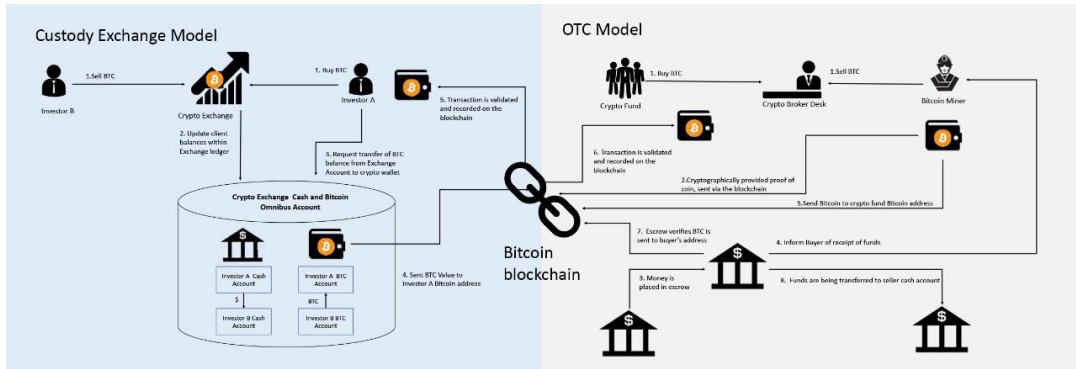
There is no reward for making a block, so the block creator takes a transaction fee.

<https://i.redd.it/0dpjppjqr6a71.jpg>

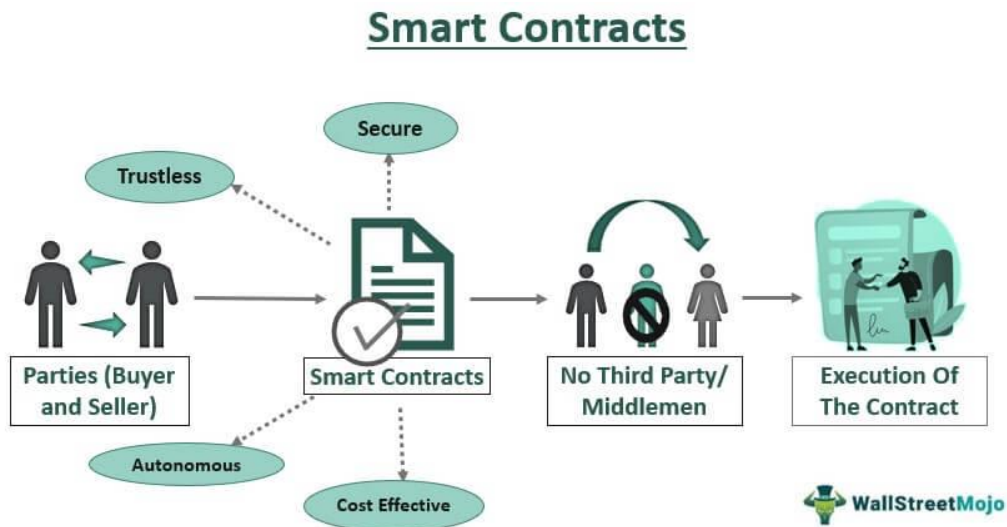
https://www.reddit.com/r/ethtrader/comments/ogv6hb/a_concise_way_of_explaining_pos_vs_pow_for_all/

การประยุกต์ใช้งาน สองอย่าง ที่สำคัญของบล็อกเชน

เงินดิจิทัลหรือคริปโทเคอร์เรนซี (Cryptocurrency)



สัญญาอัจฉริยะหรือสมาร์ตคอนแทร็กต์ (Smart Contract)



Traditional contracts	Smart contracts
1-3 Days	Minutes
Manual remittance	Automatic remittance
Escrow necessary	Escrow may not be necessary
Expensive	Fraction of the cost
Physical presence (wet signature)	Virtual presence (digital signature)
Lawyers necessary	Lawyers may not be necessary

กำเนิดเงินดิจิทัลสกุลแรก – บิทคอยน์ Bitcoin

- เริ่มต้นจากในเดือนตุลาคม ๒๕๕๑ (2008) Nakamoto ได้ทำการส่งบทความไปยัง metzdowd.com อธิบายเกี่ยวกับ bitcoin digital currency โดยมีหัวข้อว่า “Bitcoin: A Peer-to-Peer Electronic Cash System”
- หลังจากนั้นในเดือนมกราคม ๒๕๕๒ (2009) ทาง Nakamoto ได้ทำการปล่อยตัวซอฟต์แวร์เวอร์ชันแรก โดยได้เริ่มสร้างหน่วยหรือยูนิตแรกของบิทคอยน์ ในรูปแบบของคริปโตเคอร์เรนซี (cryptocurrency) และได้ปล่อยไปยัง เว็บไซต์ที่เก็บซอฟต์แวร์โอเพนซอร์ซ ชื่อตั้ง sourceforge.net ในวันที่ ๙ มกราคม ๒๕๕๒
- Nakamoto บอกว่าเขาได้เริ่มพัฒนาโค้ดของบิทคอยน์ในปี ๒๕๕๐ (2007) ซึ่งการออกแบบตั้งแต่ตอนแรกนั้นเขาได้ออกแบบให้มีการรองรับประเภทของธุรกรรมได้หลากหลายรูปแบบ ซึ่งถ้าในแต่ละประเภทต้องใช้โค้ดหรือฟิลด์ข้อมูลที่แตกต่างกันจะเป็นปัญหามาก เขาจึงแก้ไขโดยการใช้ script หรือที่นักคณิตศาสตร์เรียกว่า predicate (function) โดยมองว่าทรานซัคชันที่เข้ามาเพื่อตรวจสอบเป็นเสมือน predicate ที่ต้องตรวจสอบแทน

กำเนิดเงินดิจิทัลสกุลแรก – บิทคอยน์ Bitcoin

- โดย Nakamoto นั้นได้ทิ้งข้อความที่สำคัญไว้ใน block แรกของ bitcoin คือ “The Times 3 January 2009 Chancellor on brink of bailout for the bank” จึงเป็นหลักฐานชิ้นสำคัญว่า block แรกของ bitcoin นั้นมีการถือกำเนิดขึ้นใน วันที่ ๓ มกราคม ๒๕๕๒ ๑๘:๑๕:๐๕ GMT
- block แรกนี้ถือเป็น block ประวัติศาสตร์ของ bitcoin เพราะจะไม่เหมือนกับ block อื่น ๆ ที่ create ตามมาภายหลังจนถึงปัจจุบัน เพราะ เป็น block เดียวที่ไม่มี References อ้างไปถึง block ก่อนหน้า ซึ่งหลังจากนั้นก็ได้เริ่มมีการทดสอบ transaction ตั้งแต่ในช่วงกลางเดือนมกราคม ๒๕๖๒ และก็เริ่มมีคนมาสร้างเหมืองทำ bitcoin ต่อมาจบจนถึงปัจจุบัน
- ซึ่งจากข้อมูลที่เปิดเผยของ transaction log ที่เป็น address ของ Nakamoto นั้นประเมินว่าเขามีปริมาณ bitcoins อยู่ที่ ๑ ล้าน bitcoins ซึ่ง ณ วันที่ ๑๗ ธันวาคม ๒๕๖๐ ที่ราคาขึ้นไปแตะจุดสูงสุดของ bitcoin นั้นทำให้เขามีทรัพย์สินเป็นมูลค่ากว่า ๑๙,๐๐๐ ล้านเหรียญสหรัฐ ซึ่งทำให้เขากลายเป็นบุคคลที่รวยเป็นอันดับที่ ๔๔ ของโลกโดยทันที
- ฟังก์ชันการแฮชที่ใช้ในบล็อกเชน Bitcoin คืออัลกอริธึมแฮช SHA-256

บิทคอยน์ (Bitcoin) คืออะไร

Centralized Money Issues

Wells Fargo uncovers up to 1.4 million more fake accounts

by Matt Egan @MattEganCNN
August 31, 2017: 12:34 PM ET



US Congress clears \$700 billion bailout package

October 04, 2008 17:56 IST

India Abolishes 500 and 1,000 Rupee Notes to Fight Corruption

By Rajesh Kumar Singh and Iain Marlow
November 8, 2016, 4:59 PM GMT+2 Updated on November 9, 2016, 7:49 AM GMT+2



18 AUGUST 2008
31 OCTOBER 2008



What is Bitcoin? Bitcoin Explained Simply for Dummies
Apr 4, 2018

https://www.youtube.com/watch?v=41JCpzvnn_0

จดหมายส่งมอบรหัสต้นฉบับ (Source code) – ๑๗ มิถุนายน ๒๕๕๓

- หลังจากนั้นนาคะโมโตะได้ทำการสร้างเว็บไซต์ bitcoin.org ได้เริ่มหาความร่วมมือจากนักพัฒนาคนอื่นๆ
- จนกระทั่งกลางปี ๒๕๕๓ เขาได้เริ่มส่งมอบตัวรหัสต้นฉบับให้กับ Gavin Andresen และได้ทำการโอนอีกหลายส่วนที่เกี่ยวข้องกับ bitcoin ไปยังสมาชิกที่มีความสามารถโดดเด่นในกลุ่มของ bitcoin
- เริ่มหยุดการมีส่วนร่วมกับโครงการดังกล่าว <https://bitcointalk.org/index.php?topic=195>

satoshi
Founder
Sr. Member
Activity: 364
Merit: 3077

Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG
June 17, 2010, 06:46:08 PM
#2
Merited by ETFbitcoin (5), Bitbobb (3), BitcoinFX (1), bones261 (1), Husna QA (1), runeks (1), OWZ1337 (1)

The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime. Because of that, I wanted to design it to support every possible transaction type I could think of. The problem was, each thing required special support code and data fields whether it was used or not, and only covered one special case at a time. It would have been an explosion of special cases. The solution was script, which generalizes the problem so transacting parties can describe their transaction as a predicate that the node network evaluates. The nodes only need to understand the transaction to the extent of evaluating whether the sender's conditions are met.

The script is actually a predicate. It's just an equation that evaluates to true or false. Predicate is a long and unfamiliar word so I called it script.

The receiver of a payment does a template match on the script. Currently, receivers only accept two templates: direct payment and bitcoin address. Future versions can add templates for more transaction types and nodes running that version or higher will be able to receive them. All versions of nodes in the network can verify and process any new transactions into blocks, even though they may not know how to read them.

The design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multi-party signature, etc. If Bitcoin catches on in a big way, these are things we'll want to explore in the future, but they all had to be designed at the beginning to make sure they would be possible later.

I don't believe a second, compatible implementation of Bitcoin will ever be a good idea. So much of the design depends on all nodes getting exactly identical results in lockstep that a second implementation would be a menace to the network. The MIT license is compatible with all other licenses and commercial uses, so there is no need to rewrite it from a licensing standpoint.

การเสนอเหรียญดิจิทัลครั้งแรก (Initial Coin Offering – ICO)

- การเสนอเหรียญครั้งแรก (ICO) หรือการเสนอสกุลเงินเริ่มต้นเป็นประเภทของเงินทุนโดยใช้สกุลเงินดิจิทัล
- เป็นรูปแบบของการระดมทุน
- อย่างไรก็ตาม ICO ส่วนตัวที่ไม่แสวงหาการลงทุนจากภาครัฐก็สามารถทำได้เช่นกัน ใน ICO ปริมาณของสกุลเงินดิจิทัลจะถูกขายในรูปแบบของ "โทเคน" ("เหรียญ") ให้กับนักเก็งกำไรหรือนักลงทุน เพื่อแลกกับการประมูลทางกฎหมายหรือสกุลเงินดิจิทัลอื่น ๆ เช่น Bitcoin หรือ Ether โทเคนจะได้รับการส่งเสริมให้เป็นหน่วยสกุลเงินที่ใช้งานได้ในอนาคตหากหรือเมื่อบรรลุเป้าหมายการระดมทุนของ ICO และโครงการประสบความสำเร็จในการเปิดตัว
- ICO สามารถเป็นแหล่งเงินทุนสำหรับบริษัทสตาร์ทอัพ ICO สามารถอนุญาตให้สตาร์ทอัพหลีกเลี่ยงกฎระเบียบที่ขัดขวางไม่ให้พวกเขาแสวงหาการลงทุนโดยตรงจากสาธารณะ และตัวกลาง เช่น ผู้ร่วมทุน ธนาคาร และตลาดหลักทรัพย์ ซึ่งอาจต้องการการตรวจสอบอย่างละเอียดมากขึ้น และเปอร์เซ็นต์ของผลกำไรในอนาคตหรือการเป็นเจ้าของร่วมบางส่วน
- ICO อาจอยู่นอกเหนือกฎระเบียบที่มีอยู่ ขึ้นอยู่กับลักษณะของโครงการ หรือถูกแบนโดยสิ้นเชิงในเขตอำนาจศาลบางแห่ง เช่น จีนและเกาหลีใต้
- เนื่องจากขาดกฎระเบียบและการบังคับใช้กฎหมายหลักทรัพย์ ICO จึงเป็นเครื่องมือในการหลอกลวงและการฉ้อโกง น้อยกว่าครึ่งหนึ่งของ ICO ทั้งหมดอยู่รอดได้สี่เดือนหลังจากการเสนอ ในขณะที่เกือบครึ่งหนึ่งของ ICO ที่ขายในปี ๒๕๖๐ ล้มเหลวในเดือนกุมภาพันธ์ ๒๕๖๑ แม้จะมีบันทึกความล้มเหลวและราคาที่ลดลงของ cryptocurrencies มีการบันทึก ๗ พันล้านดอลลาร์ผ่าน ICO ตั้งแต่มกราคม-มิถุนายน ๒๕๖๑

ภาษาที่ใช้ในการออกเหรียญ

- Solidity Programming Language (soliditylang.org)

โปรแกรมซอลิติตีสร้างเงินดิจิทัล

```
pragma solidity ^0.4.18;
contract HelloCoin {

string public name = 'HelloCoin'; // currency name. Please feel free to change it
string public symbol = 'hc';      // choose a currency symbol. Please feel free to change it
mapping (address => uint) balances; // a key-value pair to store addresses and their account balances
event Transfer(address _from, address _to, uint256 _value);
    // declaration of an event. Event will not do anything but add a record to the log

constructor() public { //when the contract is created, the constructor will be called automatically
    balances[msg.sender] = 10000; //set the balances of creator account to be 10000. change it to your
    need.
}

function sendCoin(address _receiver, uint _amount)
    public returns(bool sufficient) {
    if (balances[msg.sender] < _amount) return false; // validate transfer
    balances[msg.sender] -= _amount;
    balances[_receiver] += _amount;
    emit Transfer(msg.sender, _receiver, _amount);
// complete coin transfer and call event to record the log
    return true;}

function getBalance(address _addr) public view returns(uint) { //balance check
    return balances[_addr];}}
```

1	LLL
2	Vyper
3	Simplicity
4	Varna
5	Obsidian
6	Solidity
7	WASM
8	Rholang
9	Michelson
10	Plutus
11	Sophia
12	JSON
13-15	Swift, PHP, or Kotlin
16-18	Lua, Laravel, or Ruby
19	JavaScript
20	Containers
21	C#
22	SQL

ซอลิดิตี (Solidity): ภาษาที่ใช้ในการเขียนสัญญาอัจฉริยะ

- ภาษาโปรแกรมในการเขียนโปรแกรมเชิงวัตถุสำหรับการเขียนสัญญาอัจฉริยะ ซึ่งได้ถูกนำมาใช้ในการสร้างและจัดการทำสัญญาอัจฉริยะ
- ในหลายแพลตฟอร์มบล็อกเชน โดยส่วนใหญ่จะเป็นอีเธอร์เรียม
- ซอลิดิตีพัฒนาโดย คริสเตียน ไรต์วิสเนอร์ (Reitwiessner) และ แอเล็กซ์ แบเรจส์ซัสซี (Alex Beregszaszi) พร้อมกับนักพัฒนาอีเธอร์เรียม
- ตัวโปรแกรมคอมไพล์และทำงานบนเครื่องจักรเสมือนของอีเธอร์เรียม

การเขียนโปรแกรมซอลิดิตี (Solidity) เพื่อสัญญาอัจฉริยะ

Introduction to Solidity

- Solidity is an Ethereum smart contract language



การเสนอเหรียญดิจิทัลครั้งแรก Initial Coin Offering - ICO

<https://www.sec.or.th/th/pages/lawandregulations/initialcoinoffering.aspx>

- พระราชกำหนด (พ.ร.ก.) การประกอบธุรกิจสินทรัพย์ดิจิทัล
 - การระดมทุนแบบดิจิทัลด้วยการเสนอขายโทเคนดิจิทัลผ่านระบบบล็อกเชนต่อสาธารณชน (พ.ศ. ๒๕๖๑)
 - ผู้ระดมทุนต้องเป็น บจก. บมจ.
 - ผู้ระดมทุนต้องได้รับอนุญาตจาก ก.ล.ต.
 - ขายผ่าน ICO portal ที่ได้รับความเห็นชอบจาก ก.ล.ต.
 - มีหนังสือชี้ชวน
 - รับคริปโทเคอร์เรนซีจากธุรกิจสินทรัพย์ดิจิทัลที่ได้รับอนุญาต
 - ผู้ลงทุนมีคุณสมบัติและวงเงินลงทุนได้ตามที่กำหนด
 - การเสนอขายโทเคนดิจิทัลทุกกรณีหลัง พ.ร.ก.
 - มีผลบังคับใช้ ต้องมายื่นขออนุญาตกับ ก.ล.ต.
 - และหาให้มีโทเคนดิจิทัลมีการซื้อขายเปลี่ยนมือต้องมาผ่านศูนย์ซื้อขายทรัพย์สินดิจิทัลที่ได้รับอนุญาต

The Securities and Exchange Commission, Thailand

รู้จัก พ.ร.ก. การประกอบธุรกิจสินทรัพย์ดิจิทัล



การระดมทุนด้วยการเสนอขายโทเคนดิจิทัลต่อประชาชน



- ผู้ระดมทุนต้องเป็น บจก. บมจ.
- ผู้ระดมทุนต้องได้รับอนุญาตจาก ก.ล.ต.
- ขายผ่าน ICO portal ที่ได้รับความเห็นชอบจาก ก.ล.ต.
- มีหนังสือชี้ชวน
- รับคริปโทเคอร์เรนซีจากธุรกิจสินทรัพย์ดิจิทัลที่ได้รับอนุญาต
- ผู้ลงทุนมีคุณสมบัติและวงเงินลงทุนได้ตามที่กำหนด



การเสนอขายโทเคนดิจิทัลทุกกรณีหลัง พ.ร.ก.
มีผลบังคับใช้ ต้องมายื่นขออนุญาตกับ ก.ล.ต.
และหากจะให้โทเคนดิจิทัลมีการซื้อขาย
เปลี่ยนมือต้องทำผ่านศูนย์ซื้อขาย
สินทรัพย์ดิจิทัลที่ได้รับอนุญาต



ไม่มีผลบังคับกับผู้ระดมทุน

ศึกษาข้อมูลเพิ่มเติม www.sec.or.th 1207 info@sec.or.th

จัดทำเมื่อ พฤษภาคม 2561

สกุลเงินคริปโตเรียงตามมูลค่าราคาตลาด ๒๐ สกุลแรก



ชื่อ	สัญลักษณ์	มูลค่าตามราคาตลาด	ราคา
Bitcoin	BTC	฿29,605,495,991,683	฿1,574,696.60
Ethereum	ETH	฿12,195,311,862,009	฿103,963.30
Cardano	ADA	฿3,019,747,546,003	฿93.94
Binance Coin	BNB	฿2,655,095,194,226	฿15,791.26
Tether	USDT	฿2,132,392,127,293	฿32.56
Ripple XRP	XRP	฿1,722,281,743,104	฿37.03
Dogecoin	DOGE	฿1,194,359,244,962	฿9.11
USD Coin	USDC	฿884,916,305,207	฿32.54
Solana	SOL	฿880,991,676,882	฿3,028.04
Polkadot	DOT	฿830,283,644,137	฿840.73
Uniswap	UNI	฿528,286,079,266	฿863.75
Terra	LUNA	฿455,252,784,142	฿1,129.60
Bitcoin Cash	BCH	฿404,937,057,853	฿21,503.55
Binance USD	BUSD	฿396,189,771,485	฿32.54
Litecoin	LTC	฿383,097,149,074	฿5,739.06
Chainlink	LINK	฿373,750,492,782	฿834.25
Internet Computer	ICP	฿353,341,957,649	฿2,248.58
Wrapped Bitcoin	WBTC	฿311,350,045,251	฿1,574,274.86
Polygon	MATIC	฿300,348,736,035	฿46.37
Avalanche	AVAX	฿271,178,851,852	฿1,553.55

Survive Rate only 10% ๓๐ สิงหาคม ๒๕๖๔

สกุลเงินคริปโต: 11,468
 กระดานซื้อขาย: 397
 มูลค่าตามราคาตลาด: ฿67,934,288,495,620
 ปริมาณ 24 ชม.: ฿3,034,845,267,749
 Dominance:
 BTC: 43.8%
 ETH: 18.0%
 ETH Gas: 97 Gwei
 Bitcoin blockchain size from 01/2009 to 15/8/2021
 349.15 G bytes

บิตคอยน์ ๒๑ ล้านถูกขุดออกมาแล้ว ๑๗ ล้านเหรียญ

Bitcoin whale

มีคนเพียง ๑,๐๐๐ คนเท่านั้นที่ถึง ๔๐% ของมูลค่าบิตคอยน์ (คนเหล่านี้ เรียกว่า ปลาวาฬ) จำนวน Wallet ของ Bitcoin ที่ถือมากกว่า ๑,๐๐๐ BTC (ประมาณ 200 ล้านบาท (ณ เมษายน ๒๕๖๓) เพิ่มสูงขึ้นในรอบสองปี

RANKS OF BITCOIN HOLDERS

@CryptoCrunchApp



HUMPBACK
5000 BTC



WHALE
1000 BTC



SHARK
500-1000 BTC



DOLPHIN
100-500 BTC



FISH
50-100 BTC



OCTOPUS
10-50 BTC

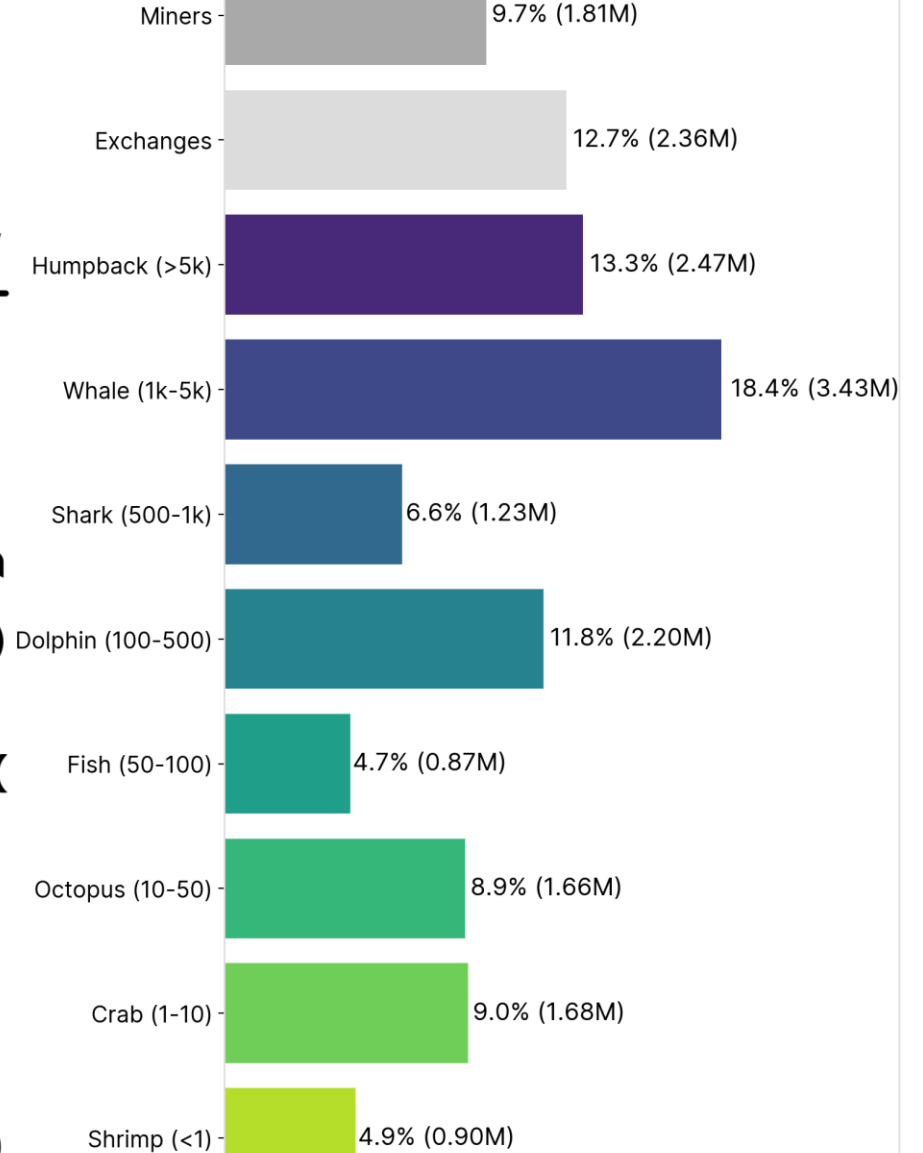


CRAB
1-10 BTC



SHRIMP
<1 BTC

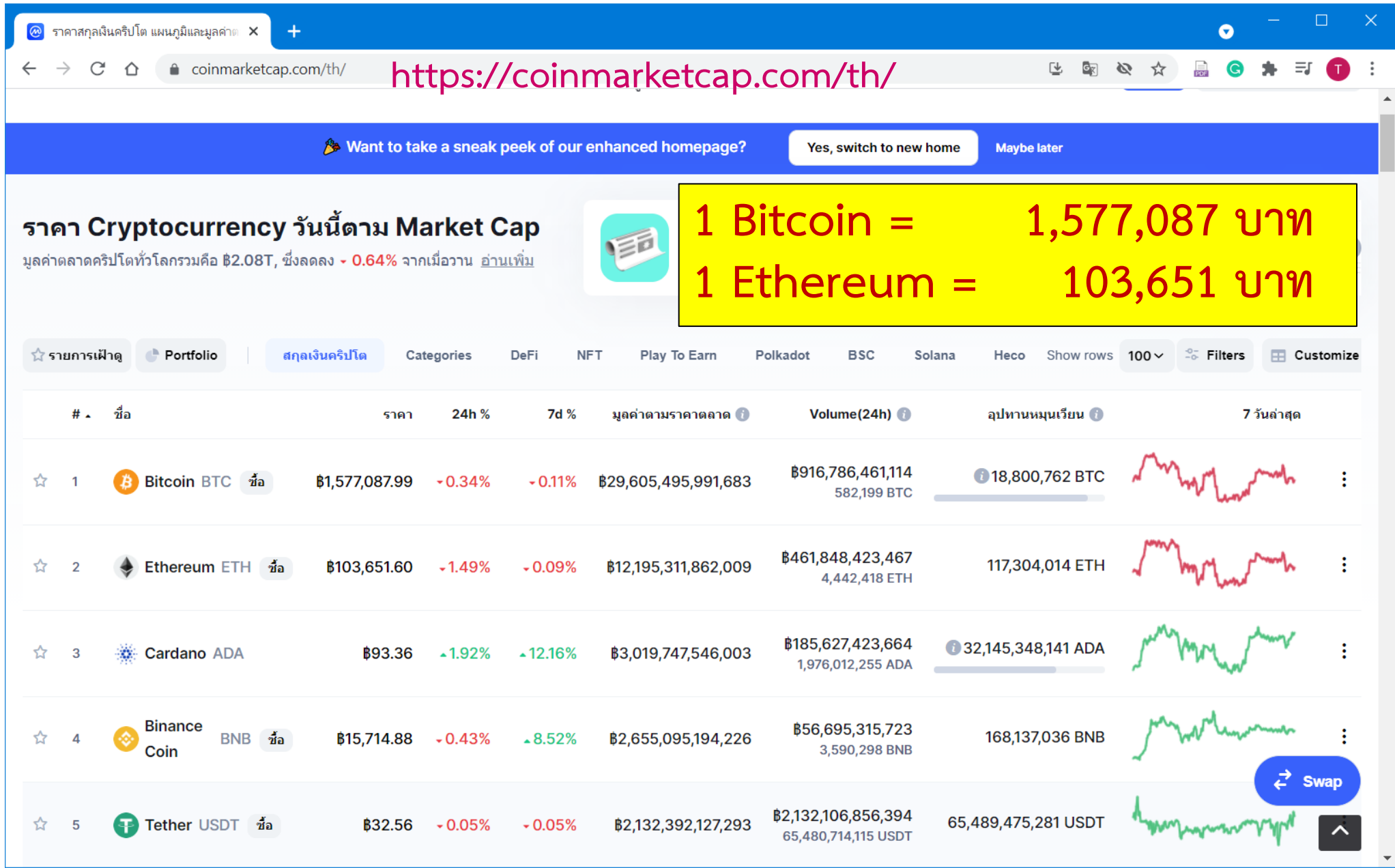
<https://insights.glassnode.com/bitcoin-supply-distribution/>



glassnode

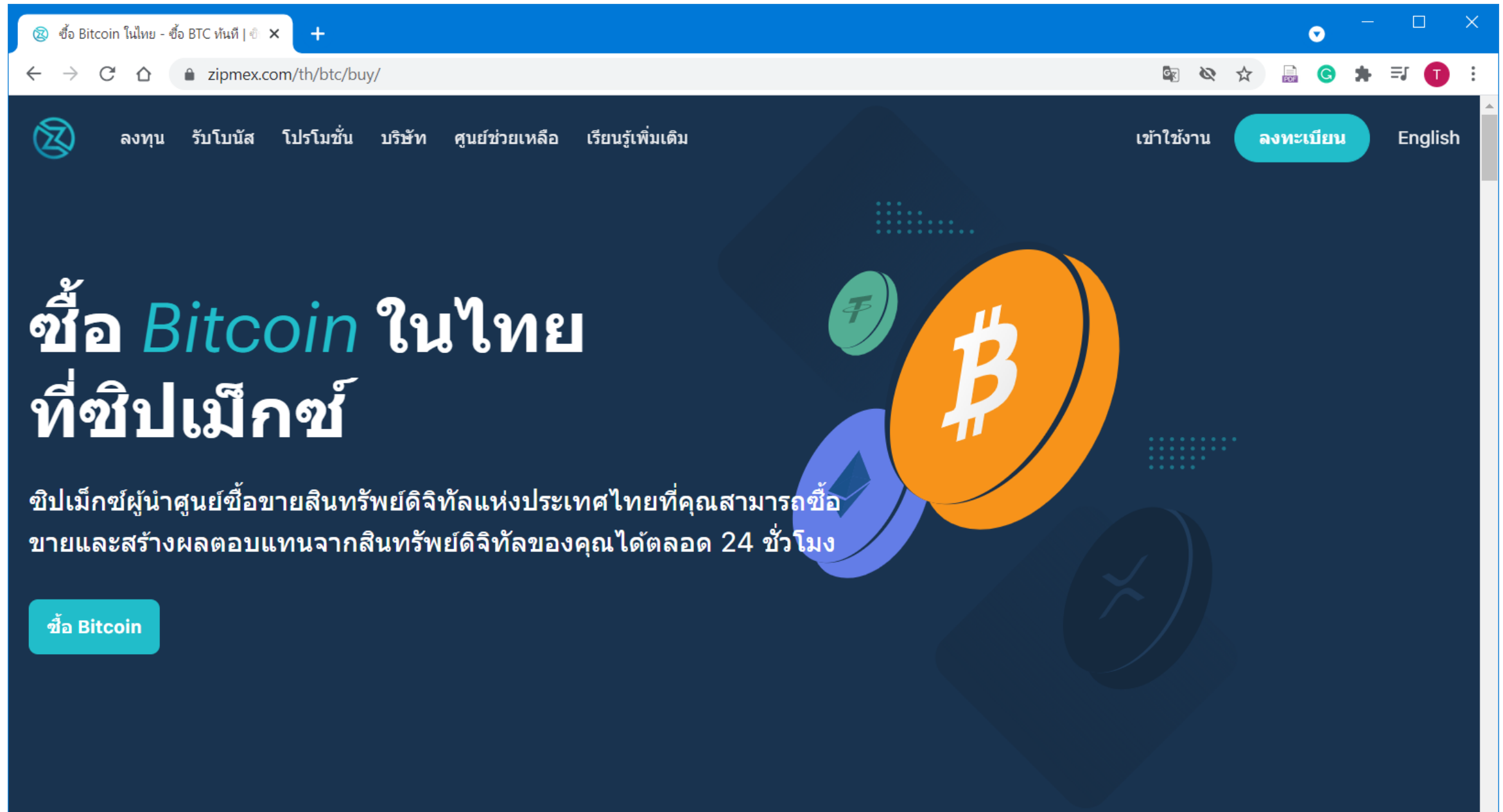
<https://www.facebook.com/cryptohindi.in/posts/visit-httpswwwcryptohindiin/125934832548950/>

ราคาเหรียญคริปโต แผนภูมิและมูลค่าตลาด (CoinMarketCap)



ซื้อบิตคอยน์ในไทย

<https://zipmex.com/th/btc/buy/>



The screenshot shows a web browser window with the URL zipmex.com/th/btc/buy/. The page features a dark blue background with several floating Bitcoin icons in orange, blue, and green. The main heading is "ซื้อ Bitcoin ในไทย ที่ชิปเม็กซ์" (Buy Bitcoin in Thailand at Zipmex). Below the heading, there is a paragraph in Thai: "ชิปเม็กซ์ผู้นำศูนย์ซื้อขายสินทรัพย์ดิจิทัลแห่งประเทศไทยที่คุณสามารถซื้อขายและสร้างผลตอบแทนจากสินทรัพย์ดิจิทัลของคุณได้ตลอด 24 ชั่วโมง" (Zipmex, the leading digital asset exchange in Thailand, where you can buy and sell digital assets and generate returns 24/7). A prominent teal button labeled "ซื้อ Bitcoin" (Buy Bitcoin) is located in the bottom left corner. The top navigation bar includes the Zipmex logo, menu items like "ลงทุน" (Invest), "รับโบนัส" (Receive Bonus), "โปรโมชั่น" (Promotion), "บริษัท" (Company), "ศูนย์ช่วยเหลือ" (Help Center), and "เรียนรู้เพิ่มเติม" (Learn More), along with "เข้าใช้งาน" (Log In) and a "ลงทะเบียน" (Sign Up) button. The language is set to "English".

ซื้อ Bitcoin ในไทย - ซื้อ BTC ทันที | [×](#)

zipmex.com/th/btc/buy/

ลงทุน รับโบนัส โปรโมชั่น บริษัท ศูนย์ช่วยเหลือ เรียนรู้เพิ่มเติม

เข้าใช้งาน [ลงทะเบียน](#) English

ซื้อ Bitcoin ในไทย ที่ชิปเม็กซ์

ชิปเม็กซ์ผู้นำศูนย์ซื้อขายสินทรัพย์ดิจิทัลแห่งประเทศไทยที่คุณสามารถซื้อขายและสร้างผลตอบแทนจากสินทรัพย์ดิจิทัลของคุณได้ตลอด 24 ชั่วโมง

[ซื้อ Bitcoin](#)

ซื้ออีเธอร์เลียมในไทย

<https://www.bitkub.com/buy-ethereum>

The screenshot shows the Bitkub website interface for buying and selling Ethereum in Thailand. The browser address bar displays "bitkub.com/buy-ethereum". The page features the Bitkub logo, navigation links for "MARKET", "EARN 20% CASHBACK", and "EN", along with "LOGIN" and "OPEN ACCOUNT" buttons. The main heading is "BUY ETHEREUM IN THAILAND", followed by a sub-heading: "Bitkub offers the easiest way to buy, sell, and store ethereum in Thailand. Convert your THB to ETH instantly!". Two large buttons are visible: "BUY ETHEREUM" and "SELL ETHEREUM". To the right, there are two panels for "BUY" and "SELL" with a price of 105199.21 ฿ and a change of -1.13% and -0.94% respectively. At the bottom, there is a section titled "HOW TO BUY ETHEREUM IN THAILAND USING BITKUB.COM" with a "Chatbox" button and a "Support" button.

ซื้อ Ethereum (ETH) ในไทยเป็นเงินบาท

bitkub MARKET EARN 20% CASHBACK EN LOGIN OPEN ACCOUNT

BUY ETHEREUM IN THAILAND

Bitkub offers the easiest way to buy, sell, and store ethereum in Thailand. Convert your THB to ETH instantly!

BUY ETHEREUM SELL ETHEREUM

BUY 105199.21 ฿ -1.13%

SELL 105199.21 ฿ -0.94%

HOW TO BUY ETHEREUM IN THAILAND USING BITKUB.COM

Chatbox Support

สกุลเงินคริปโต/เหรียญดิจิทัล สัญญาไทย (๑) ณ ๓๐ สิงหาคม ๒๕๖๔

- zCoin (XZC) : ซีคอยน์ → Firo (\$7.60)

ผู้ก่อตั้งและหัวหน้าทีมพัฒนาเหรียญเป็นคนไทย ชื่อนายปรมิินทร์ อินโสม (หนึ่ง) แต่ ZCoin ไม่ได้ระดมทุนด้วยการเสนอขายไอซีโอ จุดเริ่มต้นของการระดมทุนอยู่ที่ซิลิคอนแวลลีย์ (Silicon Valley) ศูนย์กลางของเทคโนโลยีและนวัตกรรมโลก โดยเหรียญนี้เกิดมาตั้งแต่เดือนกันยายน ๒๕๕๙

- OmiseGO (OMG) : โอมิเซะโก (\$6.57)

ผู้ก่อตั้งเป็นคนไทยชื่อ นายอิศราดร หะริณสุต (ดอน) ได้ตั้งบริษัท Omise ร่วมกับเพื่อนชาวญี่ปุ่นชื่อ นายจุน ฮาเซกาวา เริ่มแรกระดมทุนจากเวนเจอร์แคปปิตอลอยู่หลายครั้ง ก่อนจะมาเปิดระดมทุนด้วยการเสนอขายไอซีโอในกลางปี ๒๕๖๐ ด้วยโทเคนที่ชื่อ OmiseGO (OMG)

- Happycoin (HPC) : แฮปปี้คอยน์ (\$0.000000004153)

ก่อตั้งโดย นายภัชภูมิ วิตติยากร วรรณพฤกษ์ ซึ่งมีประสบการณ์สายงานไอทีมากกว่า ๑๐ ปี และนาย Lee Cham Sarm ชาวเกาหลี ที่คลุกคลีอยู่ในวงการคริปโตเคอร์เรนซีมากกว่า ๕ ปี

- JFinCoin (JFIN) : เจฟินคอยน์ (\$0.2779)

ผู้ออกเสนอขาย JFinCoin คือ บริษัท เจเวนเจอร์ส โดยมีนายธนวัฒน์ เลิศวัฒนารักษ์ (ทาโร่) เป็นซีอีโอและทีมงานหลัก และเจเวนเจอร์สยังเป็นบริษัทย่อยของ "เจมาร์ท" (JMART) ภายใต้ร่มเงาของนายอดิศักดิ์ สุขุมวิทยา ผู้ถือหุ้นใหญ่ ซึ่งเจมาร์ท เป็นบริษัทจดทะเบียนในตลาดหุ้นไทย

สกุลเงินคริปโต/เหรียญดิจิทัล สัญญาไทย (2)

- Carboneum token (C8) : คาร์บอนเนียม (Market data is untracked)
ผู้ก่อตั้งคือ นายธีระชาติ ก่อตระกูล ชื่อเล่น “แม็กซ์” เขายังเป็นเจ้าของและผู้พัฒนาแอปพลิเคชันวิเคราะห์หุ้น "StockRadars" โดยเสนอขายไอซีโอด้วยโทเคนที่ชื่อ Carboneum (คาร์บอนเนียม)
- SixNetwork (SIX) : ซิกซ์เน็ตเวิร์ค (\$0.06503)
SixNetwork เกิดจากการรวมตัวของ ๓ กลุ่มเพื่อทำการออกขายไอซีโอ โดยหนึ่งในนั้นคือ กลุ่มคนไทยและยังดำรงตำแหน่ง Co-founder, Co-CEO เหมือนกันคือ นายวัชระ เอมวัฒน์ (ก๊ก) และ นายณัฐวุฒิ พิงเจริญพงศ์ (หมู) โดยเสนอขายไอซีโอด้วย SIX Token (SIX)
- AFIN Coin (AFIN) : เอฟิน คอยน์ (\$0.087333)
ออกและเสนอขายโดย บริษัท Asian Fintech (Afin) ซึ่งมีนายสิทธิศักดิ์ มหาสิทธิวัฒน์ เป็นผู้อำนวยการและผู้ก่อตั้ง
เสนอขายไอซีโอด้วยเหรียญ Afincoin (AFIN)
- Zmine Token (ZMN) : ซีมายน์ (\$0.00798045)
ออกและเสนอขายโดยบริษัท ซีมายน์ โฮลดิ้ง ลิมิเต็ด (ZMINE Holdings Limited) ของนายกษมพัทธ์ วิจารณ์วัฒนา ผู้ร่วมก่อตั้งและประธานเจ้าหน้าที่บริหารโดยมีราคาขายไอซีโอ ๑ ZMN ประมาณ ๑.๗๘ บาท

การขุดบิทคอยน์คืออะไร (การหาฉันทามิติ)

- แค่เปิดคอมทิ้งไว้ ก็ได้เงิน
- ในช่วงเวลาที่ราคาบิทคอยน์เพิ่มขึ้นสูงแบบนี้ ผู้สนใจในการเข้ามาสร้างกำไรจากบิทคอยน์ก็เริ่มเพิ่มมากขึ้น วิธีหนึ่งที่ดีจะเป็นที่น่าจับตามองและเป็นที่ยอมรับมากรองลงมาจาก การซื้อเพื่อเก็งกำไรที่สุด คือ “การขุด” ซึ่งสังเกตได้จากราคาการ์ดจอที่สูงขึ้น และอุปกรณ์ที่เกี่ยวข้องกับการขุดตอนนี้แทบจะหมดเกลี้ยงไปจากตลาดแทบทุกที่ในโลกแล้ว แม้แต่ในประเทศไทยเองก็เริ่มหายากแล้ว
- จากการที่เคยพุ่งทะยานไปจนถึงจุดสูงสุดของมูลค่า Bitcoin ที่เป็น Crypto Currency ที่มีมูลค่าสูงสุด ซึ่งทำให้มีผู้คนร่ำรวยไปเป็นจำนวนมาก และในขณะเดียวกันก็มีอีกหลายคน ที่ขาดทุน จนหมดตัว กับการซื้อขายสกุลเงิน ดิจิตอล อย่าง Bitcoin



<https://siamblockchain.com/การ-ขุด-bitcoin-คืออะไร/>

<https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>

อาชีพขุด Bitcoin หน้าตาอย่างไร

การขุดบิตคอยน์คืออะไร? พบกับนักขุดในเกาหลีใต้

Jan 10, 2018, BBC News ไทย

<https://www.youtube.com/watch?v=em2RdmAZvqA>



ธุรกรรมซ้ำกันสองครั้ง (Double-Spending)

- ปัญหา Double-Spending กับการก่อกำเนิดขึ้นของ Blockchain
 - Satoshi Nakamoto นั้น ได้ทำการสร้าง Bitcoin และทำการ design ส่วนของ reference สำหรับการให้คนอื่นมา implement ต่อ ซึ่งเค้าได้ทำการสร้าง database ตัวแรกของ blockchain รวมถึงได้ทำการแก้ปัญหาสำคัญของ digital currency คือ การแก้ปัญหาในเรื่อง double-spending
 - ปัญหา double spending นั้นเป็นปัญหาที่สำคัญที่ทำให้เกิดการพัฒนาเทคโนโลยี blockchain ซึ่งเงินในรูปแบบ digital นั้น เราสามารถที่จะใช้ token เดียวกันในการจ่ายเงินได้มากกว่า ๑ ครั้ง ซึ่งเนื่องจาก digital token นั้นอยู่ในรูปแบบของ file digital ซึ่งสามารถที่จะทำซ้ำหรือปลอมแปลงขึ้นมาได้ง่าย เช่นเดียวกับรูปแบบของเงินปลอม ซึ่งปัญหาของ Double-Spending นั้นหากไม่ได้รับการแก้ไขอาจนำมาซึ่งอัตราเงินเฟ้อได้ในระยะยาว และอาจจะทำให้ไม่ได้รับความไว้วางใจจากผู้ใช้งานในที่สุด
 - ตัวอย่างง่าย ๆ ให้เห็นภาพของปัญหา Double-Spending
 - สมมติว่าเรามีนาฬิกา ๑ เรือน หากเราอยากจะทำมอบให้ใคร เราก็จะมอบนาฬิกาเรือนนั้น ให้คนๆนั้นได้คนเดียว แต่เมื่อการส่งนาฬิกาให้กันอยู่ในรูปแบบดิจิทัล เช่น ไฟล์ภาพนาฬิกา เราก็สามารถส่งภาพนาฬิกาได้ ทาง facebook , Line หรือ email ให้มีหลายคนได้ในเวลาพร้อมกัน ด้วยเหตุนี้ Blockchain จึงต้องมีสิ่งที่เรียกว่า “ผู้ตรวจสอบการทำธุรกรรมซ้อน” หรือ Miner ซึ่งเป็นบุคคลที่ถูกเลือกขึ้นมาในเครือข่ายของ Blockchain นั้นๆ นั่นเอง

<https://www.blockdit.com/posts/5ec0ca982ea0a20cc2be092f>

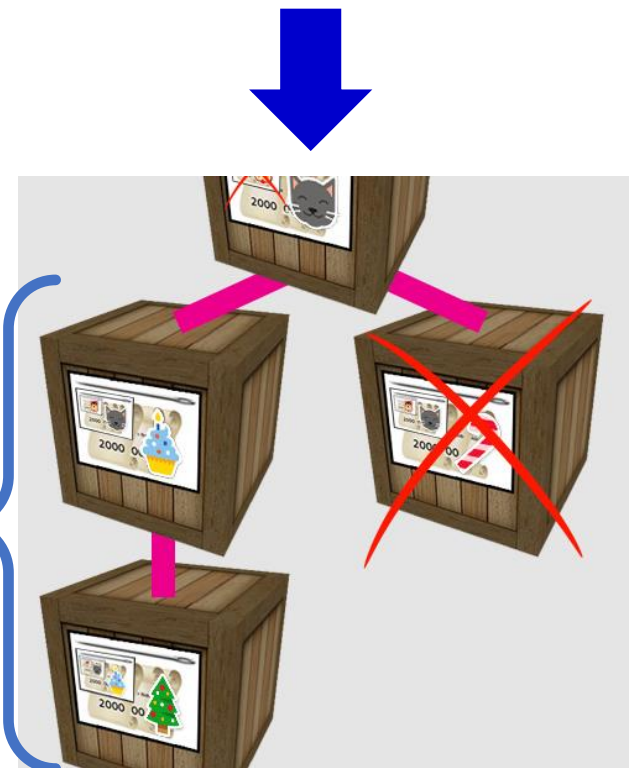
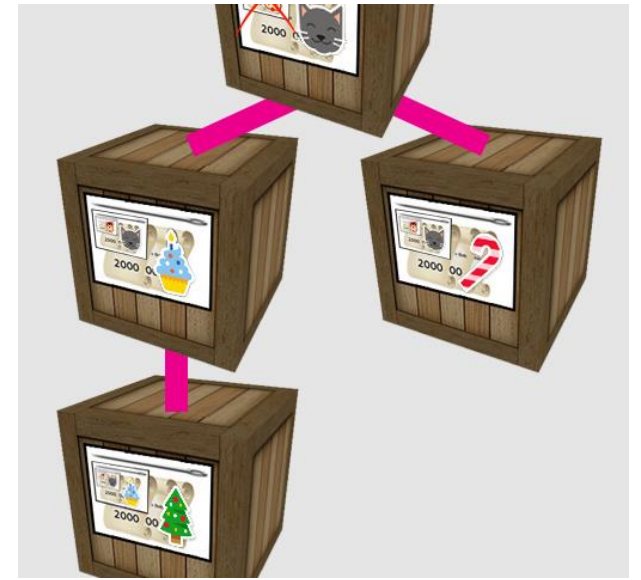
<https://en.wikipedia.org/wiki/Double-spending>

ธุรกรรมซ้ำกันสองครั้ง (Double-Spending)

- ธุรกรรมซ้ำกันสองครั้ง/ธุรกรรมไม่ตรงกัน สามารถแก้ไขโดยมีผู้ตรวจสอบ
- ระบบบล็อกเชนจะกระจายบล็อกธุรกรรมให้นักขุดหลายคนไปสุ่มเดาหาค่าพารามิเตอร์ของฟังก์ชันที่สร้างค่าแฮชที่มีลักษณะจำเพาะ เช่น ขึ้นต้นด้วย ๐๐๐๐๐๐๐ เป็นต้น (Proof of Work)
- สุดท้ายจะมีนักขุดเพียงคนเดียวที่จะมีสิทธิ์สร้างบล็อกเพิ่มเข้าไปในระบบ
- เนื่องจากเป็นระบบแบบกระจาย (distributed) ก็มีโอกาสนักขุดหลายคนเจอในเวลาใกล้เคียงกัน ทำให้อาจมีบล็อกเชนที่แยกสาขา แต่การแยกสาขานี้จะมีการต่อสายไปเรื่อยๆ ถ้าสายไหนถึง ๖ บล็อกก่อน สายอื่นๆ จะเป็นโหล่มะไป ซึ่งบล็อกที่ก่อนจะตัดสินใจ จะถือว่าเป็นบล็อกชั่วคราว

ทุกครั้งที่เราสร้างบล็อก นักขุดจะต้องตรวจสอบพร้อมหาค่าพารามิเตอร์ให้ได้ก่อนคนอื่น จึงจะมีสิทธิ์เป็นใครรับรองบล็อกนั้นและทุกคนก็จะยอมรับบล็อกนั้นผ่านการแจ้งแบบกระจายเพียร์ทูเพียร์ (Peer-to-Peer)

๖ บล็อก



สัญญาอัจฉริยะหรือสมาร์ทคอนแทร็กต์ (Smart Contract)

- Smart Contract หมายถึง กระบวนการทางดิจิทัล ที่กำหนดขั้นตอนการทำธุรกรรม โดยอัตโนมัติไว้ล่วงหน้า โดยไม่ต้องอาศัยตัวกลาง อย่างเช่น ธนาคาร ซึ่งการสร้าง Smart Contract ที่เป็นระบบอัตโนมัติอย่างเต็มรูปแบบ โดยคู่สัญญาทั้งสองฝ่ายจะมีการตกลงกันก่อนหน้านี้ ถึงขั้นตอน กลไก ในการทำการธุรกรรมดังกล่าว ซึ่งการพัฒนานี้ส่งผลกระทบต่อรูปแบบธุรกิจแบบดั้งเดิมของธนาคาร
- Smart Contract เกิดมาจาก Nick Szabo ที่เป็นผู้เสนอไอเดียว่า Blockchain สามารถใช้ในการบันทึกข้อตกลงของสัญญาที่สามารถดำเนินการได้ด้วยตัวเอง ไม่จำเป็นต้องมีคนกลาง หรือใช้พนักงานในการมานั่งตรวจสอบเอกสาร โดยทุกอย่างให้คอมพิวเตอร์และโปรแกรมจัดการ และการ Hack ข้อมูลทำได้ยาก

สัญญาอัจฉริยะหรือสมาร์ตคอนแทร็กต์ (Smart Contract)

- โปรแกรมคอมพิวเตอร์ ที่มีการดำเนินงานอัตโนมัติ ตามสัญญาหรือข้อกำหนดที่ระบุไว้ โดยเป้าหมายของสัญญาอัจฉริยะคือการลดการมีคนกลางของสัญญา ลดค่าใช้จ่ายของคนกลาง เพิ่มความโปร่งใส และลดความผิดพลาดที่เกิดขึ้น โดยการทำงานผ่านบล็อกเชน
- เครื่องขายของอัตโนมัติเป็นตัวอย่างเทคโนโลยีเก่าเทียบเท่ากับการดำเนินการของสัญญาอัจฉริยะ โดยการทำงานของคริปโทเคอร์เรนซีของบิตคอยน์เป็นตัวอย่างของสัญญาอัจฉริยะคร่าวๆ สำหรับการทำสัญญาระหว่างบุคคลที่ไม่รู้จักกัน และ หลังจากการพัฒนาอีเธอร์เรียม ทำให้มีการพัฒนาสัญญาอัจฉริยะมากขึ้น และมีการเริ่มใช้งานกันอย่างแพร่หลายระหว่างบุคคลที่ไม่รู้จักกัน อาทิการแลกเปลี่ยนสกุลเงินของคริปโทเคอร์เรนซี การซื้อขายของ การทำธุรกรรมทางการเงินผ่านการเงินแบบไม่รวมศูนย์ หรือการแลกเปลี่ยนโทเคนดิจิทัลที่ทดแทนกันไม่ได้

ตัวอย่างการใช้สัญญาอัจฉริยะหรือสมาร์ตคอนแทร็กต์



Trade finance: Smart contracts can be set up as escrow accounts that monitor an exchange between two parties. It can track the location of the goods and when ownership has been transferred it can trigger payments.



P2P insurance: Insurance firms can automate the insurance policy by writing it into a smart contract. This technology can enable P2P insurance business models through templated smart contracts.



Loyalty and rewards: E-commerce, retail, and travel & tourism are some of the industries that can create a smart contract-driven loyalty and rewards system stored on a distributed ledger allowing interoperability.



Digital rights management and micropayments: Smart contracts that allow access to digital content such as music, images, and videos with access keys stored on distributed ledgers and also automates micropayments.



Land registry: Store the ownership of land/property on a distributed database and create safeguards for secure updates to this registry when transferring ownership through involvement of government/central body.



Securities issuance: Securities based on payments and rights to be executed according to predefined rules can be written as smart contracts. Current live examples being issuance of smart bonds and private stock markets.



Syndicated loans: Smart contracts can help reduce the settlement time for syndicated loans and help reduce loan issuance time and operational risks.



Event-driven insurance: Connected devices that store data on a distributed ledger help underwrite insurance and automate claims servicing.



Post-trade services: Smart contracts are triggered to ensure regulatory compliance of trades, ensure trade is executed as per the requirements, and take corrective steps as needed.



Distributed smart power grid: Ability for users to generate power and sell it over the grid that enables P2P payments and micro-transactions using smart contracts and distributed ledger.

- การเงินเพื่อการค้า (Trade finance)
- การประกันภัยแบบเพียร์ทูเพียร์ (P2P insurance)
- ความภักดีและผลตอบแทน (Loyalty and rewards)
- การจัดการสิทธิดิจิทัล (Digital rights management)
- ไมโครเพย์เมนต์ (Micropayments)
- ทะเบียนที่ดิน (Land registry)
- หลักทรัพย์ค้ำประกัน (Securities insurance)
- เงินให้กู้ยืมร่วม (Syndicated loans)
- ประกันตามเหตุการณ์ (Event-driven insurance)
- บริการหลังการค้า (Post-trade services)
- โครงข่ายไฟฟ้าอัจฉริยะแบบกระจาย (Distributed smart power grid)

อีกตัวอย่าง NFT: การสร้างมูลค่าของ Digital Asset บนโลกดิจิทัล

- Non-Fungible Token (NFT) คือโทเคนที่ไม่สามารถใช้ซ้ำ ไม่สามารถทดแทนกันได้ หรือจะเรียกอีกอย่างมันคือโทเคนที่เราสามารถระบุตัวตน หรือความเป็นเจ้าของ รวมถึงจำนวนจำกัด ลงไปได้ ด้วยคุณสมบัตินี้ทำให้เราสามารถสร้างมูลค่าให้แก่ Digital Asset ได้ เพราะดั้งเดิมแล้วสินทรัพย์ดิจิทัลที่สามารถคัดลอกได้นั้นจะแทบไม่มีค่าอะไรเลย
 - ตัวอย่างเช่นงานศิลป์, เพลง, ของสะสม, Item ในเกม หรือแม้แต่อสังหาริมทรัพย์ ล้วนสามารถใช้ NFT แสดงความเป็นเจ้าของได้ทั้งสิ้น แตกต่างจากสกุลเงินคริปโทอย่าง Bitcoin หรือเงิน Fiat อย่างเงิน
- คงไม่มีใครคาดคิดหรือกว่า คลิปวิดีโอ ที่พ่อได้ถ่ายลูกๆ เล่นไว้อโดยไม่ตั้งใจ แล้วเกิดจับภาพ “แฮร์รี่” ที่เป็นพี่ชาย อายุสามขวบโดน "ชาร์ลี" ผู้เป็นน้องชายอายุ ๑ ขวบ กัดนิ้ว จนเกิดเป็นภาพความน่ารักน่าชังของสองพี่น้อง “ฮาวเวิร์ด เดวิส คาร์” ผู้เป็นพ่อจึงได้นำ คลิปวิดีโอความยาว ๕๕ วินาที อัปโหลดลงยูทูปเมื่อ ๑๔ ปีที่แล้ว โดยต้องการให้ครอบครัวและเพื่อนๆ ได้ดู แต่มันก็เกิดเป็นกระแสไวรัสดิโอจนมียอดรับชมถึงปัจจุบันมากกว่า ๘๘๑ ล้านครั้ง

<https://www.dailynews.co.th/it/846440/>



NFT LAUNCHPAD | Powered by Origin

DROPS

Sign up



CHARLIE BIT ME 1 OF 1 NFT

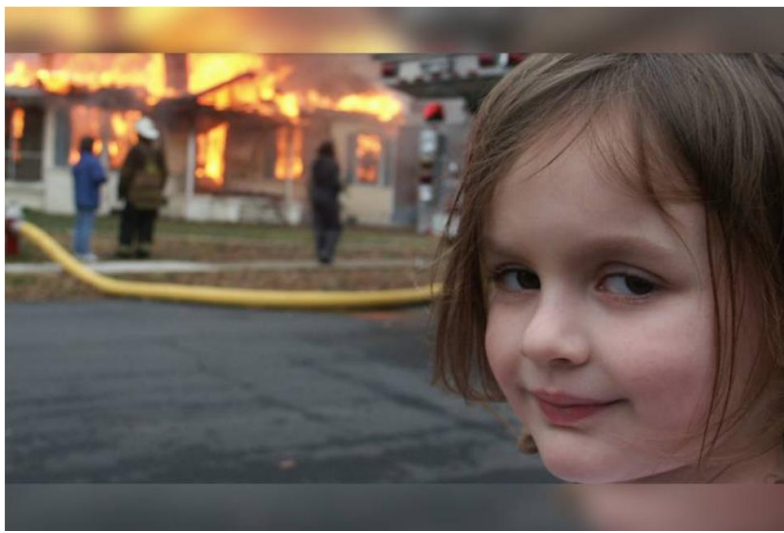
AUCTION HAS ENDED

SORRY!

You missed out on the Charlie
Bit Me 1 of 1 NFT Collection.

คลิปวิดีโอที่ว่านี้ ชื่อ “ชาร์ลีบิตมายิงเกอร์” (Charlie Bit My Finger) และได้ถูกนำไปประมูลขายในรูปแบบ NFT เมื่อวันเสาร์ที่ ๒๒ พ.ค. ๒๕๖๔ ซึ่งเป็นวันครบรอบ ๑๔ ปีของการอัปโหลดคลิปนี้ในยูทูป จนสามารถทำเงินได้ถึง ๗๖๐,๙๙๙ ดอลลาร์สหรัฐฯ หรือประมาณ ๒๓.๘๖ ล้านบาท โดยผู้ประมูลที่กล้าทุ่มเงินหลักสิบล้านใช้ชื่อว่า 3fmusic และต่อไปต้นฉบับคลิปนี้ก็จะถูกลบออกจากยูทูปอย่างถาวร

<https://www.dailynews.co.th/it/846440/>



jack ✓
@jack

just setting up my twttr

2:50 PM · Mar 21, 2006 · Twitter Web Client

120.6K Retweets 14.4K Quote Tweets 161.2K Likes



- นี่ไม่ใช่ครั้งแรกที่มีการนำผลงานแบบนี้มาขายทำเงิน ก่อนหน้านี้ ภาพถ่าย Disaster Girl หรือเด็กเผาบ้าน ที่ถูกนิยมนำมาใช้เป็นมีม หรือภาพแสดงความรู้สึกเวลานั้นๆ ซึ่งภาพเป็นเด็กหญิงยืนหน้ากองเพลิงที่กำลังเผาบ้านอยู่ ซึ่งเจ้าของภาพ ก็คือ Zoe Roth นักศึกษาอายุ ๒๑ ปี เมื่อตัวเธอต้องประสบปัญหาโควิด-19 จึงตัดสินใจนำออกมา ประมูลขายแบบ NFT เมื่อเดือนเมษายนที่ผ่านมา ได้เงิน ๕๐๐,๐๐๐ ดอลลาร์ หรือประมาณ ๑๕.๕ ล้านบาท ซึ่งรูปนี้ ถ่ายไว้เมื่อปี ๒๕๔๘ โดย David Roth ผู้เป็นพ่อของเธอ ซึ่งเงินที่ได้ก็จะนำไปใช้ในการศึกษา
- นอกจากนี้ Chris Torres ศิลปินผู้สร้าง Nyan Cat ที่เป็นผลงานอนิเมชั่นตัวแมว และได้ อัฟโหลดลง ยูทูป เมื่อปี ๒๕๕๔ ถูกประมูลขายแบบ NFT ได้ในราคาสูงถึง ๕๙๐,๐๐๐ เหรียญสหรัฐ หรือประมาณ ๑๘ ล้านบาท
- หรืออย่างที่เป็นข่าวดังหน่อย ก็คือ กรณีของ Jack Dorsey ซึ่งเป็นผู้ร่วมก่อตั้ง โซเชียล มีเดียชื่อดังอย่าง “ทวิตเตอร์” ได้แคปภาพที่เป็นโพสต์แรกของเขาบน ทวิตเตอร์ ซึ่งมีข้อความว่า "just setting up my twttr" ระบุวันที่ ๒๒ มีนาคม ๒๕๔๙ มาขายแบบ NFT เช่นกัน โดยผู้ชนะการประมูลในครั้งนี้คือ Sina Estavi ที่มีตำแหน่ง ซีอีโอ ของบริษัท Bridge Oracle ซึ่งเป็นบริษัทด้านบล็อกเชน จากประเทศมาเลเซีย ซึ่งเขาซื้อทวิตดังกล่าวด้วย Cryptocurrency สกุล Ethereum มูลค่า ๑,๖๓๐.๕๘ อีเธอร์ (ETH) ซึ่งคิดเป็นเงินประมาณ ๒.๙ ล้านบาทหรือกว่า ๘๙ ล้านบาท

เหตุการณ์เร็ว ๆ นี้เกี่ยวกับบล็อกเชนกับเงินดิจิทัล (๒๐ มิถุนายน ๒๕๖๔)

- นักขุดบิทคอยน์ในมณฑลเสฉวนเริ่มชกปลั๊กแล้ว ลึนสุดยุคสมัยจีนครองแรงขุดอย่างเป็นทางการ โดยอ้างอิงจากข้อมูลของ QKL123 พลังประมวลผลเฉลี่ยของเครือข่าย Bitcoin ปัจจุบันอยู่ที่ ๑๒๙.๕๒ EH/s ซึ่งต่ำกว่าระดับสูงสุดเป็นประวัติการณ์ที่ ๑๙๗.๖๑ EH/s (๑๓ พฤษภาคม ๒๕๖๔) ถึง ๓๔% (๒๐ มิถุนายน ๒๕๖๔, <https://siamblockchain.com/2021/06/20/lights-go-off-in-sichuan/>)
- เหตุใดจีนจึงมีกฎระเบียบที่เข้มงวดขึ้น?
 - ตลาดกระทิง (ตลาดขาขึ้น) ของ Bitcoin ในปีนี้ได้ฟื้นคืนชีพการซื้อขายสกุลเงินดิจิทัลในประเทศจีน ทำให้หน่วยงานกำกับดูแลเกี่ยวกับความเสี่ยงทางการเงินและการฟอกเงินต้องออกมาเตือนในทันที
 - เมื่อการแลกเปลี่ยนเงินคริปโตในท้องถิ่นปิดตัวลง นักลงทุนชาวจีนจำนวนมากได้เปลี่ยนไปใช้แพลตฟอร์มที่เป็นของจีนแต่ย้ายไปต่างประเทศ รวมถึง Huobi และ OKEx หรือทำการซื้อขายผ่านแพลตฟอร์มออนไลน์และห้องสนทนากการซื้อขายโซเชียลมีเดีย
 - บริษัทแลกเปลี่ยนเงินที่เน้นประเทศจีนซึ่งรวมถึง Binance และ MXC เปิดช่องให้บุคคลชาวจีนสามารถเปิดบัญชีออนไลน์ได้อย่างง่ายดาย พวกเขายังอำนวยความสะดวกในข้อตกลงแบบ peer-to-peer ในตลาด Over-the-counter (OTC) ที่ช่วยแปลงหยวนจีนเป็นคริปโต ผู้ค้าทำธุรกรรมดังกล่าวผ่านธนาคารหรือช่องทางการชำระเงินออนไลน์ เช่น Alipay หรือ WeChat Pay
 - นักลงทุนรายย่อยยังสามารถซื้อ "กำลังประมวลผล" (computing power) จากผู้ขุดคริปโตผู้ออกแบบแผนการลงทุนต่างๆ ที่ให้ผลตอบแทนที่รวดเร็วและมีกำไรงาม
 - ในขณะเดียวกัน ความกังวลเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้นของคริปโตต่อสกุลเงินทางการของจีนคือเงินหยวน ยังกระตุ้นให้ธนาคารประชาชนแห่งประเทศจีน (PBOC) เปิดตัวสกุลเงินดิจิทัลของตัวเองด้วย

ค่าเฉลี่ยของธนาคารประชาชนแห่งประเทศจีนส่งผลให้ Bitcoin ร่วงลงสู่ระดับต่ำสุดในรอบสองสัปดาห์และ Ether ลงมาสู่ระดับต่ำสุดในรอบ 5 สัปดาห์ ในวันอังคารที่ราคาของคริปโตหลักๆ จึงค่อยมีเสถียรภาพขึ้นมาบ้าง

<https://www.posttoday.com/world/656183>

วันที่ ๒๒ มิถุนายน ๒๕๖๔ เวลา ๑๖:๔๖ น.

เหตุการณ์เร็วๆนี้เกี่ยวกับบล็อกเชนกับเงินดิจิทัล (แ)

- จีนจ่อจำกัดการถือครองคริปโตของคนในประเทศ (๒๐ มิถุนายน ๒๕๖๔ ๒๑:๒๙, ผู้จัดการออนไลน์)
<https://mgronline.com/stockmarket/detail/9640000073199>
- จีนฮึม!!! หลังประกาศเดินหน้ากวาดล้างเหมืองขุดคริปโตทั่วประเทศ กูรูคริปโตคาดแนวโน้มอนาคตอาจออกกฎหมายห้ามประชาชนในประเทศถือครองเหรียญคริปโต
- รายงานจาก u.today ระบุว่า หลังจากที่รัฐบาลจีนได้ออกมาตรการปราบปรามอุตสาหกรรมขุดเหมืองคริปโต ๆ ในประเทศจีน จนทำให้ผู้ประกอบการหลายรายปิดกิจการ และย้ายแท่นขุดออกไปยังต่างประเทศที่มีราคาค่าไฟฟ้าในอัตราที่ถูกลง ซึ่งล่าสุด Bobby Lee ผู้ก่อตั้ง BTCC แพลตฟอร์มแลกเปลี่ยนคริปโตเจ้าแรก ๆ ในประเทศจีน แสดงความคิดเห็นว่ารัฐบาลจีนอาจจะไม่หยุดอยู่แค่การแบนการขุดเหมืองคริปโตในประเทศ มีโอกาสมากถึง ๕๐% ที่ประเทศจีนจะแบนการถือครองบิทคอยน์ในประเทศ
- “สิ่งต่อไปที่รัฐบาลจะทำ มองว่าน่าจะเป็นฟางเส้นสุดท้ายของธุรกิจคริปโต คือการแบนคริปโตฯ อย่างสิ้นเชิง โดยคาดการณ์ไว้ว่ามันมีความเป็นไปได้ถึง ๕๐-๕๐”
- ทั้งนี้ Lee เชื่อว่าประเทศจีนจะแบน Bitcoin อย่างเด็ดขาดเมื่อราคาติดตัวพุ่งถึง ๕๐๐,๐๐๐ ดอลลาร์ ซึ่งตัวเขายังเชื่อมั่นว่าคริปโตเคอร์เรนซีอันดับหนึ่งจะมีมูลค่าการซื้อขายเพิ่มขึ้นอีกมากในสิ้นปีนี้ แม้ว่าที่ผ่านมาจะมีการปรับฐานครั้งใหญ่หลายรอบแล้ว

ค่าเฉลี่ยของธนาคารประชาชนแห่งประเทศจีนส่งผลให้ Bitcoin ร่วงลงสู่ระดับต่ำสุดในรอบสองสัปดาห์และ Ether ลงมาสู่ระดับต่ำสุดในรอบ 5 สัปดาห์ ในวันอังคารที่ราคาของคริปโตหลักๆ จึงค่อยมีเสถียรภาพขึ้นมาบ้าง

<https://www.posttoday.com/world/656183>

วันที่ ๒๒ มิถุนายน ๒๕๖๔ เวลา ๑๖:๔๖ น.

เงินดิจิทัล: ดิจิทัลหยวน (เงินหยวนในรูปแบบใหม่)

- เมื่อเดือนต้นเดือนพฤษภาคม ๒๕๖๓ ที่ผ่านมา ได้มีข่าวว่าธนาคารกลางจีน (PBoC) ได้เริ่มมีการทดสอบเงินหยวนดิจิทัลแล้วใน ๔ เมืองหลัก คือ ซูโจว เซินเจิ้น สงอัน และเฉิงตู.
- ความพยายามของจีนในการผลักดันสกุลเงินดิจิทัลเกิดขึ้นเมื่อช่วงราวๆ ปี ๒๕๕๗ เมื่อรัฐบาลจีนต้องการที่จะลดการพึ่งพาเงินดอลลาร์สหรัฐ.
- แม้ทางการจีนในช่วงแรก ของยุคของรัฐบาลสีจิ้นผิงจะไม่ยอมรับเงินคริปโตเคอร์เรนซี (Cryptocurrency) แบบสำเร็จรูป.
- แต่จีนได้ให้ความสนใจและศึกษาเทคโนโลยีบล็อกเชนมาตลอด โดยมีการทดลองใช้งานมาเรื่อยๆ จนกระทั่งเมื่อ วันที่ ๓๑ ตุลาคม ๒๕๖๒ ธนาคารกลางของจีน (PBOC) ได้ประกาศจะเริ่ม ทดลองใช้เงินหยวนในรูปแบบดิจิทัล โดยใช้ชื่อเรียกว่า Digital Currency Electronic Payment (DCEP) เป็นครั้งแรก.

ตัวอย่างการการใช้บล็อกเชนในประเทศไทย



- กสิกรไทยเปิดบริการหนังสือค้ำประกันบนบล็อกเชนครั้งแรกของโลก จับมือกับพันธมิตรทางธุรกิจ ได้แก่ การไฟฟ้าานครหลวง การไฟฟ้าส่วนภูมิภาค บมจ. พีทีที โกลบอล เคมิคอล และ บมจ. พีทีที โพลีเมอร์ มาร์เก็ตติ้ง
- ร่องใช้บริการหนังสือค้ำประกันบนเทคโนโลยีบล็อกเชน โดยมี ไอบีเอ็มร่วมสนับสนุนการนำบล็อกเชนสร้างระบบต้นแบบ

<https://www.facebook.com/IBMThailand/posts/10154561426701987/>
<https://thestandard.co/news-business-kasikorn-bank-ibm-blockchain/>

วันที่ ๑๙ กรกฎาคม ๒๕๖๐ ๑๘:๒๒ น.

ตัวอย่างการการใช้บล็อกเชนในประเทศไทย



นำระบบหนังสือค้ำประกันวงเงิน ๑.๓๕ ล้านล้านบาทสู่ยุคเอกสารอิเล็กทรอนิกส์ ๑๐๐% ลดค่าใช้จ่ายได้ถึง ๒ เท่า โดยอยู่ในระหว่างทดสอบภายใต้การกำกับของธนาคารแห่งประเทศไทย

- ไทยพาณิชย์ ขานรับ รพท. ผนีกสมาคมธนาคารไทย รัฐวิสาหกิจ และองค์กรธุรกิจใหญ่ ร่วมสร้าง Thailand Blockchain Community Initiative แห่งแรกในไทย (๒๐ มีนาคม ๒๕๖๑)
- นำเทคโนโลยีบล็อกเชนมายกระดับประสิทธิภาพและความสามารถในการแข่งขันทางธุรกิจของประเทศ เริ่มต้นด้วยโครงการบริการหนังสือค้ำประกันอิเล็กทรอนิกส์บนระบบบล็อกเชน สร้างโครงข่ายหนังสือค้ำประกันที่สะดวกปลอดภัยบนบล็อกเชนเป็นครั้งแรกของไทย

จุดเปลี่ยนการบริหารงานภาครัฐด้วยระบบบล็อกเชน

- งานที่นำสมาร์ตคอนแทร็กต์หรือบล็อกเชนมาใช้ได้
 - การบริหารจัดการระบบทะเบียนที่ดินของภาครัฐ
 - การลงคะแนนเสียงเลือกตั้ง
 - การป้องกันและแก้ไขปัญหาการทุจริตคอร์รัปชันในภาครัฐ
 - การให้บริการด้านสาธารณสุขของภาครัฐ
 - การจัดซื้อจัดจ้างภาครัฐ
- ปัจจุบันภาครัฐทั่วโลกต่างเริ่มตื่นตัวกับการนำระบบบล็อกเชนมาใช้ในการบริหารงานภาครัฐกันอย่างมาก เนื่องจากระบบบล็อกเชนสามารถนำมาใช้ประโยชน์ได้หลากหลายด้าน ทั้งการนำพาภาครัฐไปสู่ ภาครัฐดิจิทัลที่มีการบูรณาการข้อมูลระหว่างหน่วยงานภาครัฐ การลดขั้นตอนในการดำเนินงานของหน่วยงาน ภาครัฐ ทำให้ประหยัดเวลาและต้นทุน รวมทั้งการอำนวยความสะดวกในการให้บริการประชาชนได้อย่าง รวดเร็วแบบที่ไม่เคยมีมาก่อน ซึ่งจะเป็นการยกระดับการให้บริการภาครัฐแก่ประชาชนขึ้นไปอีกขั้น
- ศึกษาให้รอบคอบ ระมัดระวัง จัดระบบ และมีแผนการดำเนินการที่เหมาะสม โดยภาครัฐอาจจะทำโครงการนำร่องหรือการทดลองดำเนินการก่อน เพื่อไม่ให้ล้มเหลว

สิงหาคม ๒๕๖๑



เอกสารวิชาการ

Academic Focus

จุดเปลี่ยนการบริหารงานภาครัฐด้วยระบบบล็อกเชน (Blockchain)

สำนักวิชาการ

สำนักงานเลขาธิการสภาผู้แทนราษฎร

ISBN 2287-0520

ดาวน์โหลดเอกสารได้จาก <http://www.parliament.go.th/library>

ใครคือซาโตชิ นากาโมโตะ (Satoshi Nakamoto, サトシ・ナカモト)

ผู้สร้างบล็อกเชน

- ยังไม่แน่ชัด อาจจะเป็นบุคคลเหล่านี้หรืออาจเป็นกลุ่มบุคคล

- Vili Lehdonvirta
- Shinichi Mochizuki
- Dorian Nakamoto
- Nick Szabo
- Hal Finney



Dorian Nakamoto
Japanese-American, retired physicist and well-educated engineer, Los Angeles



Prof. Vili Lehdonvirta
Economic Sociology and Digital Social Research
Oxford Internet Institute,
University of Oxford.



Prof. Shinichi Mochizuki
Japanese mathematician
Kyoto University



Nick Szabo
A computer scientist, legal scholar, and cryptographer

Harold Thomas Finney II

(May 4, 1956 – August 28, 2014)

A developer for PGP Corporation
A lead developer on console games



- สาเหตุที่ไม่เปิดเผยตัวตน อาจจะเป็นดังนี้

- เหตุผลที่ ๑ อาจเป็นเพราะความเกี่ยวข้องกับความปลอดภัยของผู้ใช้บริการในเครือข่าย และการพัฒนาของสกุลเงินในอนาคต หากบุคคลหรือกลุ่มคนที่อยู่เบื้องหลังถูกเปิดเผยสู่สาธารณะชน รัฐบาลและ ธนาคารทั่วโลกอาจกดดันให้พวกเขาจำกัดข้อบังคับบางอย่างในการทำธุรกรรม ซึ่งขณะเดียวกันการทำงานของ Bitcoin คือเครือข่ายแบบ Peer-to-Peer และไม่มีตัวกลางใดๆ ควบคุม การออกข้อบังคับจะเป็นปัญหากับระบบอย่างมาก รวมถึงผู้ใช้ในเครือข่ายจะรู้สึกไม่ปลอดภัยหากกฎระเบียบต่างๆ ถูกออกโดยบุคคลหรือกลุ่มคนเพียงกลุ่มเดียว
- เหตุผลที่ ๒ ความเป็นส่วนตัว ความเป็นส่วนตัวของ Satoshi Nakamoto จะถูกละเมิดโดยแหล่งข่าวจากหลายแห่งที่ต้องการสัมภาษณ์เขา ซึ่งเหตุการณ์คล้ายกับแบบที่เกิดขึ้นกับ Dorian Satoshi Nakamoto หนึ่งในบุคคลต้องสงสัยว่าเป็น Satoshi Nakamoto เนื่องจากมีชื่อและความชอบบางส่วนที่คล้ายคลึงกัน โดยมีคนเชื่อว่าพวกเขาอาจเป็นเป้าหมายของการฟ้องร้องคดีจำนวนมาก (แม้ว่าตัว Satoshi จะไม่ผิดกฎหมายอะไรก็ตามในทางเทคนิค)

บทสรุป

- ระบบบล็อกเชนเป็นระบบที่จะมาเปลี่ยนโลก หรือป่วนโลก ทั้งด้าน การค้า การลงทุน การบริหารราชการ การศึกษา การใช้ชีวิตประจำวัน เนื่องจากเราไม่ต้องมีตัวกลาง แต่ทุกคนจะเป็นตรวจสอบไปพร้อม ๆ กัน
- อย่างไรก็ตาม บล็อกเชนไม่ใช่ยาสรรพัตประโยชน์ บางเรื่องเราใช้ดี บางอย่างไม่จำเป็น. แต่ถ้าต้องการ การยืนยันการกระทำ เราจะใช้บล็อกเชน ถ้าไม่ต้องการการยืนยันการกระทำ ก็ไม่ต้องใช้บล็อกเชน.
- ระบบบล็อกเชนจะช่วยลดขั้นตอนการดำเนินงานของหน่วยงาน โดยเฉพาะการยืนยันการกระทำ ทำให้ ประหยัดเวลาและต้นทุน ทำให้การดำเนินงานหรือการให้บริการทำได้รวดเร็วแบบที่ไม่เคยมีมาก่อน
- สำหรับภาครัฐ ระบบบล็อกเชนจะเป็นเครื่องมือหนึ่งที่จะช่วยสนับสนุนนโยบายของรัฐบาล ในการ ขับเคลื่อนประเทศด้วยนวัตกรรมไปสู่ยุคไทยแลนด์ ๔.๐ และสามารถนำมาประยุกต์ใช้ในการแก้ไขปัญหา หลาย ๆ ด้านที่เกิดขึ้นในภาครัฐและภาคเอกชน ตั้งแต่ การแก้ปัญหาการเข้าถึงบริการ ไปจนถึง การ แก้ปัญหาการทุจริตคอร์รัปชันในภาครัฐ
- แต่ระบบบล็อกเชนยังถือได้ว่าเป็นเทคโนโลยีที่ค่อนข้างใหม่ อาจยังเป็นสิ่งที่เข้าใจยาก และจะต้องวาง กฎระเบียบเพื่อการควบคุมและกำกับดูแล ในขณะที่อีกด้านหนึ่งจะต้องไม่ปิดกั้นระบบบล็อกเชน

บทสรุป

- ประชาชนคนไทย องค์กรภาครัฐ องค์กรภาคเอกชน องค์กรภาคประชาชน ในประเทศไทยคงไม่สามารถหลีกเลี่ยงเทคโนโลยีบล็อกเชนนี้ที่กำลังจะมาเปลี่ยนองค์กร ประเทศ และโลกได้
- การศึกษา การสร้างการรับรู้ การเตรียมความพร้อม และการสร้าง ความเข้าใจในระบบบล็อกเชนจะกลายเป็นข้อได้เปรียบของประชาชนที่สามารถนำไปประยุกต์ใช้สร้าง มูลค่าเพิ่มให้กับตนเองและธุรกิจได้อย่างทันยุคสมัยและก่อให้เกิดประโยชน์มากที่สุด
- บล็อกเชนจะเป็นกลไกสำคัญ ที่จะช่วยส่งเสริมให้ประเทศไทยเป็นประเทศที่ได้เปรียบทั้งภาคเศรษฐกิจหรือภาคสังคมในเวทีโลก หรืออย่างน้อย ก็อยู่รอดได้ในโลกที่กำลังเปลี่ยนแปลงไปสู่โลกแห่งดิจิทัลที่มีประสิทธิภาพ ประสิทธิผล สะดวกสบาย และรวดเร็ว.

เว็บที่ค่อนข้างอธิบายบล็อกเชนได้เข้าใจง่าย

- https://nuuneoi.com/blog/blog.php?read_id=900
- <https://th.wikipedia.org/wiki/บล็อกเชน>
- <https://www.youtube.com/watch?v=2oaLjzx6tZY>
- https://www.bot.or.th/Thai/Segmentation/Public/PublicHearing/Documents/Hearing_Blockchain.pdf
- <https://thestandard.co/podcast/thesecondsauce140/>
- <https://www.dailynews.co.th/it/846440/>
- EP.1 สารคดี #Bitcoin และเงิน Crypto เป็นอนาคตโลกหรือฟองสบู่ดิจิทัล? ตอนที่ 1
<https://www.youtube.com/watch?v=6ZtA3KWn8nM> (๒๖ มกราคม ๒๕๖๑)
- EP.2 สารคดี #BitCoin และเงิน Crypto เป็นอนาคตโลกหรือฟองสบู่ดิจิทัล? ตอนที่ 2
<https://www.youtube.com/watch?v=Cd9ZWy8I5ws> (๑๓ กุมภาพันธ์ ๒๕๖๑)
- EP.3 สารคดี Bitcoin และเงิน Crypto เป็นอนาคตโลกหรือฟองสบู่ดิจิทัล? ตอนที่ 3
<https://www.youtube.com/watch?v=V8ga71GQRu0> (๒๓ เมษายน ๒๕๖๑)



ราชบัณฑิตยสภา

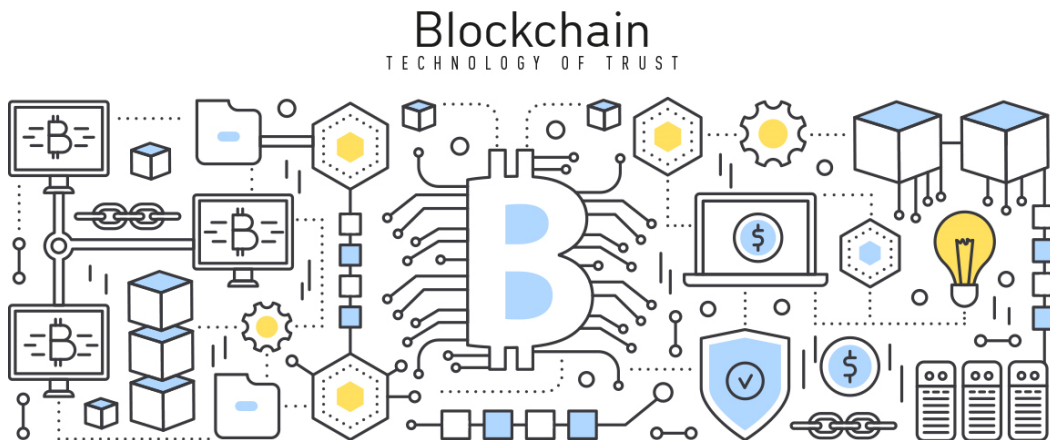
The Royal Society of Thailand



บล็อกเชน: เทคโนโลยีที่ป่วนโลก

Blockchain: A Disruptive Technology

Technology of Trust



๑ กันยายน ๒๕๖๔

ศ.ดร.ธนารักษ์ วีระมั่นคง ราชบัณฑิต
และ อาจารย์ สถาบันเทคโนโลยีนานาชาติสิรินธร
มหาวิทยาลัยธรรมศาสตร์