

Cryptocurrency มาจากคำนี้ Cryptography + Cerrency = Cryptocurrency

ออกเสียงยังไง “คลิบโทเคเรนซี” <https://pantip.com/topic/36860363>

= การถอดรหัส หรือ รหัสลับ=

ศาสตราจารย์ ดร.กิตตินันต์ พิศสุวรรณ

School of Business and Finance

London University

Illinois State University

เอกสารอ้างอิง <https://www.scbeic.com/th/detail/product/4161>

<https://pantip.com/topic/36860363>

เงินคืออะไร?

ก่อนอื่นขอปูพื้นเรื่องเงินก่อน เงินคือสิ่งที่สังคมกำหนดใช้เป็นตัวกลางในการแลกเปลี่ยนสินค้าและบริการ นั่นคือ ที่เงินมีค่าก็เพราะเราเอาไปใช้แลกเปลี่ยนสินค้า/บริการ ได้นั่นเอง นอกจากนี้ สิ่งที่หนุนค่าเงินอีกอย่างคือ ทองคำ/เงินตราต่างประเทศ ซึ่งสามารถเอาไปแลกเปลี่ยนได้ อย่างน้อยก็ที่ธนาคารกลางของประเทศนั้นๆ สามารถทำให้ผู้ถือเงินมั่นใจได้ว่าสิ่งที่ตัวเองถือไม่ใช่เพียงแค่กระดาษเปื้อนหมึก

ref: <https://www.wikipedia.org/wiki/เงิน>

### Cashless Society

เทรนด์ที่กำลังมาขณะนี้อันหนึ่งคือ สังคมไร้เงินสดซึ่งเป็นการเปลี่ยนรูปแบบเงินกระดาษให้เป็นเงินดิจิทัลในระบบคอมพิวเตอร์เพื่อให้การจับจ่ายได้สะดวก รวดเร็วและปลอดภัย(จากการฉกชิงวิ่งราว)มากขึ้นโดยสกุลเงินในระบบยังคงเป็นสกุลเดียวกับเงินกระดาษอยู่ผลพลอยได้คือภาครัฐสามารถจัดเก็บภาษีได้เต็มเม็ดเต็มหน่วยขึ้นจะหลบภาษีแบบแต่ก่อนไม่ได้ละ เพราะรัฐมีข้อมูลการไหลของเงินทั้งหมด

<https://finance.rabbit.co.th/blog/cashless-society>

### Blockchain

Blockchain เป็นเทคโนโลยีที่กำลังมาแรงอีกตัวหนึ่งคือ วิธีการเก็บข้อมูลแบบกระจายศูนย์โดยจะเก็บข้อมูลเป็นก้อนๆ (block) และอ้างอิงต่อเนื่องเป็นสายโซ่(chain)ต่อกันไปเรื่อยๆ(มันเลยได้ชื่อว่า blockchain)ระบบนี้เหมาะกับข้อมูลที่มีคุณลักษณะ

-ยอมทุกคนในระบบเห็นได้เหมือนกันหมด

(แต่ใครเข้าถึงระบบได้ก็อีกเรื่อง ซึ่งจำกัดคนเข้าถึงก็จะเป็น private blockchain)

-ไม่สามารถแก้ไขย้อนหลังได้

ซึ่งข้อมูลใน block นั้นจะเป็นอะไรก็ได้ เช่น กรรมธรรม์ประกันภัย ข้อมูลสุขภาพ ฯลฯ รวมทั้งรายการการเงิน ดูเหมือนว่าภาคธนาคารต่างๆก็กำลังทำ blockchain เพื่อใช้เป็นระบบเก็บ transaction ระหว่างธนาคาร อยู่เช่นกัน

<https://techsauce.co/technology/blockchain/understand-blockchain-in-5-minutes/>

ส่วน Crypto Currency (ที่อ้างว่า)คือ เงินดิจิทัลสกุลหนึ่งซึ่งจัดเก็บด้วย blockchain (ส่วนรายละเอียดน่าจะหาอ่านที่อื่นได้ไม่ยาก)โอ้ว.. ทั้ง Cashless Society, Blockchain กำลังมาCrypto Currency คาบเกี่ยวทั้ง 2 อย่างเลยถ้าอย่างนั้นเราควรลงทุนซื้อ Crypto Currency มาครอบครองสินะ?

- cashless society นั้นเป็นสกุลเงินของประเทศนั้นๆพูดให้อ้อ ก็คือ promptpay นั่นเองที่กำลังมา มันเกี่ยวอะไรกับ coin ต่างๆ? (ยกเว้นอ้างว่าไม่ต้องพกเงินสดเหมือนกัน)

- blockchain กำลังนำมาใช้ในระบบธนาคารต่างๆ

มันเกี่ยวอะไรกับ coin ที่ต่างคนต่างซุดกันทั่วโลก?เริ่มแปลกๆแล้วใช้มีัยครับ?พูดง่าย ๆคือ"การอ้างว่า Cashless Society, Blockchain กำลังมาให้เราลงทุนไปหา Crypto Currency มาครอบครอง" นั้นเป็นการผิดฝาผิดตัวซะจนดูเหมือนเป็นการหลอกลวงด้วยซ้ำ!!

## Crypto Currency

เรามาดูกันชัดๆดีกว่าว่า Crypto Currency จะสามารถเป็นอะไรได้บ้าง ตั้งแต่ แย่สุดจนดีสุด

### -แย่สุด คุปองศูนย์อาหารร้าง

อย่างที่เขียนไว้ตอนแรกว่า สกุลเงินจะมีค่า ก็ต่อเมื่อเอามาแลกเปลี่ยน/บริการ ได้การที่เราเอาเงินจริงๆไปแลก คุปองศูนย์อาหารร้าง ที่ไม่มีอะไรขายนั้น ไม่ต่างกับการเอาเงินจริงๆไปแลกกับเศษกระดาษแถมไม่มีธนาคารกลางที่รอรับแลกกลับเป็นเงินจริงอีกด้วยการซื้อขายสิ่งที่ไม่ได้มีคุณค่าจริง ไปๆมาๆมันเป็นอย่างไรได้นอกจากเก็งกำไร?บางคนคิดว่า อย่างน้อยมันคงไม่โหดเท่า ดอกทิวลิป หรือเพราะดอกทิวลิปเน่าได้ แต่คุปองมันไม่เน่า เรียกว่าไม่ขายไม่ขาดทุนเออ.. แต่กรณีนี้ถ้าคนไม่ใช่ คนซุดก็ไม่ได้เหรียญใหม่/ค่าธรรมเนียมจะพาลเล็กกันหมด เอามันคือเหมือนปิดเซฟเกม online นะคร้าบเรียกว่าแจ้งถั่วหน้า แบบไม่มีเศษกระดาษให้ถือด้วย

### -ตั้งไข่ แลกเปลี่ยนสินค้าได้

ถ้า coin นั้นๆ สามารถหาคนทำสินค้า/บริการ ที่ยอมรับ coin ได้ จะด้วยวิธีใดก็แล้วแต่(เช่น การเสนอว่า coin ที่จะนำมาขายสามารถนำมาแลกเปลี่ยนของบ.ตัวเองได้coin นั้นก็ดูเหมือนมีค่ามีตัวมีตนขึ้นมาหน่อยแต่จะมีสินค้า/บริการอื่นๆมายอมรับด้วยทีหลังหรือไม่ก็เป็นเรื่องที่ไม่แน่นอน)ร้านค้าและคนในระบบ coin นั้นจะเจอเรื่องปวดหัวกับ บัญชีที่ต้องทำเป็น2สกุลเงิน (เงินปกติ+coin)อย่ารู้ว่าเป็นยังลงไปกัมพูชาดู (เงินเรียล+ดอลลาร์ โอ.. ชื่อ-กบาล:"ปวดหัว" ภาษาเขมร)และ จะซ้ำให้ปวดหัวหนักขึ้นด้วย ความผันผวนของราคา coin เพราะการตั้งราคาในระบบที่ผันผวนนั้นลำบากมาก

-ถ้า coin กำลังขึ้น คนซื้อจะไม่ซื้อ เพราะเทียบกับเงินจริงแล้วแพงขึ้น

ก็จะขาดไม่ออก จนกว่าเราจะลดราคา ยอมรับ coin ให้น้อยลงเพื่อว่าเมื่อเทียบเงินจริงแล้วเท่าๆกัน

-ถ้า coin กำลังตก แล้วรับ coin มาเท่าเดิม .. อ้าว ขาดทุน! ต้องรีบเปลี่ยนราคาเรียก coin ให้มากขึ้นเรียกว่า เหมือนพยายามจะต้องอยู่รอดในระบบเศรษฐกิจที่ไม่มีธนาคารกลางคอยดูแลเลย

### -ที่สุด สกุลเงินหลักของโลก

ด้วยเหตุผลอะไรก็แล้วแต่ถ้าคนยอมรับซื้อขายสินค้าบริการกันเยอะ+ราคานิ่งพอควรมันอาจจะสามารถ

เทียบเท่ากับเงินสกุลหลักอื่นของโลก(หรือทองคำ...อย่างที่มีขิมขณากัน)จนธนาคารกลางของแต่ละประเทศต้องเอามาใช้มาเก็บ ในคลัง/ในตระกร้าเงิน เลยทีเดียวโอ.. ถ้ามันไปถึงจุดนั้นได้จะยอดเยี่ยมเลยนะจอร์จนั่นสิ ซา ราห์..ว่าแต่มีตั้งคี่ให้ยืมซักแสนนึงก่อนมัย? จะเอาไปซื้อ coinนี้ไม่คิดถามสุขภาพกระเป๋าตังค์ขึ้นซ้ากคาก่อนหรือ?

### มุมมองรัฐ

ข้างบนนั่นคือมุมมองภาค micro-economyแต่ภาค macro-economy นั้นจะต้องมองแบบรัฐซึ่งมุมมองของรัฐต่อ crypto currency นั้นน่าจะเป็นลบเพราะ

1) ธรรมชาติค่าเงินนั้นต้องมี สินค้า/บริการ หนุนหลังจะเกิดอะไรขึ้นกับเงินบาท ถ้าคนหันไปใช้ coin กันหมด

...เงินบาทก็จะไร้ค่ายังไงละ!!กลายเป็นว่าคนไทยต้องขายบาทออกไปซื้อ coin เพื่อมาซื้อสินค้า/บริการในประเทศ

และไม่มีท่าทีจะแลกลับเป็นเงินบาทด้วย เพราะเมื่อแพร่หลายแล้วจะสามารถเอาไปซื้อสินค้า/บริการอื่นต่อได้!!!

เทียบกับ บ.ส่งออกจะแลกเงินดอลลาร์กลับเป็นบาทมาใช้จ่ายในประเทศเพราะสินค้า/วัตถุดิบล้วนเป็นเงินบาท ทำให้เศรษฐกิจฝนประเทศดีขึ้น และ ธนาคารประเทศไทยก็จะมีเงินดอลลาร์สำรองเพิ่มขึ้นสถานะการคลังของประเทศก็แข็งแกร่งขึ้น

2) รัฐจะเก็บภาษีไม่ได้เพราะข้อมูลไม่ผ่านระบบการเงินปกติถึงจะเสนอให้รัฐไปเก็บภาษีตรงที่แลก บาท <-> coin

แต่เงินปกติถ้าซื้อกันหลายทอด รัฐยังได้ภาษี เช่น

นาย A ชื้อนาย B 100 บาท มีภาษี 7 บาท เหลือ 93

นาย B ชื้อนาย C 93 บาท มีภาษี 6.51 บาท เหลือ 86.49

ไปเรื่อยๆ

แต่ถ้าเป็น coin

นาย A แลก 107 บาท หักภาษี 7 บาท เหลือเป็น coin ที่มีมูลค่า 100

ซึ่ง coin นี้จะวนในระบบไปไม่รู้กี่ทอด โดยรัฐไม่ได้ภาษีจนกระทั่งแลกออก

นาย Z แลก coin ที่มีมูลค่า 100 บาท หักภาษี 7 บาท เหลือออกมา 93 บาท

เท่ากับรัฐได้ภาษีแค่ 14 บาท จากการซื้อขายกันไม่รู้กี่รอบยิ่งถ้าแพร่หลายจนมันวนในระบบได้โดยไม่ต้องแลก

กลับเป็นเงินบาทรัฐจะได้ภาษี 7 บาทในปีแรกๆ และปีที่เหลือเป็น 0 ... ตลอดกาล!!! จะเห็นว่า crypto

currency มีข้อเสียใหญ่ในมุมมองของรัฐถึง 2 ข้อและการปรับแก้ บังคับให้ส่งบัญชี crypto ด้วยนั้นดูจะ

วุ่นวายมากกว่ายังมีระบบ cashless society ที่ทำงานได้ดีอยู่แล้วก็ไม่มีความจำเป็นจะต้องมี crypto

currency ในระบบเศรษฐกิจของประเทศเลย!!

**ศูนย์อาหารใต้ดิน** นอกจากเหตุผลข้างต้นที่เป็นสิ่งบนดินยังคงดูแยะในสายตารัฐเหตุผลจากใต้ดินยิ่งหนักเข้าไปใหญ่

เพราะ cashless society นั้นสามารถติดตามเส้นทางการเงินได้ทั้งหมดการฟอกเงินจะยาก และตามคน

เกี่ยวข้องกับมาเฟีย/แก๊งค์อาชญากรรมได้ง่ายผ่านเส้นทางการเงินหากถูกจับได้เพียงคนเดียว อาจโดนลาก

ออกมาทั้งแก๊งค์!! ยิ่งถ้า cashless society ล้ำไปถึงข้อมูล biometric เหมือนที่จีน ใช้ใบหน้า จ่ายเงินแทน QR

code กันแล้วโจรที่ถูกรอกหมายจับจะหนีรอดยากมาก

<https://www.blognone.com/node/95182> แต่ถ้า crypto currency เกิดมันจะเป็นทางเลือกทางหนึ่งของ

ธุรกิจมืด ในการฟอกเงินที่ได้มาโดยผิดกฎหมายเนื่องจากเป็นการยากที่จะรู้ว่าใครเป็นใครในระบบเพราะระบบ

มันเก็บเจ้าของเงินเป็นค่า hash จึงไม่มีทางรู้เลยว่าเป็นใครเรียกว่า อยู่บนดินก็ทำลายระบบเศรษฐกิจปกติอยู่

ใต้ดินก็ส่งเสริมให้ธุรกิจใต้ดินเฟื่องฟูด้วยดังนั้นไม่ต้องแปลกใจ ถ้าจะมีรัฐบาลไหนที่เริ่มจะแบนเงิน crypto

currency ขึ้นอยู่กับรัฐนั้นรู้ตัวช้าหรือเร็ว

เพิ่มเติม:

### ICO = IPO ของ Startup?

อีก keyword หนึ่งที่เข้าใจผิดกันคือ StartupStartup คือ กิจการใหม่ เหนือใหม่ = กิจการใหม่รูปแบบหนึ่ง ชื้อ

เหนือบัญชี ICO = ลงทุนในกิจการใหม่เหมือน IPO ถ้าเลือกเหรียญดีๆ กิจการเจ๋งๆ เราจะได้มูลค่าเพิ่มหลายเท่า

มาก จึงน่าลองเสี่ยงแต่ๆๆ จริงๆแล้วการลงทุนใน Startup ที่แท้จริงต้องเป็นแบบ venture capital คือลง

เงินแล้วได้เป็นหุ้นของกิจการ ครับ!! แต่มี fund rising ที่มาวันนี้มีใช้คำว่า "ระดมทุน" ในช่วงที่ Startup กำลังบู

มสึดซัดแต่ปรากฏว่าลงเงินแล้วจะแค้ได้สินค้ในราคาถูกพิเศษเหมือนๆกับ pre-order ตั้งแต่ยังไม่มีพิมพ์เขียว มีแต่ภาพ mock upซึ่งกลุ่มนี้ช่วงหลังๆ คนเริ่มรู้ว่าไม่ใช่การลงทุนแต่เป็นซื้อสินค้ จึงระดมเงินไม่ได้เลยพอมี กระแส coin ก็เลยหันมาออก coin กันสังเกตุว่า ICO ส่วนใหญ่สัญญาว่าจะใช้แลกสินค้ที่นั่นแล้วหยอดค้ หวานว่า ถ้าไม่รับซื้อ เตี่ยวราคา coin ค้จะขึ้นอ้ว ถ้า coin คุณขึ้น คนก็ไปซื้อสินค้/บริการ จากเจ้าอื่นสิ!! จะมาซื้อ coin แพงๆเพื่อมาแลกสินค้/บริการคุณทำไม?จริงๆแล้วการเอาเงินไปลงใน ICOค้คือการลงทุนได้เป็น หุ่นส่วนของกิจการ Startup

## Cryptocurrency มาจากค้นี้ Cryptography + Cerency

ZeroCash ค้สกุลเงินดิจิทัลที่ต้งการตบใจท้งของการปกปิดตัวตนของผู้ใช้อย่างสมบูรณ์ โดยมีหลักการ คร่าวๆ ค้ผู้ใช้สามารถทำธุรกรรมได้โดยการเอาเงินไปแลกกับใบเสร็จจึรนาม แล้วใช้ใบเสร็จนั้นทำธุรกรรม สิ่งที่จะปรากฏอยู่ให้ทุกคนเห็นในภายหลังค้ใบเสร็จไหนทำธุรกรรมอะไรไป แต่ไม่สามารถสืบกลับไปถึงต้น น้ำได้ว่าผู้ใช้ ZeroCash ที่ทำการสุ่มใบเสร็จนี้ค้ใคร

หากพูดถึง cryptocurrency หรือเงินดิจิทัล หลายคนอาจคุ้นหูกับสกุลเงินอย่าง Bitcoin ที่ราคาพุ่ง ทะยานขึ้นมาเรื่อยๆ จนทุบสถิติ ทำ New High สูงกว่า 7,000 ดอลลาร์สหรัฐฯ ต่อ 1 Bitcoin ในช่วง เดือนพฤศจิกายนที่ผ่านมา หรือมีราคาเพิ่มขึ้นมากกว่า 1 แสนเท่า นับตั้งแต่มีการเริ่มใช้สกุลเงินนี้มา ในปี 2009 ความร้อนแรงของปรากฏการณ์ครั้งนี้สร้างคำถามให้กับหลายฝ่ายว่าสิ่งนี้จะเป็สิ่งที่สร้างความสั่นคลอนให้กับสกุลเงินแบบดั้งเดิมหรือไม่ หรือจะเป็นเพียงฟองสบู่ที่เกิดจากการเก็งกำไรของ นักลงทุนบางกลุ่มที่สามารถรับความเสี่ยงได้สูงเท่านั้น?

แม้ความต้องการสกุลเงินดิจิทัลจะเพิ่มขึ้นมาอย่างท่วมท้น แต่อีไอซีมองว่า cryptocurrency ยังต้ง เผชิญกับความท้าทายอีกหลายอย่าง ทั้งความผันผวนของอัตราแลกเปลี่ยนและมุมมองของหน่วยงาน กำกับดูแลของแต่ละประเทศ ทำให้โอกาสที่คนทั่วไปจะนำมาใช้ในวงกว้างอาจไม่ถ่ายนัก อย่างไรก็ตาม แนวคิดของ cryptocurrency อย่างเทคโนโลยี blockchain ที่เป็นรากฐานของ bitcoin นับว่ามี ศักยภาพและสามารถนำไปประยุกต์ใช้กับองค์กรต่างๆ เพื่อให้ขั้นตอนการทำงานเป็นไปอย่างรวดเร็ว และมีประสิทธิภาพสูงสุด

**What is cryptocurrency and how cryptocurrencies emerged as a side product of digital cash**  
 What is cryptocurrency: 21st-century unicorn – or the money of the future?

This introduction explains the most important thing about cryptocurrencies. After you've read it, you'll know more about it than most other humans.

Today cryptocurrencies ([Buy Crypto](#)) have become a global phenomenon known to most people. While still somehow geeky and not understood by most people, banks, governments and many companies are aware of its importance.

In 2016, you'll have a hard time finding a major bank, a big accounting firm, a prominent software company or a government that did not research cryptocurrencies, publish a paper about it or start a so-called blockchain-project.

But beyond the noise and the press releases the overwhelming majority of people – even bankers, consultants, scientists, and developers – have a very limited knowledge about cryptocurrencies. They often fail to even understand the basic concepts.

So let's walk through the whole story. What are cryptocurrencies?

Where did cryptocurrency originate?

Why should you learn about cryptocurrency?

And what do you need to know about cryptocurrency?

Few people know, but cryptocurrencies emerged as a side product of another invention.

Satoshi Nakamoto, the unknown inventor of [Bitcoin](#), the first and still most important cryptocurrency, never intended to invent a currency.

In his announcement of Bitcoin in late 2008, Satoshi said he developed "A Peer-to-Peer Electronic Cash System."

His goal was to invent something; many people failed to create before digital cash.

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority. – Satoshi Nakamoto, 09 January 2009, announcing Bitcoin on SourceForge.

The single most important part of Satoshi's invention was that he found a way to build a decentralized digital cash system. In the nineties, there have been many attempts to create digital money, but they all failed.

... after more than a decade of failed Trusted Third Party based systems (Digicash, etc), they see it as a lost cause. I hope they can make the distinction, that this is the first time I know of that we're trying a non-trust based system. – Satoshi Nakamoto in an E-Mail to Dustin Trammell

After seeing all the centralized attempts fail, Satoshi tried to build a digital cash system without a central entity. Like a Peer-to-Peer network for file sharing.

This decision became the birth of cryptocurrency. They are the missing piece Satoshi found to realize digital cash. The reason why is a bit technical and complex, but if you get it, you'll know more about cryptocurrencies than most people do. So, let's try to make it as easy as possible:

To realize digital cash you need a payment network with accounts, balances, and transaction. That's easy to understand. One major problem every payment network has to solve is to prevent the so-called double spending: to prevent that one entity spends the same amount twice. Usually, this is done by a central server who keeps record about the balances.

In a decentralized network, you don't have this server. So you need every single entity of the network to do this job. Every peer in the network needs to have a list with all transactions to check if future transactions are valid or an attempt to double spend.

But how can these entities keep a consensus about this records?

If the peers of the network disagree about only one single, minor balance, everything is broken. They need an absolute consensus. Usually, you take, again, a central authority to

declare the correct state of balances. But how can you achieve consensus without a central authority?

Nobody did know until Satoshi emerged out of nowhere. In fact, nobody believed it was even possible.

Satoshi proved it was. His major innovation was to achieve consensus without a central authority. Cryptocurrencies are a part of this solution – the part that made the solution thrilling, fascinating and helped it to roll over the world.

What are cryptocurrencies really?

If you take away all the noise around cryptocurrencies and reduce it to a simple definition, you find it to be just limited entries in a database no one can change without fulfilling specific conditions. This may seem ordinary, but, believe it or not: this is exactly how you can define a currency.

Take the money on your bank account: What is it more than entries in a database that can only be changed under specific conditions? You can even take physical coins and notes: What are they else than limited entries in a public physical database that can only be changed if you match the condition than you physically own the coins and notes? Money is all about a verified entry in some kind of database of accounts, balances, and transactions.

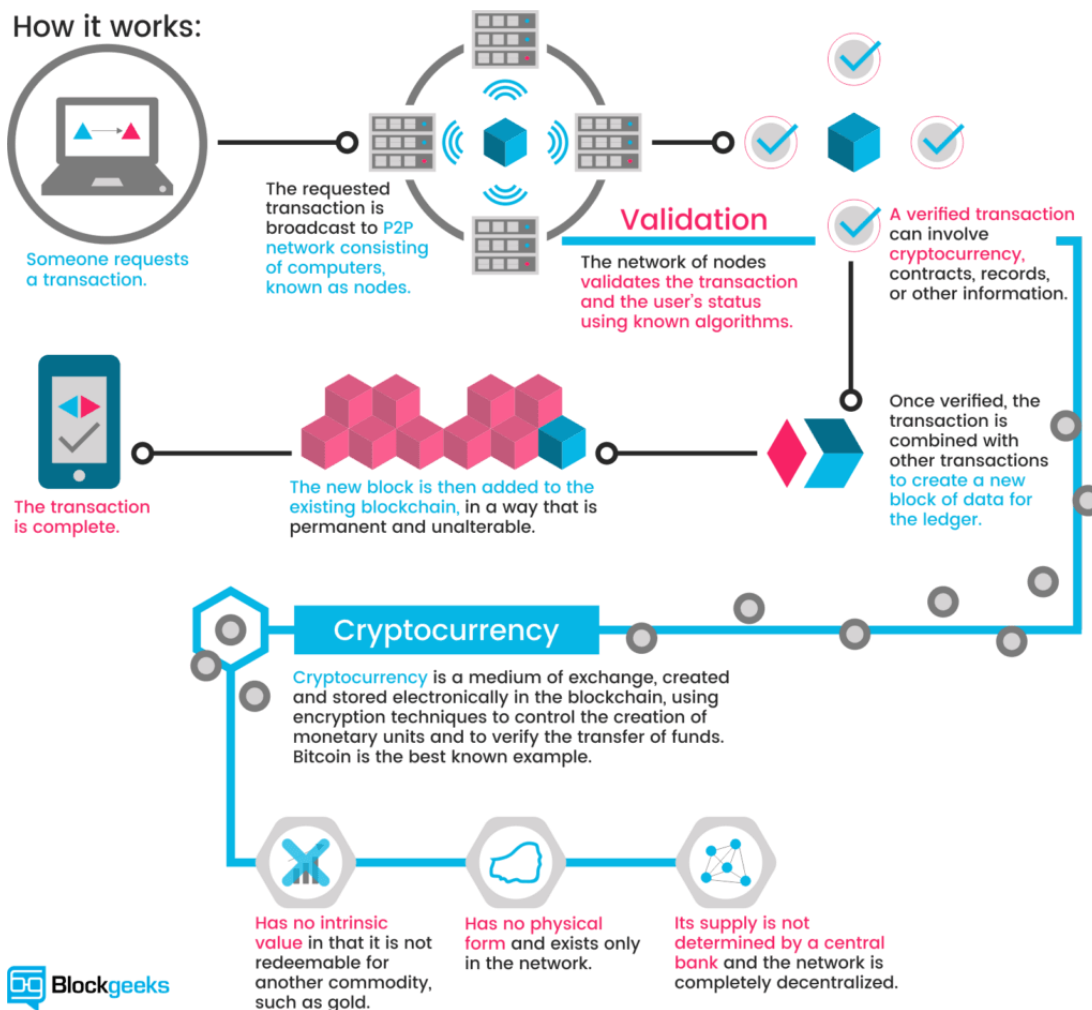
How miners create coins and confirm transactions

Let's have a look at the mechanism ruling the databases of cryptocurrencies. A

cryptocurrency like Bitcoin consists of a network of peers. Every peer has a record of the complete history of all transactions and thus of the balance of every account.

A transaction is a file that says, "Bob gives X Bitcoin to Alice" and is signed by Bob's private key. It's basic public key cryptography, nothing special at all. After signed, a transaction is broadcasted in the network, sent from one peer to every other peer. This is basic p2p-technology. Nothing special at all, again.





The transaction is known almost immediately by the whole network. But only after a specific amount of time it gets confirmed.

Confirmation is a critical concept in cryptocurrencies. You could say that cryptocurrencies are all about confirmation.

As long as a transaction is unconfirmed, it is pending and can be forged. When a transaction is confirmed, it is set in stone. It is no longer forgeable, it can't be reversed, it is part of an immutable record of historical transactions: of the so-called blockchain.

Only miners can confirm transactions. This is their job in a cryptocurrency-network. They take transactions, stamp them as legit and spread them in the network. After a transaction is

confirmed by a miner, every node has to add it to its database. It has become part of the blockchain.

For this job, the miners get rewarded with a token of the cryptocurrency, for example with Bitcoins. Since the miner's activity is the single most important part of cryptocurrency-system we should stay for a moment and take a deeper look on it.

“In the next few years, we are going to see national governments take large steps towards instituting a cashless society where people transact using centralized digital currencies.

Simultaneously, the decentralized cryptocurrencies – that some even view as harder money – will see increased use from all sectors.” – Caleb Chen [London Trust Media](#)

Principally everybody can be a miner. Since a decentralized network has no authority to delegate this task, a cryptocurrency needs some kind of mechanism to prevent one ruling party from abusing it. Imagine someone creates thousands of peers and spreads forged transactions. The system would break immediately.

So, Satoshi set the rule that the miners need to invest some work of their computers to qualify for this task. In fact, they have to find a hash – a product of a cryptographic function – that connects the new block with its predecessor. This is called the [Proof-of-Work](#). In Bitcoin, it is based on the [SHA 256 Hash algorithm](#).



You don't need to understand details about SHA 256. It's only important you know that it can be the basis of a cryptologic puzzle the miners compete to solve. After finding a solution, a miner can build a block and add it to the blockchain. As an incentive, he has the right to add a so-called coinbase transaction that gives him a specific number of Bitcoins. This is the only way to create valid Bitcoins.

Bitcoins can only be created if miners solve a cryptographic puzzle. Since the difficulty of this puzzle increases the amount of computer power the whole miner's invest, there is only a specific amount of cryptocurrency token that can be created in a given amount of time. This is part of the consensus no peer in the network can break.

Revolutionary properties

If you really think about it, Bitcoin, as a decentralized network of peers which keep a consensus about accounts and balances, is more a currency than the numbers you see in your bank account. What are these numbers more than entries in a database – a database which can be changed by people you don't see and by rules you don't know?

“It is that narrative of human development under which we now have other fights to fight, and I would say in the realm of Bitcoin it is mainly the separation of money and state.”

– Erik Voorhees, [cryptocurrency entrepreneur](#)

Basically, cryptocurrencies are entries about token in decentralized consensus-databases. They are called CRYPTOcurrencies because the consensus-keeping process is secured by strong cryptography. Cryptocurrencies are built on [cryptography](#). They are not secured by people or by trust, but by math. It is more probable that an asteroid falls on your house than that a bitcoin address is compromised.

Describing the properties of cryptocurrencies we need to separate between transactional and monetary properties. While most cryptocurrencies share a common set of properties, they are not carved in stone.

Transactional properties:

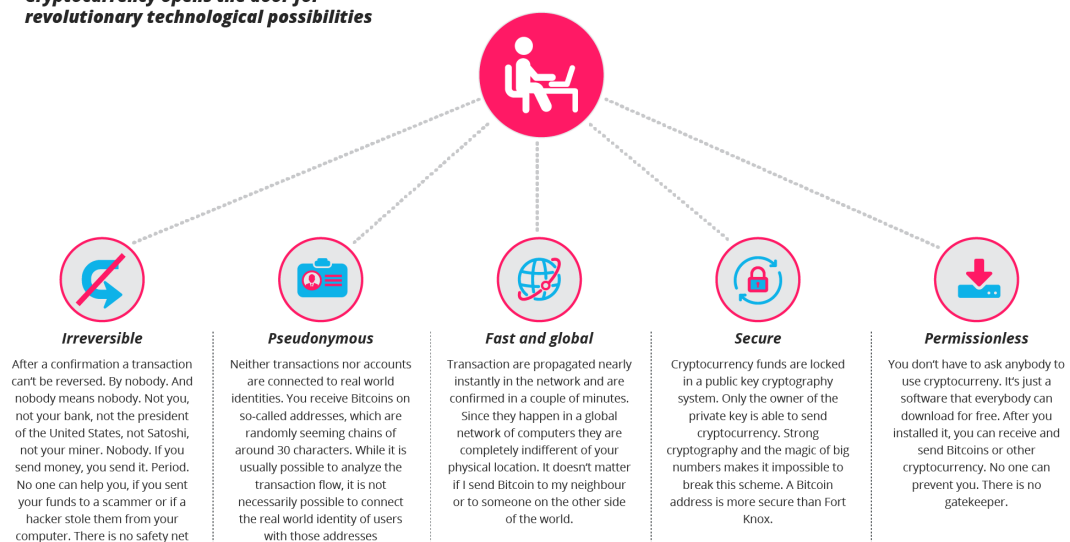
- 1.) Irreversible: After confirmation, a transaction can't be reversed. By nobody. And nobody means nobody. Not you, not your bank, not the president of the United States, not Satoshi, not your miner. Nobody. If you send money, you send it. Period. No one can help you, if you sent your funds to a scammer or if a hacker stole them from your computer. There is no safety net.
- 2.) Pseudonymous: Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction flow, it is not necessarily possible to connect the real world identity of users with those addresses.
- 3.) Fast and global: Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent of your physical location. It doesn't matter if I send Bitcoin to my neighbour or to someone on the other side of the world.

4.) Secure: Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.

5.) Permissionless: You don't have to ask anybody to use cryptocurrency. It's just a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.

**Cryptocurrency opens the door for revolutionary technological possibilities**

Blockgeeks



Monetary properties:

1.) Controlled supply: Most cryptocurrencies limit the supply of the tokens. In Bitcoin, the supply decreases in time and will reach its final number somewhere in around 2140. All cryptocurrencies control the supply of the token by a schedule written in the code. This means the monetary supply of a cryptocurrency in every given moment in the future can roughly be calculated today. There is no surprise.

2.) No debt but bearer: The Fiat-money on your bank account is created by debt, and the numbers, you see on your ledger represent nothing but debts. It's a system of IOU.

Cryptocurrencies don't represent debts. They just represent themselves. They are money as hard as coins of gold.

To understand the revolutionary impact of cryptocurrencies you need to consider both properties. Bitcoin as a permissionless, irreversible and pseudonymous means of payment is an attack on the control of banks and governments over the monetary transactions of their citizens. You can't hinder someone to use Bitcoin, you can't prohibit someone to accept a payment, you can't undo a transaction.

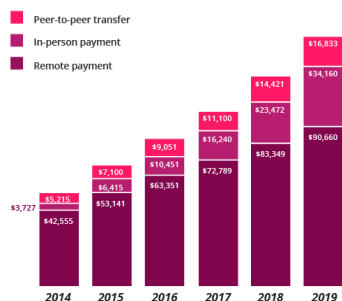
As money with a limited, controlled supply that is not changeable by a government, a bank or any other central institution, cryptocurrencies attack the scope of the monetary policy. They take away the control central banks take on inflation or deflation by manipulating the monetary supply.

“While it's still fairly new and unstable relative to the gold standard, cryptocurrency is definitely gaining traction and will most certainly have more normalized uses in the next few years. Right now, in particular, it's increasing in popularity with the post-election market uncertainty. The key will be in making it easy for large-scale adoption (as with anything involving crypto) including developing safeguards and protections for buyers/investors. I expect that within two years, we'll be in a place where people can shove their money under the virtual mattress through cryptocurrency, and they'll know that wherever they go, that money will be there.” – Sarah Granger, Author, and Speaker.

Cryptocurrencies: Dawn of a new economy

Mostly due to its revolutionary properties cryptocurrencies have become a success their inventor, Satoshi Nakamoto, didn't dare to dream of it. While every other attempt to create a digital cash system didn't attract a critical mass of users, Bitcoin had something that provoked enthusiasm and fascination. Sometimes it feels more like religion than technology.

**US mobile payments are expected to hit \$142 billion by 2019**



"Peer-to-peer" transfer occur when one person pays another person using a mobile device. The device uses either a preloaded app or a browser-based app to initiate, authenticate, and transfer funds

**Peer-to-peer**



"In-person" purchases are initiated using a mobile device where the buyer and seller are in-person, usually at a brick-and-mortar retail location where the product/ service is immediately delivered.

**In-person**



"Remote" payments are made when a buyer purchases goods or services using a mobile device, but the buyer is not physically present with the seller and the good are not immediately delivered(as with eCommerce).

**Remote**

Source: Forrester research, "US mobile payments forecast, 2014 to 2019" November 17, 2014





















Cryptocurrencies are digital gold. Sound money that is secure from political influence. Money that promises to preserve and increase its value over time. Cryptocurrencies are also a fast and comfortable means of payment with a worldwide scope, and they are private and anonymous enough to serve as a means of payment for black markets and any other outlawed economic activity.

But while cryptocurrencies are more used for payment, its use as a means of speculation and a store of value dwarfs the payment aspects. Cryptocurrencies gave birth to an incredibly dynamic, fast-growing market for investors and speculators. Exchanges like Okcoin, [poloniex](#) or [shapeshift](#) enables the trade of hundreds of cryptocurrencies. Their daily trade volume exceeds that of major European stock exchanges.

At the same time, the praxis of [Initial Coin Distribution](#) (ICO), mostly facilitated by Ethereum's smart contracts, gave live to incredibly successful crowdfunding projects, in which often an idea is enough to collect millions of dollars. In the case of "The DAO" it has been more than 150 million dollars.

In this rich ecosystem of coins and token, you experience extreme volatility. It's common that a coin gains 10 percent a day – sometimes 100 percent – just to lose the same at the next day. If you are lucky, your coin's value grows up to 1000 percent in one or two weeks.

While Bitcoin remains by far the most famous cryptocurrency and most other cryptocurrencies have zero non-speculative impact, investors and users should keep an eye on several cryptocurrencies. Here we present the most popular cryptocurrencies of today.

▲#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$11,382,240,050	\$712.76	15,969,336 BTC	\$67,288,200	-1.60%	
2	 Ethereum	\$904,848,975	\$10.54	85,831,133 ETH	\$4,069,260	-1.21%	
3	 Ripple	\$290,446,848	\$0.008121	35,765,131,899 XRP *	\$2,386,420	0.26%	
4	 Litecoin	\$184,904,214	\$3.82	48,378,029 LTC	\$2,258,970	-1.05%	
5	 Monero	\$83,466,495	\$6.27	13,311,446 XMR	\$3,134,490	5.38%	
6	 Ethereum Classic	\$80,817,441	\$0.942637	85,735,486 ETC	\$603,573	2.21%	
7	 Dash	\$66,519,213	\$9.68	6,874,532 DASH	\$596,632	-0.77%	
8	 Augur	\$52,038,360	\$4.73	11,000,000 REP *	\$396,072	6.38%	
9	 NEM	\$37,322,550	\$0.004147	8,999,999,999 XEM *	\$86,817	4.40%	
10	 Waves	\$35,727,500	\$0.357275	100,000,000 WAVES *	\$133,650	-3.94%	

Source: [coinmarketcap](https://coinmarketcap.com)

## Bitcoin

The one and only, the first and most famous cryptocurrency. Bitcoin serves as a digital gold standard in the whole cryptocurrency-industry, is used as a global means of payment and is the de-facto currency of cyber-crime like darknet markets or ransomware. After seven years in existence, Bitcoin's price has increased from zero to more than 650 Dollar, and its transaction volume reached more than 200.000 daily transactions.



There is not much more to say: Bitcoin is here to stay.

## Ethereum

The brainchild of young crypto-genius Vitalik Buterin has ascended to the second place in the hierarchy of cryptocurrencies. Other than Bitcoin its blockchain does not only validate a set of accounts and balances but of so-called states. This means that Ethereum can not only process transactions but complex contracts and programs.

This flexibility makes Ethereum the perfect instrument for blockchain -application. But it comes at a cost. After the Hack of the DAO – an Ethereum based smart contract – the developers decided to do a hard fork without consensus, which resulted in the emerge of Ethereum Classic. Besides this, there are several clones of Ethereum, and Ethereum itself is a host of several Tokens like DigixDAO and Augur. This makes Ethereum more a family of cryptocurrencies than a single currency.

## Ripple

Maybe the less popular – or most hated – project in the cryptocurrency community is Ripple. While Ripple has a native cryptocurrency – XRP – it is more about a network to process IOUs than the cryptocurrency itself. XRP, the currency, doesn't serve as a medium to store and exchange value, but more as a token to protect the network against spam.

Ripple Labs created every XRP-token, the company running the Ripple network, and is distributed by them on will. For this reason, Ripple is often called pre-mined in the community and dissed as no real cryptocurrency, and XRP is not considered as a good store of value.

Banks, however, seem to like Ripple. At least they adopt the system with an increasing pace.

## Litecoin

Litecoin was one of the first cryptocurrencies after Bitcoin and tagged as the silver to the digital gold bitcoin. Faster than bitcoin, with a larger amount of token and a new mining algorithm, Litecoin was a real innovation, perfectly tailored to be the smaller brother of bitcoin. “It facilitated the emerge of several other cryptocurrencies which used its codebase but made it, even more, lighter“. Examples are Dogecoin or Feathercoin.

While Litecoin failed to find a real use case and lost its second place after bitcoin, it is still actively developed and traded and is hoarded as a backup if Bitcoin fails.

Monero

Monero is the most prominent example of the cryptonite algorithm. This algorithm was invented to add the privacy features Bitcoin is missing. If you use Bitcoin, every transaction is documented in the blockchain and the trail of transactions can be followed. With the introduction of a concept called ring-signatures, the cryptonite algorithm was able to cut through that trail.

The first implementation of cryptonite, Bytecoin, was heavily premined and thus rejected by the community. Monero was the first non-premined clone of bytecoin and raised a lot of awareness. There are several other incarnations of cryptonote with their own little improvements, but none of it did ever achieve the same popularity as Monero.

Monero's popularity peaked in summer 2016 when some darknetmarkets decided to accept it as a currency. This resulted in a steady increase in the price, while the actual usage of Monero seems to remain disappointingly small.

Besides those, there are hundreds of cryptocurrencies of several families. Most of them are nothing more than attempts to reach investors and quickly make money, but a lot of them promise playgrounds to test innovations in cryptocurrency-technology.

## What is Cryptocurrency?



Cryptocurrency is a digital money, created from code.



Free of all governmental oversight, The cryptocurrency economy is monitored by a peer-to-peer internet protocol .



Cryptocurrency is an encrypted string of data or a hash, encoded to signify one unit of currency

## Examples of Cryptocurrency



Bitcoin Market Cap  
\$11,322,347,786



Ethereum Market Cap  
\$928,068,434



Ripple Market Cap  
\$293,888,278

What is the future of Cryptocurrency?

The market of cryptocurrencies is fast and wild. Nearly every day new cryptocurrencies emerge, old die, early adopters get wealthy and investors lose money. Every cryptocurrency comes with a promise, mostly a big story to turn the world around. Few survive the first months, and most are pumped and dumped by speculators and live on as zombie coins until the last bagholder loses hope ever to see a return on his investment.

“In 2 years from now, I believe cryptocurrencies will be gaining legitimacy as a protocol for business transactions, micropayments, and overtaking Western Union as the preferred remittance tool. Regarding business transactions – you’ll see two paths: There will be financial businesses which use it for it’s no fee, nearly-instant ability to move any amount of

money around, and there will be those that utilize it for its blockchain technology. Blockchain technology provides the largest benefit with trustless auditing, single source of truth, smart contracts, and color coins.”

– Cody Littlewood, and I’m the founder and CEO of Codelitt

Markets are dirty. But this doesn’t change the fact that cryptocurrencies are here to stay – and here to change the world. This is already happening. People all over the world buy Bitcoin to protect themselves against the devaluation of their national currency. Mostly in Asia, a vivid market for Bitcoin remittance has emerged, and the Bitcoin using darknets of cybercrime are flourishing. More and more companies discover the power of Smart Contracts or token on Ethereum, the first real-world application of blockchain technologies emerge.

The revolution is already happening. Institutional investors start to buy cryptocurrencies. Banks and governments realize that this invention has the potential to draw their control away. Cryptocurrencies change the world. Step by step. You can either stand beside and observe – or you can become part of history in the making.