Blockchain as a New Framework for Unmanned Systems

Misty Blowers, PhD
Datalytica, LLC

Overview

- **Background on Blockchain Technologies**
- **Why Blockchain as a Framework for Unmanned Systems?**
- **Emerging trends in blockchain ecosystems**
  - Monero
  - Ethereum
  - DAOs
  - Singularity Net
- **Unmanned Systems**
- **Logistics Chain Management**

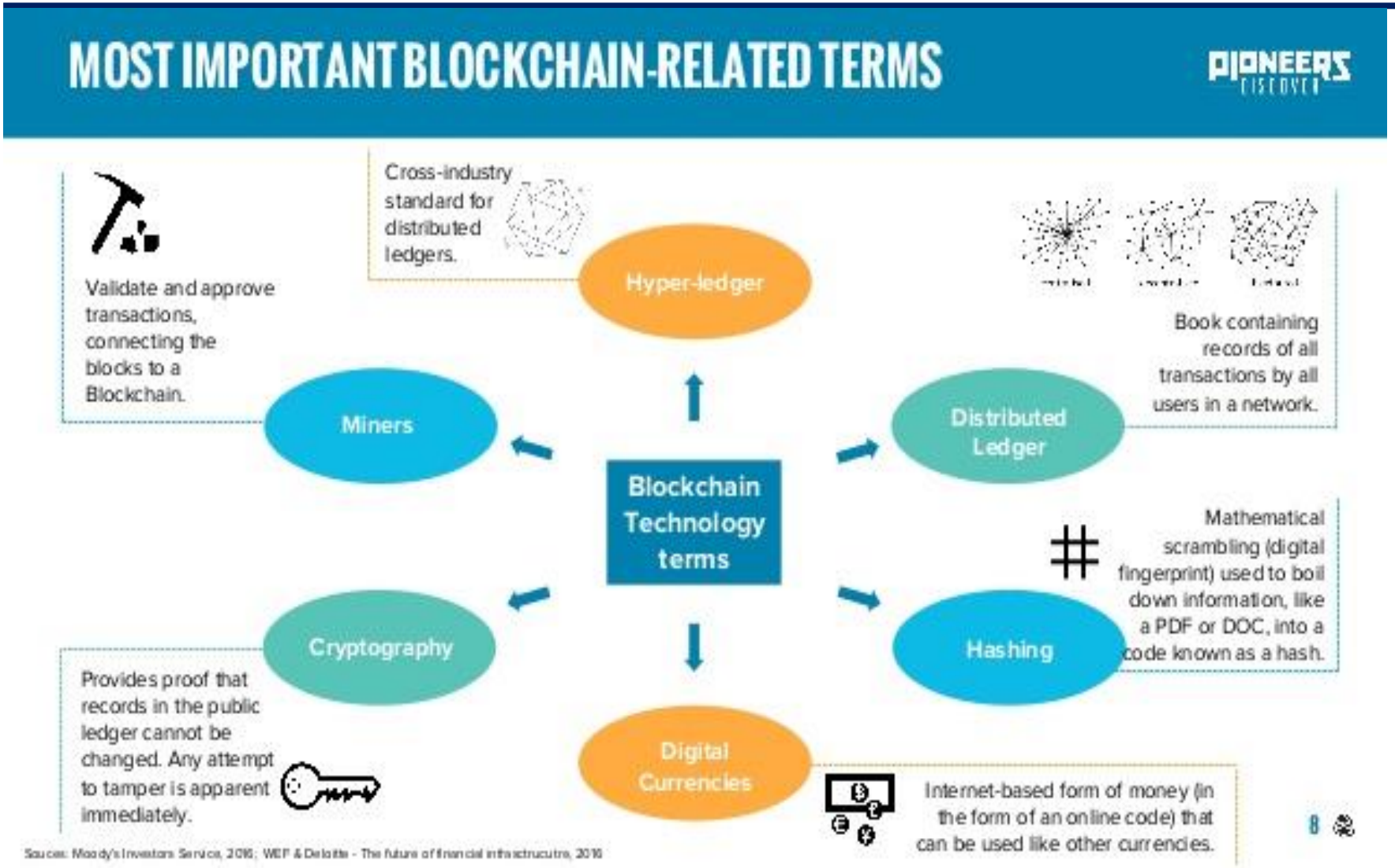
Background on Use for Unmanned Systems

- **In the governance of a system of unmanned systems, blockchain technologies and smart contracts have been explored for their potential to provide the following benefits**
  - A security-enhanced control mechanism that permits or prohibits access to an off-chain resource in an intelligent manner, and allows contracts to be timebound, condition-bound, or open-ended
  - A formalism for translating any contract or structured corresponding contract into a corresponding contract model
  - Method for implementing intelligent computing agents that follow and execute the logic embedded in a contract model and deterministic finite automation for holding a secure, transparent record of agents code on the blockchain
  - Mechanism for maintaining a hierarchy of subcontracts allowing control over different aspects of the overall command structure to be partitioned
  - Mechanism to hold a secure, public record of contracts on the blockchain, in a manner that allows automated determination of their validity, and release of their details to authorized entities upon validation.
  - Potential for Cross-Domain Solutioning – maintaining multiple levels of classification across communication channels

A. Kapitonov, S. Lonshakov, A. Krupenkin and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, Linkoping, 2017, pp. 84-89.

B. C. Wright and A. Serguieva, "Sustainable blockchain-enabled services: Smart contracts," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 4255-4264.

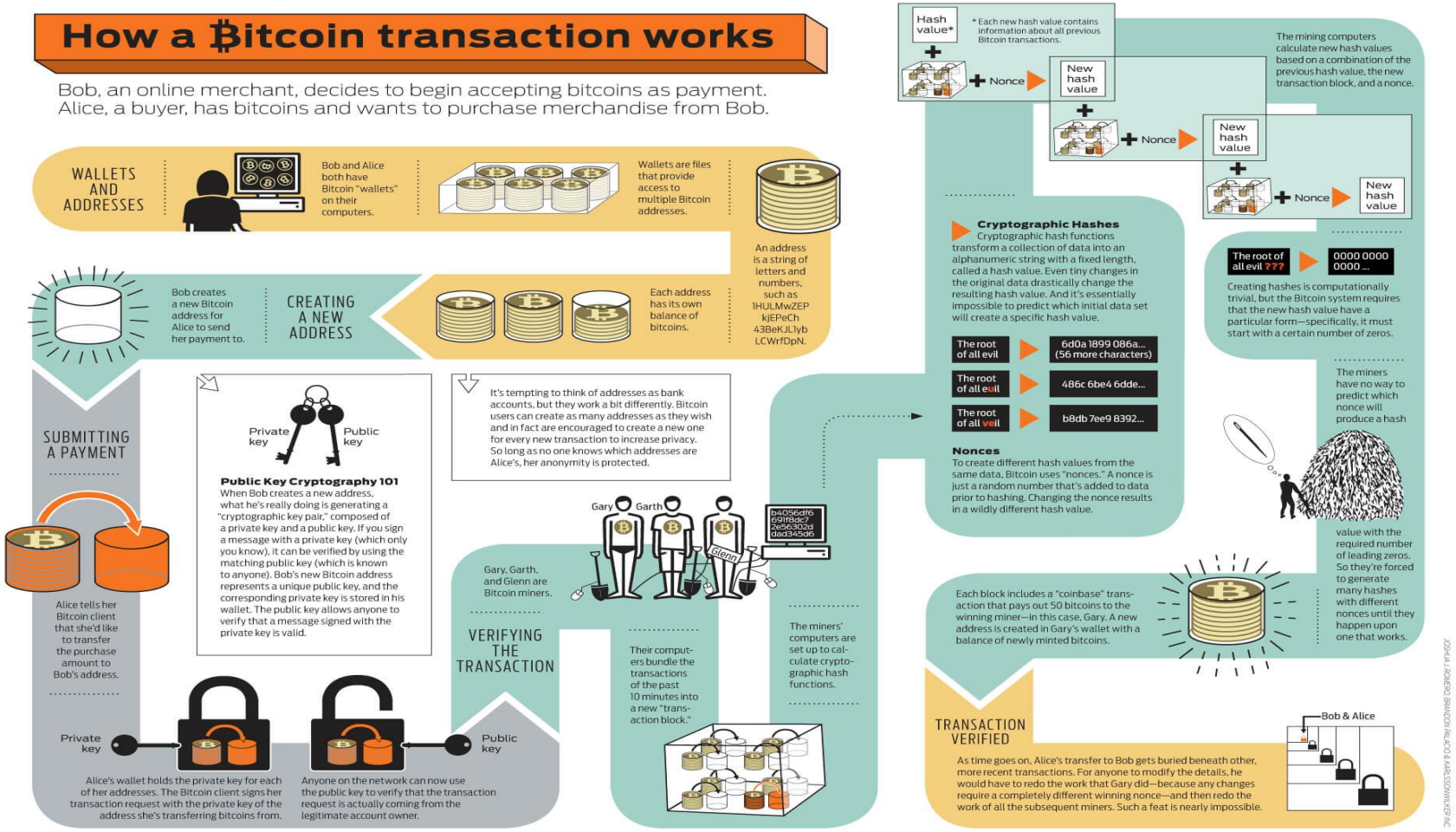
Blockchain Related Terms



History of Blockchain Technologies

- **2007 – Keyless Signature Infrastructure**
  - Keyless Signature Infrastructure (KSI) technology was developed in 2007 with the goal to impart a tag on any digital file that would forever be effective in determining its authenticity. Exploiting a mathematically derived artifact of a file called a hash along with the hashes of other files created in the same time increment, and combining them in a mathematically known manner called a hash tree or a Merkle Tree; this cryptographically linked all the artifacts of the files created or modified in that time increment and creates a top root hash that can be used in a proof that shows the contribution of every file
- **2008 - Bitcoin Whitepaper by Nakamoto is published**
- **2010- Documented first bitcoin purchase (for a $25 pizza)**
- **2014- Ethereum Project- a blockchain platform with the ability to build decentralized applications- fully funded by a "crowd sale"**
- **2016- First Distributed Autonomous Organization (DAO)**
  - One central factor that is driving market demand for the most popular cryptocurrencies (like Bitcoin and Ethereum) is the "red hot" initial coin offering (ICO) market, where a company issues digital coins or tokens that provide access to a service (often called a "utility" or "app" token) or that represent an investment opportunity in the company (like a traditional security).
- **2017 - ICOs generated over $1.2 billion of new start-up capital**
- **2018 – Government institutions start openly publishing funding opportunities for innovative applications of blockchain technologies and distributed ledger technologies for military applications**

History and Origins- Bitcoin Overview



Source:
https://www.zerohedge.com/sites/default/files/images/user3303/imageroot/2013/05/20130512_BTC.jpg

Pros and Cons of Bitcoin Architecture: Bitcoin Traceability

- **You send bitcoin by pointing to a previous transaction in the chain**
- **That transaction points to the previous transactions all of the way back until the "coinbase" transaction that it was originally created in.**
  - The coinbase transaction is the first transaction in a new block. The recipient of the coinbase transaction can choose to have the block reward, and transaction fees sent to one bitcoin address, or the bitcoins can be sent to a multitude of different addresses.
- **Numerous researches have demonstrated the feasibility of linking Bitcoin addresses with IP addresses**
- **You can look up your transaction in a blockchain explorer.**

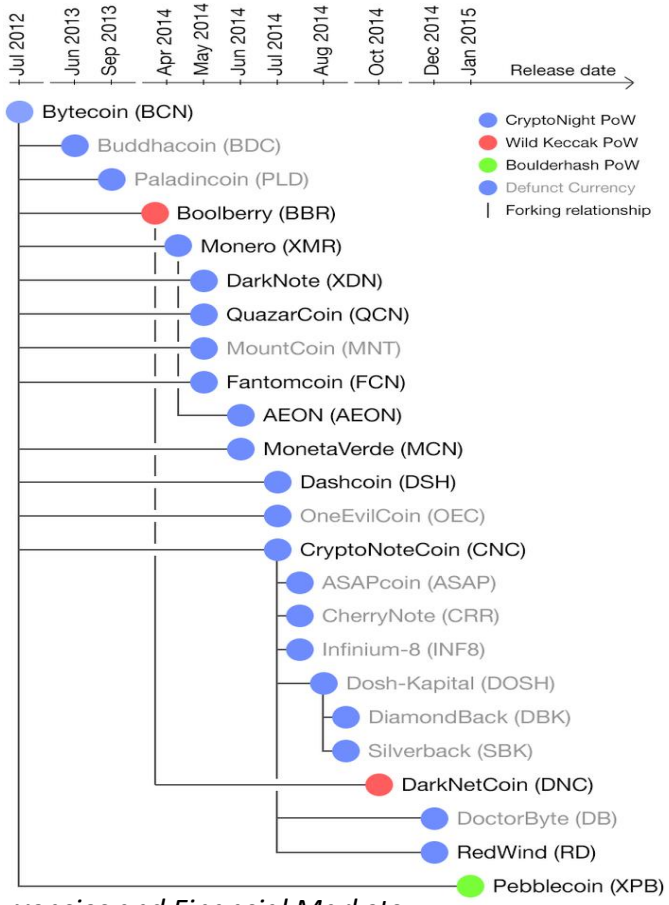
https://blockchain.info/

- The beauty of Bitcoin, from a detective's point of view, is that the blockchain records all.

"If you catch a dealer with drugs and cash on the street, you've caught them committing one crime," but if you catch people using something like Silk Road, you've uncovered their whole criminal history, it's like discovering their books."- Quote from Meiklejohn, Pen State

Truly Anonymizing Cryptocurrency

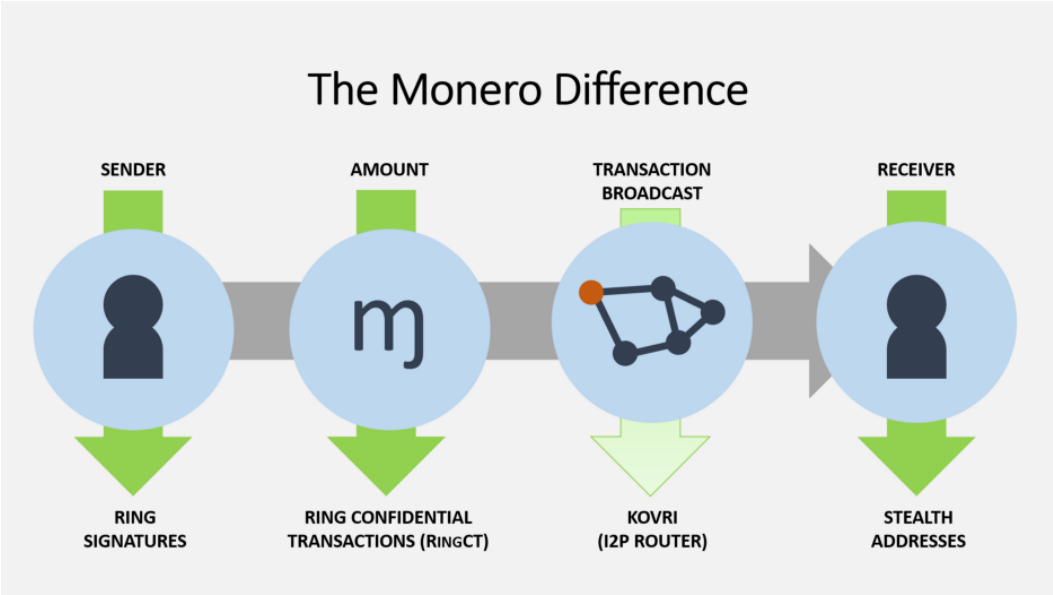
- **New virtual currencies have been designed with explicit support for mixing and anonymizing the users transactions**
  - Make use of strategies to explicitly unlink the addresses and past transactions.
  - Examples:
    - Monero
    - Z-Cash
    - PIVX
    - Komodo
    - Z-coin
    - NAV Coin
    - ZenCash
    - Verge



"Chart of the Day." *Insider.pro Is an Illustrated Edition about Cryptocurrencies and Financial Markets.*, en.insider.pro/infographics/2018-05-08/chart-day/

Architecture Behind the Anonymous Cryptocurrency- Monero

- Monero has been ranked one of the highest for privacy features
  - Has proven itself in past cases: Example: law enforcement wasn't able to find how much Monero the Alphabay owner had at the time of shutdown.
- Uses complex on-chain cryptographic methods such as Ring signatures, RingCT, Kovri and Stealth addresses to protect privacy
- Downside - complicated cryptography, which results in the transaction sizes being 50 times bigger than that of Bitcoin.



"Zcash vs Monero: An in-Depth Look." *AtoZ*, atozmarkets.com/news/zcash-vs-monero-comparison/.

Bitcoin vs Monero

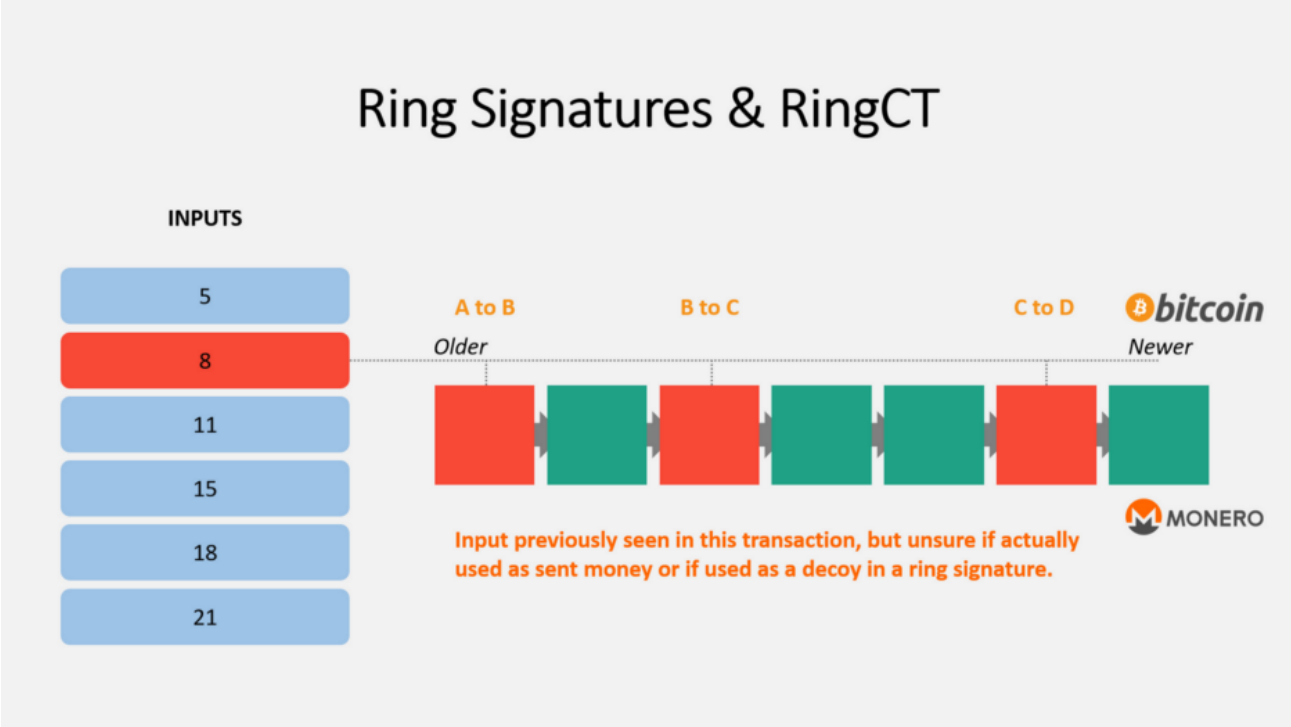
- **In Bitcoin….**
  - Public address looks like this: 1EjqMGa5j6JNQDMNXkrRZq7WSmqLRzn9fU
  - Use it to receive funds, anyone can see how much
    - When sending funds, your transaction is announced to the entire Bitcoin network. The funds that you own now belong to the recipient's public address. The transaction is fully public.

- **In Monero….**
  - Public address looks like this:
    - 43EH3omZSUYCmJYskCUx2tV5oB5tLVrp58AeMYLrFhcz2umUVQHiHu62nG5CS3mvcfgKHC3fPtq6DHkEbMjqvCAZJW5nw9E
  - Unlike Bitcoin, your funds are not associated with your public address.
    - Funds are sent to a randomly created brand new one-time destination address. No public record of sending or receiving funds.
    - Your public address will never appear in the public record of transactions. -'stealth address' is recorded
    - When the recipient checks for funds, they need to scan the Monero blockchain to see if any transactions are destined for them.
      - Recipient has a secret view key which is used to check each transaction to see if it was addressed to them.
      - Since recipient is the only one that knows the secret view key, only the recipient can see that funds have been sent to them.

"Zcash vs Monero: An in-Depth Look." *AtoZ*, atozmarkets.com/news/zcash-vs-monero-comparison/

Monero

- **Ring confidential transactions, or RingCT, and Ring Signatures hide the value actually being spent and the transaction origins.**

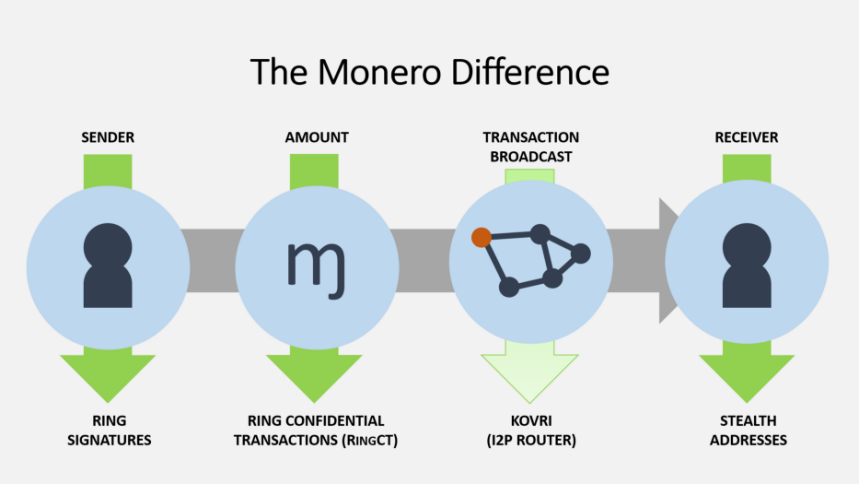


"Zcash vs Monero: An in-Depth Look." *AtoZ*, atozmarkets.com/news/zcash-vs-monero-comparison/

Kovri- Invisible Internet Project

Uses go beyond cryptocurrency obfuscation

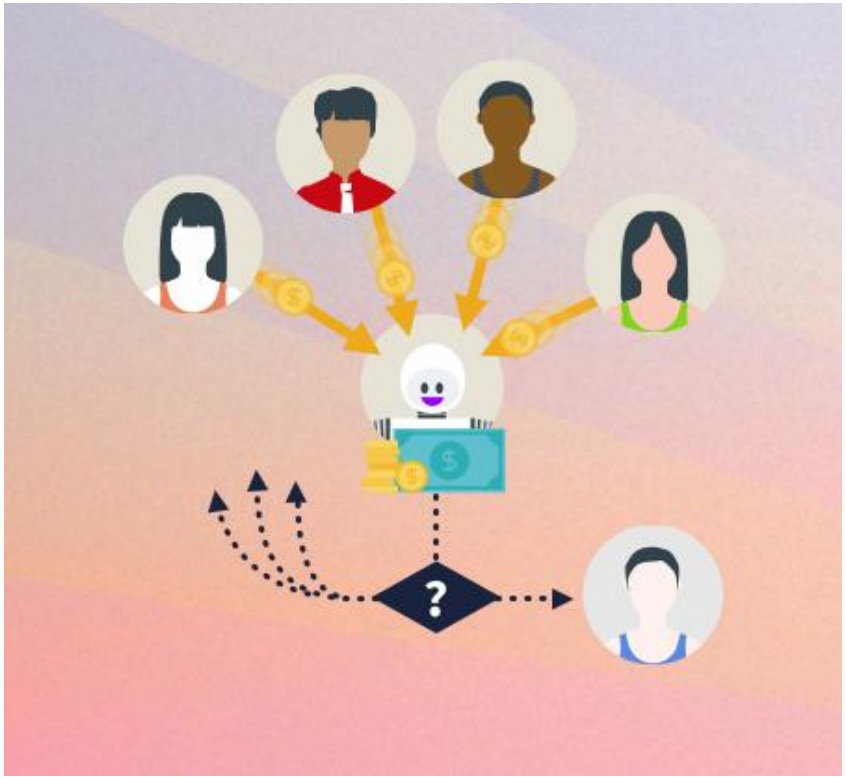
- **Project Kovri - currently in development**
  - Hides your internet traffic so that passive network monitoring cannot reveal that you are using Monero at all.
  - Achieved by encrypting all of your Monero traffic and routing it through I2P (Invisible Internet Project) nodes.
    - Nodes pass your messages along and have no visibility over what is in them.
    - Obfuscates information about whether the destination they're sending your messages to is the final destination or just a waypoint which will further forward your message.
    - Passive listeners can tell you are using I2P, but cannot tell what you are using it for or what destinations you are interacting with.



"Zcash vs Monero: An in-Depth Look." *AtoZ*, atozmarkets.com/news/zcash-vs-monero-comparison/

Ethereum- Architecture

- Using Ethereum, a contract can be created that will hold a contributor's money until any given date or goal is reached.
- Depending on the outcome, the funds will either be released to the project owners or safely returned back to the contributors.
- All of this is possible without requiring a centralized arbitrator, clearinghouse or having to trust anyone.



Source: https://www.ethereum.org/

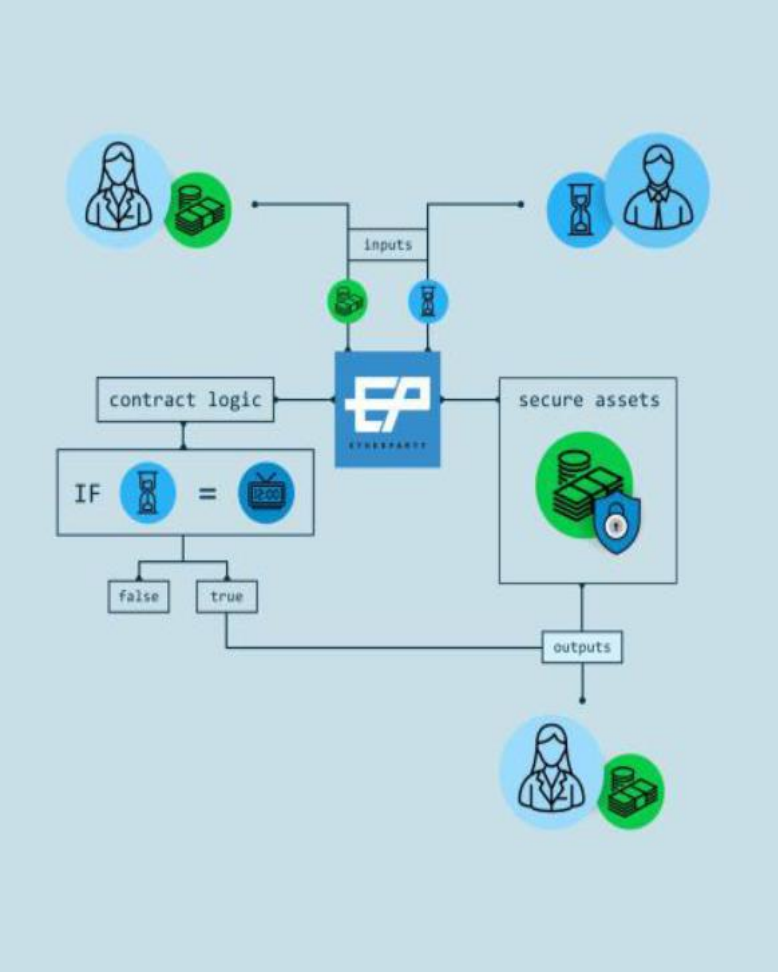
Ethereum- Architecture

- An Ethereum contract can also be designed to collect proposals from the group that backs the organization and submit them through a completely transparent voting process.
- One of the many advantages of having a robot run your organization is that it is immune to any outside influence as it's guaranteed to execute only what it was programmed to.

Source: https://www.ethereum.org/

Architecture -Distributed Autonomous Organization (DAO)

- **Smart contracts are pieces of code that live on the blockchain and execute commands exactly how they are instructed**
  - They can read other contracts, make decisions, send ether and execute other contracts.
  - Contracts will exist and run as long as the whole network exists, and will only stop if they run out of gas or if they were programmed to self destruct.
- **Think of a DAO as the constitution of a country, the executive branch of a government or maybe like a robotic manager for an organization.**
  - A DAO receives the money that your organization raises, keeps it safe and uses it to fund whatever its members want.
- **ICO's can be translated to tokens - distributed using a crowd-sale.**
  - In one use of tokens- they are considered securities and must be registered by the SEC. (See *Analysis under the Howey Test*)
    - Similar to being a shareholder in a company, the token can be traded on the open market and the vote is proportional to amounts of tokens the voter holds.
  - Many other uses of tokens



Lange, Felix. "Ethereum/Go-Ethereum." *GitHub*, github.com/ethereum/go-ethereum/wiki/Contract-Tutorial.

SingularityNET

Where blockchain meets AI…

- **Started as "Artificial Intelligence as a Service"**
- **Eventually will evolve into a completely self-organizing AI network**
- **Open marketplace where AI developers exchange their tools and services for SingularityNET's AGI token or even for other tools and services.**
  - To make these transactions as simple as possible, SingularityNET provides APIs to incorporate standard AI services, like image and language processing, into smart contracts.
  - The platform also uses smart contracts to facilitate other types of services such as matchmaking the favorable combination of exchanges between Agents and powering votes for governance issues.
  - Agents are the entities that execute the smart contracts on the platform. These are most commonly nodes on the network.

"What Is SingularityNET (AGI)? | Beginner's Guide." *CoinCentral*, 1 May 2018, coincentral.com/singularitynet-beginner-guide/.

SingularityNET

- **Agent's rank each other after each exchange on a 0 or 1 scale. Leaving a ranking isn't required and can also be automated. If an Agent marks a task complete and sends payment, it's safe to assume that a 1 ranking is appropriate.**

- **Agent rankings are multi-faceted, though, expanding beyond exchange reputation. Other factors that determine the overall ranking of an Agent include:**
  - AGI Token Staking. Agents will lose portions of what they stake if their ratings in some aspects fall below a certain level.
  - Benefit Ranking. This is a ranking specific to the beneficial tasks an Agent performs. These are tasks that improve the overall ecosystem and don't necessarily have monetary backing.
  - External Validation. Agents receive additional ranking bonuses when they prove ownership by a reputable company through a Know Your Customer (KYC) service.

SingularityNET

- **The self-organizing AI internetworking vision**
  - Example: Sophia
    - uses a combination of AI Agents that range from natural language processing to physical motor controls to operate.
    - User **"very nicely asks"** Sophia to summarize a video that's embedded in a webpage.
      - Sophia sends a request to Agent A. Through its AI, Agent A knows that Agent B specializes in analyzing and transcribing video while Agent C specializes in summarizing text.
      - Agent A pays Agent B and Agent C to perform these tasks while Sophia pays Agent A to coordinate.
      - All the while, each Agent has updated their own AI with the network information gained from these tasks and combines it with their previous experiences and knowledge.
      - Therefore, the collective AI of the system grows at a faster rate than any individual Agent.

- **AI Agents will eventually be able to produce new AI Agents from the information that they obtain overtime. This network grows and self-organizes automatically.**

https://vimeo.com/248331801

Blockchain as a Framework for Unmanned System

- By combining peer-to-peer networks with cryptographic algorithms a group of agents can reach an agreement on a particular state of affairs and record that agreement.
- Smart contracts provide a supervised means of governance and negotiation in an autonomous fashion with the added benefit of transparency and security through the underlying blockchain by which the task are executed
- The combination of blockchain with the governance of a smart contract can provide the necessary capabilities to make robotic swarm operations more secure, autonomous, and flexible.

References

1. Durden, Tyler. *Visualizing How A Bitcoin Transaction Works*, 12 May 2013, www.zerohedge.com/sites/default/files/images/user3303/imageroot/2013/05/20130512_BTC.jpg
2. A. Kapitonov, S. Lonshakov, A. Krupenkin and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, Linkoping, 2017, pp. 84-89.
3. C. Wright and A. Serguieva, "Sustainable blockchain-enabled services: Smart contracts," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 4255-4264.
4. doi: 10.1109/BigData.2017.8258452
5. Yeow , Addy. “Global Bitcoin Nodes Distribution.” *Global Bitcoin Nodes Distribution - Bitnodes*, 3 July 2018, https://bitnodes.earn.com
6. “Bitcoin Block Explorer - Blockchain.” *Blockchain.info*, https://www.blockchain.com/en/explorer
7. Falcon, Ernesto. “Actually, Congress Did Undermine Our Internet Privacy Rights.” *Electronic Frontier Foundation*, 6 May 2017, www.eff.org/deeplinks/2017/05/congress-repealing-our-internet-privacy-rights-meant-congress-repealed-internet
8. Shepardson, David. “Trump Signs Repeal of U.S. Broadband Privacy Rules.” Reuters, Thomson Reuters, 4 Apr. 2017, www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR
9. “Chart of the Day.” *Insider.pro Is an Illustrated Edition about Cryptocurrencies and Financial Markets.*, en.insider.pro/infographics/2018-05-08/chart-day/
10. “Zcash vs Monero: An in-Depth Look.” *AtoZ*, atozmarkets.com/news/zcash-vs-monero-comparison/
11. “Treasure Wallpaper Enam Wallpaper.” *Wallpaper.enam.site*, wallpaper.enam.site/treasure-wallpaper/.
12. Sward, Andrew, Ivy Vecna, and Forrest Stonedahl. "Data Insertion in Bitcoin's Blockchain." Ledger 3 (2018)
13. Drake, Nate. “How to Use a Bitcoin Tumbler.” *TechRadar*, TechRadar The Source for Tech Buying Advice, 14 Nov. 2017, www.techradar.com/how-to/how-to-use-a-bitcoin-tumbler.
14. Kandpal, Akash. “Monero - An Anonymous CryptoCurrency – Akash Kandpal – Medium.” *Medium*, Augmenting Humanity, 29 Dec. 2017, medium.com/@harrypotter0/how-does-monero-work-17f18ea37652.
15. Möser, Malte, et al. “Monero: Response To.” *Getmonero.org, The Monero Project*, 13 Apr. 2017, getmonero.org/2018/03/29/response-to-an-empirical-analysis-of-traceability.html.
16. Darrell, Gilbert A. “A Connected World, Communications in Smart Cities – Gilbert A. Darrell – Medium.” *Medium*, Augmenting Humanity, 16 May 2018, medium.com/@artiedarrell/a-connected-world-communications-in-smart-cities-3fe793a7c429.
17. Sward, Andrew, Ivy Vecna, and Forrest Stonedahl. "Data Insertion in Bitcoin's Blockchain." Ledger 3 (2018).
18. Lange, Felix. “Ethereum/Go-Ethereum.” *GitHub*, github.com/ethereum/go-ethereum/wiki/Contract-Tutorial

References

19. “Bitcoin's Been Linked to Child Pornography. That Means It Could Be Declared Illegal (or Already Is).” *ABC News*, Australian Broadcasting Corporation, 21 Mar. 2018, www.abc.net.au/news/2018-03-21/bitcoins-blockchain-has-been-linked-to-child-pornography/9571384.
20. “The DAO (Organization).” *Wikipedia*, Wikimedia Foundation, 5 July 2018, en.wikipedia.org/wiki/The_DAO_(organization).
21. “Someone Spent $114,000 on a Virtual Kitten That Runs on Blockchain.” *CNBC*, CNBC, 6 Dec. 2017, www.cnbc.com/video/2017/12/06/someone-spent-114000-buying-a-virtual-cat-on-cryptokitties.html
22. “What Is SingularityNET (AGI)? | Beginner's Guide.” *CoinCentral*, 1 May 2018, coincentral.com/singularitynet-beginner-guide/
23. *SingularityNET - The Single Most Valuable Technology of All Time*. 5 July 2018, vimeo.com/248331801

Slide Backups

Following slides for background purposes….

Cryptocurrency and Blockchain Attraction

- **Ease of Access**
  - The ease with which you can purchase cryptocurrencies – the most common method is via online exchanges such as Coinbase or Kraken – combined with increased media attention, has led to an influx of new, less sophisticated, buyers who have contributed to the price surge.
- **Technological Familiarity and Network Effects**
  - Courses are starting to be offered worldwide on cryptocurrency.
  - Bloomberg reports that many people like cryptocurrency's "underlying concept" (ie. decentralized payments through the blockchain) and that is why it is so popular.
  - Market speculation, ease of access, and familiarity is being amplified by a "network effect" – which describes the phenomenon when a technology or innovation becomes more valuable simply because more people are using it.
- **Criminal Havens and Anonymous Transactions**
  - Cryptocurrencies facilitate criminal activity and are perceived to make transactions anonymous – away from the informational reach of government and regulators.

Cryptocurrency and Blockchain Attraction (cont.)

- **Initial Coin Offering (ICO) Purchase Mechanics**
  - One central factor that is driving market demand for the most popular cryptocurrencies (like Bitcoin and Ethereum) is the "red hot" initial coin offering (ICO) market, where a company issues digital coins or tokens that provide access to a service (often called a "utility" or "app" token) or that represent an investment opportunity in the company (like a traditional security).
  - ICOs generated over $1.2 billion of new start-up capital in 2017.
- **Growing Distrust in Traditional Banking: Post Financial Crisis Fallout**
  - Another demand factor that has been suggested is a continuing, post-financial crisis, distrust of the traditional banking sector.
- **International Safe Havens and Geopolitical Volatility: Is Bitcoin A New Gold?**
  - Some investors (primarily those outside of stable monetary systems) view Bitcoin and other cryptocurrencies as a hedge against volatile local currencies and geopolitical risk.

Bitcoin Anonymity

- **If you use BitCoin, your privacy depends entirely on your ability to prevent your address from being associated with your identity**
  - Sophisticated programs can perform pattern analysis and link our identity to our transactions on the blockchain

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Jul 03 2018 10:40:30 GMT-0400 (Eastern Daylight Time).

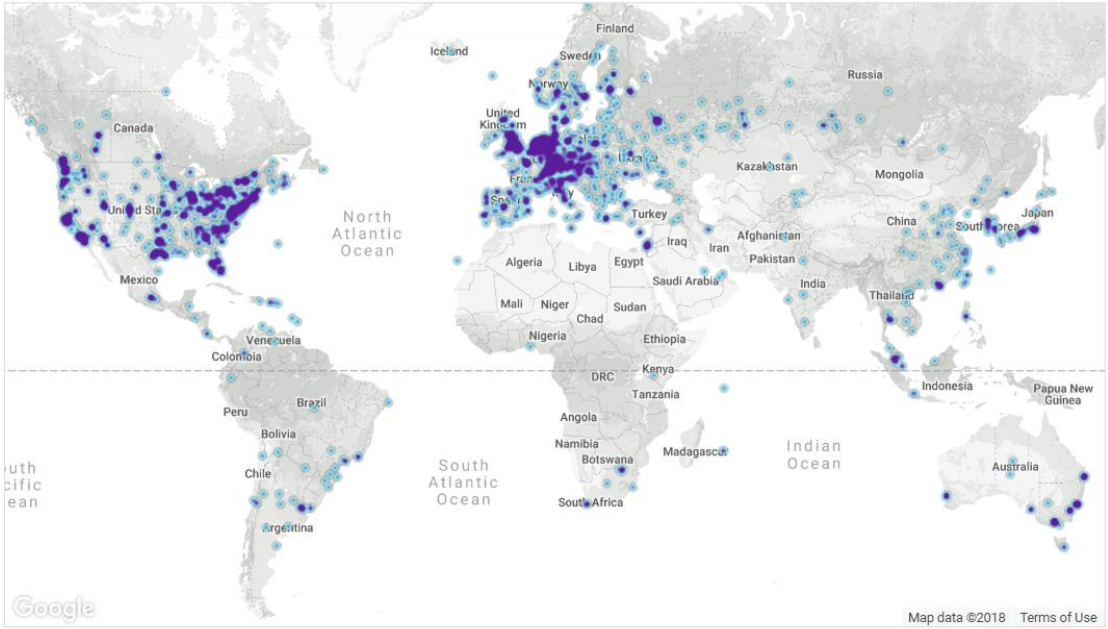
10013 NODES

24-hour charts »

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

RANK	COUNTRY	NODES
1	United States	2444 (24.41%)
2	Germany	1767 (17.65%)
3	China	900 (8.99%)
4	France	667 (6.66%)
5	Netherlands	461 (4.60%)
6	n/a	361 (3.61%)
7	Canada	346 (3.46%)
8	United Kingdom	314 (3.14%)
9	Russian Federation	295 (2.95%)
10	Japan	230 (2.30%)

More (100) »



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

LIVE MAP

Yeow , Addy. "Global Bitcoin Nodes Distribution." *Global Bitcoin Nodes Distribution - Bitnodes*, 3 July 2018, bitnodes.earn.com/

Section 222 of the Communications Act

Your DATA is worth money….

- **Congress revoked a FCC ruling that protected internet privacy in April 2017**
- **Congress had created Section 222 in 1996 as a means to protect our privacy from telecommunications carriers who have unique access to our communications and personal information.**
- **ISPs spent close to $8 million lobbying for this**
- **Impact: ISP can now monetize all of your online activity and data without any respect for privacy**
  - https://www.eff.org/deeplinks/2017/05/congress-repealing-our-internet-privacy-rights-meant-congress-repealed-internet
  - https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR

Published March 29, 2018 ***"What to expect now that Internet providers can collect and sell your Web browser history" Brian Fung***

Cryptocurrency Anonymizing Strategies

- **Virtual Currencies and Cryptocurrencies can be anonymized in several ways. The most popular strategies for anonymizing transactions include:**
  - Mixing
  - Tumbling
  - Use of untraceable currencies and tokens

Linking Transactions to IP addresses

Bitcoin is NOT Anonymous

- **Bitcoin does not have any built-in encryption when it comes to broadcasting transactions across it's P2P network.**
  - When your client relays transactions over the network, they pass through your ISP's gateway servers in plain text.
  - Your ISP can intercept and analyze this traffic, and then determine which of these transactions belong to your IP address (versus those transactions which you are only relaying).
  - The transactions that belong to you will first appear on the network via your IP address, differentiating them from transactions that have already been propagated by other nodes. And then your IP address can be used by your ISP to lookup your personal identity — they have it on file from when you subscribed to their service.

Anonymity Drivers

Who wants to be anonymous?

- **Criminals**
  - Nefarious actors who don't want a "money trail"
  - Crime syndicates that don't want authorities to be able to make connections, associations, or attributed behaviors that could lead to prosecution
- **Non-State Actors and Terrorist Organizations**
  - Human trafficking
  - Weapons Sales
  - Drug trafficking
- **Government Sponsored Hacking Groups**
- **Growing number of citizens who don't want their data exploited (spending profiles, transaction history, etc.)**

Section 222 of the Communications Act

Your DATA is worth money….

- **Congress revoked a FCC ruling that protected internet privacy in April 2017**
- **Congress had created Section 222 in 1996 as a means to protect our privacy from telecommunications carriers who have unique access to our communications and personal information.**
- **ISPs spent close to $8 million lobbying for this**
- **Impact: ISP can now monetize all of your online activity and data without any respect for privacy**
  - https://www.eff.org/deeplinks/2017/05/congress-repealing-our-internet-privacy-rights-meant-congress-repealed-internet
  - https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR

Published March 29, 2018 ***"What to expect now that Internet providers can collect and sell your Web browser history" Brian Fung***

Cryptocurrency Anonymizing Strategies

- **Virtual Currencies and Cryptocurrencies can be anonymized in several ways. The most popular strategies for anonymizing transactions include:**
  - Mixing
  - Tumbling
  - Use of untraceable currencies and tokens

Cryptocurrency Exchanges

Exchanges link transactions to bank accounts

- **Exchanges**
  - Private and Public keys give the user a feeling that their identity is protected, but bitcoin becomes public when a user cashes out using a wallet or an exchange.
    - User wallets (called addresses) are pseudonymous rather than anonymous: multiple actions of the same user can be linked together.
    - Most users link their exchange wallets to their bank accounts
    - Information about the users physical address can be linked to a soft wallet when users enter in their shipping address

Mixing

- **Cryptocurrency Mixing is the process of transferring funds between two address without recording their relationship to the public block chain. There are many types of mixing services.**
  - Examples of centralized mixing services include SharedCoin and DarkWallet.
    - Analogous to providing Web browsing anonymity with a single anonymizing proxy, rather than using Tor.
    - In these specific examples, the central mixing agent must be completely trusted as it knows which users exchange funds with others.

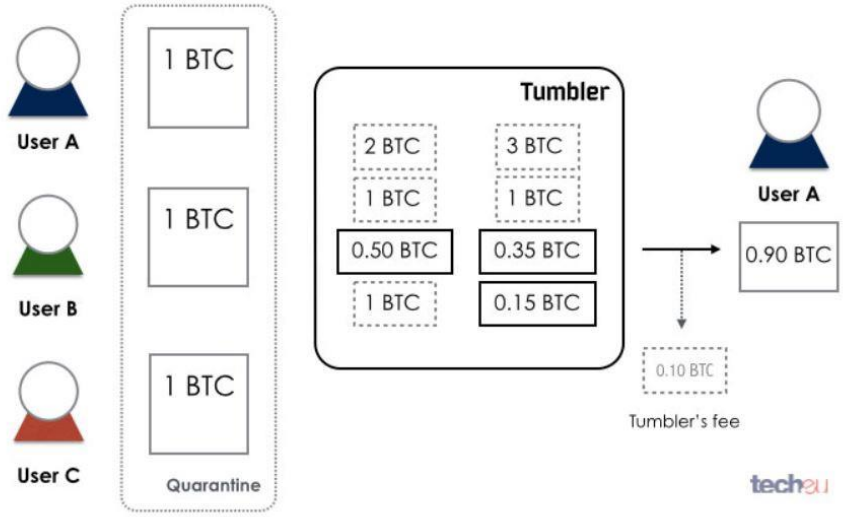
Tumblers

- **Cryptocurrency Tumblers**

  1) Aggregates your money with many other funds

  2) Sweeps the funds through large financial institutions

  3) Transfer funds out to smaller wallets in random intervals, in small random balances



Kandpal, Akash. "Monero - An Anonymous CryptoCurrency – Akash Kandpal – Medium." *Medium*, Augmenting Humanity, 29 Dec. 2017, medium.com/@harrypotter0/how-does-monero-work-17f18ea37652.

Research continues into ways to track Monero..

What happens when you tell a hacker they can't hack something?

- **"An Empirical Analysis of Traceability in the Monero Blockchain", Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, Nicolas Christin (Submitted on 13 Apr 2017 (v1), last revised 28 Mar 2018 (this version, v3))**
- **Challenged the claim that Monero was untraceable**
  - Research showed that about 62% of transaction inputs with one or more mixins are vulnerable to "chain-reaction" analysis— that is, the real input can be deduced by elimination.
  - Monero mixins are sampled in such a way that they can be easily distinguished from the real coins by their age distribution; in short, the real input is usually the "newest" input. We estimate that this heuristic can be used to guess the real input with 80 % accuracy over all transactions with 1 or more mixins.
- **Despite attempts to compromise Monero's multiple encryption and decoy strategies, Monero is still recognized as the best cryptocurrency for preserving user anonymity**

Möser, Malte, et al. "Monero: Response To." *Getmonero.org, The Monero Project*, 13 Apr. 2017, getmonero.org/2018/03/29/response-to-an-empirical-analysis-of-traceability.html.

Why does all this matter?

Cryptocurrency community quickly outpacing advancements in the US DoD

- **Drivers to create new secure, private, and untraceable cryptocurrencies (and the blockchain architectures on which they reside) are causing this community to outpace technological development in the US DoD**
- **CPU's and GPU's are no longer powerful enough to keep up with an ASIC**
  - Barrier for entry into the mining community favors large scale miners over individuals
  - It's estimated that 80% of the hash rate (mining power) for bitcoin mining is coming from China
  - AntMiner S9 (and probably more) defaults to BitMain's mining pool

"Treasure Wallpaper Enam Wallpaper." *Wallpaper.enam.site*, wallpaper.enam.site/treasure-wallpaper/.

Blockchain Information Hiding

Blockchain in the news…

- **Bitcoin's blockchain can be used to store small quantities of information**
  - Sward, Andrew, Ivy Vecna, and Forrest Stonedahl. "Data Insertion in Bitcoin's Blockchain." Ledger 3 (2018).
  - On March 20, 2018, researchers discovered that illegal imagery was being stored.

Bitcoin's blockchain contains child abuse images, meaning the cryptocurrency's possession could be 'illegal'

Updated 21 Mar 2018, 1:59am

PHOTO: German researchers have found the bitcoin blockchain unlocks more than users are aware of. (Reuters: Dado Ruvic)

The multi-billion-dollar markets behind cryptocurrencies are in jeopardy after child abuse images were found in bitcoin's blockchain.

"Bitcoin's Been Linked to Child Pornography. That Means It Could Be Declared Illegal (or Already Is)." *ABC News*, Australian Broadcasting Corporation, 21 Mar. 2018, www.abc.net.au/news/2018-03-21/bitcoins-blockchain-has-been-linked-to-child-pornography/9571384.

Ethereum Compromise

In 2016 a decentralized autonomous organization called The DAO, a set of smart contracts developed on the platform, raised a record US $150 million in a crowd-sale to fund the project.

The DAO was exploited in June when US $50 million in ether were claimed by an anonymous entity.

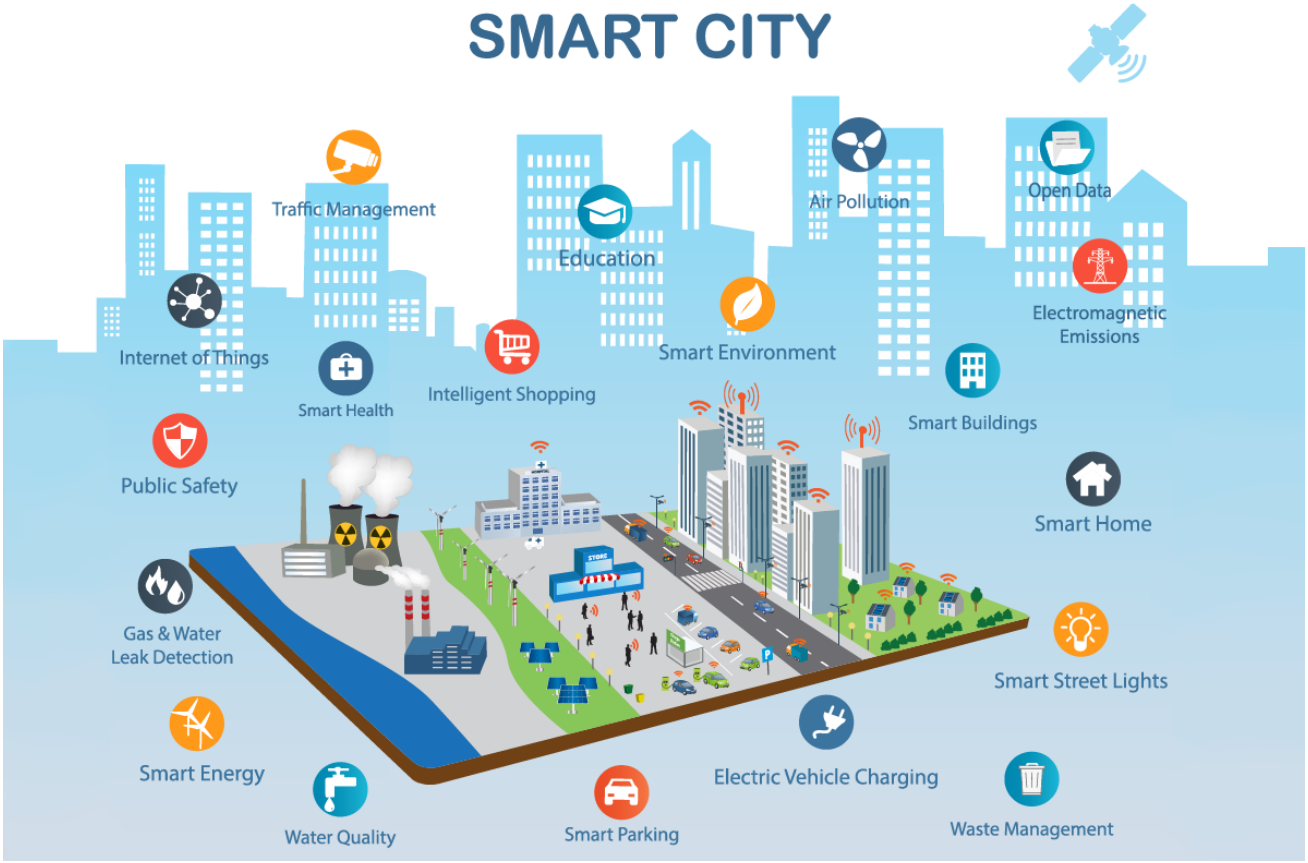
As a result of the dispute, the network split in two.

- Ethereum continued on the forked blockchain
- Ethereum Classic continued on the original blockchain
- The hard fork created a rivalry between the two networks
- After the hard fork related to The DAO, Ethereum subsequently forked twice in the fourth quarter of 2016 to deal with other attacks.
- By the end of November 2016, Ethereum had increased its DDoS protection, de-bloated the blockchain, and thwarted further spam attacks by hackers.

"The DAO (Organization)." *Wikipedia*, Wikimedia Foundation, 5 July 2018, en.wikipedia.org/wiki/The_DAO_(organization).

Tokenization

- **An appropriately designed Blockchain Token that "consists of rights" and does not include any investment interests "should" not be deemed to be a security**
  - Subject to the specific facts, circumstances and characteristics of the Blockchain Token itself



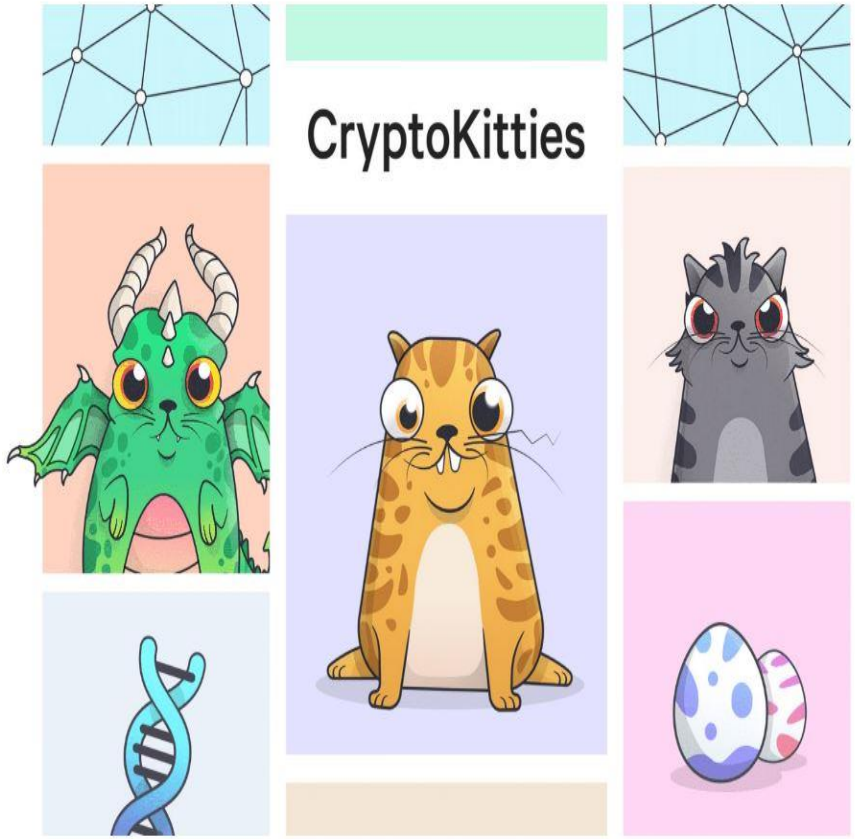
Darrell, Gilbert A. "A Connected World, Communications in Smart Cities – Gilbert A. Darrell – Medium." *Medium*, Augmenting Humanity, 16 May 2018, medium.com/@artiedarrell/a-connected-world-communications-in-smart-cities-3fe793a7c429.

The CryptoKittie

- Practical application of smart contracts and cryptocurrency transactions
- CryptoKitties showcasing a practical use for blockchain technology outside of the financial industry
- There goal is to broaden the public's understanding of the technology and its potential application.

https://www.cnbc.com/video/2017/12/06/someone-spent-114000-buying-a-virtual-cat-on-cryptokitties.html

https://www.dropbox.com/s/a5h3zso545wuqkm/CryptoKitties_WhitePapurr_V2.pdf?dl=0



"Someone Spent $114,000 on a Virtual Kitten That Runs on Blockchain." *CNBC*, CNBC, 6 Dec. 2017, www.cnbc.com/video/2017/12/06/someone-spent-114000-buying-a-virtual-cat-on-cryptokitties.html

The Virtual Kittie Uprising

Evelyn Cheng | @chengevelyn

Published 12:42 PM ET Wed, 6 Dec 2017 | Updated 5:30 PM ET Wed, 6 Dec 2017

CNBC

"Think breedable Beanie Babies."