





## What is Virtual Currency???

A digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically.



*Virtual Currency is any medium of exchange that operates like a fiat currency but does not have legal tender status in any jurisdiction.*

*Digital currencies are money used on the Internet.*

[Virtual Currency or Digital money](#) exists only in the digital form. It doesn't have any physical equivalent in the real world. Nevertheless, it has all the characteristics of traditional money. Just as classic fiat money, you can obtain, transfer or exchange it for another currency. You can use it to pay for the goods and services, such as mobile and Internet communication, online stores and others. Digital currencies don't have geographical or political borders; transactions might be sent from any place and received at any point in the world. Actually, digital accounts and wallets may be regarded as bank deposits.

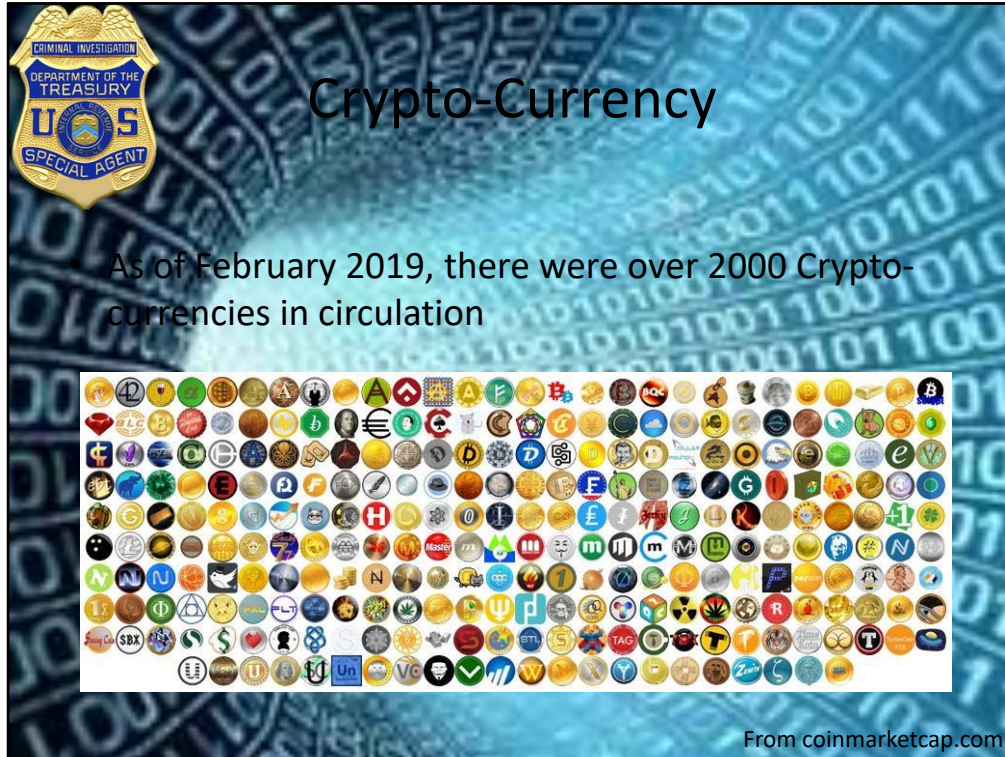
Types of

*Most distinctions can be considered as both advantages and disadvantages.*

In a centralized system, there is a group of people responsible for the state of the whole system. If you made a mistake in a transaction, you can make a request to the company and rely on the successful outcome. You cannot do this in the decentralized system. On the other hand, centralized networks keep a lot of confidential information about the users. This data may get lost, hacked or be transferred to law enforcement agencies at court request. Decentralized networks do not have these problems. The same goes for a transaction cancellation. If the system is revocable, you can make changes to a transaction.

At the same time, it opens room for fraudulent activities.





A [cryptocurrency](#) is a digital currency using cryptography to secure transactions and to control the creation of new currency units. Since not all virtual currencies use cryptography, not all virtual currencies are cryptocurrencies.

*Cryptocurrencies are a variety of digital currencies.*

[Cryptocurrency](#) is an asset used as a means of exchanging. It is considered reliable because it's based on cryptography.

One of the cryptography's primary objectives is communications and how to make them secure. It creates and analyzes the algorithms and protocols so no information is changed or interrupted during the conversation by third parties. Cryptography is a mix of a large number of different sciences, with mathematics as the basic. It's math that attaches the severity and reliability to algorithms and protocols.


Cryptocurrencies use Blockchain and a decentralized [ledger](#). It means that no supervisory authority controls all the actions in the network. This comes at the expense of all the users.

The slide features a blue background with a binary code pattern. In the top left corner is the UOS logo, which includes the text 'CRIMINAL INVESTIGATION', 'DEPARTMENT OF THE TREASURY', 'UOS', and 'SPECIAL AGENT'. The title 'Top 14 Crypto-Currencies' is centered at the top. Below the title is a list of 14 cryptocurrencies, numbered 1 through 14. The list is split into two columns. The first column contains items 1 through 7, and the second column contains items 8 through 14. The source 'coinmarketcap.com' is noted in the bottom right corner.

Rank	Cryptocurrency
1	Bitcoin
2	Ethereum
3	XRP
4	Bitcoin Cash
5	Litecoin
6	EOS
7	Binance Coin
8	Bitcoin SV
9	Tether
10	Stellar
11	TRON
12	Cardano
13	Monero
14	Dash

coinmarketcap.com

[Presenter may want to update this screen shot from the website listed on the slide]



# Bitcoin

- Date Started: 1/3/2009
- Current Supply: 17,740,200
- Max Supply: 21,000,000
- Current Value: \$7,991.20
- Market Cap: \$141,765,444,988
- Address: 25-36 characters beginning with a 1 or a 3

As of 6/4/2019

On 18 August 2008, the domain name bitcoin.org was registered. In October 2008, Satoshi Nakamoto published a paper on the cryptography mailing list at metzdowd.com describing the bitcoin digital currency. It was titled "Bitcoin: A Peer-to-Peer Electronic Cash System". In January 2009, Nakamoto released the first bitcoin software that launched the network and the first units of the bitcoin cryptocurrency, called bitcoins. Satoshi Nakamoto released the Version 0.1 of bitcoin software on Sourceforge on 9 January 2009.

Nakamoto claimed that work on the writing of the code began in 2007. The inventor of Bitcoin knew that due to its nature, the core design would have to be able to support a broad range of transaction types. The implemented solution enabled specialized codes and data fields from the start through the use of a predicative script.

Nakamoto created a website with the domain name bitcoin.org and continued to collaborate with other developers on the bitcoin software until mid-2010. Around this time, he handed over control of the source code repository and network alert key to Gavin Andresen, transferred several related domains to various prominent members of the bitcoin community, and stopped his involvement in the project. Until shortly before his absence and handover, Nakamoto made all modifications to the source code himself.

One of the first supporters, adopters, contributor to bitcoin and receiver of the first bitcoin transaction was programmer Hal Finney. Finney downloaded the bitcoin software the day it was released, and received 10 bitcoins from Nakamoto in the world's first bitcoin transaction on 12 January 2009. Other early supporters were Wei Dai, creator of bitcoin

predecessor b-money, and Nick Szabo, creator of bitcoin predecessor bit gold.

In the early days, Nakamoto is estimated to have mined 1 million bitcoins. Before disappearing from any involvement in bitcoin, Nakamoto in a sense handed over the reins to developer Gavin Andresen, who then became the bitcoin lead developer at the Bitcoin Foundation, the 'anarchic' bitcoin community's closest thing to an official public face.

The value of the first bitcoin transactions were negotiated by individuals on the bitcoin forum with one notable transaction of 10,000 BTC used to indirectly purchase two pizzas delivered by Papa John's.









Ripple is more known for its digital payment protocol than its cryptocurrency, XRP. Ripple operates on an open source and peer-to-peer decentralized platform that allows for a seamless transfer of money in any form, whether USD, Yen, litecoin, or bitcoin.

To understand how the system works, consider a money transfer structure where the two parties on either end of the transaction use their preferred middlemen to receive the money. Lawrence needs to send \$100 to David who lives in a different city. He gives his local agent, Kate, the money to send to David with a password that David is required to answer correctly to receive the funds. Kate alerts David's agent, Rose, of the transaction details – recipient, funds to be reimbursed, and password. If David gives Rose the right password, Rose gives him \$100. However, the money comes from Rose's account which means that Kate would owe Rose \$100. Rose can either record a journal of all Kate's debt or IOUs which Kate would pay on an agreed day, or make counter transactions which would balance the debt. For example, if Rose was also Martin's agent and Martin needed to transfer \$100 to Itios whose agent is Kate, this would balance out the \$100 owed to Rose, since Itios will be paid from Kate's account.

Although the Ripple network is a little more complex than this example, the example demonstrates the basics of how the Ripple system works. From the example above, one can see that trust is required to initiate a transaction – trust between Lawrence and Kate, Kate and Rose, and David and Rose. Ripple uses a medium known as Gateway that serves as the link in the trust chain between two parties wanting to make a transaction. Gateway acts as the credit intermediary that receives and sends currencies to public addresses over



the Ripple network. Anyone or any business can register and open a gateway which authorizes the registrant to acting as the middleman for exchanging currencies, maintaining liquidity, and transferring payments on the network.

The digital currency, XRP, acts as a bridge currency to other currencies. It does not discriminate between one fiat/crypto currency and another, and thus, makes it easy for any currency to be exchanged for another. Each currency on the ecosystem has its own gateway e.g. CADBluzelle, BTCbitstamp, and USDsnapswap. If David wanted bitcoins as payment for the services rendered to Lawrence, Lawrence does not necessarily have to have bitcoins. He can send the payment to his gateway in Canadian dollars (CAD), and David can receive bitcoins from his gateway. One gateway is not needed to initiate a complete a transaction, multiple gateways can be used, forming a chain of trust rippling across the users.

Holding balances with a gateway, exposes the user to counterparty risk which is also a risk that is apparent in the traditional banking system. If the gateway does not honor its IOU or liability, the user could lose the value of his money held at that gateway. Users that don't trust a gateway, can therefore transact with a trusted gateway that in turn deals with the 'untrusted' gateway. This way the IOU will be with the trusted or creditworthy-certified gateway. Counterparty risk does not apply to bitcoins and most other altcoins since a user's bitcoin is not another user's IOU or liability.

The Ripple network does not run with a proof-of-work system like bitcoin or a proof-of-stake system like Nxt. Instead, transactions rely on a consensus protocol in order to validate account balances and transactions on the system. The consensus works to improve the integrity of the system by preventing double spending. A Ripple user that initiates a transaction with multiple gateways but craftily sends the same \$100 to the gateway systems will have all but the first transaction deleted. Individual distributed nodes decide by consensus which transaction was made first by taking a poll to determine the majority vote. The confirmations are instant and take roughly 5 seconds. Since there's no central authority that decides who can set up a node and confirm transactions, the Ripple platform is described as decentralized.

Ripple keeps track of all IOUs in a given currency for any user or gateway. IOU credits and transaction flows that occur between Ripple wallets are publicly available on the Ripple consensus ledger. But even though financial transaction history is publicly recorded and made available on the block chain, the data is not linked to the ID or account of any individual or business. However, the public record of all dealings, make the information susceptible to de-anonymization measures.

Ripple improves on some of the drawbacks attributed to traditional banks. Transactions are settled within seconds on the Ripple network even though the platform handles millions of transactions frequently. This is unlike banks which could take days or weeks to complete a wire transfer. The fee to conduct transactions on Ripple is also minimal, with the minimum transaction cost required for a standard transaction set at 0.00001 XRP, compared to the

large fees charged by banks for conducting cross-border payments.

Read more: Ripple (Cryptocurrency) Definition | Investopedia

<https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp#ixzz5CBdpjoCF>

Ripple is more known for its digital payment protocol than its cryptocurrency, XRP. Ripple operates on an open source and peer-to-peer decentralized platform that allows for a seamless transfer of money in any form, whether USD, Yen, litecoin, or bitcoin.

To understand how the system works, consider a money transfer structure where the two parties on either end of the transaction use their preferred middlemen to receive the money. Lawrence needs to send \$100 to David who lives in a different city. He gives his local agent, Kate, the money to send to David with a password that David is required to answer correctly to receive the funds. Kate alerts David's agent, Rose, of the transaction details – recipient, funds to be reimbursed, and password. If David gives Rose the right password, Rose gives him \$100. However, the money comes from Rose's account which means that Kate would owe Rose \$100. Rose can either record a journal of all Kate's debt or IOUs which Kate would pay on an agreed day, or make counter transactions which would balance the debt. For example, if Rose was also Martin's agent and Martin needed to transfer \$100 to Itios whose agent is Kate, this would balance out the \$100 owed to Rose, since Itios will be paid from Kate's account.

Although the Ripple network is a little more complex than this example, the example demonstrates the basics of how the Ripple system works. From the example above, one can see that trust is required to initiate a transaction – trust between Lawrence and Kate, Kate and Rose, and David and Rose. Ripple uses a medium known as Gateway that serves as the link in the trust chain between two parties wanting to make a transaction. Gateway acts as the credit intermediary that receives and sends currencies to public addresses over

the Ripple network. Anyone or any business can register and open a gateway which authorizes the registrant to acting as the middleman for exchanging currencies, maintaining liquidity, and transferring payments on the network.

The digital currency, XRP, acts as a bridge currency to other currencies. It does not discriminate between one fiat/crypto currency and another, and thus, makes it easy for any currency to be exchanged for another. Each currency on the ecosystem has its own gateway e.g. CADBluzelle, BTCbitstamp, and USDsnapswap. If David wanted bitcoins as payment for the services rendered to Lawrence, Lawrence does not necessarily have to have bitcoins. He can send the payment to his gateway in Canadian dollars (CAD), and David can receive bitcoins from his gateway. One gateway is not needed to initiate a complete a transaction, multiple gateways can be used, forming a chain of trust rippling across the users.

Holding balances with a gateway, exposes the user to counterparty risk which is also a risk that is apparent in the traditional banking system. If the gateway does not honor its IOU or liability, the user could lose the value of his money held at that gateway. Users that don't trust a gateway, can therefore transact with a trusted gateway that in turn deals with the 'untrusted' gateway. This way the IOU will be with the trusted or creditworthy-certified gateway. Counterparty risk does not apply to bitcoins and most other altcoins since a user's bitcoin is not another user's IOU or liability.

The Ripple network does not run with a proof-of-work system like bitcoin or a proof-of-stake system like Nxt. Instead, transactions rely on a consensus protocol in order to validate account balances and transactions on the system. The consensus works to improve the integrity of the system by preventing double spending. A Ripple user that initiates a transaction with multiple gateways but craftily sends the same \$100 to the gateway systems will have all but the first transaction deleted. Individual distributed nodes decide by consensus which transaction was made first by taking a poll to determine the majority vote. The confirmations are instant and take roughly 5 seconds. Since there's no central authority that decides who can set up a node and confirm transactions, the Ripple platform is described as decentralized.

Ripple keeps track of all IOUs in a given currency for any user or gateway. IOU credits and transaction flows that occur between Ripple wallets are publicly available on the Ripple consensus ledger. But even though financial transaction history is publicly recorded and made available on the block chain, the data is not linked to the ID or account of any individual or business. However, the public record of all dealings, make the information susceptible to de-anonymization measures.

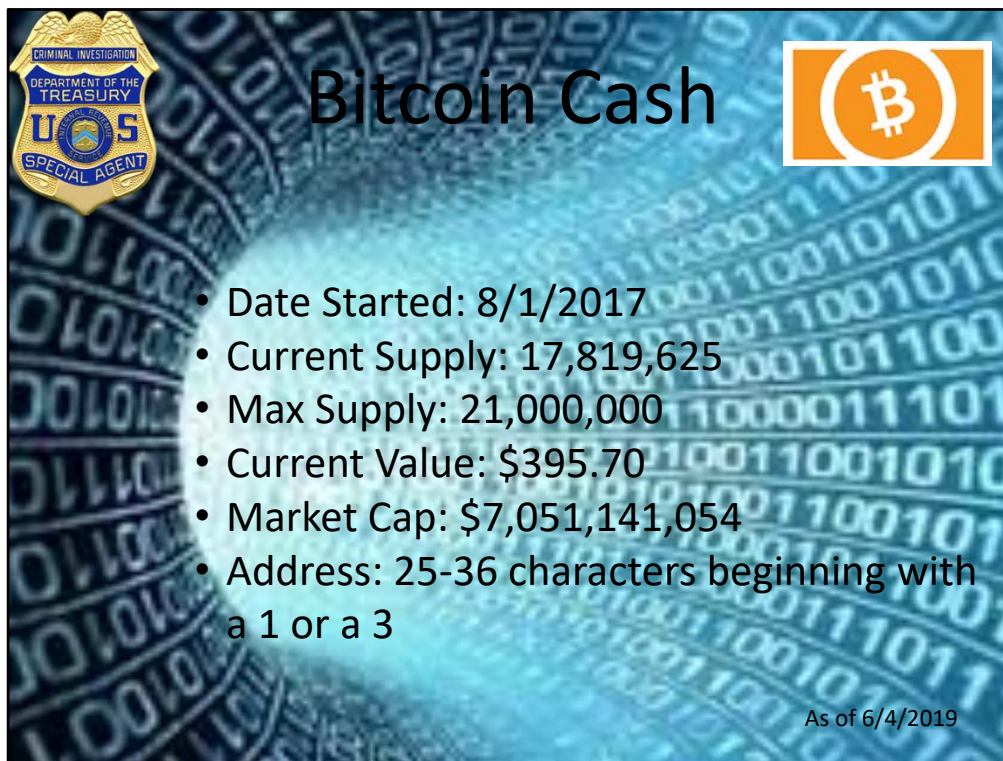
Ripple improves on some of the drawbacks attributed to traditional banks. Transactions are settled within seconds on the Ripple network even though the platform handles millions of transactions frequently. This is unlike banks which could take days or weeks to complete a wire transfer. The fee to conduct transactions on Ripple is also minimal, with the minimum transaction cost required for a standard transaction set at 0.00001 XRP, compared to the



large fees charged by banks for conducting cross-border payments.

Read more: Ripple (Cryptocurrency) Definition | Investopedia

<https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp#ixzz5CBdpjoCF>

A presentation slide for Bitcoin Cash. The background is a blue and white digital tunnel of binary code. In the top left corner is the U.S. Department of Treasury Criminal Investigation Special Agent badge. In the top right corner is the Bitcoin Cash logo (an orange square with a white circle containing a Bitcoin symbol). The title "Bitcoin Cash" is centered at the top. A bulleted list of statistics is in the center, and the date "As of 6/4/2019" is in the bottom right corner.

# Bitcoin Cash

- Date Started: 8/1/2017
- Current Supply: 17,819,625
- Max Supply: 21,000,000
- Current Value: \$395.70
- Market Cap: \$7,051,141,054
- Address: 25-36 characters beginning with a 1 or a 3

As of 6/4/2019

Bitcoin Cash (BCH) is a cryptocurrency. It is a result of a prolonged disagreement on how to handle the bitcoin scalability problem. The change, called a hard fork, took effect on August 1, 2017. As a result, the bitcoin ledger called the blockchain and the cryptocurrency split in two. At the time of the fork anyone owning bitcoin was also in possession of the same number of Bitcoin Cash units. [Fork described later]



Bitcoin Cash (BCH) is a cryptocurrency. It is a result of a prolonged disagreement on how to handle the bitcoin scalability problem. The change, called a hard fork, took effect on August 1, 2017. As a result, the bitcoin ledger called the blockchain and the cryptocurrency split in two. At the time of the fork anyone owning bitcoin was also in possession of the same number of Bitcoin Cash units. [Fork described later]



# Litecoin

- Date Started: 10/7/2011
- Current Supply: 62,075,376
- Max Supply: 84,000,000
- Current Value: \$401.92
- Market Cap: \$6,513,055,850
- Address: 33 characters beginning with a L

As of 6/4/2019

Litecoin was released via an open-source client on GitHub on October 7, 2011 by Charlie Lee, a former Google employee. The Litecoin network went live on October 13, 2011. It was a fork of the Bitcoin Core client, differing primarily by having a decreased block generation time (2.5 minutes), increased maximum number of coins, different hashing algorithm (script, instead of SHA-256), and a slightly modified GUI.

The main difference is that litecoin can confirm transactions must faster than bitcoin. The implications of that are as follows:

- Litecoin can handle a higher volume of transactions thanks to its faster block generation. If bitcoin were to try to match this, it would require significant updates to the code that everyone on the bitcoin network is currently running.
- The disadvantage of this higher volume of blocks is that the litecoin blockchain will be proportionately larger than bitcoin's, with more orphaned blocks.
- The faster block time of litecoin reduces the risk of double spending attacks - this is theoretical in the case of both networks having the same hashing power.
- A merchant who waited for a minimum of two confirmations would only need to wait five minutes, whereas they would have to wait 10 minutes for just one confirmation with bitcoin.
- Transaction speed (or faster block time) and confirmation speed are often touted as moot points by many involved in bitcoin, as most merchants would allow zero-confirmation transactions for most purchases. It is necessary to bear in mind that a transaction is instant, it is just confirmed by the network as it propagates.



During the month of November 2013, the aggregate value of Litecoin experienced massive growth which included a 100% leap within 24 hours.

Litecoin reached a \$1 billion market capitalization in November 2013.

In May 2017, Litecoin became the first of the top 5 (by market cap) cryptocurrencies to adopt Segregated Witness. Later in May of the same year, the first Lightning Network transaction was completed through Litecoin, transferring 0.00000001 LTC from Zürich to San Francisco in under one second.

The formal title "**Segregated Witness** (Consensus layer)" had Bitcoin Improvement Proposal number BIP141. The purpose was to solve malleability. It was also intended to mitigate a blockchain size limitation problem that reduces Bitcoin transaction speed. It does this by splitting the transaction into two segments, removing the unlocking signature ("witness" data) from the original portion and appending it as a separate structure at the end.[4] The original section would continue to hold the sender and receiver data, and the new "witness" structure would contain scripts and signatures. The original data segment would be counted normally, but the "witness" segment would, in effect, be counted as a quarter of its real size.

**Malleability** is a property of some cryptographic algorithms.[1] An encryption algorithm is "malleable" if it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext. That is, given an encryption of a plaintext  $m$   $\{\displaystyle m\}$ , it is possible to generate another ciphertext which decrypts to  $f(m)$   $\{\displaystyle f(m)\}$ , for a known function  $f$   $\{\displaystyle f\}$ , without necessarily knowing or learning  $m$   $\{\displaystyle m\}$ .

Malleability is often an undesirable property in a general-purpose cryptosystem, since it allows an attacker to modify the contents of a message

In February 2018, the EU online retailer Alza.cz began accepting Litecoin as a payment method.



As of 2/19/2019

Litecoin was released via an open-source client on GitHub on October 7, 2011 by Charlie Lee, a former Google employee. The Litecoin network went live on October 13, 2011. It was a fork of the Bitcoin Core client, differing primarily by having a decreased block generation time (2.5 minutes), increased maximum number of coins, different hashing algorithm (script, instead of SHA-256), and a slightly modified GUI.

The main difference is that litecoin can confirm transactions must faster than bitcoin. The implications of that are as follows:

- Litecoin can handle a higher volume of transactions thanks to its faster block generation. If bitcoin were to try to match this, it would require significant updates to the code that everyone on the bitcoin network is currently running.
- The disadvantage of this higher volume of blocks is that the litecoin blockchain will be proportionately larger than bitcoin's, with more orphaned blocks.
- The faster block time of litecoin reduces the risk of double spending attacks - this is theoretical in the case of both networks having the same hashing power.
- A merchant who waited for a minimum of two confirmations would only need to wait five minutes, whereas they would have to wait 10 minutes for just one confirmation with bitcoin.
- Transaction speed (or faster block time) and confirmation speed are often touted as moot points by many involved in bitcoin, as most merchants would allow zero-confirmation transactions for most purchases. It is necessary to bear in mind that a transaction is instant, it is just confirmed by the network as it propagates.

During the month of November 2013, the aggregate value of Litecoin experienced massive growth which included a 100% leap within 24 hours.

Litecoin reached a \$1 billion market capitalization in November 2013.

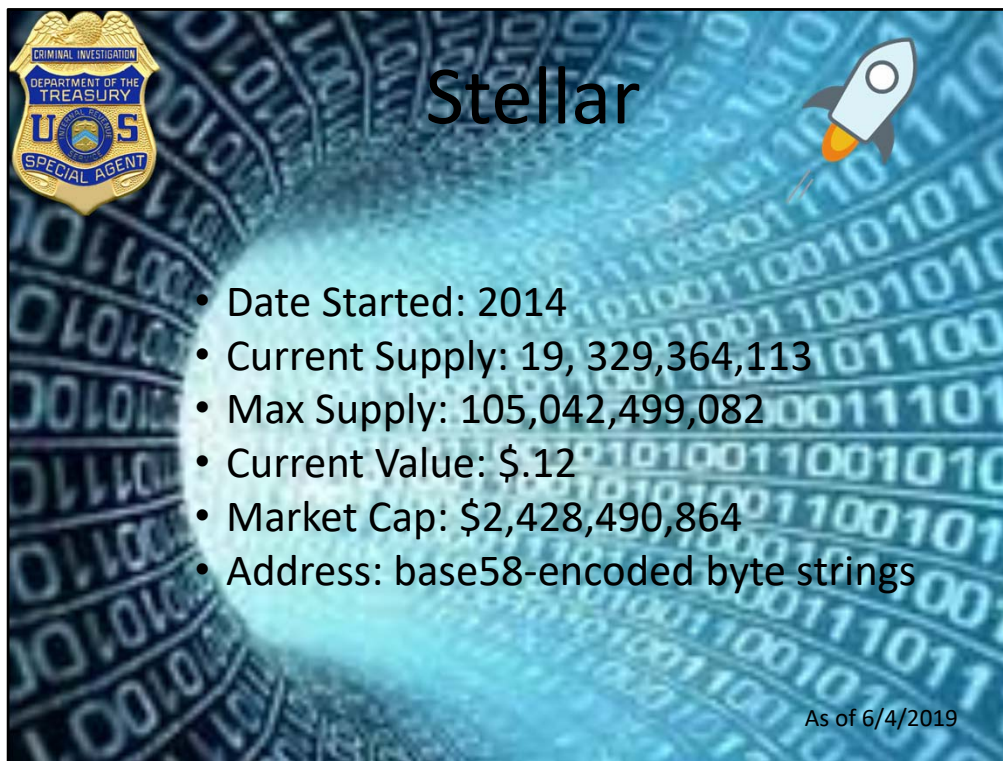
In May 2017, Litecoin became the first of the top 5 (by market cap) cryptocurrencies to adopt Segregated Witness. Later in May of the same year, the first Lightning Network transaction was completed through Litecoin, transferring 0.00000001 LTC from Zürich to San Francisco in under one second.

The formal title "**Segregated Witness** (Consensus layer)" had Bitcoin Improvement Proposal number BIP141. The purpose was to solve malleability. It was also intended to mitigate a blockchain size limitation problem that reduces Bitcoin transaction speed. It does this by splitting the transaction into two segments, removing the unlocking signature ("witness" data) from the original portion and appending it as a separate structure at the end.[4] The original section would continue to hold the sender and receiver data, and the new "witness" structure would contain scripts and signatures. The original data segment would be counted normally, but the "witness" segment would, in effect, be counted as a quarter of its real size.

**Malleability** is a property of some cryptographic algorithms.[1] An encryption algorithm is "malleable" if it is possible for an adversary to transform a ciphertext into another ciphertext which decrypts to a related plaintext. That is, given an encryption of a plaintext  $m$   $\{\displaystyle m\}$ , it is possible to generate another ciphertext which decrypts to  $f(m)$   $\{\displaystyle f(m)\}$ , for a known function  $f$   $\{\displaystyle f\}$ , without necessarily knowing or learning  $m$   $\{\displaystyle m\}$ .

Malleability is often an undesirable property in a general-purpose cryptosystem, since it allows an attacker to modify the contents of a message

In February 2018, the EU online retailer Alza.cz began accepting Litecoin as a payment method.

A slide titled "Stellar" with a background of binary code. In the top left corner is the U.S. Department of Treasury Criminal Investigation Special Agent badge. In the top right corner is a rocket icon. The slide lists the following statistics:

- Date Started: 2014
- Current Supply: 19, 329,364,113
- Max Supply: 105,042,499,082
- Current Value: \$.12
- Market Cap: \$2,428,490,864
- Address: base58-encoded byte strings

In the bottom right corner, it says "As of 6/4/2019".

### Stellar Lumens Explained

Stellar is a distributed hybrid blockchain platform that aims to help facilitate cross-asset transfer of value at a fraction of a penny. Stellar is aiming to be an open financial system that gives people of all income levels access to low-cost financial services. These services include, but are not limited to:

- Remittances
- Micropayments
- Mobile Branches
- Mobile Money

In addition to these services, another feature of the network is their **Distributed Exchange**.

### Distributed Exchange

Through use of its intermediary currency **Lumens (XLM)**, a user can send any currency that they own to anyone else in a different currency.

For example, if Alice wanted to send EUR to Bob using her USD, an offer is submitted to the distributed exchange selling USD for EUR. This submitted offer forms what is known as an **order book**. The network will use the order book to find the best exchange rate for the transaction in-order to minimize the fee paid by a user.

This **multi-currency transaction** is possible because of what are known as **Anchors**.

Anchors are trusted entities that hold people's deposits and can issue credit. In essence, Anchors act as a bridge between different currencies and the Stellar network.

### Lumens (XLM)

Lumens are the native asset (digital currency) that exist on the Stellar network. They



currently serve two distinct purposes:

Facilitate multi-currency transactions

Anti-spam role

**Multi-currency transactions:** Lumens is the digital currency that acts a bridge in-order to facilitate multi-currency transactions. Transactions such as: sending money in EUR, and then receiving it in USD. XLM is the digital intermediary that allows for such a transaction to occur at a low cost.

**Anti-spam:** In-order to prevent DoS attacks that would inevitably occur on the Stellar network, a small fee of 0.00001 XLM is associated with every transaction that occurs on the network. This fee is small enough so it does not significantly affect the cost of transaction, but large enough so it dissuades bad actors from spamming the network. The collected fee is then redistributed and added to an **inflation pool**. This inflation pool releases Lumens at a rate of 1% each year.

### **Incentive Program**

In-order further facilitate the growth of the Stellar eco-system, Stellar currently offers the following incentive programs:

Stellar Build Challenge

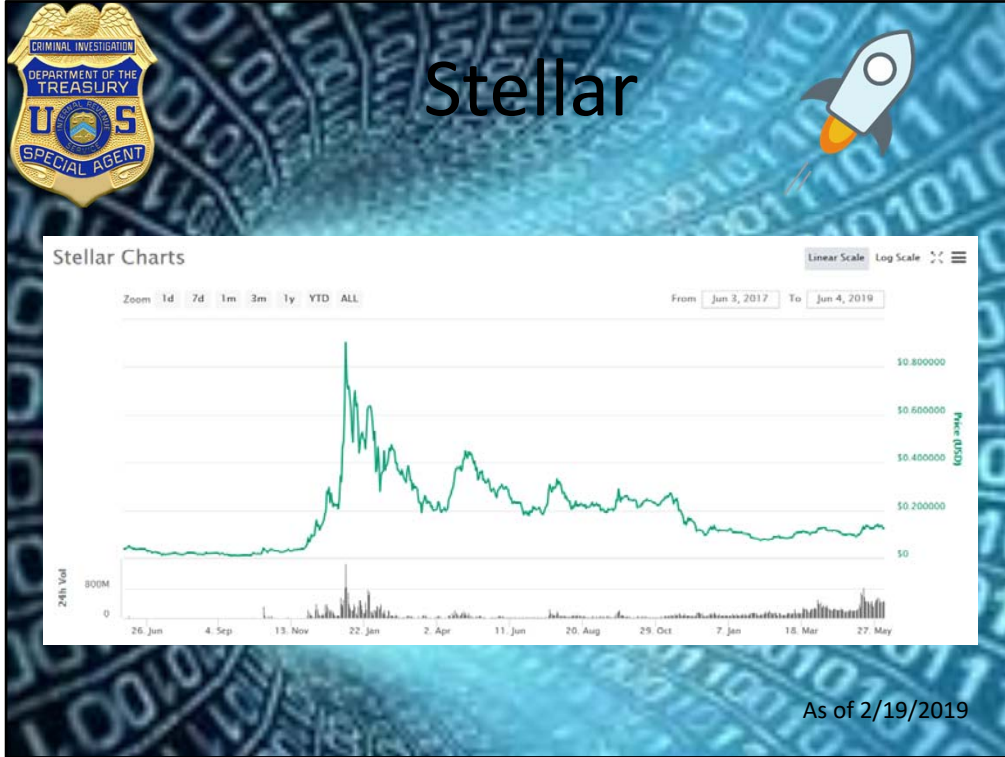
Partnership Grant Challenge

**Stellar Build Challenge:** This is an ongoing program that is intended to encourage and reward innovation on the Stellar network. With rewards of up to 2,000,000 XLM, developers are encouraged to innovate in areas such as: Wallets, remittance applications and token issuance. By providing a monetary incentive, the eco-system is able to quickly develop into a reputable and established distributed system.

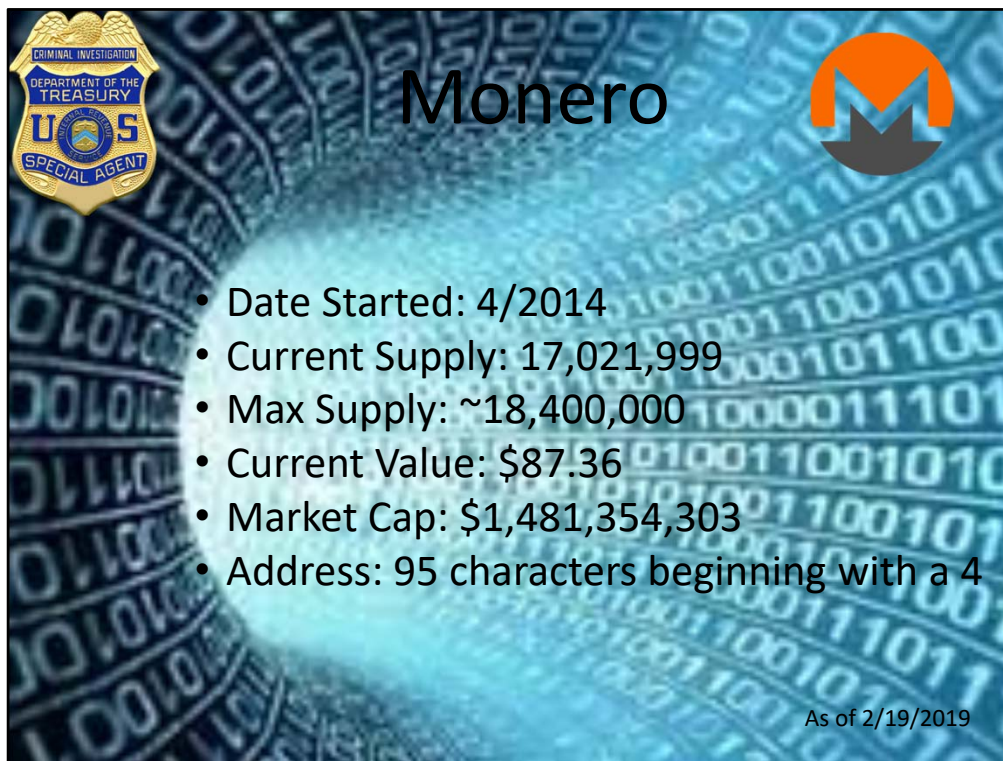
### **Where to Buy Stellar**

A list of cryptocurrency exchanges that currently list Lumens (XLM) include:

- Bittrex
- Binance
- Kraken
- Poloniex



As of 2/19/2019

A presentation slide for Monero. The background is a blue-tinted image of a tunnel with binary code (0s and 1s) on the walls. In the top left corner is the U.S. Department of Treasury logo, featuring a shield with 'CRIMINAL INVESTIGATION', 'DEPARTMENT OF THE TREASURY', 'U.S.', and 'SPECIAL AGENT'. In the top center, the word 'Monero' is written in a large, black, sans-serif font. In the top right corner is the Monero logo, a stylized 'M' inside a circle with an orange-to-black gradient. Below the title, there is a bulleted list of statistics. In the bottom right corner, the text 'As of 2/19/2019' is displayed.

- Date Started: 4/2014
- Current Supply: 17,021,999
- Max Supply: ~18,400,000
- Current Value: \$87.36
- Market Cap: \$1,481,354,303
- Address: 95 characters beginning with a 4

As of 2/19/2019

**Monero (XMR)** is an open-source cryptocurrency created in April 2014 that focuses on privacy and decentralization that runs on Windows, macOS, Linux, Android, iOS, and FreeBSD. Monero uses a public ledger to record transactions while new units are created through a process called mining. Monero aims to improve on existing cryptocurrency design by obscuring sender, recipient and amount of every transaction made as well as making the mining process more egalitarian.

The focus on privacy has attracted illicit use by people interested in evading law enforcement. The egalitarian mining process made it viable to distribute the mining effort opening new funding avenues for both legitimate online publishers and malicious hackers who covertly embed mining code into websites and apps.

Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNight proof-of-work hash algorithm, which comes from the CryptoNote protocol. It possesses significant algorithmic differences relating to blockchain obfuscation. By providing a high level of privacy, Monero is fungible, meaning that every unit of the currency can be substituted by another unit. This makes Monero different from public-ledger cryptocurrencies like Bitcoin, where addresses with coins previously associated with undesired activity can be blacklisted and have their coins refused by other users.

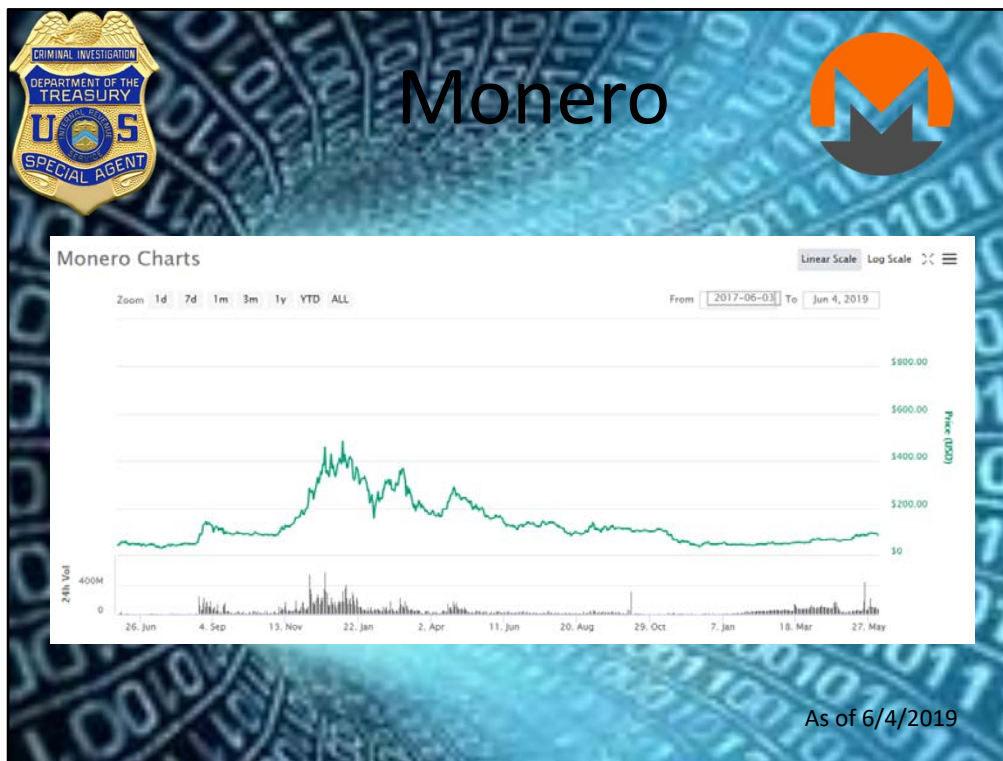
In particular, the ring signatures mix the spender's input with a group of others, making it exponentially more difficult to establish a link between each subsequent transaction. Also, the "stealth addresses" generated for each transaction make it impossible to discover the

actual destination address of a transaction by anyone else other than the sender and the receiver. Finally, the "ring confidential transactions" mechanism hides the transferred amount.

Monero is designed to be resistant to application-specific integrated circuit mining, which is commonly used to mine other cryptocurrencies such as Bitcoin. It can be mined somewhat efficiently on consumer grade hardware such as x86, x86-64, ARM and GPUs.

In April 2017 research highlighted three major threats to Monero user's privacy. The first relies on leveraging the ring signature size of zero, and ability to see the output amounts. The second, described as "Leveraging Output Merging", involves tracking transactions where two outputs belong to the same user, such as when a user is sending the funds to himself ("churning"). Finally the third threat, "Temporal Analysis", shows that predicting the right output in a ring signature is easier than previously thought.

Monero development team addressed the first concern in early 2017 with introduction of Ring Confidential Transactions (ringCT) as well as mandating a minimum size of ring signatures in the March 2016 protocol upgrade. Monero developers also noted that Monero Research Labs, their academic and research arm, already noted and outlined the deficiency in two public research papers in 2014 and 2015.



**Monero (XMR)** is an open-source cryptocurrency created in April 2014 that focuses on privacy and decentralization that runs on Windows, macOS, Linux, Android, iOS, and FreeBSD. Monero uses a public ledger to record transactions while new units are created through a process called mining. Monero aims to improve on existing cryptocurrency design by obscuring sender, recipient and amount of every transaction made as well as making the mining process more egalitarian.

The focus on privacy has attracted illicit use by people interested in evading law enforcement. The egalitarian mining process made it viable to distribute the mining effort opening new funding avenues for both legitimate online publishers and malicious hackers who covertly embed mining code into websites and apps.

Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNight proof-of-work hash algorithm, which comes from the CryptoNote protocol. It possesses significant algorithmic differences relating to blockchain obfuscation. By providing a high level of privacy, Monero is fungible, meaning that every unit of the currency can be substituted by another unit. This makes Monero different from public-ledger cryptocurrencies like Bitcoin, where addresses with coins previously associated with undesired activity can be blacklisted and have their coins refused by other users.

In particular, the ring signatures mix the spender's input with a group of others, making it exponentially more difficult to establish a link between each subsequent transaction. Also, the "stealth addresses" generated for each transaction make it impossible to discover the

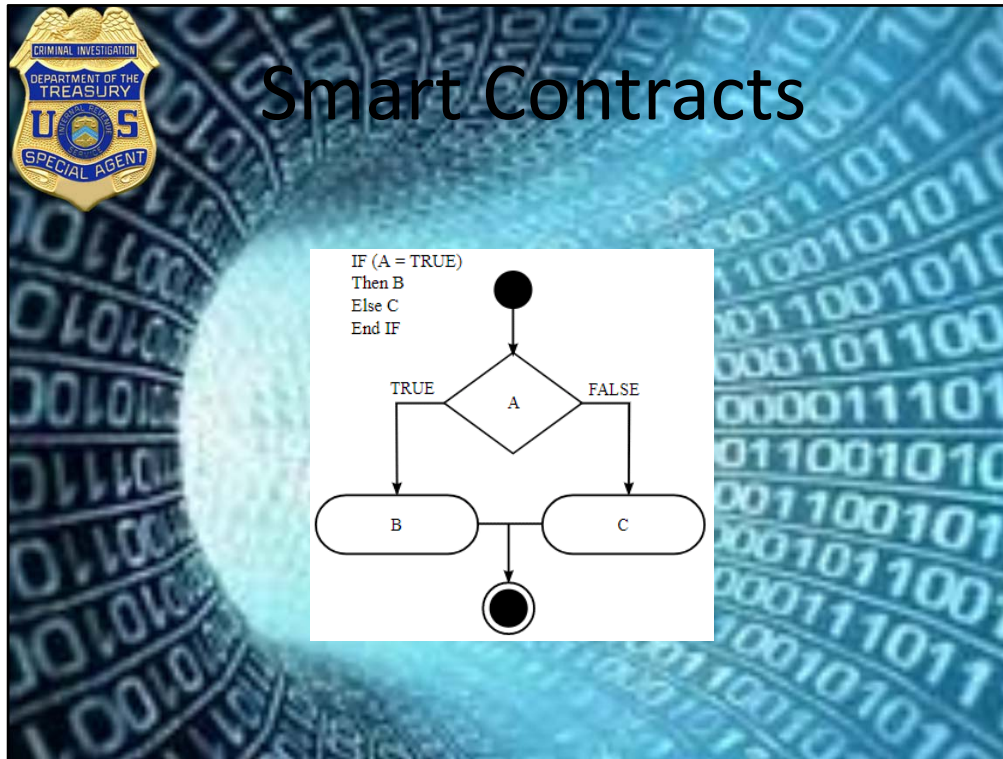
actual destination address of a transaction by anyone else other than the sender and the receiver. Finally, the "ring confidential transactions" mechanism hides the transferred amount.

Monero is designed to be resistant to application-specific integrated circuit mining, which is commonly used to mine other cryptocurrencies such as Bitcoin. It can be mined somewhat efficiently on consumer grade hardware such as x86, x86-64, ARM and GPUs.

In April 2017 research highlighted three major threats to Monero user's privacy. The first relies on leveraging the ring signature size of zero, and ability to see the output amounts. The second, described as "Leveraging Output Merging", involves tracking transactions where two outputs belong to the same user, such as when a user is sending the funds to himself ("churning"). Finally the third threat, "Temporal Analysis", shows that predicting the right output in a ring signature is easier than previously thought.

Monero development team addressed the first concern in early 2017 with introduction of Ring Confidential Transactions (ringCT) as well as mandating a minimum size of ring signatures in the March 2016 protocol upgrade. Monero developers also noted that Monero Research Labs, their academic and research arm, already noted and outlined the deficiency in two public research papers in 2014 and 2015.





**Smart contracts** According to Black’s law dictionary, a contract is: “An agreement, upon sufficient consideration, to do or not to do a particular thing.” Sounds simple right? Contract law is a deep rabbit hole that spans a myriad of offshoots which many dedicate their lives to but there is one key shift in this digital age, the law is now programmed code.

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman. The best way to describe smart contracts is to compare the technology to a vending machine. Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a bitcoin into the vending machine (i.e. ledger), and your escrow, driver’s license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

In the US, the ESIGN act passed federally in 2000 which legalized the use of digital signatures as a legally binding construct. In China, a similar contract law and legal use of digital signatures were put on the books in 2007. This means the legal system now has a bridge with the digital realm and opens a plethora of new opportunities for digital contracts.

Contracts govern an agreement between two (or more) individuals and/or parties. If X occurs then Y is provided. If X does not occur, here is Z recourse. This ties in quite nicely

with the conditional programming structure in computer science where “if-then-else” expressions can easily be built around traditional contract law in effect making law into code.



- Government/Management
- Supply Chain
- Automobile
- Real Estate
- Healthcare

### ***Government***

Insiders vouch that it is extremely hard for our voting system to be rigged, but nonetheless, smart contracts would allay all concerns by providing an infinitely more secure system. Ledger-protected votes would need to be decoded and require excessive computing power to access. No one has that much computing power, so it would need God to hack the system! Secondly, smart contracts could hike low voter turnout. Much of the inertia comes from a fumbling system that includes lining up, showing your identity, and completing forms. With smart contracts, volunteers can transfer voting online and millennials will turn out en masse to vote for their Potus.

### ***Management***

The blockchain not only provides a single ledger as a source of trust, but also shaves possible snarls in communication and workflow because of its accuracy, transparency, and automated system. Ordinarily, business operations have to endure a back-and-forth, while waiting for approvals and for internal or external issues to sort themselves out. A blockchain ledger streamlines this. It also cuts out discrepancies that typically occur with independent processing and that may lead to costly lawsuits and settlement delays.

### ***Supply Chain***

Smart contracts work on the If-Then premise so, to put in [Jeff Garzik's words](#), **"UPS can execute contracts that say, 'if I receive cash on delivery at this location in a developing, emerging market, then this other [product], many, many links up the supply chain, will trigger a supplier creating a new item since the existing item was just delivered in that developing market.'" All too often, supply chains are hampered by paper-based systems, where forms have to pass through numerous channels for**

**approval, which increases exposure to loss and fraud. The blockchain nullifies this by providing a secure, accessible digital version to all parties on the chain and automates tasks and payment.**

### ***Automobile***

There's no doubt that we're progressing from slothful pre-human vertebrates to super-smart robots. Think of a future where everything is automated. Google's getting there with smartphones, smart glasses, and even smart cars. That's where smart contracts help. One example is the self-autonomous or self-parking vehicles, where smart contracts could put into play a sort of 'oracle' that could detect who was at fault in a crash; the sensor or the driver, as well as countless other variables. Using smart contracts, an automobile insurance company could charge rates differently based on where, and under which, conditions customers are operating their vehicles.

### ***Real Estate***

You can get more money through smart contracts. Ordinarily, if you wanted to rent your apartment to someone, you'd need to pay a middleman such as Craigslist or a newspaper to advertise and then again you'd need to pay someone to confirm that the person paid rent and followed through. The ledger cuts your costs. All you do is pay via bitcoin and encode your contract on the ledger. Everyone sees, and you accomplish automatic fulfillment. Brokers, real estate agents, hard money lenders, and anyone associated with the property game can profit.

### ***Healthcare***

Personal health records could be encoded and stored on the blockchain with a private key which would grant access only to specific individuals. The same strategy could be used to ensure that research is conducted via HIPAA laws (in a secure and confidential way). Receipts of surgeries could be stored on a blockchain and automatically sent to insurance providers as proof-of-delivery. The ledger, too, could be used for general healthcare management, such as supervising drugs, regulation compliance, testing results, and managing healthcare supplies.



**Autonomy** – You’re the one making the agreement; there’s no need to rely on a broker, lawyer or other intermediaries to confirm. Incidentally, this also knocks out the danger of manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

**Trust** – Your documents are encrypted on a shared ledger. There’s no way that someone can say they lost it.

**Backup** – Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends has your back. Your documents are duplicated many times over.

**Safety** – [Cryptography](#), the encryption of websites, keeps your documents safe. There is no hacking. In fact, it would take an abnormally smart hacker to crack the code and infiltrate.

**Speed** – You’d ordinarily have to spend chunks of time and paperwork to manually process documents. Smart contracts use software code to automate tasks, thereby shaving hours off a range of business processes.

**Savings** – Smart contracts save you money since they knock out the presence of an intermediary. You would, for instance, have to pay a notary to witness your transaction.

**Accuracy** – Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.





An initial coin offering (**ICO**) is a controversial means of crowdfunding centered around cryptocurrency, which can be a source of capital for startup companies. In an ICO, a quantity of the crowdfunded cryptocurrency is sold to investors in the form of "tokens", in exchange for legal tender or other cryptocurrencies such as bitcoin or ethereum. These tokens supposedly become functional units of currency if or when the ICO's funding goal is met and the project launches.

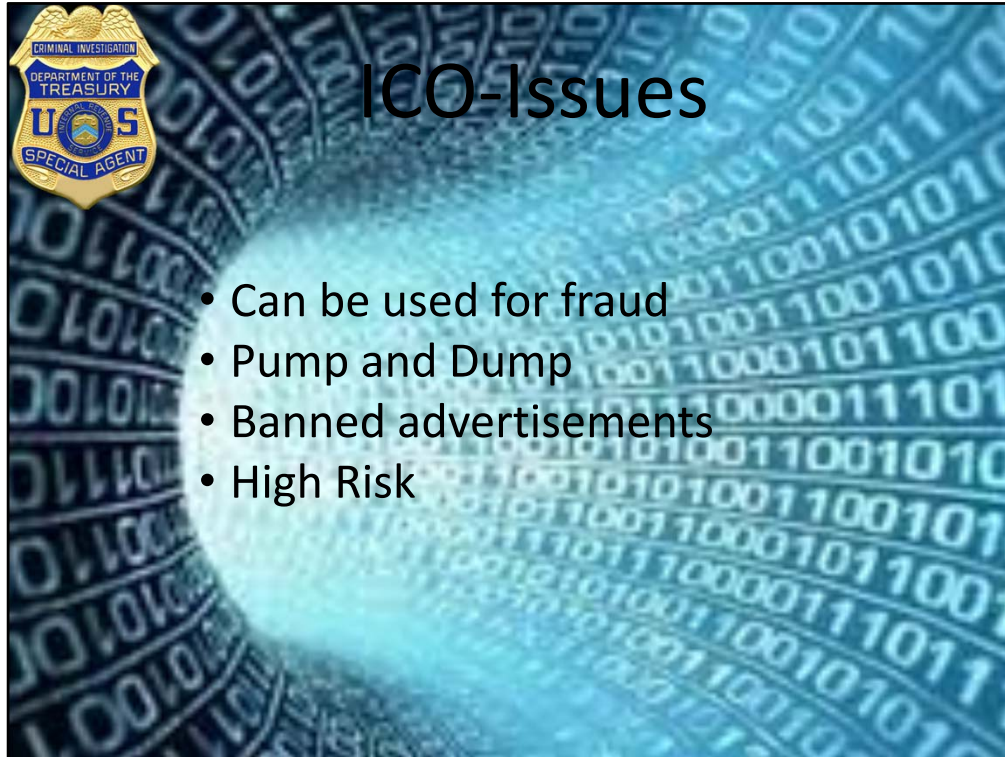
ICOs provide a means by which startups avoid costs of regulatory compliance and intermediaries, such as venture capitalists, bank and stock exchanges, while increasing risk for investors. ICOs may fall outside existing regulations depending on the nature of the project, or are banned altogether in some jurisdictions, such as China and South Korea.

ICOs and token sales became popular in 2017. There were at least 18 websites tracking ICOs before mid-year. In May, the ICO for a new web browser called Brave generated about \$35 million in under 30 seconds. Messaging app developer Kik's September 2017 ICO raised nearly \$100 million. At the start of October 2017, ICO coin sales worth \$2.3 billion had been conducted during the year, more than ten times as much as in all of 2016. As of November 2017, there were around 50 offerings a month, with the highest-grossing ICO as of January 2018, being Filecoin raising \$257 million (and \$200 million of that within the first hour of their token sale).

Kik had previously issued \$50 million in tokens called "Kin" to institutional investors, and sought to raise an additional \$125 million from the public. In connection with this ICO, an

unidentified third party executed a phishing scam by circulating a fake URL for the offering through social media.





- Can be used for fraud
- Pump and Dump
- Banned advertisements
- High Risk

ICOs can be used for fraud, as well as legal activities such as corporate finance and charitable fundraising. The U.S. Securities and Exchange Commission (SEC) has warned investors to beware of scammers using ICOs to execute "pump and dump" schemes, in which the scammer talks up the value of an ICO in order to generate interest and drive up the value of the coins, and then quickly "dumps" the coins for a profit. The developers themselves can be guilty of such tactics.

Facebook has banned ICO and cryptocurrency advertisements on its platform stating that many of them were "not currently operating in good faith." Google and Twitter have also banned ICO and cryptocurrency advertisements.

Snapchat, LinkedIn and MailChimp all have limited companies from marketing ICOs via their platforms. Jimmy Wales, founder of Wikipedia, stated in 2017 that "there are a lot of these initial coin offerings which are in my opinion are absolute scams and people should be very wary of things that are going on in that area."

Chinese internet platforms Baidu, Tencent, and Weibo have also prohibited ICO advertisements. The Japanese platform Line and the Russian platform Yandex have similar prohibitions.

The SEC has also acknowledged that ICOs "may provide fair and lawful investment opportunities". The UK Financial Conduct Authority has also warned that ICOs are very high risk and speculative investments, are scams in some cases, and often offer no protections

for investors. Even in cases of legitimate ICOs, funded projects are typically in an early and therefore high-risk stage of development. The European Securities and Markets Authority (ESMA) notes high risks associated with ICOs and the risk that investors may lose all of their cash.

By the end of 2017, ICOs had raised almost 40 times as much capital as they had raised in 2016, although still amounting to less than two percent of the capital raised by IPOs. According to Cointelegraph, companies raised around \$6 billion via ICOs in 2017; 37% of that amount was made by only 20 ICOs. Already by February, 2018, an estimated 46% of the 2017 ICOs had failed.



### **ONECOIN**

One of the worst ICOs of 2017 was OneCoin, a textbook scam from start to finish. OneCoin was a multi-level marketing Ponzi scheme (think Cutco knives). It's difficult to give more detail, because there's no information a token was ever created. The team had little concrete to show investors, and certainly no working prototype. Some of the team's biggest members had previously been linked to other scams. Dr. Ruja Ignatov, founder and COO, may have falsified her qualifications on the company's website. Speaking of the website, it was a parody of a scam site. Spelling was poor, and technical problems were common. Numerous governments warned against investing. On April 24th, Indian authorities raided a OneCoin meeting. 18 were jailed, but not before OneCoin scammed investors out of 350 million. Tellingly, they accepted funding in standard currency, not Bitcoin or Ethereum like most ICOs. The story was a black eye on the crypto world.

### **ENIGMA**

Some crypto scandals aren't a result of poor intentions; just poor execution. Such was the case for Enigma. Enigma is a security and cryptography coin, that boasted about its new encryption methods. Named after the German encryption machine in World War II, Enigma's mailing list, website, and Slack accounts were all hacked ahead of the company's ICO. Hackers used Slack to reach out to investors about a fake early ICO. Some rightly called the email a scam, but many others pulled the trigger, and hackers made off with around \$500,000 in Ethereum. Enigma CEO Guy Zizkind's account was hacked, because he hadn't set up two-factor authentication. This is a staggering mistake. Two-factor authentication is a common feature on wallets and exchanges, and is regularly emphasized as one of the most important things users can do to protect their coins. The CEO of a security-focused

ICO neglecting this is comical. Many prospective investors were scared off for good.

### **DROPLEX**

Thankfully for investors, many ICOs barely even put effort into appearing legit. Droplex was a lazy scam attempt that was quickly called out. Droplex's whitepaper was a carbon copy of QRL's whitepaper. Literally word for word, but with "Droplex" substituted for the word "QRL." College kids put more effort into plagiarizing. Droplex's Github repository was also a direct copy of QRL's for a while. Once people became aware, they changed it, but they've added no new code in months. Fortunately, Droplex was lambasted early and often, and they only made off with around 25K.

### **COINDASH**

Another prominent recent hack occurred when someone boosted a \$10M off of CoinDash, an Israeli company. The hacking method is uncertain. Some sources speculate the hacker created an identical website to the team's. Others think he or she simply changed the payment address, to divert funds. Either way, the hacker netted a huge sum. CoinDash had previously raised around 6.4M, so they aren't totally broke. And the company nobly pledged to send tokens even to those who had donated to the fraudulent address. But it was just another reminder of the risks of ICOS, with many furious investors accusing the company of pulling an inside job.

### **VERITASEUM**

Veritaseum had red flags before hackers jacked \$5.4M from the company. The coin claimed to be a peer-to-peer personal banking service. Investors who balked cited the team's sketchy website, and its paid promotion by YouTube accounts. An extensive Reddit thread poked numerous holes in the team's technology. The hack itself couldn't have been sketchier. The team has been shady about how exactly it occurred, mentioning "social engineering" and an unnamed corporate partner who was negligent. A large amount of VERI tokens were stolen, and traded for Ethereum. The flash liquidation by the hacker boosted the price of VERI, and someone cruised to a large payday. Many investors and non-investors alike blasted the Veritaseum team, accusing them of pocketing the funds and claiming a hack. In the Wild West of crypto, there's no way to know for sure. But it's an unfortunate situation no matter how you slice it.

### **PARITY**

Most crypto investors know to keep their coins in a wallet, and not on exchanges. But sometimes even that doesn't help; a hacker exploited a vulnerability in Parity's Multisig Wallets, netting \$30M. Using a flaw in the code and a two-step process, the hacker cracked what was thought to be a safe wallet. The hacker took Ether from multi-signature wallets containing funds from Edgeless, Swarm City, and Aeternity, three other projects. Fortunately, heroic "white hat" hackers were able to track down and return most of the stolen Ether to their rightful owners. It's still early days in the crypto world, and this won't be the last wallet hacked, but hopefully it's a learning experience.

Source: <https://www.coinist.io/6-worst-icos-of-all-time/>

The image shows a screenshot of the ICOALERT website. At the top left is the U.S. Department of Treasury logo with 'CRIMINAL INVESTIGATION' and 'SPECIAL AGENT' text. The word 'ICO' is displayed in large letters at the top right. Below the logo is the 'ICOALERT' text. The main content area is divided into three columns: 'ACTIVE ICOS', 'UPCOMING ICOS', and 'CONCLUDED ICOS'. Each column lists ICOs with their names, descriptions, and dates. The 'ACTIVE ICOS' column lists TRUEGAME (1 day left), RXEAL (2 days left), and KELTA (6 days left). The 'UPCOMING ICOS' column lists PROOF OF TOSS (12 APR), ARCONA (15 APR), and ELIGMA (17 APR). The 'CONCLUDED ICOS' column lists SPHERE SOCIAL (ENDED 07 APR 2018), TIHOSAY (ENDED 08 APR 2018), and LEMOCHAIN (ENDED 08 APR 2018). Each entry includes a 'My Portfolio' button and a 'View Website' button. The source is cited as 'Source: Icoalert.com' at the bottom right.

ACTIVE ICOS	UPCOMING ICOS	CONCLUDED ICOS
<b>1 DAY LEFT</b> <b>TRUEGAME</b> A smart contract based iGaming platform. Active Since: Mar 26th 2018	<b>12 APR</b> <b>PROOF OF TOSS</b> Decentralized betting ecosystem aiming to modernize the betting industry.	<b>ENDED 07 APR 2018</b> <b>SPHERE SOCIAL</b> View Website
<b>2 DAYS LEFT</b> <b>RXEAL</b> An awaited solution for global rental markets on blockchains. Active Since: Mar 12th 2018	<b>15 APR</b> <b>ARCONA</b> Blockchain-powered ecosystem merging real and virtual worlds worldwide.	<b>ENDED 08 APR 2018</b> <b>TIHOSAY</b> Converting your cryptocurrencies into spendable capital.
<b>6 DAYS LEFT</b> <b>KELTA</b> Decentralized computing power for scientific researchers, scholars, and cryptocurrency miners. Active Since: Apr 8th 2018	<b>17 APR</b> <b>ELIGMA</b> Eligma is an AI-driven and blockchain based cognitive commerce platform.	<b>ENDED 08 APR 2018</b> <b>LEMOCHAIN</b> Data Circulation Infrastructure connecting every day businesses.

List of ICO's Active and upcoming





## How to Obtain Bitcoins

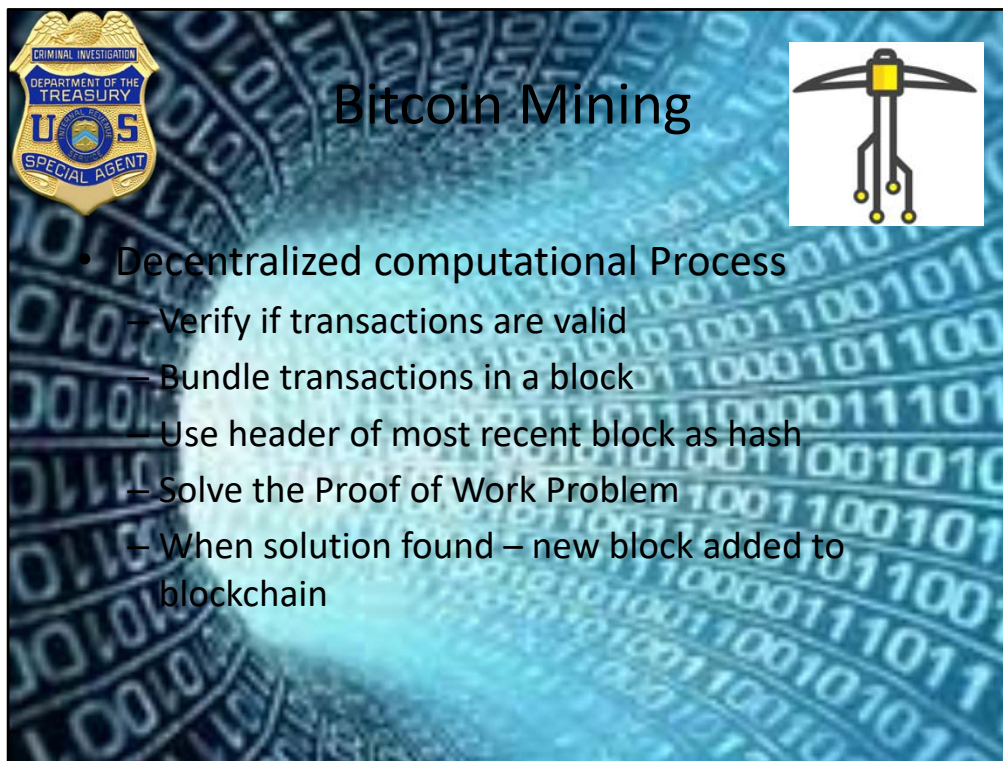


**Mining**

**Direct  
Purchase**

**Exchanger**





## Bitcoin Mining

- Decentralized computational Process
  - Verify if transactions are valid
  - Bundle transactions in a block
  - Use header of most recent block as hash
  - Solve the Proof of Work Problem
  - When solution found – new block added to blockchain

Bitcoin mining is the process by which transactions are verified and added to the public ledger, known as the block chain, and also the means through which new bitcoin are released. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released bitcoin.

Bitcoin mining is accomplished by running SHA256 double round hash verification processes in order to validate Bitcoin transactions and provide the requisite security for the public ledger of the Bitcoin network. The speed at which you mine Bitcoins is measured in hashes per second.

No advanced math or computation is involved. You may have heard that miners are solving difficult mathematical problems--that's not true at all. What they're actually doing is trying to be the first miner to come up with a 64-digit hexadecimal number (a "[hash](#)") that is less than or equal to the target hash. It's basically guess work.

It may seem that the group of individuals most directly effected by the limit of the Bitcoin supply will be the Bitcoin miners themselves. On one hand, there are detractors of the Bitcoin limitation who that say that miners will be forced away from the block rewards they receive for their work once the Bitcoin supply has reached 21 million in circulation. In this

case, these miners may need to rely on transaction fees in order to maintain operations. Bitcoin.com points to an argument that miners will then find the process unaffordable, leading to a reduction in the number of miners, a centralization process of the Bitcoin network, and numerous negative effects on the Bitcoin system.



At first, miners used their **central processing unit** (CPU) to mine, but soon this wasn't fast enough and it bogged down the system resources of the host computer.

Miners quickly moved on to using the **graphical processing unit** (GPU) in computer graphics cards because they were able to hash data 50 to 100 times faster and consumed much less power per unit of work.

During the winter of 2011, a new industry sprang up with custom equipment that pushed the performance standards even higher. The first wave of these specialty bitcoin mining devices were easy to use Bitcoin miners were based on **field-programmable gate array** (FPGA) processors and attached to computers using a convenient USB connection. FPGA miners used much less power than CPU's or GPU's and made concentrated mining farms possible for the first time.

*Today's modern and best bitcoin mining hardware*

**Application-specific integrated circuit** (ASIC) miners have taken over completely. These ASIC machines mine at unprecedented speeds while consuming much less power than FPGA or GPU mining rigs. Several reputable companies have established themselves with excellent products.

ASICs are bitcoin mining hardware created solely to solve Bitcoin blocks. They have only minimal requirements for other normal computer applications. Consequently, ASIC Bitcoin mining systems can solve Bitcoin blocks much quicker and use less less electricity or power

than older bitcoin mining hardware like CPUs, GPUs or FPGAs.

As Bitcoin mining increases in popularity and the Bitcoin price rises so does the value of ASIC Bitcoin mining hardware. As more Bitcoin mining hardware is deployed to secure the Bitcoin network the Bitcoin difficulty rises. This makes it impossible to profitably compete without a Bitcoin ASIC system. Furthermore, Bitcoin ASIC technology keeps getting faster, more efficient and more productive so it keeps pushing the limits of what makes the best Bitcoin mining hardware.

Some models of Bitcoin miners include Antminer S5, Antminer U3, ASICMiner BE Tube, ASICMiner BE Prisma, Avalon 2, Avalon 3, BTC Garden AM-V1 616 GH/s, VMC PLATINUM 6 MODULE, and USB miners. Prices range from \$500 - \$2000 per machine.



Mining pools are groups of cooperating miners who agree to share block rewards in proportion to their contributed mining hash power.

While mining pools are desirable to the average miner as they smooth out rewards and make them more predictable, they unfortunately concentrate power to the mining pool's owner.

Miners can, however, choose to redirect their hashing power to a different mining pool at anytime.





In addition to purchasing hardware to do mining, people can now purchase into cloud mining.

### Types of Bitcoin Cloud Mining

There are two forms of cloud mining:

**Hosted Mining** – You send your mining machine to a Firm, which provides electricity, cooling and configurations. It is also possible, that you lease yourself a mining machine.

**Buying Hashing Power** – The most popular method of cloud mining – You buy an amount of hashing power (Hash Rate). Which means, that you don't need to own a physical or virtual mining machine (computer).

The pros of the one are the cons of the other and vice versa.

### Hosted Mining vs. Buying Hashing Power

If you decide to get an hosted bitcoin mining contract, than you need to check if the provider is a registered venture. If this is the case, you have high certainly, that you may not get scammed.

Cons:

**Scam Risk** – you can always have bad luck and find a cloud mining fraud.



**Cost of Mining Operations** – you need to pay for the hardware management  
**Less fun** – at least for some it can be less fun to just virtually own something.  
**Lack of control and flexibility** – harder to control where to mine or when to sell the bitcoin miner.

Pros:

**Higher Profits** – because cloud mining providers optimize everything, it yields out higher returns.

**Tranquil and cooler home** – no more permanent sound and heat.

**Less electricity** – the electricity bills will get a lot lower.

**'No' equipment problems** – no need to sell the bitcoin miners, when they stop being profitable. No need to configure the bitcoin hardware.

**Less risky** – the possibility to get let down by the equipment is decreased by a lot.

**Better prices** – Bitcoin Cloud Mining operations involve millions of dollars. This is why the companies are able to negotiate better energy and hardware prices.

The slide features a background of a glowing blue tunnel with binary code (0s and 1s) on the walls. In the top left corner is the U.S. Department of Treasury logo with 'CRIMINAL INVESTIGATION' and 'SPECIAL AGENT' text. In the top right corner is an icon of a mining rig. The title 'Bitcoin Mining' is centered at the top. Below the title is a bulleted list of mining reward details.

**Bitcoin Mining**

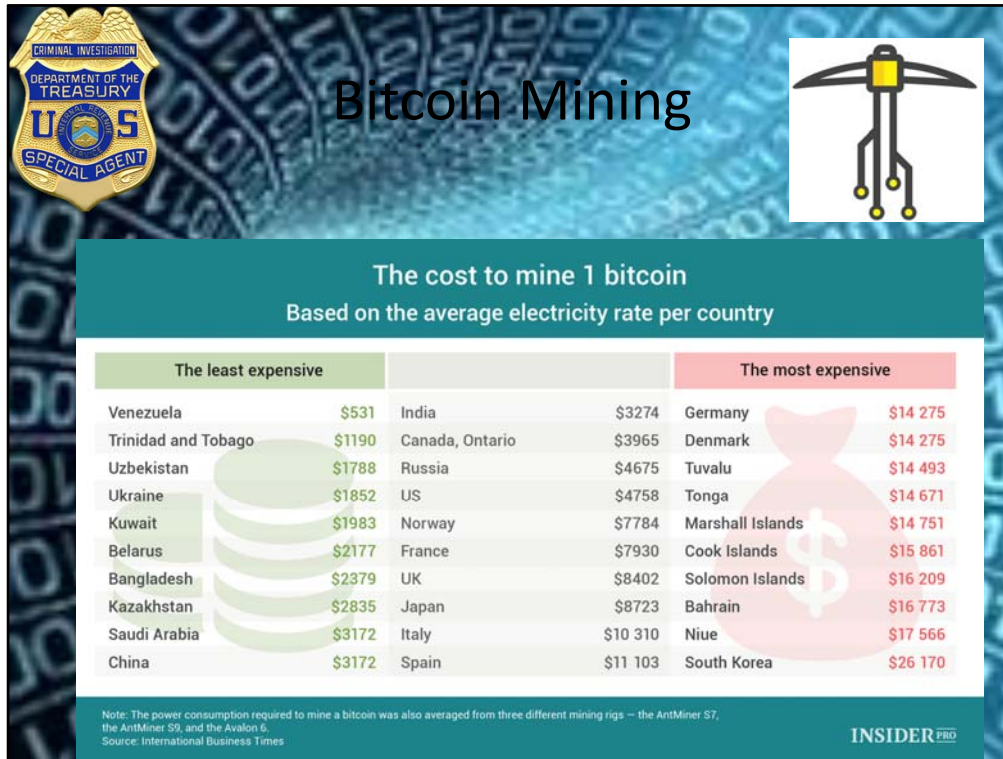
- Mining reward
  - Currently 12.5 Bitcoins
  - Reward value will halve every 210,000 blocks
  - Next project halve will occur on 6/13/2020

The block reward started at 50 BTC in block #1 and halves every 210,000 blocks. This means every block up until block #210,000 rewards 50 BTC, while block 210,001 rewards 25. Since blocks are mined on average every 10 minutes, 144 blocks are mined per day on average. At 144 blocks per day, 210,000 blocks take on average four years to mine.

The block reward creates an incentive for miners to add hash power to the network. The block reward is what miners try to get using their ASICs, which make up the entirety of the Bitcoin network hash rate.

ASICs are expensive, and have high electricity costs. Miners are profitable when their hardware and electricity costs to mine one bitcoin are lower than the price of one bitcoin. This means miners can mine bitcoins and sell them for a profit.

The more hash power a miner or mining pool has, the greater the chance is that the miner or pool has to mine a block. As miners add more hash rate, more security is provided to the network. The block reward acts as a subsidy and incentive for miners until transaction fees can pay the miners enough money to secure the network.



Bitcoin is expensive — whether you buy it from a broker or mine it yourself. But it's a lot more expensive to mine in some countries than others.

Elite Fixtures has compiled a list of mining costs throughout the world, using averaged data from three mining rigs and average electricity rates in 115 countries as of January 2018. And, based on those results, you absolutely do not want to launch a mining operation in South Korea,

It costs \$26,170 to mine a single Bitcoin in that country — more than twice the current cost of buying one. Niue (an island country in the South Pacific, if you didn't know) was the second most expensive, coming in at \$17,566.

The U.S. was a little more than midway down the list, with the average cost coming in at \$4,758. (If you really want to cut costs, do your U.S. mining in Louisiana, where the average cost for one coin is \$3,224.)

And Venezuela is the cheapest place on earth to do your mining, with an average cost of \$531, as energy rates are subsidized by the government there.

So what areas should Bitcoin miners avoid and where should they consider setting up operations? Here's what it costs in the most and least expensive countries.

Most expensive countries to mine Bitcoin

South Korea — \$26,170

Niue — \$17,566  
Bahrain — \$16,773  
Solomon Island — \$16,209  
Cook Islands — \$15,861

#### Least expensive countries to mine Bitcoin

Venezuela — \$531  
Trinidad and Tobago — \$1,190  
Uzbekistan — \$1,788  
Ukraine — \$1,852  
Myanmar — \$1,983

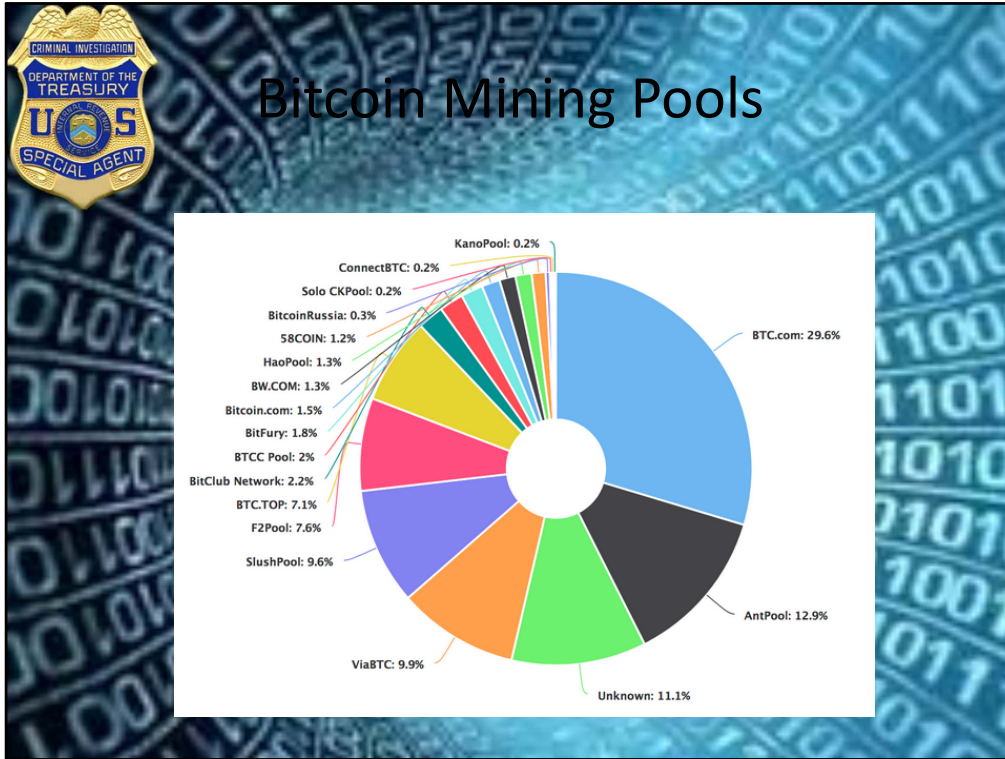
#### Mining costs are only likely to increase

Making matters even worse, the cost to mine a single bitcoin is only likely to grow over time, for a couple for a couple of reasons. For starters, electricity is a basic-needs service for most everyone, and as such electric utilities tend to possess strong pricing power that allows them to pass along inflation-matching or –topping price increases. In short, inflation all but assures that electricity costs are going to move higher over time.

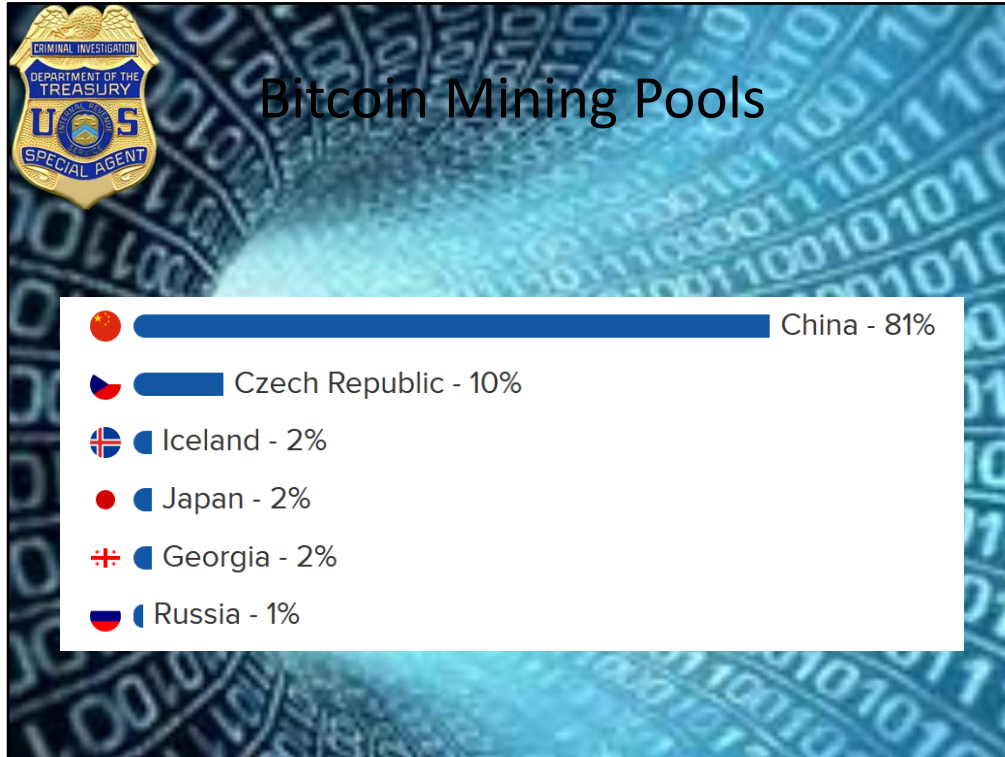
The bitcoin regulatory environment is also a potential issue for costs. Bitcoin and other cryptocurrencies are banned in around a half-dozen countries around the world, while the regulatory environment is growing more constrictive in other countries where it isn't banned. In China, for example, cryptocurrency exchanges and initial coin offerings have been stamped out, while mining operations have had their electricity usage throttled back. An increasingly regulated environment doesn't bode well for bitcoin mining costs.

Finally, it also can't be overlooked that the difficulty of mining bitcoin is only going to increase over time. There are more than 16.8 million bitcoin tokens in circulation, leaving fewer than 4.1 million left to be mined. As that difficulty increases and block rewards decline, the margin for mining bitcoin is probably going to decrease.

In other words, if bitcoin's price keeps falling, or if mining costs keep climbing, look for mining operations to become more consolidated in just a handful of the most profitable countries in the months and years to come.

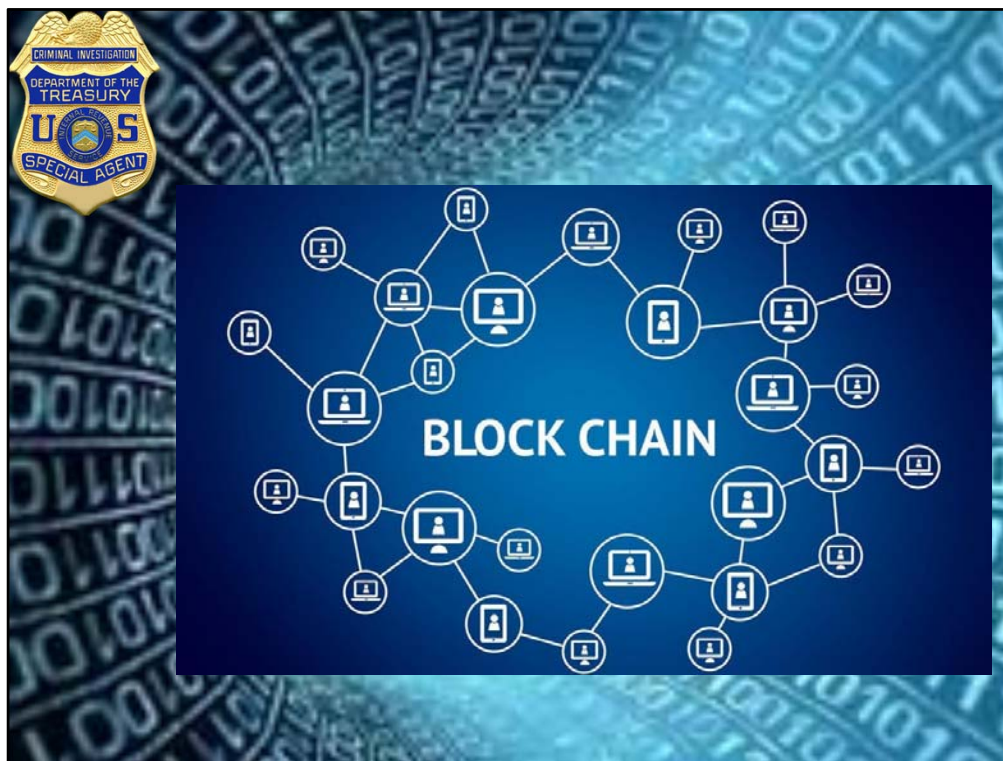


Breakdown of the bitcoin mining pools and the approximate percentage share of the mining done by each pool

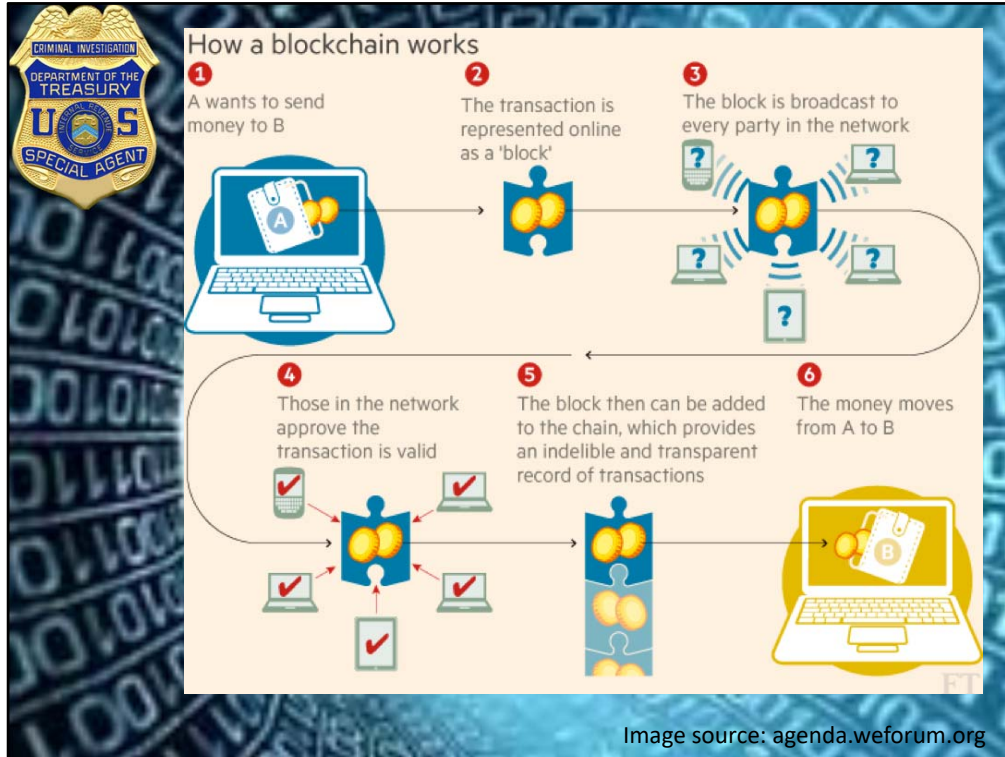


Breakdown of the bitcoin mining pools and the approximate percentage share of the mining done by each pool

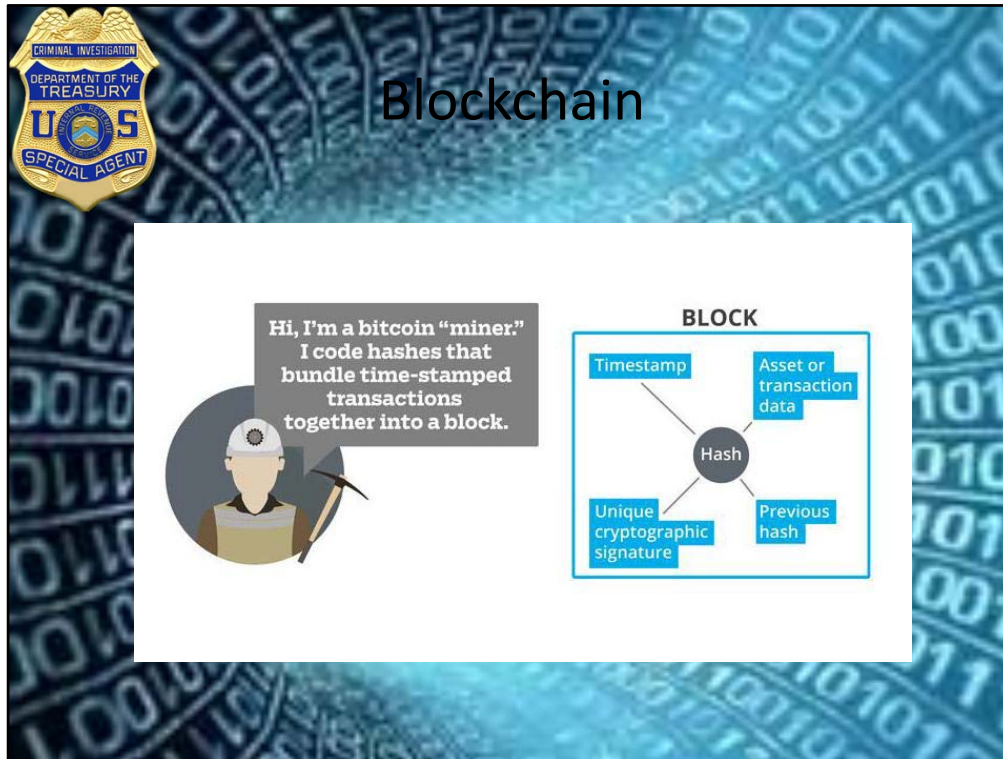




A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. This allows the participants to verify and audit transactions inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. The result is a robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. Blockchains have been described as a value-exchange protocol. This blockchain-based exchange of value can be completed more quickly, more safely and more cheaply than with traditional systems. A blockchain can assign title rights because it provides a record that compels offer and acceptance.



How blockchain works in regards to virtual currency transactions



Bitcoin blockchain is a distributed ledger of all transactions that have ever taken place in the network. Every transaction in the ledger is fully transparent to each node and depending on the type of implementation it also visible to anyone on the internet.

Blockchain is a merge of a consensus algorithm, the protocol that the network implements and a group of nodes running that protocol. Hence this has to be differentiated from a database as 'database' is just a piece of software.

Each transaction entry in the blockchain is irreversible or immutable i.e it cannot be changed either by manual intervention or by any participating node of the network. Transactions are transmitted and added to the digital ledger by very strong cryptography techniques. Each time a new node is added then a majority of the participating nodes validate the newly connected node. Once validated then the node has to download the entire ledger and sync with the network. Now each transaction that gets appended to a block (and the block subsequently to the blockchain) then the newly added node will have a copy of it and is in sync with the entire network.

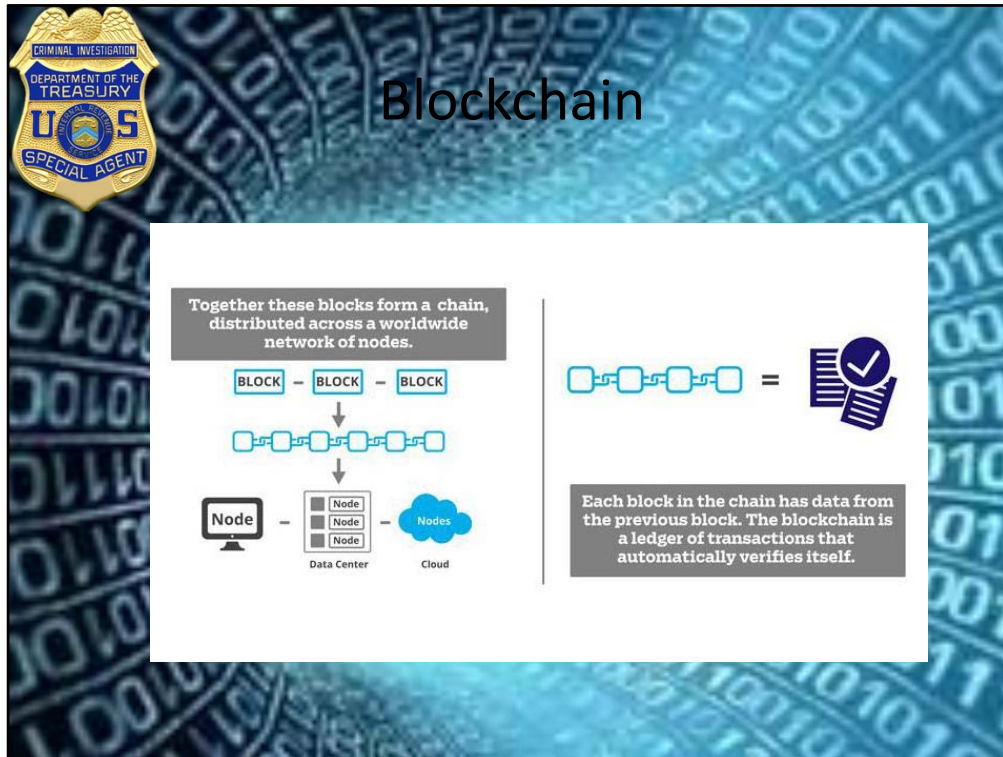
**Bitcoin Transaction: Similar to Checks**

**Check Fields:**  
Date/Timestamp: \_\_\_\_\_ 19\_\_\_\_  
91-548/1221  
PAY TO THE ORDER OF: \_\_\_\_\_ \$ \_\_\_\_\_  
DOLLARS  
FOR: \_\_\_\_\_  
Routing Number: 22105278  
Account Number: 6724301068  
Check Number: 2400

**Bitcoin Transaction Fields:**  
Transaction Hash: \_\_\_\_\_  
Bitcoin Amount: \_\_\_\_\_  
Input Bitcoin address: \_\_\_\_\_  
Input Private Key: \_\_\_\_\_  
Output Bitcoin address: \_\_\_\_\_

The comparisons to between a check and a bitcoin transaction





Technically speaking, blockchain is simply a data structure where each block is linked to another block. The blocks are linked to each other in a time-stamped chronological order. To access data of the first ever created block, you have to traverse from the last created block, then the block before that, so on and so forth till you reach the first block. Each block contains elements like the version #, reference of the address of the previous block, timestamp, transactional data, block size etc.

Each blockchain solution implements its own algorithm as a 'consensus mechanism'. Since every node in the network has equal weightage in terms of authority, they have to execute the same algorithm to validate each transaction. The consensus in terms of blockchain means the collective agreement or the decision making process of majority nodes. The consensus is carried out to collectively depend upon the 'state' of the entire network. Consensus helps to solve Double spend and [Byzantine's General Problem](#) of Distributed decentralized systems.

Bitcoin blockchain implements a 'difficulty level'. If the nodes are agreeing upon the consensus too quickly then the algorithm is designed in such a way that the difficulty increases and vice-versa. This has to ensure that the block creation time remains more or less constant.



# Blockchain

## Bitcoin Transaction confirmation



**Node A** submits  
a send transaction  
for 1.25 BTC  
payable to  
address 1i2PqM28zvUtnT

```
{  
  "account": "My Payment Address",  
  "address": "1i2PqM28zvUtnT",  
  "category": "send",  
  "amount": -1.25,  
  "fee": -0.0001,  
  "confirmations": 0,  
  "blockhash": "",  
  "blockindex": ,  
  "blocktime": ,  
  "txid": "7f77",  
  "time": 1391750000,  
  "timereceived": 1391750111  
}
```

Once block mining has solved the block hash,  
the block is inserted in the blockchain

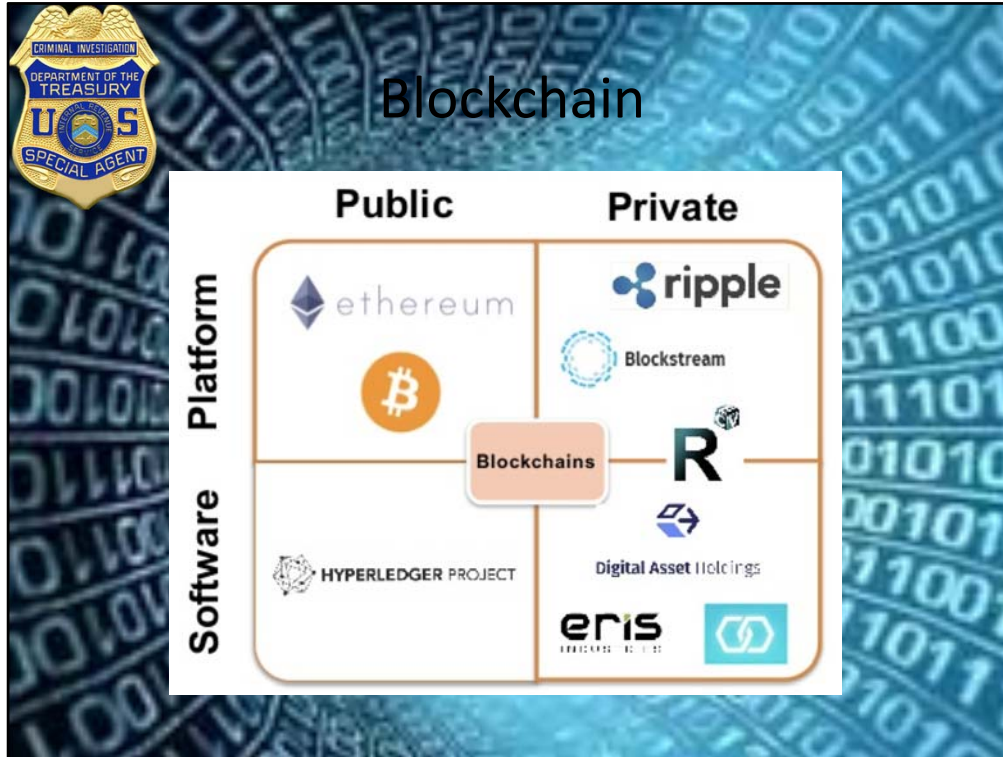
A miner includes the  
transaction in a block and  
1.25 BTC confirms for address  
1i2PqM28zvUtnT

**Node A**

**Node B**

owner of wallet address  
1i2PqM28zvUtnT





Many flavors of blockchain have evolved over the years and the terminology is often misconstrued. This is easy to do because public and private blockchain have many similarities:

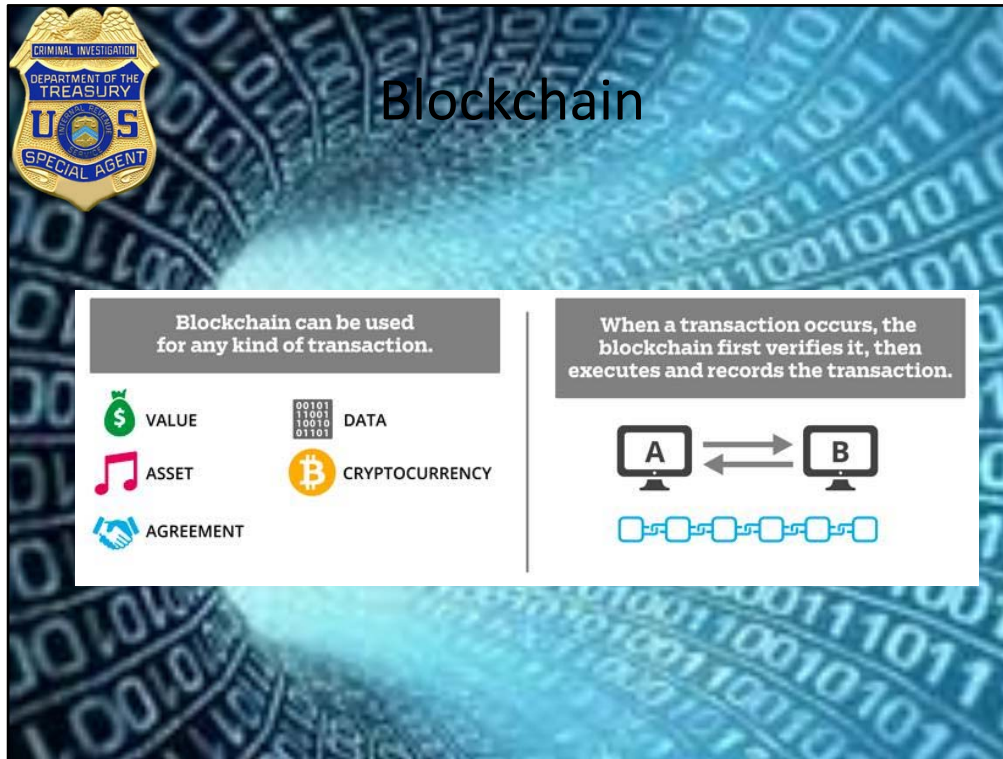
- Both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions.
- Both maintain the replicas in sync through a protocol referred to as consensus.
- Both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious.

The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the *consensus* protocol and maintain the shared ledger. A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today.

One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale. More specifically, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all are in sync.

Another disadvantage is the openness of public blockchain, which implies little to no privacy for transactions and only supports a weak notion of security. Both of these are important considerations for enterprise use cases of blockchain.

A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. Businesses who set up a private blockchain, will generally set up a *permissioned* network. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or *permission* to join. The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead. Once an entity has joined the network, it will play a role in maintaining the blockchain in a decentralized manner.



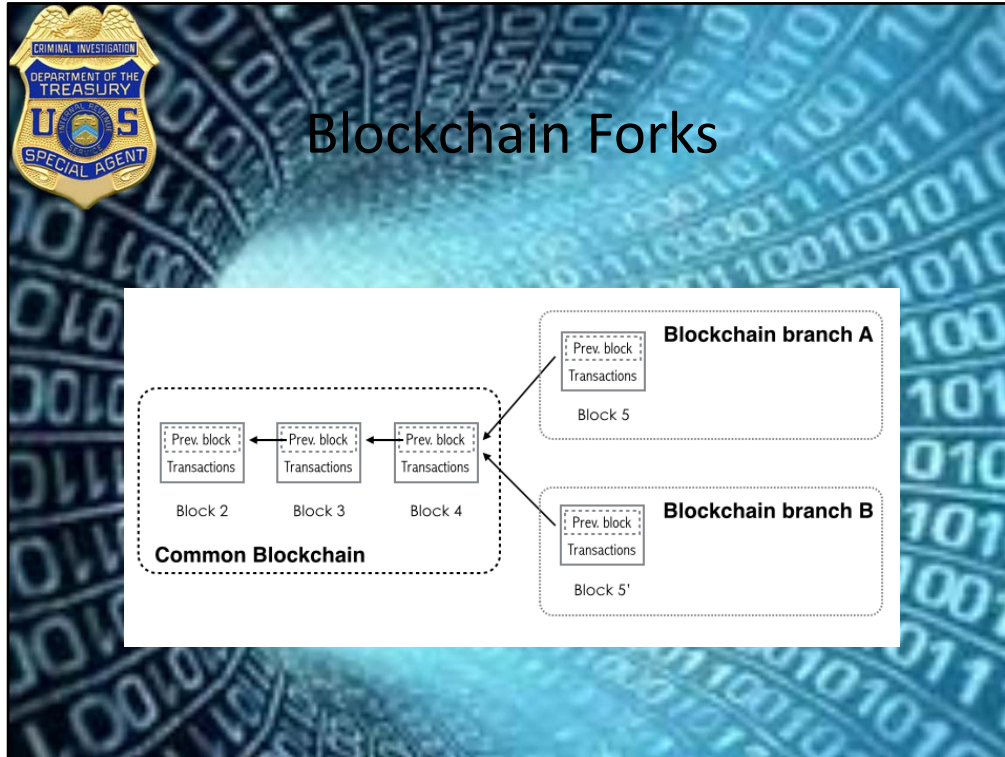
Although blockchain is most commonly associated with Bitcoin, there are many uses for this technology. There are several broad categories of blockchain applications, a couple of which include:

#### **Currency and Digital Assets**

The Blockchain that makes up Bitcoin sends money globally to individuals and merchants. But Blockchains can also create digital assets like stocks and bonds.

#### **Verifiable Data and Contracts**

A Blockchain can create a verifiable record of any data, file, or contract. This can be useful in any industry that uses big data, like the medical industry or government.



In cryptocurrencies, a fork is defined variously as

"what happens when a blockchain diverges into two potential paths forward"  
"a change in protocol" or  
a situation that "occurs when two or more blocks have the same block height"

Forks are related to the fact that different parties need to use common rules to maintain the history of the blockchain. Forks (in the sense of protocol changes) have been used in order to add new features to a blockchain, to reverse the effects of hacking or catastrophic bugs on a blockchain. Notably, blockchain forks have been widely discussed in the context of the bitcoin scalability problem.

Forks are further classified as accidental or intentional. Accidental fork happens when two or more miners find a block at nearly the same time. The fork is resolved when subsequent block(s) are added and one of the chains becomes longer than the alternative(s). The network abandons the blocks that are not in the longest chain (they are called orphaned blocks). A block containing invalid transactions is similarly abandoned.

Intentional forks that modify the rules of a blockchain can be classified as follows:

### **Hard fork**

A hard fork is a rule change such that the software validating according to the old rules will

see the blocks produced according to the new rules as invalid. In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software.

If one group of nodes continues to use the old software while the other nodes use the new software, a split can occur.

A hard fork is a software upgrade that introduces a new rule to the network that isn't compatible with the older software. You can think of a hard fork as an expansion of the rules. (A new rule that allows block size to be 2MB instead of 1MB would require a hard fork).

Nodes that continue running the old version of the software will see the new transactions as invalid. So, to switch over to the new chain and to continue to mine valid blocks, all of the nodes in the network need to upgrade to the new rules.

### **Soft fork**

In contrast to a hard fork, a soft fork is a change of rules that creates blocks recognized as valid by the old software, i.e. it is backwards-compatible.[1] As for a hard fork, a soft fork can also split the blockchain when non-upgraded software creates blocks not considered valid by the new rules.

A soft fork, by contrast, is any change that's backward compatible. Say, instead of 1MB blocks, a new rule might only allow 500K blocks.

### **User-activated soft fork**

A user-activated soft fork (UASF) is a controversial idea that explores how a blockchain might add an upgrade that is not directly supported by those who provide the network's hashing power.

The idea with UASF is that instead of waiting for a threshold of support from mining pools, the power to activate a soft fork goes to the exchanges, wallets and businesses who are running full nodes. (In bitcoin, a full node, even if it is not a mining node, is still responsible for validating blocks.)

The majority of major exchanges would need to publicly support the change before it could be written into a new version of code. After that, the new software (which has an activation point in the future) gets installed on nodes that want to participate in the soft fork.

This method requires a much longer lead time to work than a hash-power-triggered soft fork. In fact, it's believed it may take as long as a year or more to write the code and get everyone ready.

Further, if the majority of miners end up not 'falling in line' and activating the new rules, they could use their overwhelming hash power to split the network.





Prior to August 2017, the bitcoin community has debated how to handle the scaling of bitcoin. During this time, most blocks hit the 1MB blocksize limit of the bitcoin blockchain. That meant higher fees, lower transaction throughput, and slow transactions. It was making bitcoin an increasingly worse payment platform and wasn't get better in the future without a major change.

There had been several attempts to solve bitcoin's scaling issue. Unfortunately, until August 2017, there's was no clear victor. This has led to the formation of multiple factions. Members of these factions believe their solution is the best way forward for bitcoin, while believing opposing factions will lead to the ruin of bitcoin.

August 1, 2017, one of those factions went live. That faction is the User Activated Soft Fork (UASF). When this happened, the bitcoin chain split into two and created a "fork".

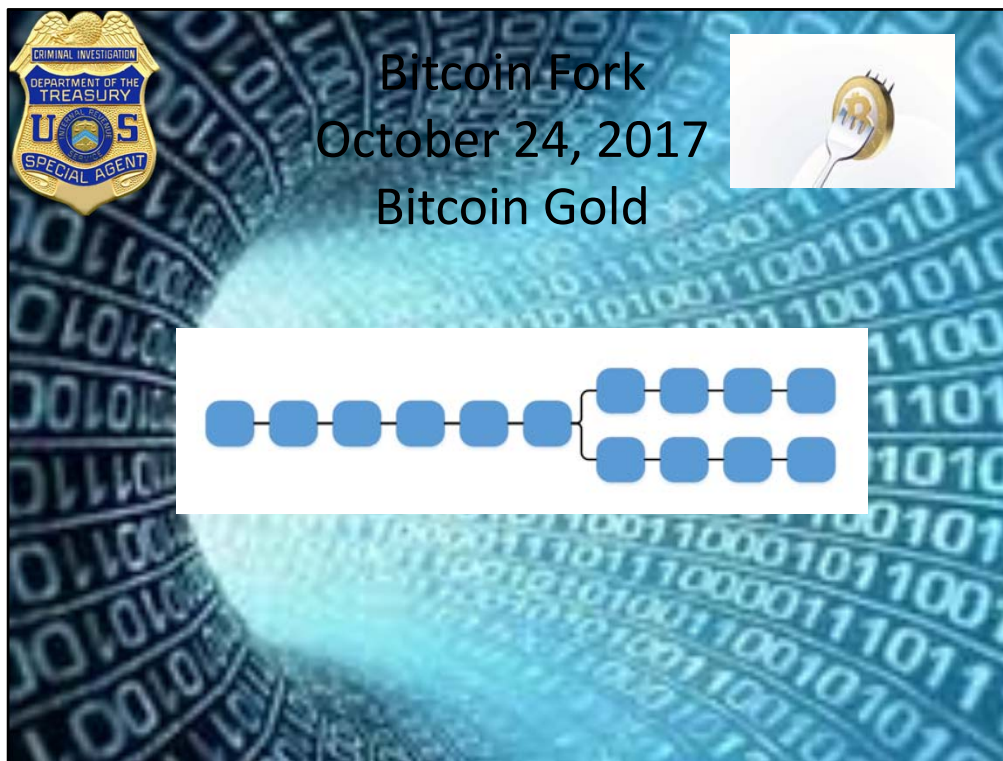
When a cryptocurrency forks, it leads to duplication. Any transactions and coins that were present prior to the fork are valid on all subsequent chains.

**On Chain Scalability** - Bitcoin Cash follows the Nakamoto roadmap of global adoption with on-chain scaling. As a first step, the blocksize limit has been made adjustable, with an increased default of 8MB.

**New Transaction Signatures** - A new SigHash type provides replay protection, improved hardware wallet security, and elimination of the quadratic hashing problem.



**New Difficulty Adjustment Algorithm (DAA)** - Responsive Proof-of-Work difficulty adjustment allows miners to migrate from the legacy Bitcoin chain as desired, while providing protection against hashrate fluctuations.



Bitcoin Gold aims to correct what its backers see as a serious flaw in the design of the original Bitcoin.

Bitcoin Gold is branding itself as a version of Bitcoin rather than merely new platforms derived from Bitcoin's source code. It has also chosen to retain Bitcoin's transaction history, which means that, if you owned bitcoins before the fork, you now own an equal amount of "gold" bitcoins.

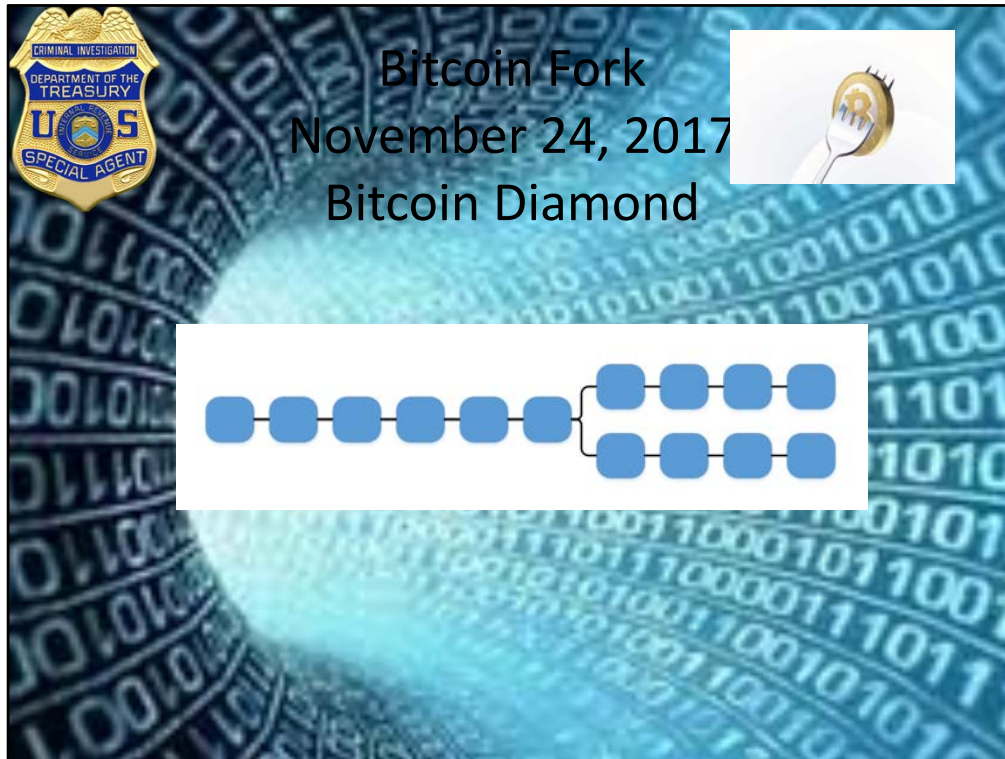
While Bitcoin Cash was designed to resolve Bitcoin's capacity crunch with larger blocks, Bitcoin Gold aims to tackle another of Bitcoin's perceived flaws: the increasing centralization of the mining industry that verifies and secures Bitcoin transactions.

The original vision for Bitcoin was that anyone would be able to participate in Bitcoin mining with their personal PCs, earning a bit of extra cash as they helped to support the network. But as Bitcoin became more valuable, people discovered that Bitcoin mining could be done much more efficiently with custom-built application-specific integrated circuits (ASICs).

As a result, Bitcoin mining became a specialized and highly concentrated industry. The leading companies in this new industry wield a disproportionate amount of power over the Bitcoin network.

Bitcoin Gold aims to dethrone these mining companies by introducing an alternative mining

algorithm that's much less susceptible to ASIC-based optimization. In theory, that will allow ordinary Bitcoin Gold users to earn extra cash with their spare computing cycles, just as people could do in the early days of Bitcoin.



Bitcoin Diamond (BCD) which probably gained the most support across exchanges before they launched. They have some code that's based on Bitcoin Core.

The main difference with Bitcoin Diamond is that they multiplied the supply by 10. If you had 1 BTC before block 495866, you now have 10 BCD. This is done by moving the decimal point rather than making the coin more divisible. That is, with Bitcoin, 100 million satoshi = 1 BTC. With Bitcoin Diamond, 10 million satoshi = 1 BCD.



# Bitcoin Forks



Name	Block Number / Date
Bitcoin Cash (BCH)	478558 / Aug 01 2017
Bitcoin Gold (BTG)	491407 / Oct 24 2017
Bitcore (BTX)	492820 / Nov 2 2017
Bitcoin Diamond (BCD)	495866 / Nov 24 2017
Bitcoin Lightning (BLG)	498553 / Dec 10 2017
Bitcoin Hot (BTH)	498848 / Dec 12 2017
United Bitcoin (UBTC)	498777 / Dec 12 2017
Super Bitcoin (SBTC)	498888 / Dec 14 2017


**Super Bitcoin (SBTC)** forked on block 498,888 December 12, 2017 and is a 1:1 fork, no special decimal point manipulation needed. The coin purportedly will have Lightning, zero-knowledge proofs and smart contracts.

**Lightning Bitcoin** forked on block 499,999 December 19, 2017 and is a 1:1 fork, The coin purportedly will have Lightning, zero-knowledge proofs and smart contracts.


**Bitcoin God** forked January 12, 2018 and is a 1:1 fork, The coin purportedly will have Lightning, zero-knowledge proofs and smart contracts.

From their website: “Bitcoin God is a completely self monitored decentralized community. The community will decide on the quantity and receivers of its tokens. The tokens mined each day will be used for charitable purposes, out of which, 17 million will be airdropped to the current holders of Bitcoins (close to the outstanding amount of BTC). The remaining 4 million will be airdropped for charitable donation. The process will be via users sharing their wallet address to our social network, and the community will vote to decide on the ratio and amount of airdrops. Bitcoin God will become the first charity platform built on a blockchain. Our goal is to fill the world with love and make the world a better place! “





## Bitcoin Forks



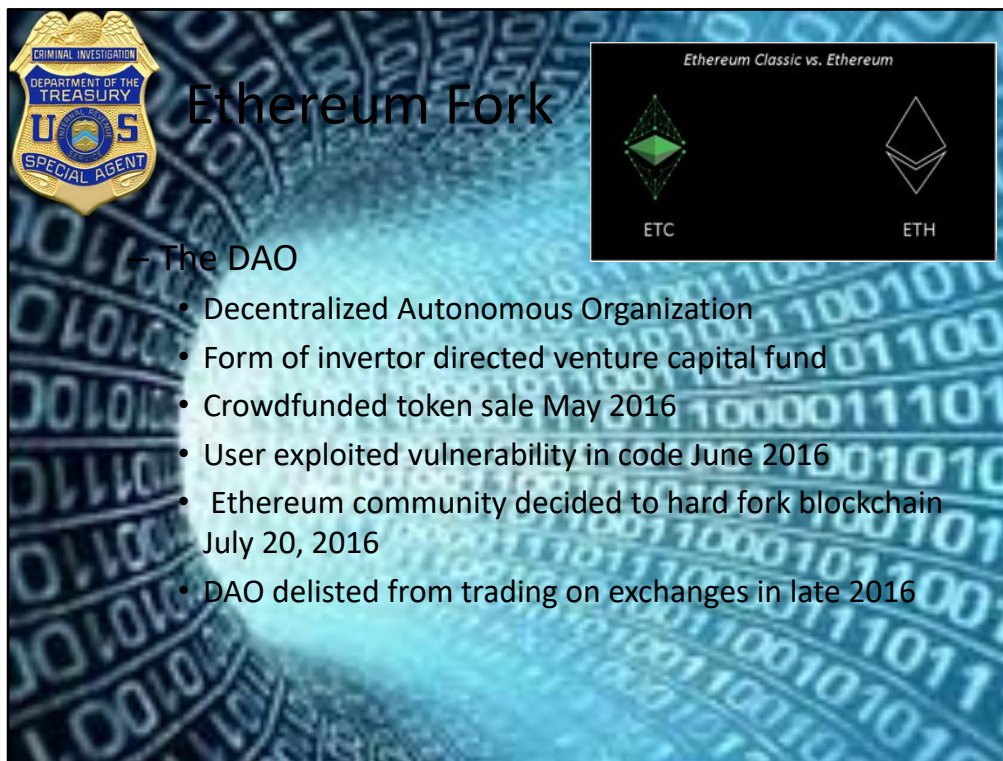
Name	Block Number / Date
BitcoinX (BCX)	498888 / Dec 14 2017
Oil Bitcoin (OBTC)	498888 / Dec 14 2017
Bitcoin Neuro (NRO)	498967
Bitcoin World (BTW)	499777
Bitcoin Faith	500000
Bitcoin God (GOD)	501225 / Dec 25 2017
Bitcoin Atom (BCA)	505888 / Jan 25 / 26
Bitcoin Uranium (BUM)	Dec 31 2017

**Super Bitcoin (SBTC)** forked on block 498,888 December 12, 2017 and is a 1:1 fork, no special decimal point manipulation needed. The coin purportedly will have Lightning, zero-knowledge proofs and smart contracts.

**Lightning Bitcoin** forked on block 499,999 December 19, 2017 and is a 1:1 fork, The coin purportedly will have Lightning, zero-knowledge proofs and smart contracts.

**Bitcoin God** forked January 12, 2018 and is a 1:1 fork, The coin purportedly will have Lightning, zero-knowledge proofs and smart contracts.

From their website: “Bitcoin God is a completely self monitored decentralized community. The community will decide on the quantity and receivers of its tokens. The tokens mined each day will be used for charitable purposes, out of which, 17 million will be airdropped to the current holders of Bitcoins (close to the outstanding amount of BTC). The remaining 4 million will be airdropped for charitable donation. The process will be via users sharing their wallet address to our social network, and the community will vote to decide on the ratio and amount of airdrops. Bitcoin God will become the first charity platform built on a blockchain. Our goal is to fill the world with love and make the world a better place! “



**Ethereum Fork**

– The DAO

- Decentralized Autonomous Organization
- Form of investor directed venture capital fund
- Crowdfunded token sale May 2016
- User exploited vulnerability in code June 2016
- Ethereum community decided to hard fork blockchain July 20, 2016
- DAO delisted from trading on exchanges in late 2016

Ethereum Classic vs. Ethereum

ETC ETH

Source: <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>

The Decentralized Autonomous Organization (known as The DAO) was meant to operate like a venture capital fund for the crypto and decentralized space. The lack of a centralized authority reduced costs and in theory provides more control and access to the investors.

At the beginning of May 2016, a few members of the Ethereum community announced the inception of The DAO, which was also known as Genesis DAO. It was built as a smart contract on the Ethereum blockchain. The coding framework was developed open source by the Slock.it team but it was deployed under "The DAO" name by members of the Ethereum community. The DAO had a creation period during which anyone was allowed to send Ether to a special wallet address in exchange for DAO tokens on a 1-100 scale. The creation period was an unforeseen success as it managed to gather 12.7 Ether (worth around \$150M at the time), making it the biggest crowdfund ever. At some point, when Ether was trading at \$20, the total Ether from The DAO was worth over \$250 million.

The DAO was a complex Smart Contract with many features and it should have allowed companies to make proposals for funding. Once a proposal was white-listed by one of the curators, the DAO token holders (aka DAO investors) would then need to vote on the proposal. If the proposal got a 20% quorum the requested funds would be released into the white-listed contractor's wallet address. The team of curators that could white-list addresses was put in place in order to avoid spam proposals and to have some human

overview over the automated process. Most of the curators were notable members of the Ethereum community.

In order to allow investors to leave the organization, in case a proposal that they saw as damaging or of poor quality was accepted, The DAO was created with an "exit door" known as the "split function". This function allowed users to revert the process and to get back the Ether they sent to the DAO. If somebody decided to split from The DAO, they would create their own "Child DAOs" and approve their proposal to send Ether to an address after a period of 28 days. You could also split with multiple DAO token holders and start accepting proposals to the new "Child DAO".

The DAO launch went smoothly and proposals were created and voted on, security issues were raised during the coming weeks, there was a big community call for a moratorium, but it was not implemented and most of the security issues were not addressed fast enough.

On the 18th of June, members of the Ethereum community noticed that funds were being drained from The DAO and the overall ETH balance of the smart contract was going down. A total of 3.6m Ether (worth around \$70M at the time) was drained by the hacker in the first few hours. The attack happened due to an exploit found in the splitting function. The attacker/s withdrew Ether from The DAO smart contract multiple times using the same DAO Tokens. This was possible due to what is known as a recursive call exploit. In this exploit, the attacker was able to "ask" the smart contract (DAO) to give the Ether back multiple times before the smart contract could update its own balance. There were two main issues that made this possible: the fact that when the DAO smart contract was created the coders did not take into account the possibility of a recursive call and the fact that the smart contract first sent the ETH funds and then updated the internal token balance.

A solution was then put up for vote, the Hard-fork which had the sole function of returning all the Ether taken from the DAO to a refund smart contract. The new contract would have only one function: withdraw. The DAO token holders can request to be sent 1 ETH for every 100 DAO. The investors that had paid more than 1 ETH for 100 DAO could request the difference from the original address. This proposal created a lot of controversy among the Ethereum community.



## Bitcoin Direct Purchase Off-Chain Transactions

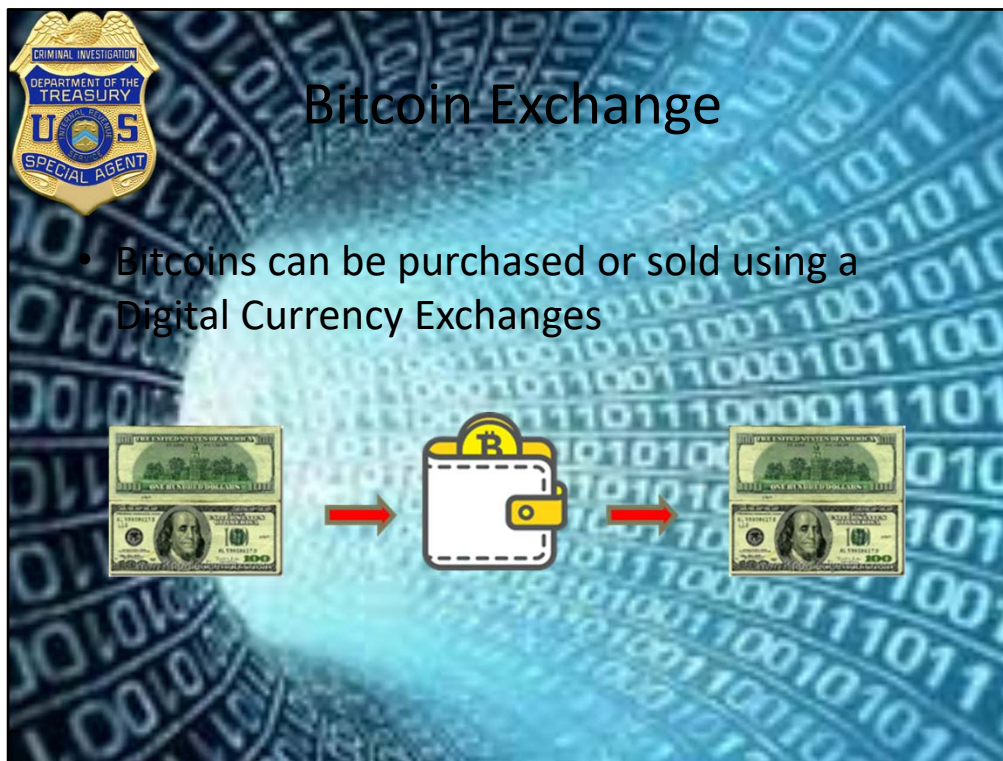
- Bitcoins can be purchased directly from another person

The concept of an off-chain transaction is relatively easy to explain. It all revolves around transferring value outside of the blockchain. Most people think Bitcoin can only be moved on-chain when transacting between different parties, but that is not entirely true. While on-chain transactions are far more common compared to their off-chain counterparts, the latter category can have its use more often than people would think.

There are quite a few different benefits to using off-chain transactions. First of all, one avoids the network transaction fee. Some users pay 10% of their transaction in fees. Another benefit of off-chain transactions is how they are much quicker. To be more specific, these transactions can be recorded immediately, without having to wait for network confirmations.

Furthermore, off-chain transactions provide more privacy and a certain degree of anonymity. These transfers do not need to be visible on the public blockchain. This is quite an interesting trait which is often associated with on-chain transactions, even though Bitcoin is not anonymous in this regard by any means.

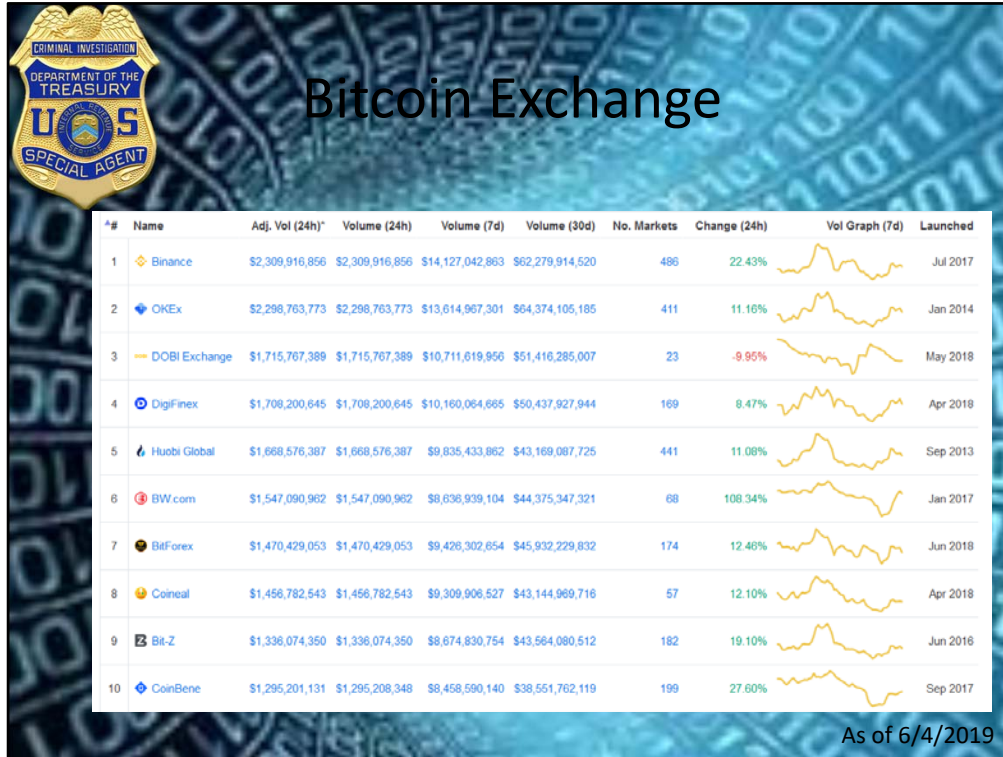




Cryptocurrency exchanges or digital currency exchanges (DCE) are businesses that allow customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or different digital currencies. They can be market makers that typically take the bid/ask spreads as transaction commissions for their services or simply charge fees as a matching platform.

DCEs may be brick-and-mortar businesses, exchanging traditional payment methods and digital currencies, or strictly online businesses, exchanging electronically transferred money and digital currencies. Most digital currency exchanges operate outside of Western countries, avoiding regulatory oversight and complicating prosecutions, but DCEs often handle Western fiat currencies, sometimes maintaining bank accounts in several countries to facilitate deposits in various national currencies. They may accept credit card payments, wire transfers, postal money orders, cryptocurrency or other forms of payment in exchange for digital currencies.





Cryptocurrency exchanges or digital currency exchanges (DCE) are businesses that allow customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or different digital currencies. They can be market makers that typically take the bid/ask spreads as transaction commissions for their services or simply charge fees as a matching platform.

**Bitcoin Exchangers**

Broker	Pay with...	Available Coins	Min Deposit
<b>BINANCE</b>	✓ NEM ✓ Cryptocurrency ✓ Cardano		£100

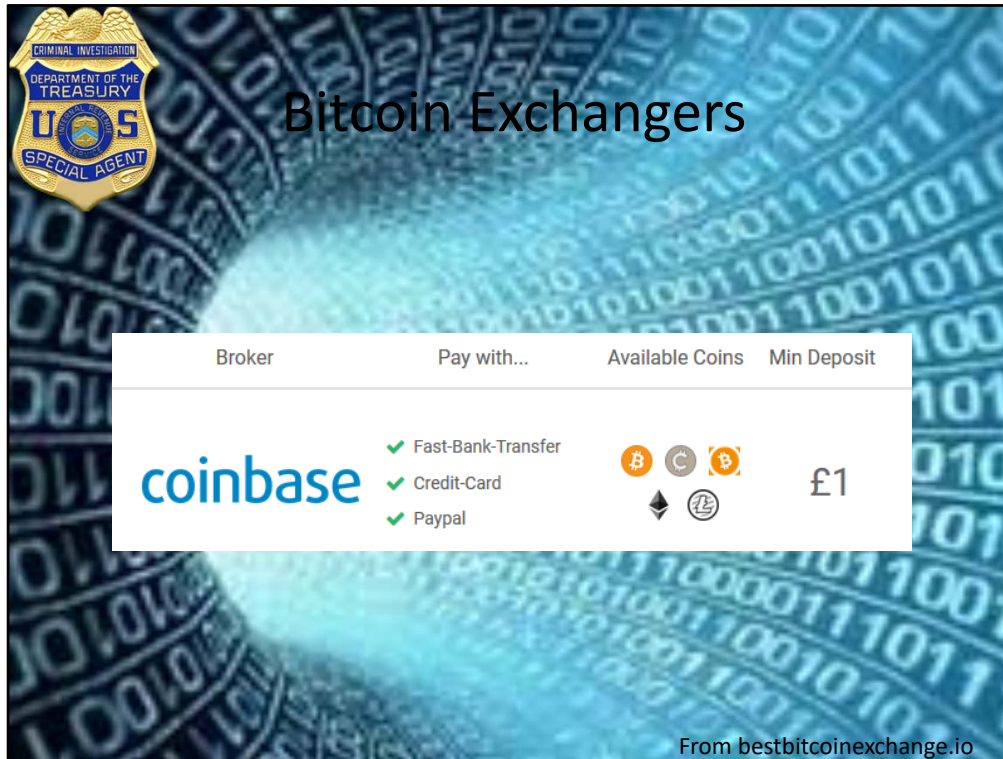
From [bestbitcoinexchange.io](http://bestbitcoinexchange.io)

**Binance** (Shibuya-ku, Tokyo) is an up and coming cryptocurrency exchange with a focus on crypto-to-crypto trading. The platform has started to gain popularity in the blockchain community thanks to its impressive coin offerings and insanely low trading fees. The company raised around \$15 million in an ICO this past July (2017) and immediately acquired 20,000 registered users as part of the raise.

Although the company was launched just a few months ago (via ICO), the exchange is already being promoted as a good alternative to Bittrex.

There are two options for trading platforms on Binance: **Basic and Advanced**.

Binance was not created for the casual investor. The main dashboard has several charts and graphs including the **order books**, a **candlestick chart**, as well as the **trade history**. There's also a depth chart of the orders that you can view in a separate tab from the candlestick chart.



Coinbase was founded in July 2011 by Brian Armstrong and Fred Ehrsam. Blockchain.info co-founder Ben Reeves was part of the original founding team but later parted ways with Armstrong due to a difference in how the Coinbase wallet should operate. The remaining founding team enrolled in the Summer 2012 Y Combinator startup incubator program. In October 2012, the company launched the services to buy and sell bitcoin through bank transfers. In May 2013, the company received a US\$5 million Series A investment led by Fred Wilson from the venture capital firm Union Square Ventures. In December 2013, the company received a US\$25 million investment, from the venture capital firms Andreessen Horowitz, Union Square Ventures (USV) and Ribbit Capital.

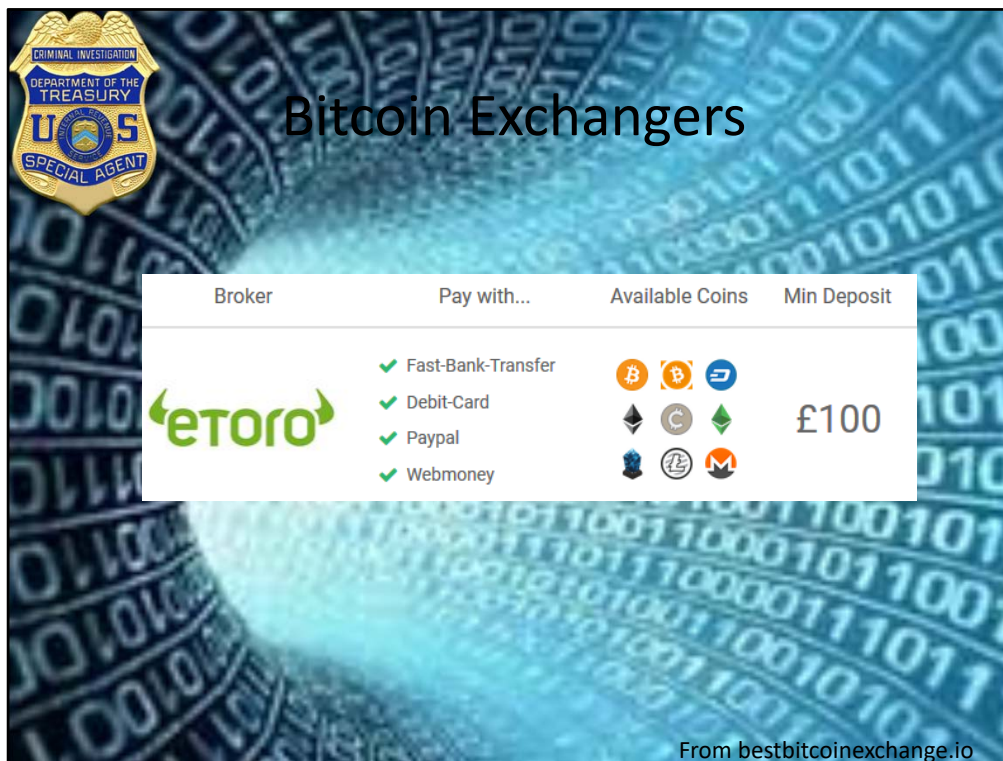
In 2014, the company grew to one million users, acquired the blockchain explorer service Blockr and the web bookmarking company Kippt, secured insurance covering the value of bitcoin stored on their servers, and launched the vault system for secure bitcoin storage. Throughout 2014, the company also formed partnerships with Overstock, Dell, Expedia, Dish Network, Time Inc. to power accepting bitcoin payments. The company also added bitcoin payment processing capabilities to the traditional payment companies Stripe, Braintree, and PayPal.

In January 2015, the company received a US\$75 million investment, led by Draper Fisher Jurvetson, the New York Stock Exchange, USAA, and several banks. Later in January, the company launched a U.S.-based bitcoin exchange for professional traders called Coinbase Exchange. Coinbase began to offer services in Canada in 2015, but in July 2016, Coinbase announced it would halt services in August after the closure of their Canadian online

payments service provider Vogogo.

In May 2016, the company rebranded the Coinbase Exchange, changing the name to Global Digital Asset Exchange (GDAX) and offering Ether, the value token of Ethereum, for trade to professionals, and in July 2016, they added retail support for Ether.

In January and then March 2017, Coinbase obtained the BitLicense and licensed to trade in Ethereum and Litecoin from the New York State Department of Financial Services (DFS).



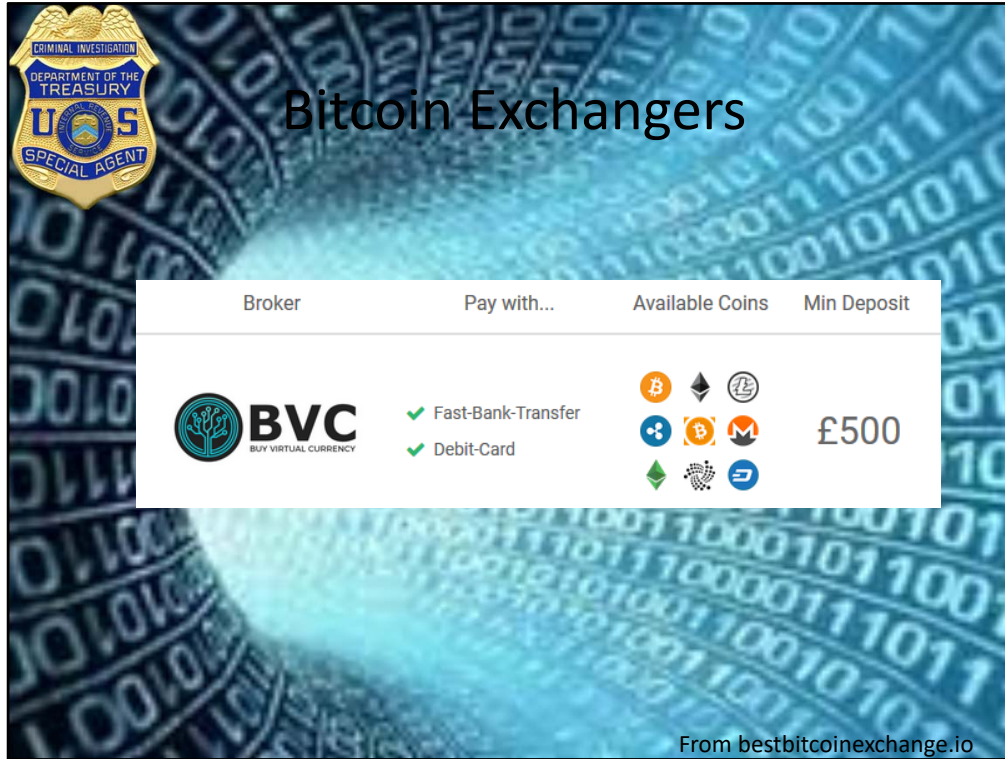
Based in Tel Aviv, Israel, eToro was founded in 2006 by two brothers, Ronen and Yoni Assia and partner David Ring. The brokerage was founded with the vision of a popular financial trading and investment platform suitable for everyone. eToro has grown significantly since its founding and is currently ranked among the top social trading networks, as well as an online forex broker.

As far as oversight and regulation is concerned, eToro (Europe) Ltd. is based in Limassol, Cyprus and is a registered Cypriot Investment Firm or CIF, registered under the number HE200585. The company is regulated by the Cyprus Securities and Exchange Commission or CySEC under license number 109/10.



In the United Kingdom, eToro (UK) Ltd. is headquartered in London and is a registered UK firm under registration number 7973792. eToro UK is authorized and regulated by the Financial Conduct Authority or FCA under the firm reference number 583263. Both eToro (UK) Ltd. and eToro (Europe) Ltd. comply and operate under the Markets in Financial Instruments Directive or MiFID.

eToro currently has more than 5 million users in over 170 countries. The company's clients have access to trade in currencies, indices, CFDs and commodities. eToro's online platform attracts thousands of new accounts every day as one of the world's premiere social investment networks.





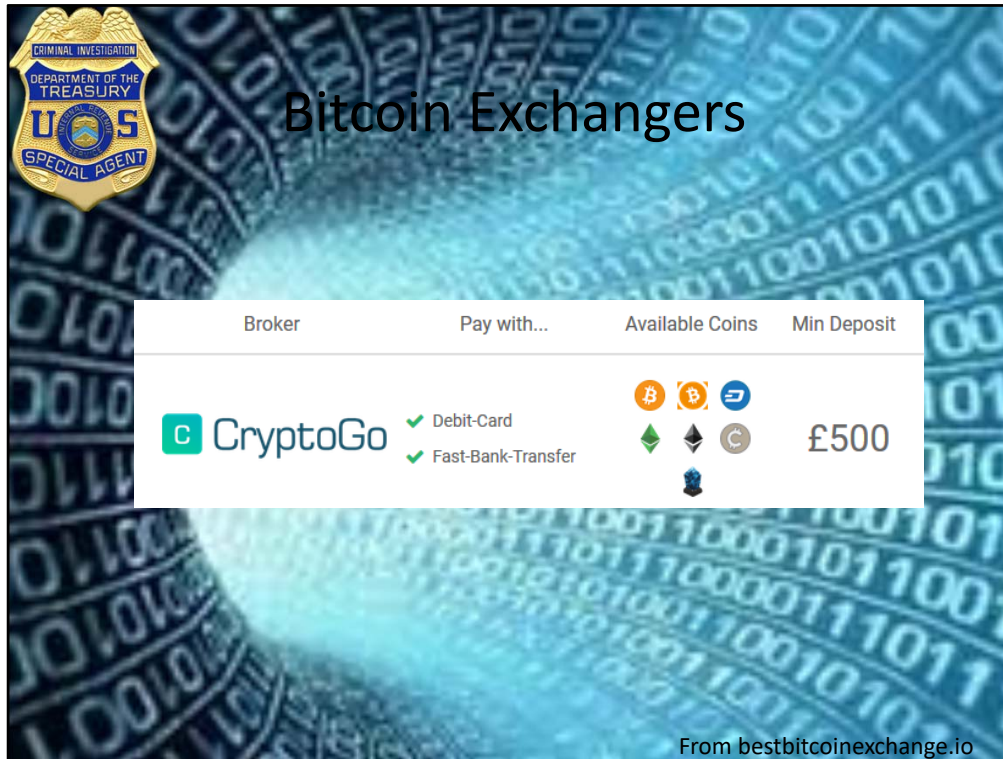
The image shows a screenshot of a website titled "Bitcoin Exchangers". In the top left corner, there is a badge for the "DEPARTMENT OF THE TREASURY U.S. COINTEGRATED SPECIAL AGENT". The background features a blue and white binary code pattern. The main content is a table with the following columns: "Broker", "Pay with...", "Available Coins", and "Min Deposit". The row for "BVC" (BUY VIRTUAL CURRENCY) shows "Fast-Bank-Transfer" and "Debit-Card" as payment methods, and a list of cryptocurrency icons including Bitcoin, Ethereum, Litecoin, Ripple, Bitcoin Cash, Monero, and Dash. The minimum deposit is listed as "£500".

Broker	Pay with...	Available Coins	Min Deposit
 <b>BVC</b> BUY VIRTUAL CURRENCY	✓ Fast-Bank-Transfer ✓ Debit-Card		£500

From [bestbitcoinexchange.io](http://bestbitcoinexchange.io)

**Buy Virtual Currency (BVC)** is a UK cryptocurrency broker

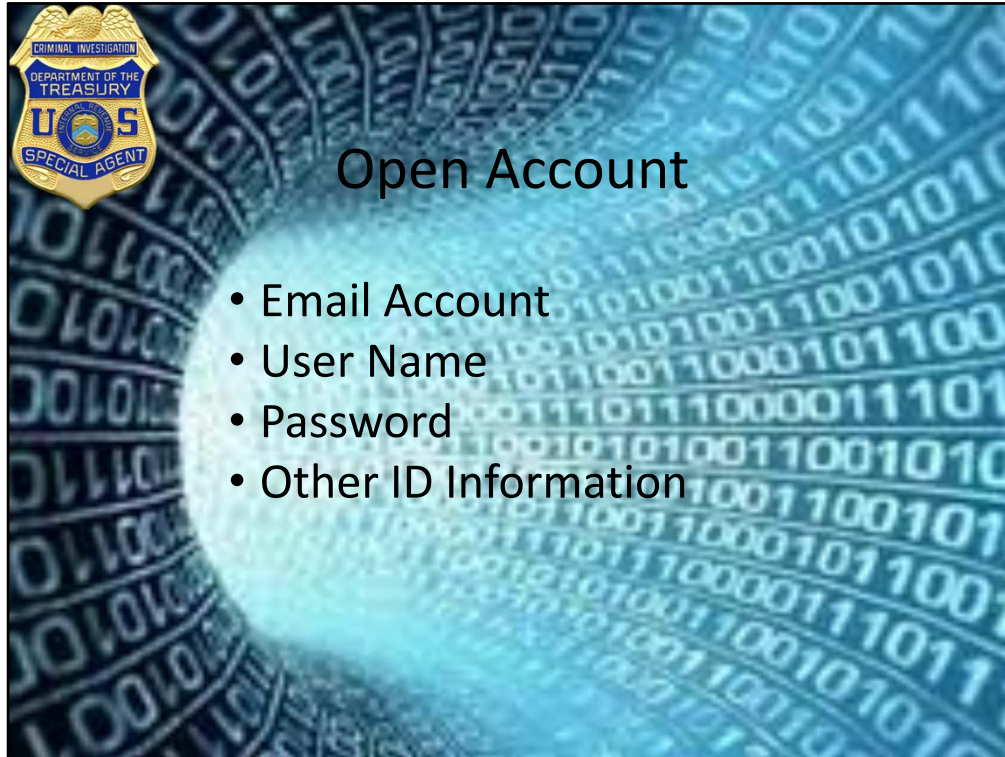
BVC performs a simple function. You send them your money, and they buy the cryptocurrencies you want with it. They take a small fee, send your new cryptocurrencies to your wallet.



**CryptoGo** is a newly developed platform that was launched for trading various cryptocurrencies by way of Fiat. The platform has a lot of different enhanced features not see on other cryptocurrencies.

*CryptoGo* started their operations very recently, so it's not exactly an exchange. The platform operates as more of a medium of sorts, but it's still ideal for people who find most of the exchanges in the industry hard to setup, navigate and manage.

It basically operates as a system that functions between the exchanges and the user. And that is why they offer a massive number of cryptocurrencies to purchase on it. You can also deposit money in several ways, like with a deposit directly from your bank or from regular fiat money, debit card, etc. The platform even accepts payments from PayPal and Neteller as well. The company is based out of London by the Investoo Group. And they are veterans when it comes to trading, investing and broking, as well as analytics.



Pretty much every person today has a PayPal account and uses it to make purchases or send and receive payments from other people. A cryptocurrency wallet provides the same functionality, but with a couple differences.

- Coinbase (a Virtual Currency Exchange) is for cryptocurrencies such as Bitcoin, Ethereum, and Litecoin and not for currencies such as USD or EUR.
- Coinbase is used as an exchange between your local currency and cryptocurrency. So if a person wanted to own Bitcoin, Ethereum or Litecoin as a investment they can simply buy the currency with USD and hold it in the wallet. If the price goes up you can then exchange your cryptocurrency back to USD for a profit.
- One of the reasons I use my cryptocurrency wallet is to have my cloud mining proceeds deposited in BTC daily. I can then exchange my proceeds to USD or leave as BTC in hopes of a price increase relative to USD.

When you go to [Coinbase.com](https://Coinbase.com) to create your wallet a screen will be presented where you can enter your first/last name, email address, and password.

Once your wallet is created there are a few steps necessary for security purposes and to link your bank account, PayPal, and/or credit/debit card so you can start exchanging your currency for Bitcoin, Ethereum, or Litecoin.

- Phone Verification
- Add Payment Accounts
- Validate Identity

Once the phone number is validated we need to link a bank account, credit/debit card, or PayPal to transfer money into and out of the Coinbase wallet.





## Bitcoin Kiosks

- First Bitcoin opened on October 29<sup>th</sup> 2013 in Vancouver, Canada
- 81 transactions took place with more than \$10,000 exchanged

A bitcoin ATM is an internet machine that allows a person to exchange bitcoins and cash. Some Bitcoin ATMs offer bi-directional functionality enabling both the purchase of Bitcoin as well as the redemption of Bitcoin for cash. In some cases, Bitcoin ATM providers require users to have an existing account to transact on the machine.

Bitcoin machines are not ATMs in the traditional sense and probably use the wording ATM as a neologism. Bitcoin kiosks are machines which are connected to the Internet, allowing the insertion of cash in exchange for bitcoins given as a paper receipt or by moving money to a public key on the blockchain. They look like traditional ATMs, but Bitcoin kiosks do not connect to a bank account and instead connect the user directly to a Bitcoin exchange. They may charge high transaction fees between 7% and 18%.





Bitcoin Kiosk operators need to adjust the limits on deposits and withdrawals according to AML/KYC standards applicable in the jurisdiction where their Kiosks are placed. In some countries / states this requires a money transmitter license. VC Kiosks are subject to the same MSB requirements, but many owners of the Kiosks have not registered with FinCEN.



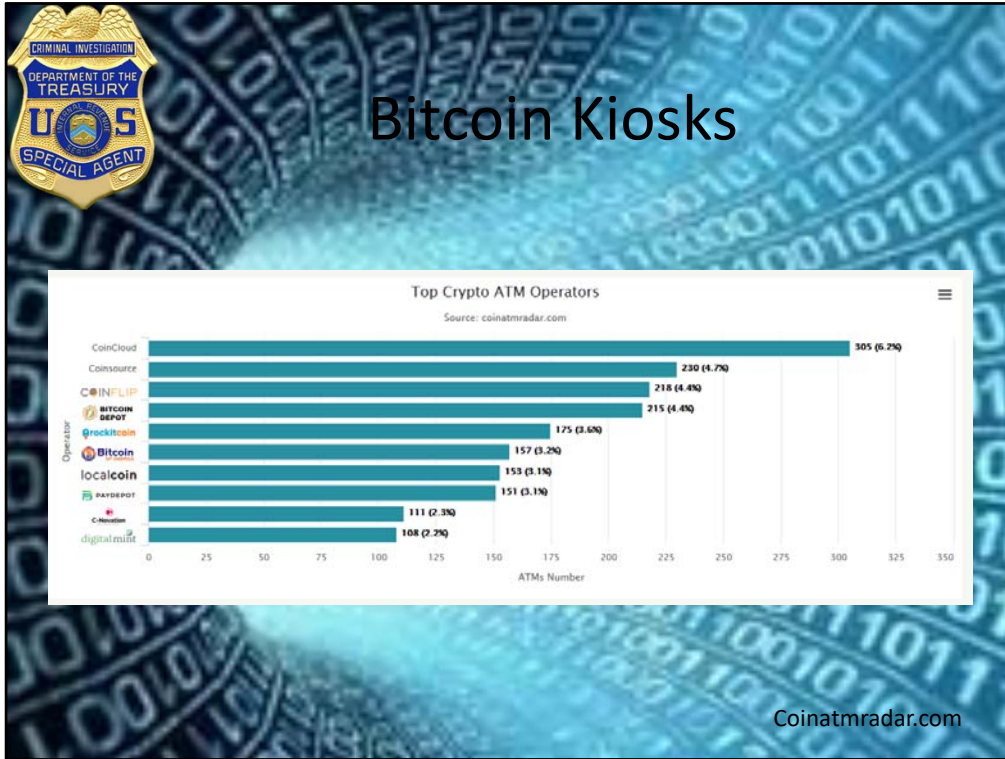
Bitcoin Kiosks are going at a rate of over 6 Kiosks a day with a total of 3800 known Kiosks around the world,



Bitcoin Kiosks are going at a rate of over 6 Kiosks a day with a total of 3800 known Kiosks around the world,



Other countries do not have the same KYC requirements as in the US and thus allows for unlimited amount of fiat currency to be converted to virtual currency. This would allow people to move money across international borders without the ability to track the source of funds



Top 10 operators run **1823 crypto ATMs (37.1%)**. There are **544 other operators**, who run **3092 Crypto ATMs (62.9%)**.







There is more to a bitcoin wallet than just the address itself. It also contains the public and private key for each of your bitcoin addresses.

**Public key** [*Like you street address*] – This is the address you would share to receive funds. The public key is used to ensure you are the owner of an address that can receive funds. The public key is also mathematically derived from your private key, but using reverse mathematics to derive the private key would take the world’s most powerful supercomputer many trillion years to crack.

**Private Key** [*Like the key to your house*] is a randomly generated string (numbers and letters), allowing bitcoins to be spent. A *private* key is always mathematically related to the bitcoin wallet address, but is impossible to reverse engineer thanks to a strong encryption code base.



## Bitcoin Wallets

- A **Bitcoin Wallet** is typically a data file that stores the digital credentials for your bitcoin holdings and allows you to access (and spend) them.

Besides these key pairs and a bitcoin wallet address, your bitcoin wallet also stores a separate log of all of your incoming and outgoing transactions. Every transaction linked to your address will be stored by the bitcoin wallet to give users an overview of their spending and receiving habits.



There are several types of wallets that provide different ways to store and access your digital currency. Wallets can be broken down into three distinct categories – software, hardware, and paper. Software wallets can be a desktop, mobile or online.

**Desktop:** wallets are downloaded and installed on a PC or laptop. They are only accessible from the single computer in which they are downloaded. Desktop wallets offer one of the highest levels of security however if your computer is hacked or gets a virus there is the possibility that you may lose all your funds.

**Online:** wallets run on the cloud and are accessible from any computing device in any location. While they are more convenient to access, online wallets store your private keys online and are controlled by a third party which makes them more vulnerable to hacking attacks and theft.

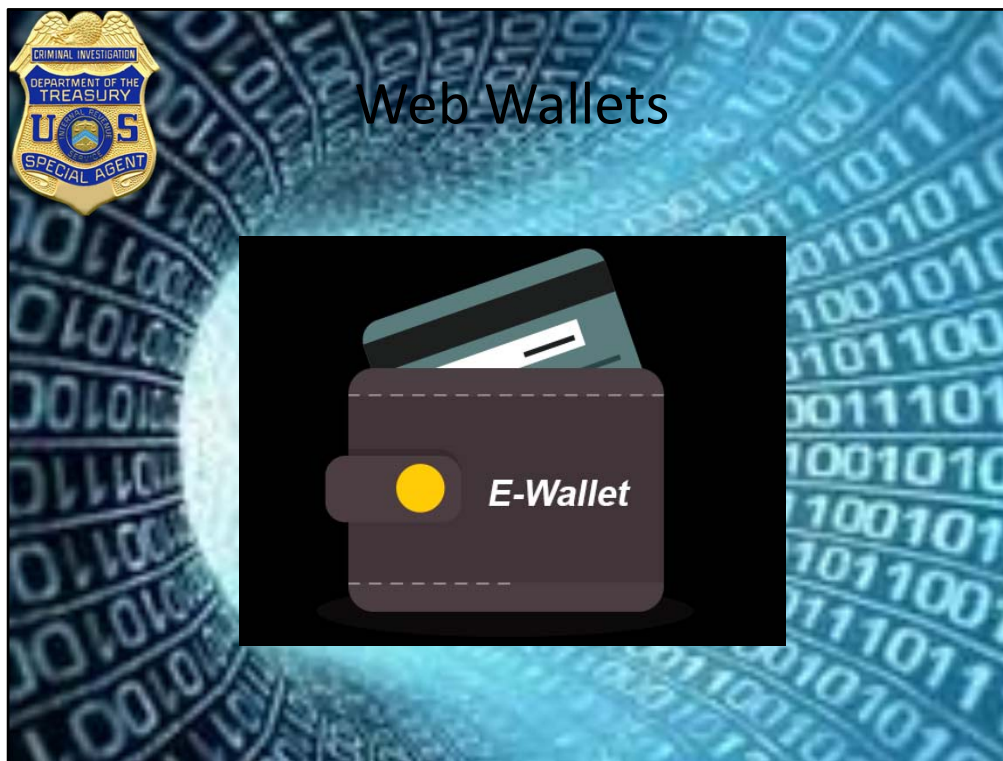
**Mobile:** wallets run on an app on your phone and are useful because they can be used anywhere including retail stores. Mobile wallets are usually much smaller and simpler than desktop wallets because of the limited space available on a mobile.

**Hardware:** wallets differ from software wallets in that they store a user's private keys on a hardware device like a USB. Although hardware wallets make transactions online, they are stored offline which delivers increased security.

**Paper:** wallets are easy to use and provide a very high level of security. While the term

paper wallet can simply refer to a physical copy or printout of your public and private keys, it can also refer to a piece of software that is used to securely generate a pair of keys which are then printed.





Online wallets are typically cryptocurrency wallets that you access via your web browser. In some cases people refer to all hot wallets as online wallets, but that only gets confusing when we start to discuss individual platforms that your wallet resides on, such as mobile or desktop wallets. Do not put the bulk of your crypto onto these wallets –trust me.

**Advantages:**

- Fastest way to complete transactions (no lag between locations of app and server)
- Ideal for holding small amounts of cryptocurrency
- Some are able to manage multiple cryptocurrencies, transfer amounts between them, or be directly integrated into an exchange
- TOR network can be used for more privacy

**Disadvantages:**

- Users are susceptible to phishing scams, malware, insider hacking, DDOS attacks, and outdated security measures
- Your wallet is “out of your hands” and coin information is stored on a third-party
- Your computer is open to malware, keyloggers, and viruses (never use an internet café, never view porn, keep your software updated, get Avira or AVG and MalwareBytes, read [org](#) and keep up with the latest geek news).

**Examples:** Exchanges like Bittrex or QuadrigaCX, and online wallets like Coins.ph and GreenAddress.



Mobile wallets provide access to your cryptocurrencies wherever you are with your mobile device and provide additional features above and beyond wallets that are completely internet-based, however they also come with additional security risks.

**Advantages:**

- More practical and easier to use than other crypto wallet types, great to accept or send payments on the fly
- Additional features above and beyond both online and hardware wallets like QR code scanning
- TOR network can be used for more privacy

**Disadvantages:**

- Phones are incredibly insecure devices –nothing will save your crypto if your phone has been maliciously compromised or rooted, not even wallet app encryption
- Your phone is open to malware, keyloggers, and viruses

**Examples:** Jaxx, BreadWallet, Mycelium, and CoPay.



A desktop cryptocurrency wallet is considered somewhat more secure than both an online (web) wallet and mobile wallet, however that depends on your commitment to online security.

In cases where you use an older laptop, completely offline, on a clean operating system install –you could consider this a really effective cold storage method. Like phones, most people have an older laptop floating around and this could be a great use for it.

**Advantages:**

- Incredibly easy to use crypto wallet type
- If “never been kissed” by an internet connection this is a great cold storage solution
- Private keys not stored on a third-party server
- TOR network can be used for more privacy

**Disadvantages:**

- If connected to the internet there are security and privacy caveats
- Computer repair people! If you rely on the Nerd Squad, they could make away with your coins
- If you forget to back it up and your computer dies, you are out of luck
- Your computer is open to malware, keyloggers, and viruses
- Some wallets ask for really strange privacy permissions (security certificates)

**Examples:** Exodus, Multibit, Armory, and Bitcoin Core.

### **Best Laptop for Crypto Cold Storage**

It's common to get a standalone, air-gapped (not connected to the internet) laptop for crypto cold storage –a laptop that you don't use for anything else *but* a crypto wallet, or lightweight crypto mining rig.

The best laptop store crypto will have a supported, secure operating system such as Ubuntu, Mac OS (albeit far too pricey for a crypto laptop if you ask me), or Chrome OS (Chromebook), Android and be generally inexpensive.

Using a new, separate laptop for a crypto wallet will probably mean you don't need the most powerful specs –just something that is durable and can do the job.





Hardware wallets are slightly less user-friendly cryptocurrency wallets than web wallets and desktop wallets, but they're easier to work with than paper wallets and more secure than hot wallets (most of the time).

Some require batteries, some don't. Some have screens which mean you don't need an insecure computer to back up your private keys, some don't. Some handle hard forks better than others (Trezor had a short-lived issue during the BCH fork, Ledger Nano had no issues –any issue during a hard fork can be an emotional rollercoaster), and they all are often sold out, so snatch one up while you can if they're available.

They are great for storing large amounts of cryptocurrency you don't need to move around often, and they offer more control.

Advantages:

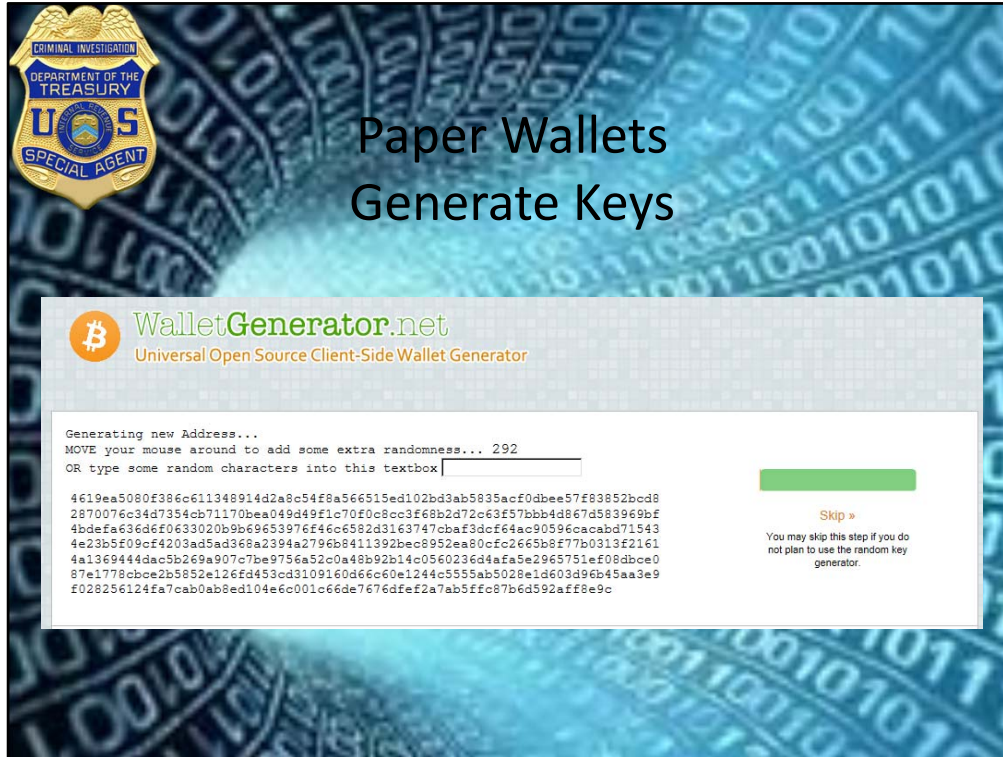
- If it has a screen, it's the most secure way to store crypto long-term
- Stronger security than all other wallets, for the most part

Disadvantages:

- Cumbersome for some beginners to use, but an absolute must for large quantities of cryptocurrencies
- Often sold out, Amazon is your best bet



Examples: We recommend any product by Ledger, although Trezor and KeepKey are really great solutions (fanboys exist on all sides for their own valid reasons, do your research, read their reviews).



**Paper:** wallets are easy to use and provide a very high level of security. While the term paper wallet can simply refer to a physical copy or printout of your public and private keys, it can also refer to a piece of software that is used to securely generate a pair of keys which are then printed. Using a paper wallet is relatively straightforward. Transferring Bitcoin or any other currency to your paper wallet is accomplished by the transfer of funds from your software wallet to the public address shown on your paper wallet. Alternatively, if you want to withdraw or spend currency, all you need to do is transfer funds from your paper wallet to your software wallet. This process, often referred to as 'sweeping,' can either be done manually by entering your private keys or by scanning the QR code on the paper wallet.

Following slides show how to generate the public and private keys to create a paper wallet

Before hardware wallets, paper wallets were the defacto standard for cold storage of cryptocurrencies. There are paper wallets and then there are *secure* paper wallets.

**Advantages:**

- One of the most hacker-proof crypto wallet choices
- Not stored on a computer
- Private keys not stored on a third party server

**Disadvantages:**

- More effort required to move cryptocurrencies around
- More technical understand required

**Examples:** BitAddress.org and Bitcoin Armory can help you create and print your paper wallet.

**CRIMINAL INVESTIGATION**  
**DEPARTMENT OF THE TREASURY**  
**U.S.**  
**SPECIAL AGENT**

## Paper Wallets Generate Keys

**WalletGenerator.net**  
Universal Open Source Client-Side Wallet Generator

Generating new Address...  
MOVE your mouse around to add some extra randomness... 164  
OR type some random characters into this textbox

```
fc3cb5ff6d0c9686858781c94f5e479b48666100daelac1e7b53595c9514a2c0a5c61fc2e5  
e3879319b1406a08d0965838555487f58d8cb2bb9742bce4eaf51299915dd8d9d6d7f01042  
ac694eca06099374e0ba6051bdb2dd6b8f609210a1f6e4c25294e69dc60b492fbeca104f9d9  
f312641a59797743306ff8de4937160b59ca6c3ea88af64022b67fce41a4f69928440alb08  
ecf73b43e3027227d9934ef83f01e64ece4b1525943bcd0d8b709eea064a743c60c9d65a4  
d59933eed569d5771b9400d31dd89efad895d411b2d7641514d405da3a9a2547de3f6f4f  
54bf40f56154ffee27c1cbf0222d84815115c8c0bdacd2f9380be7465a4611a0a3d
```

[Skip »](#)

You may skip this step if you do not plan to use the random key generator.

Slide show how to generate the public and private keys to create a paper wallet.

**CRIMINAL INVESTIGATION**  
**DEPARTMENT OF THE TREASURY**  
**U.S. SPECIAL AGENT**

## Paper Wallets Generate Keys

**WalletGenerator.net**  
Universal Open Source Client-Side Wallet Generator

Generating new Address...  
MOVE your mouse around to add some extra randomness... 52  
OR type some random characters into this textbox

```
021ee3553a6af5ff6cd14951fd345394ab12d08052612f9ced6824b4f5280907846928103  
cbda5261e032ab956e86047932111986df9594c@d58187f7c74cccc99b2adaaf1a20e947c4  
c366fd22cb40a35de6df0b445de04073f7107f4c9a4217b20f47f142e7a966ace645463  
40780b3038c2477d5fbbd66ad3e579055e31cc6d8c7a62b6c851810e507fd2df462cbbf32d  
f699a04af5955b4973b282e2fd6f9710a43c824b573f9e3878d9abd386e77aed340ee33f8  
097fda8a8602baed1b377afe475819bd1dae0ada482bae061ad72ealfadec95b7997ea834  
121d2b0a1f909fcdfla502fe9452f7e6d90ec3379963da3ba8fcl7cfbdb509d78e87
```

**Skip »**

You may skip this step if you do not plan to use the random key generator.

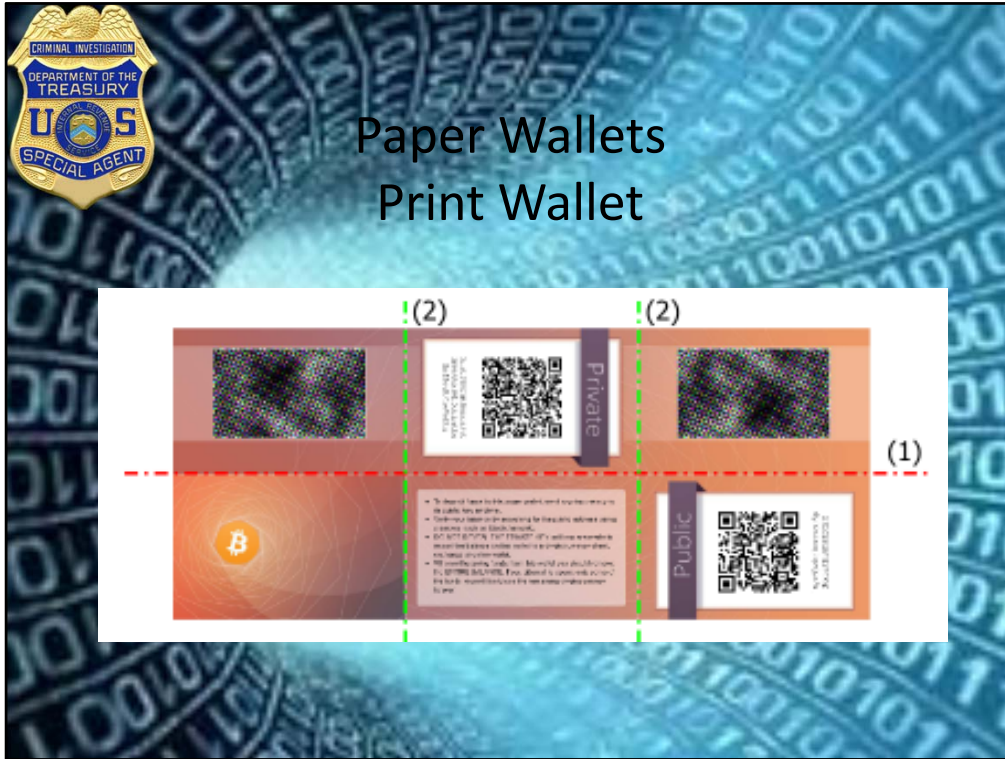
Slide show how to generate the public and private keys to create a paper wallet.



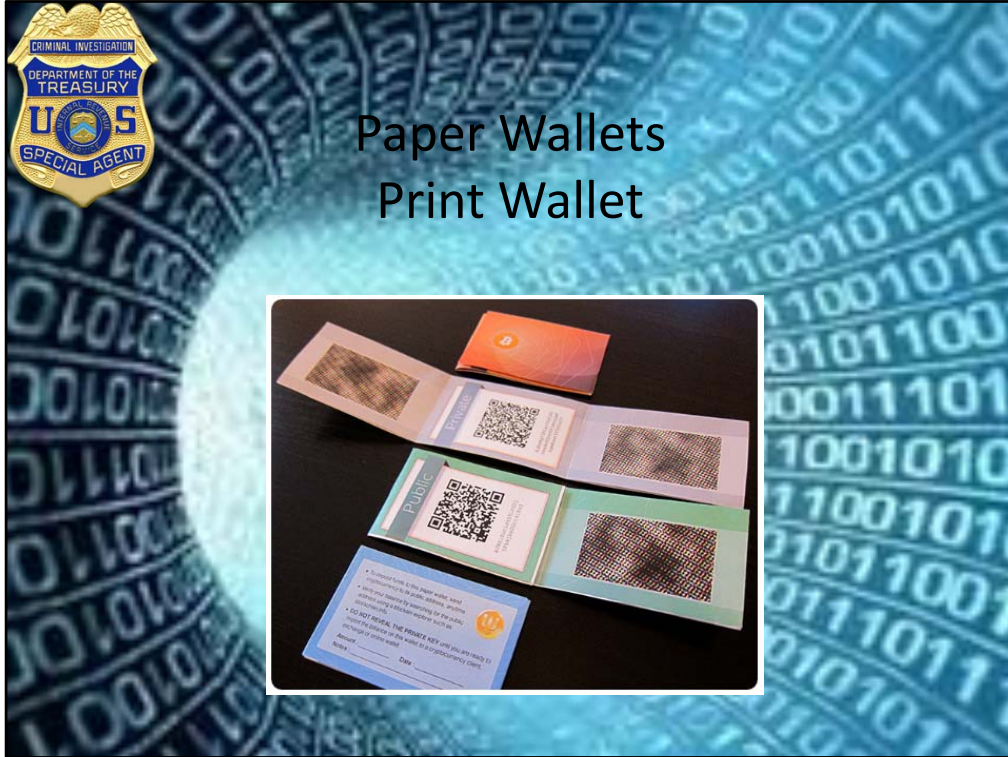



Slide show how to generate the public and private keys to create a paper wallet.

Select the currency type



Print wallet

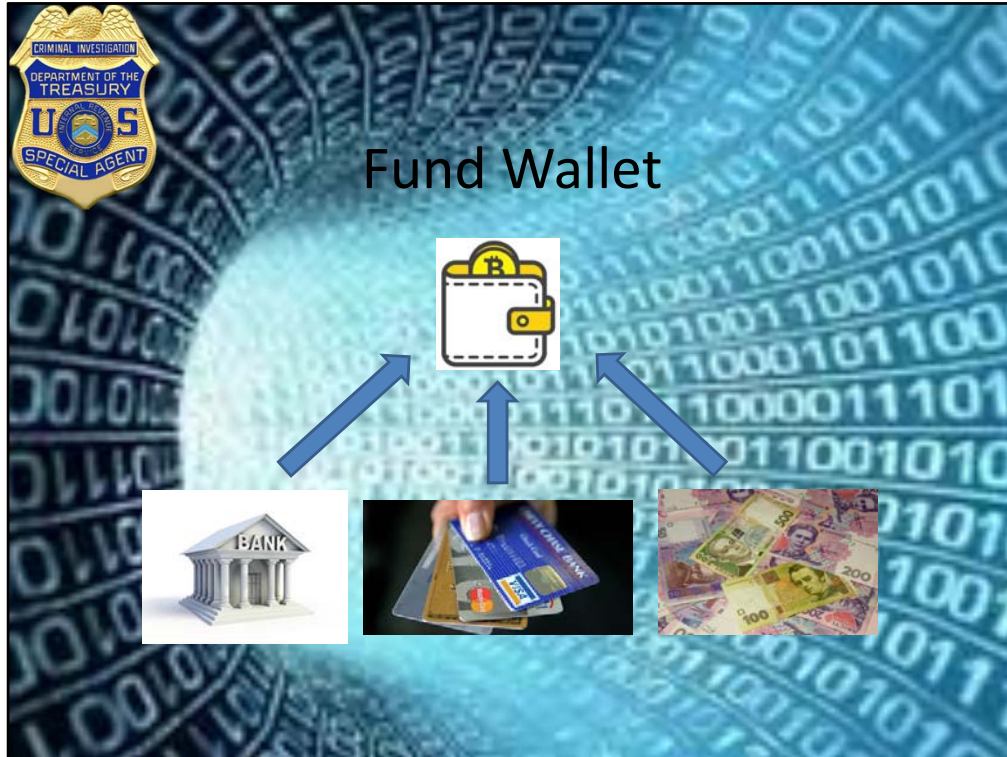




## Paper Wallets Security Concerns

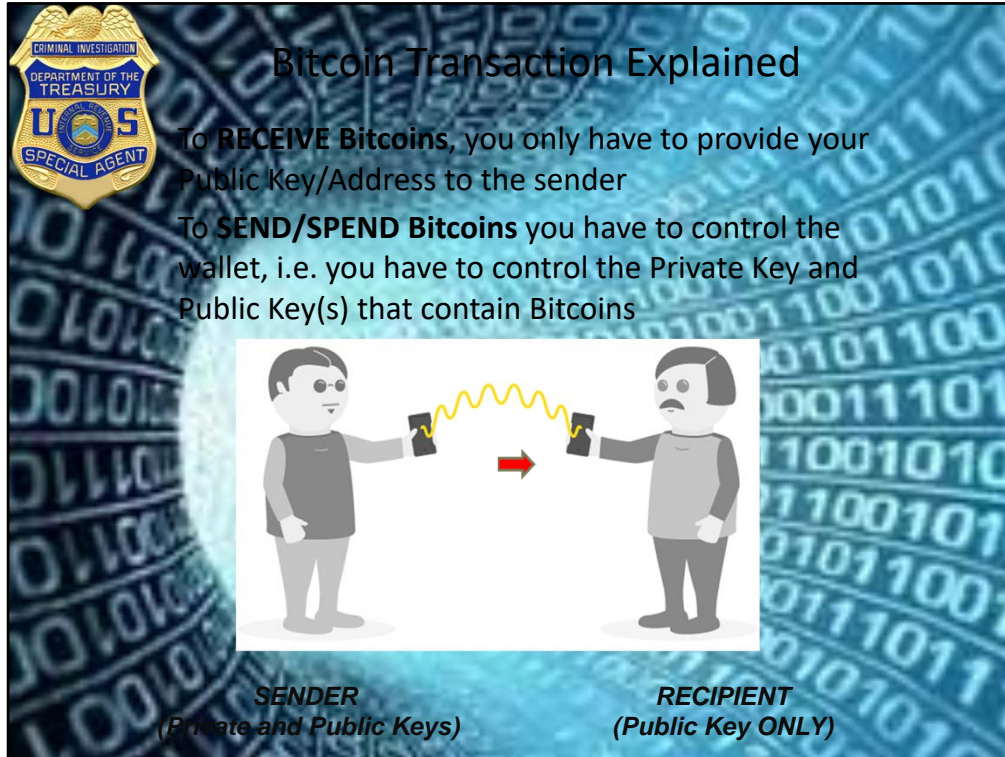
- **Download** this website from [Github](#) and open the index.html file directly from your computer.
- For extra security, **unplug your Internet access** while generating your wallet.





Wallets can be funded using the linked bank accounts, pay pal accounts, or ATMs. They can also be funded by receiving funds from others.

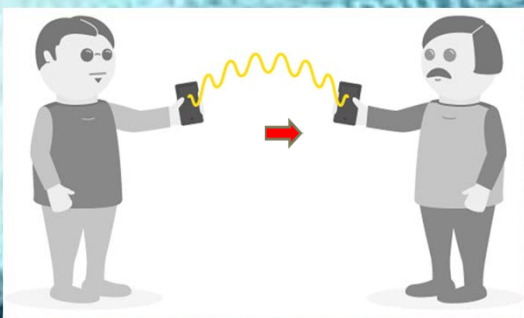




**Bitcoin Transaction Explained**

To **RECEIVE** Bitcoins, you only have to provide your Public Key/Address to the sender

To **SEND/SPEND** Bitcoins you have to control the wallet, i.e. you have to control the Private Key and Public Key(s) that contain Bitcoins



**SENDER**  
(Private and Public Keys)

**RECIPIENT**  
(Public Key ONLY)

Public Key is like an acct #  
Private Key is like a password

**WHO ACCEPTS BITCOIN?**

Approximately 60,000 to 80,000 businesses, including:

PayPal, Dell, Amazon, Tesla, Virgin Galactic, TigerDirect.com, Expedia, Overstock, Dish

Many large companies are accepting bitcoins as a legitimate source of funds. They allow their online products to be bought with bitcoins. With the extreme facilitation of transfer and earning of bitcoins, it would be a mistake not to accept these new-found online coins as cash. With a fluctuating value, the funds can either help or hurt the company.



digital currency exchanges can send cryptocurrency to your personal cryptocurrency wallet. Many can convert digital currency balances into anonymous prepaid cards which can be used to withdraw funds from ATMs worldwide.



## Why Use Bitcoins?

- Fast – can be instantaneous if there are zero-confirmation transactions or about 10 minutes.
- It's cheap for consumers and merchants
- There are no chargebacks
- People can't steal your payment information from merchants (need both keys)
- It isn't inflationary
- Anonymity

Fast – can be instantaneous if there are zero-confirmation transactions or about 10 minutes.

It's cheap for consumers and merchants

There are no chargebacks

People can't steal your payment information from merchants (need both keys)

It isn't inflationary

Anonymity





## Why Use Bitcoins?

- You own the private key and the corresponding public key
- You can create your own money by mining it
- Can be used worldwide with no currency conversion rates
- Completely mobile

You own the private key and the corresponding public key  
You can create your own money by mining it  
Can be used worldwide with no currency conversion rates  
Completely mobile





## Tumbling/Mixing Bitcoins

**BITCOIN TUMBLING (MIXING) SERVICES**

**TRUSTED BITCOIN MIXERS:**

- Helix**  
Helix by Grams  
Short Link: [drk.li/Helix](https://drk.li/Helix)
- Bitcoin Blender**  
Bitcoin Blender  
Short Link: [drk.li/Blender](https://drk.li/Blender)

**OTHER BITCOIN MIXERS:**

- BitMixer.io**  
Short Link: [drk.li/BitMixer](https://drk.li/BitMixer)
- Bitcoin Fog**  
Short Link: [drk.li/Fog](https://drk.li/Fog)
- Pay Shield**  
Short Link: [drk.li/Payshield](https://drk.li/Payshield)

Cryptocurrency tumbler or cryptocurrency mixing service is a service offered to mix potentially identifiable or 'tainted' cryptocurrency funds with others, so as to obscure the trail back to the fund's original source. Tumblers have arisen to improve the anonymity of cryptocurrencies, usually bitcoin (hence Bitcoin mixer), since the currencies provide a public ledger of all transactions.

In traditional financial systems, the equivalent would be moving funds through banks located in countries with strict bank secrecy laws, such the Cayman Islands, the Bahamas, or Panama. Tumblers take a percentage transaction fee of the total coins mixed to turn a profit, typically 1-3%. Mixing helps protect privacy and can also be used for money laundering by mixing illegally obtained funds.



Bitmixer.io website – now currently closed



## Tumbling/Mixing Bitcoins




### Why should I mix my coins?

While using bitcoins is an excellent way to make your purchases, donations, and p2p payments, without losing money through inflated transaction fees, transactions are never truly anonymous. Bitcoin activities are recorded and available publicly via the blockchain; a comprehensive database which keeps a record of bitcoin transactions.

All exchanges require the user to scan ID documents, and large transactions must be reported to the proper governmental authority. When you use Bitcoin to pay for goods and services, you will of course need to provide your name and address to the seller for delivery purposes.

This means that a third party with an interest in tracking your activities can use your visible balance and ID information as a basis from which to track your future transactions or to study previous activity. In short, you have compromised your security and privacy.

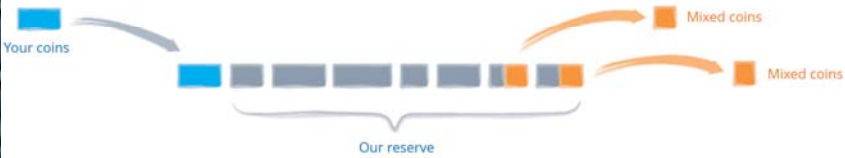
To avoid this, we recommend using a quality mixing service such as the one we provide to periodically exchange your bitcoins for different ones which cannot be associated with the original owner. In order to further enhance the security of your transactions we provide the opportunity to use two or more forward addresses as well as convenient time delays. In addition, we immediately delete all archival logs related to your transactions.




# Tumbling/Mixing Bitcoins

## How does it work?

All of this may seem super complicated, so let's get down to the meat and bone of it. BitMixer has a huge reserve of Bitcoins already in its system. A user sends us their BTC and we cap it onto the end of our reserve chain. We then pay the amount of what was purchased from the beginning of our reserve.




This method of mixing means that you do not have to wait for other customers - coins already mixed are instantly available.



# Tumbling/Mixing Bitcoins

## Using bitmixer code

The problem with this is that the user's coins may still be in our reserve. Meaning, on the second transaction, there could be a possibility of the user receiving the same BTC s/he had originally had. This is why we created a generator referred to as "bitcode."




Using the BitMixer code means that a user's previous coins will not be used in further mixing operations. Our problem is solved – every user continues to remain anonymous and private.





# Tumbling/Mixing Bitcoins



## Fees

Our minimum fee is 0.5% plus 0.001 BTC for every forward address.

We recommend to set higher custom fee to prevent advanced amount-based blockchain analysis.

### Why should I set custom fee?

If attacker knows service fee, he can analyse blockchain to find exact sum transferred and discover your destination account.

For example if you send 100 BTC with a fixed fee 0.5% + 0.0005 BTC, you should receive 99.4995 BTC. It is not so difficult to check blockchain after 24 hours and find all exact transactions. Even if you use several forward addresses it is quite easy. That is why we strongly recommend to set custom fee, combined with several forward addresses and time delay.

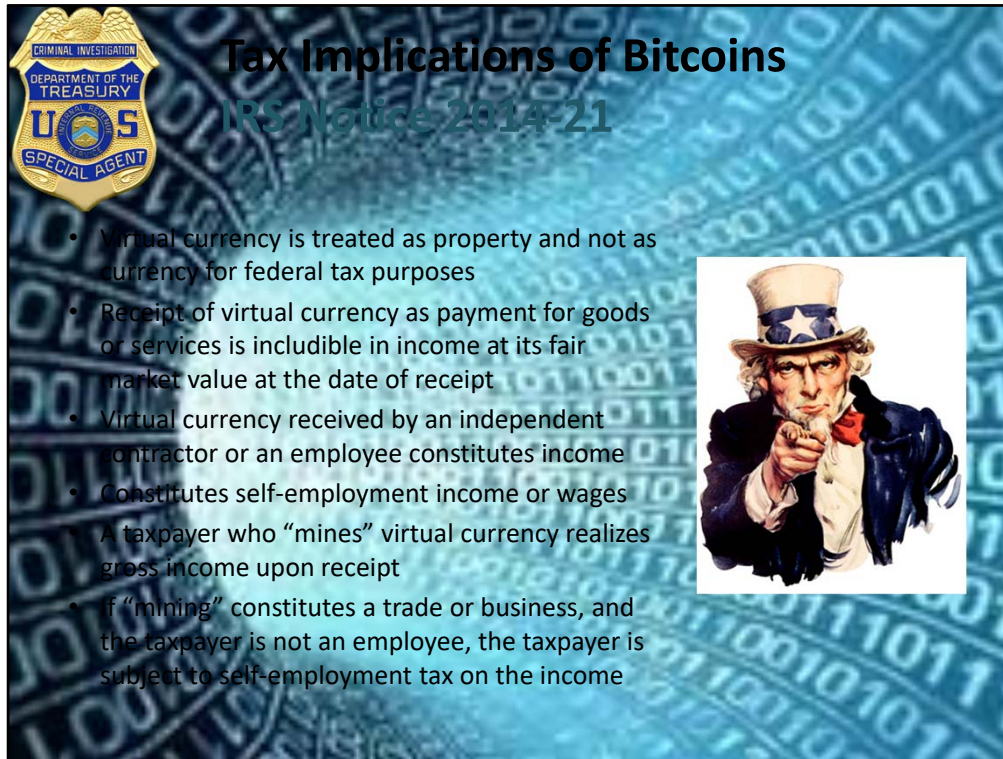


## Tumbling/Mixing Bitcoins

- Bitmixer.io closed operations in July 2017
  - Owner originally believed bitcoin should be private
  - Changed his mind and now believes the bitcoin blockchain should be public
  - Owner stated “You may use Dash or Zerocoin if you want to buy some weed. Not Bitcoin”

Bitmixer.io was one of the most popular bitcoin mixing and tumbling services on the web and caters to large volumes of BTC. The service has been operating since 2014, and the platform was processing 65,000 BTC per month according to the operator of the site. Bitmixer provided digitally signed proof of every order and offered instant mixing with a big reserve. In addition to Bitmixer’s website on clearnet, the operation also had an official Tor mirror as well on the deep web. For over three years the tumbling service operated for those who wanted to mix quantities of bitcoins. Then on July 24, the sites operator announced, “the largest bitcoin mixer is about to stop working.”

“Despite the huge profit we earn, we are closing our activity,” explains Bitmixer. “Let me explain why. I’m bitcoin enthusiast since 2011. When we started this service, I was convinced that any Bitcoin user has a natural right to privacy. I was totally wrong. Now I grasp that Bitcoin is a transparent non-anonymous system by design. Blockchain is a great open book.”



## Tax Implications of Bitcoins

### IRS Notice 2014-21

- Virtual currency is treated as property and not as currency for federal tax purposes
- Receipt of virtual currency as payment for goods or services is includible in income at its fair market value at the date of receipt
- Virtual currency received by an independent contractor or an employee constitutes income
- Constitutes self-employment income or wages
- A taxpayer who “mines” virtual currency realizes gross income upon receipt
- If “mining” constitutes a trade or business, and the taxpayer is not an employee, the taxpayer is subject to self-employment tax on the income

- Virtual currency is treated as property and not as currency for federal tax purposes
- Receipt of virtual currency as payment for goods or services is includible in income at its fair market value at the date of receipt
- Virtual currency received by an independent contractor or an employee constitutes income
- Constitutes self-employment income or wages
- A taxpayer who “mines” virtual currency realizes gross income upon receipt
- If “mining” constitutes a trade or business, and the taxpayer is not an employee, the taxpayer is subject to self-employment tax on the income





The determination of whether or not a Subject transacts in or maintains a balance of bitcoins can be accomplished by several methods, such as interviews, Open Source searches, and electronic surveillance. However, one method that should be considered is serving Grand Jury Subpoenas to a variety of companies. Issuance of a Grand Jury Subpoena should be considered for Apple, Google, and Microsoft for the Subject's complete application download history. Each application's function should be explored to determine whether or not the application can transmit, or otherwise allow, transactions in bitcoin. If it is determined that an application was downloaded by the Subject that allows for the storage or transmission of bitcoins, it should be determined if the application only allows for P2P or P2B transactions or if it allows for the exchange of bitcoins via P2B2P transactions.

Such as those who know the financial habits of the Subject, including, but not limited to, bank tellers, family and friends of the Subject (if feasible), and establishments the Subject frequents that may accept bitcoins.

Facebook, Twitter, and other social media outlets.

Notification of the Subject about the obtainment of information regarding their use of bitcoin may be detrimental to the seizure of any bitcoin balance.

This can be accomplished via a simple Google search for the application.

Several companies offer services in which a user can back-up their Bitcoin Wallet online so that a secure backup with a 3<sup>rd</sup> party of all of the user's Bitcoin Addresses and Private Keys exists.

Such as a Bitcoin Address generator application.  
Such as the Mt.Gox, CoinLab, or Gyft applications.





A Grand Jury Subpoena should also be considered for (and may already have been obtained during the normal course of the investigation) the Subject's financial accounts, including, but not limited to, the Subject's bank, credit card, and PayPal records. In the Subject's bank and credit card accounts, ACHs and wire transfers should be identified to see if any of them are related to bitcoin or other TPEs. Transfers to and from a Subject's PayPal account should be analyzed in much the same way, verifying the parties involved with each transactions. Once again, a determination should be made, if a TPE is discovered, as to whether the party exchanged with only allows for P2P or P2B transactions or if it allows for the exchange of bitcoins via P2B2P transactions.

Vendors who accept bitcoin, such as Amazon Payments, can also be considered for subpoena. However, this method may not reliably yield results.

Automated Clearing House

Again, this can be accomplished via a Google search for the ACH name or ID number, or by contacting the bank.




If it is identified that the Subject does maintain a bitcoin balance, an attempt should be made to identify the Subject's Bitcoin Wallet and associated Bitcoin Addresses, as well as the balance for each Bitcoin Address. The number of Bitcoin Addresses for the user may be numerous. If the Subject does not appear to use a TPE, the obtainment of the Bitcoin Addresses and Private Keys may be quite difficult, as the Subject's Bitcoin Wallet may only exist locally, such as on their cellular phone. However, the Subject's Bitcoin Addresses may be publicly available and tied to the Subject, such as through posts by the Subject on his Facebook page or Twitter account.

If it is learned that the Subject utilizes a specific TPE or online Bitcoin Wallet service, a subpoena for records could be issued to the company to identify the Subject's bitcoin balance, Bitcoin Addresses, and any identifying information. Additionally, the TPE may be able to provide any linked financial accounts, login times and information, correspondence, and transaction details.

The reliability of this method, both in record retention and non-notification of the customer, has yet to be extensively tested. As such, it may not be advised to send a Subpoena for records if not critically necessary.

# Bitcoin Transactions



**Latest Blocks**

Height	Age	Transactions	Mined by	Size
476870	8 minutes ago	2378	AntMiner	998161
476869	32 minutes ago	1863		996289
476868	43 minutes ago	1975		999255
476867	an hour ago	1719		999183
476866	an hour ago	2180		999145

[See all blocks](#)

**Latest Transactions**

Hash	Value Out
a308f4f001b5c8c0bf050ca5489f1cc879a3e1932f35b...	0.04976261 BTC
97f8ed3577fa23f7491894a0ec1577d3235d38811f04...	0.01499456 BTC
f79244d895103613f11c8fac70b3a6e91469249647a1...	0.35244063 BTC
c21f81bd4e7df40195f08834fa3b35a8ff5aff0d0504...	16.02897244 BTC
dfcb323f0b9e905f3cabe5c0d6e19b979df81rfd8fe...	34.98159707 BTC
c5fabbb881746c0503d20934279e138d0fb042af8b...	0.14671336 BTC
v29182da2d5a940fa579b1bbca4d4e4678ed9d55...	0.06723058 BTC
a699dfe106dca0436a76b88915fa9ad74977ab410d...	0.21317655 BTC
76af657200634e1a6a81d2c8570c78a571889320a14...	0.65942189 BTC
480a47568befc844e362890c1e5de9f008a951f6ac2c...	0.04331884 BTC

**About Block Explorer**

Bitcoin Block Explorer is an open source web tool that allows you to view information about blocks, addresses, and transactions on the Bitcoin blockchain. The source code is on GitHub.


If you are new to Bitcoin, check out [We Use Coins](#) and [Bitcoin.org](#).

**Public Bitcoin API:** Machine readable stats & blockchain info can be accessed directly through the REST and WebSocket APIs.

**Testnet:** In Bitcoin's sandbox. Block Explorer supports viewing both the *testnet* and *mainnet* blockchains.

**Other projects:** [BitKey](#) - The Bitcoin swiss army knife  
Thanks to [Private Internet Access](#) for hosting the site. They provide a VPN Service that accepts Bitcoin.

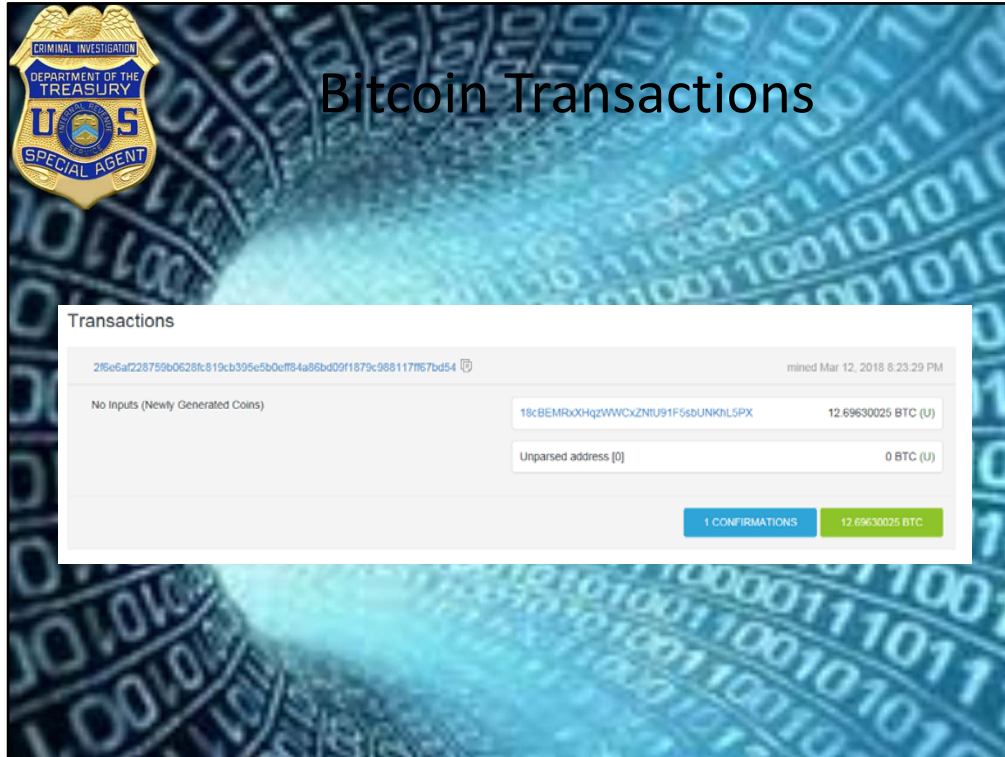
Powered by:



Once a Bitcoin Address is identified, it can be looked up on a Bitcoin Block Chain Explorer to find information such as value, transaction times, transaction locations, which may help in corroborating information, identifying additional addresses, or assist in locating the Subject. It can also be used to show if bitcoins were transferred after a seizure warrant was served, which is discussed below. Such as <http://blockexplorer.com/>

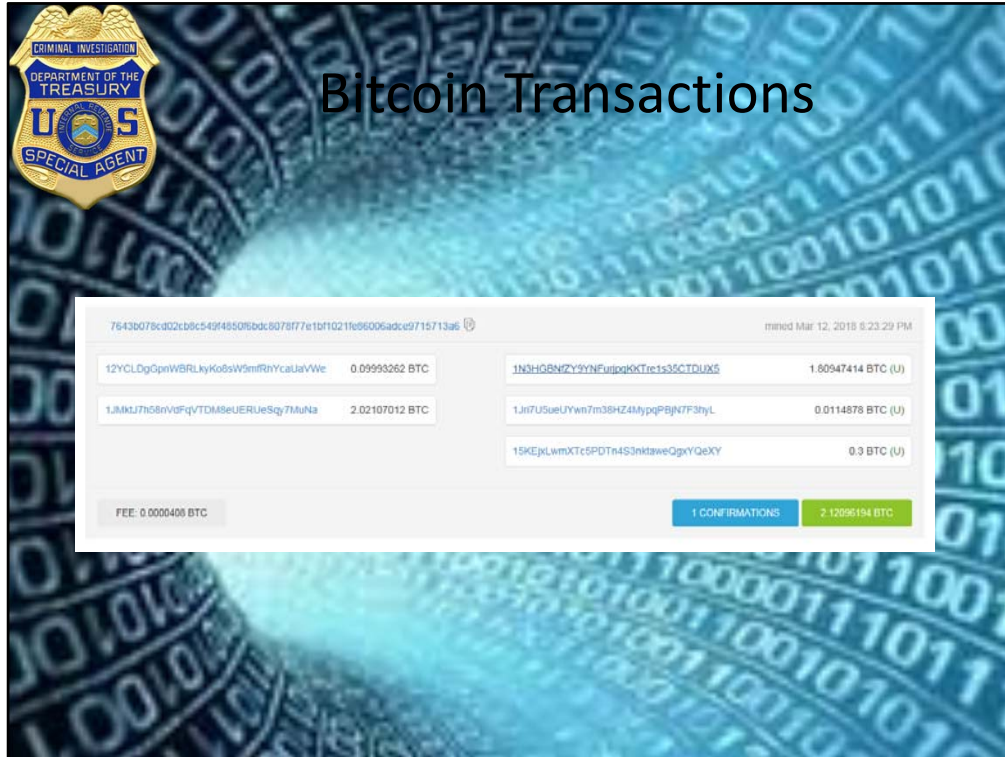




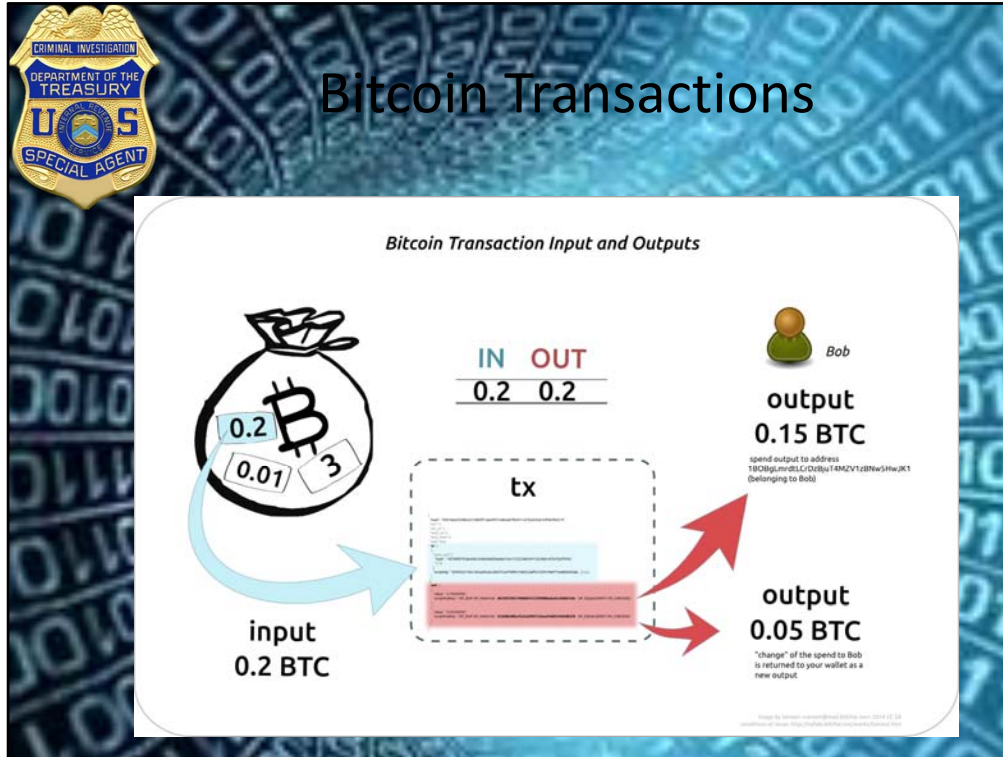


Once a Bitcoin Address is identified, it can be looked up on a Bitcoin Block Chain Explorer to find information such as value, transaction times, transaction locations, which may help in corroborating information, identifying additional addresses, or assist in locating the Subject. It can also be used to show if bitcoins were transferred after a seizure warrant was served, which is discussed below. Such as <http://blockexplorer.com/>





Once a Bitcoin Address is identified, it can be looked up on a Bitcoin Block Chain Explorer to find information such as value, transaction times, transaction locations, which may help in corroborating information, identifying additional addresses, or assist in locating the Subject. It can also be used to show if bitcoins were transferred after a seizure warrant was served, which is discussed below. Such as <http://blockexplorer.com/>



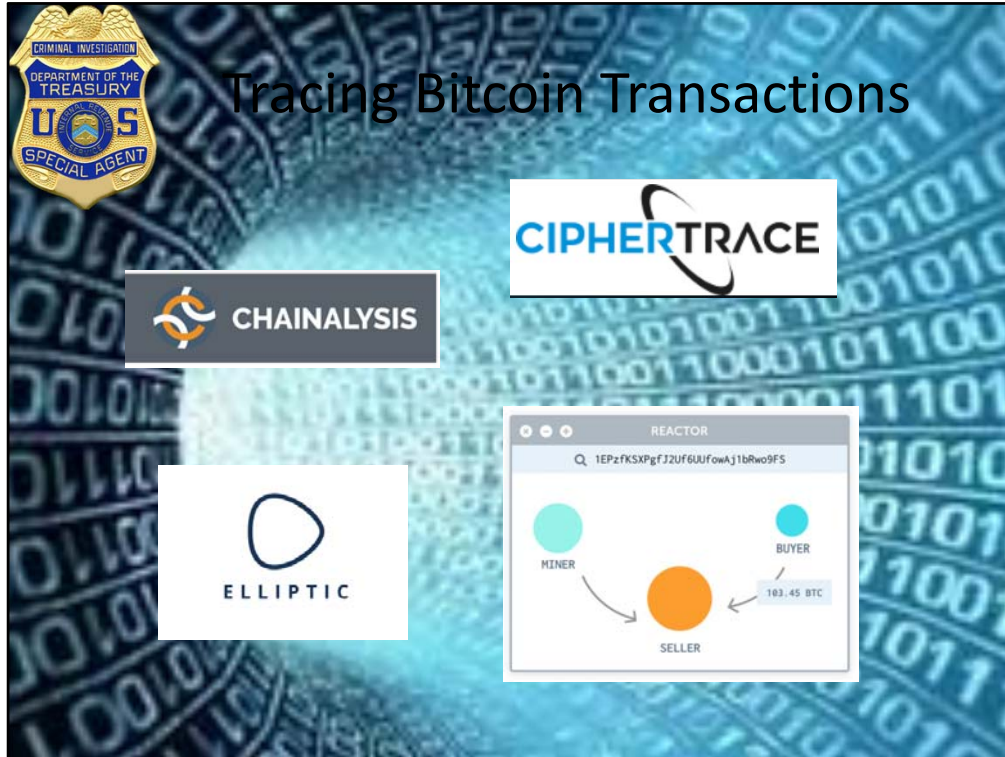
### Input

An input is a reference to an output from a previous transaction. Multiple inputs are often listed in a transaction. All of the new transaction's input values (that is, the total coin value of the previous outputs referenced by the new transaction's inputs) are added up, and the total (less any transaction fee) is completely used by the outputs of the new transaction.

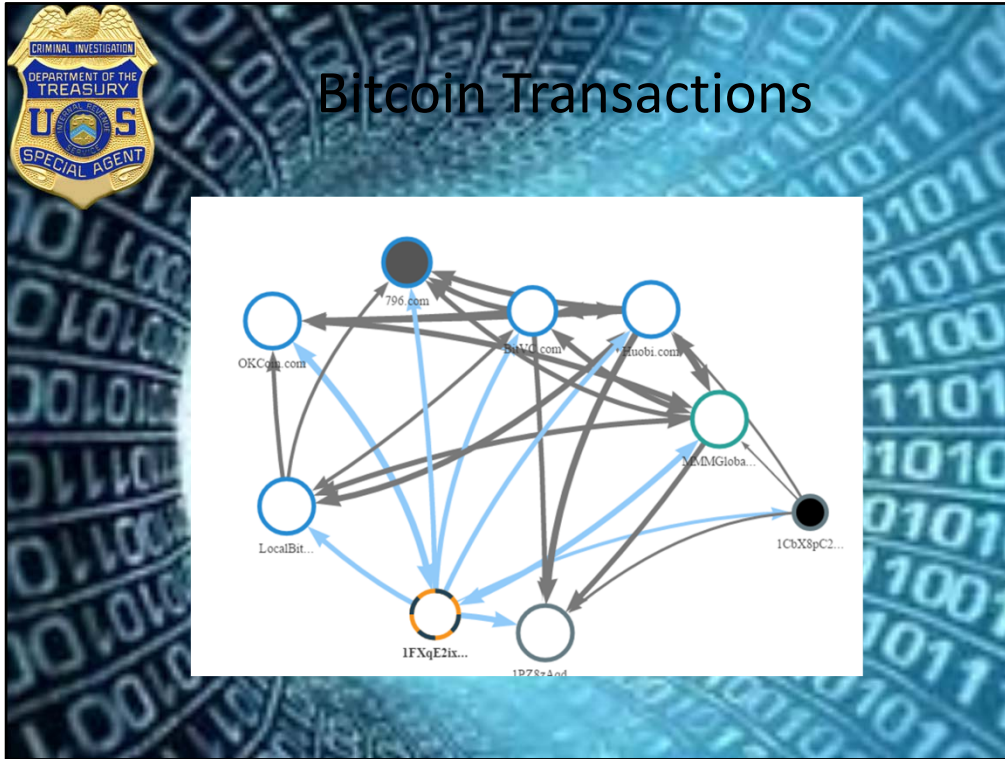
The script contains two components, a signature and a public key. The public key must match the hash given in the script of the redeemed output. The public key is used to verify the redeemer's signature, which is the second component.

### Output

An output contains instructions for sending bitcoins. Value is the number of Satoshi (1 BTC = 100,000,000 Satoshi) that this output will be worth when claimed. There can be more than one output, and they share the combined value of the inputs. Because each output from one transaction can only ever be referenced once by an input of a subsequent transaction, the entire combined input value needs to be sent in an output if you don't want to lose it. Any input bitcoins not redeemed in an output is considered a transaction fee; whoever generates the block will get it.



This software could accurately trace the history of bitcoin payments and wallets. Moreover, it is able to map wallets into known "clusters"—that is, mapping addresses to known entities like Silk Road, Coinbase, and other large Bitcoin players. (Wallet Explorer, and its commercial successor, Chainalysis, made use of academic research that first debuted in October 2013.)

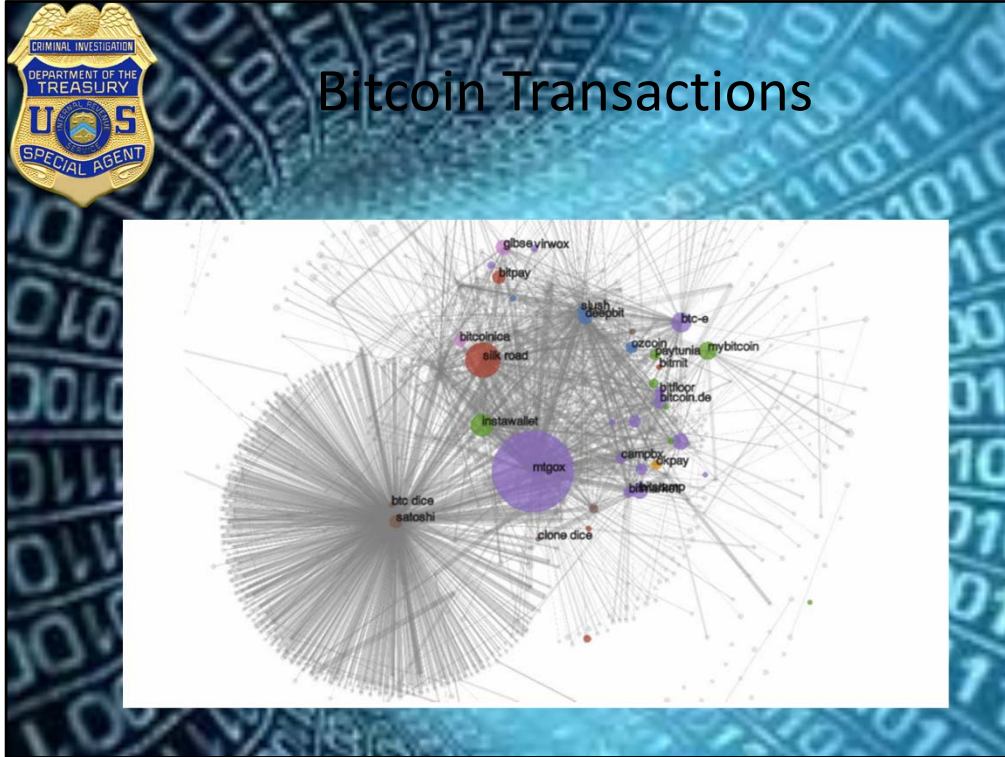



Example of what the tracing looks like.







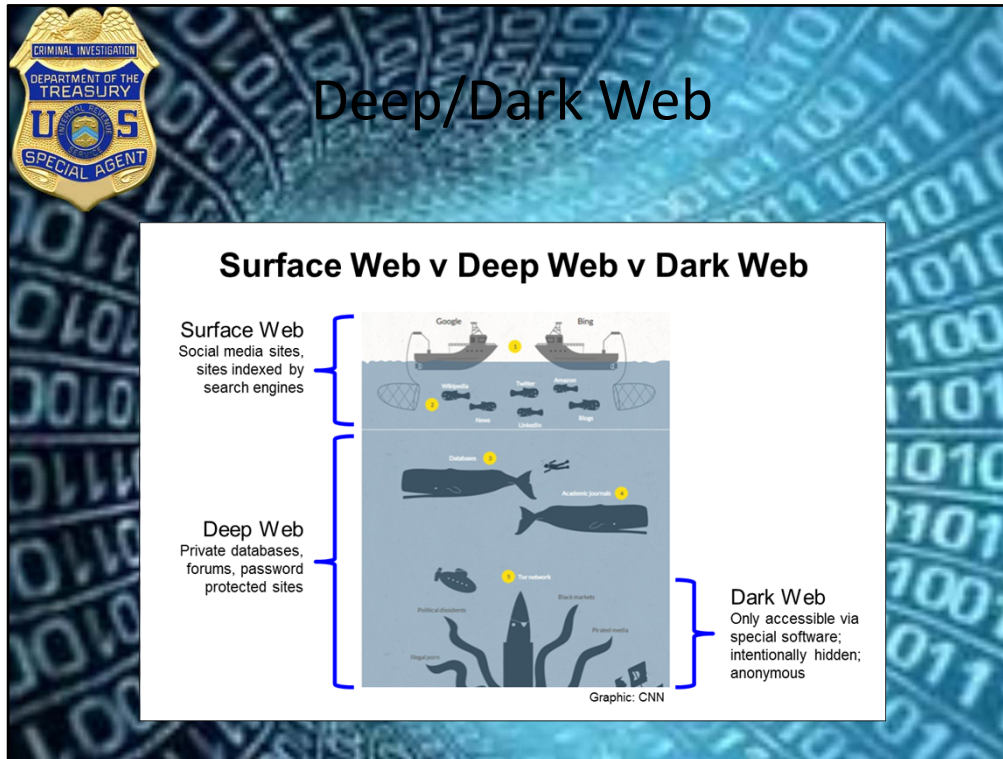




**Contact Information**

**James Daniels**  
**Program Manager – Cyber Crimes**  
**IRS-Criminal Investigation**  
**James.Daniels@ci.irs.gov**  
**360-905-1142**

The background of the slide features a blue-toned tunnel of binary code (0s and 1s) receding into the distance, creating a sense of depth and digital connectivity.



## Summary

### **Surface Web**

- Accessible
- Indexed for Search Engines
- Little illegal activity
- Relatively small in size

### **Deep Web**

- Accessible by password, encryption, or through gateway software
- Not indexed for Search Engines
- Little illegal activity outside of Dark Web
- Huge in size and growing exponentially

### **Dark Web**

- Restricted to special browsers
- Not indexed for Search Engines
- Large scale illegal activity
- Unmeasurable due to nature

## Surface Web

The Surface Web has been part of the World Wide Web since the first browser was first invented in 1990 by Tim Berner-Lee and is the part of the web you will be most familiar with, as it anything that can be discovered through your internet browser using any of the main search engines (Google, Bing, Yahoo etc.). This is what you use when you read the news, buy something on Amazon, or visit any of your usual daily websites, and is also the area of the web that is under constant surveillance by governments across the world.

Making up under 5 percent of the total World Wide Web content that is known to exist is a figure that is already miniscule, but estimates suggest that the Deep Web could be anywhere from 500 to 5000 times larger. In perspective, there are roughly twenty terabytes (TB) of data and roughly one billion documents on the surface web compared to 7,500 terabytes (TB) of discovered data and almost 600 billion discovered documents on the deep web.

### **Deep Web**

The Deep Web was also part of the web at its conception, and in basic terms it is the opposite of the surface as it anything that search engines cannot find. This is the key difference between the two in real data terms; sites on the surface internet are indexed for search engines to find, but the deep web is not indexed. However both are also accessible by the public, they just require different methods to access them - usually a specific password encrypted browser or a set of log in details.

Despite containing the Dark Web, it isn't actually so bad and without it we wouldn't be able to use the internet as we do today: the Deep Web contains all of our medical records, financial records, social media files, and plenty other important information we want and need to keep secure. It is this need to keep secure files that gave rise to the need to keep a portion of the web secured away from being "Googled" at the whim of anybody at any time.

A good example is when you have to either generate a pin number or have memorable information to enter to access your bank accounts online. This information is stored on the Deep Web and you have to use your details to allow you special access, but as you can see you can (and do) still have relative access to the Deep Web, and it isn't the entirely illicit, dangerous part of the web it is often confused with.

### **Dark Web**

The Dark Web IS part of the Deep Web, but it has one major difference in that it has been intentionally hidden and is inaccessible to normal web browsers. The technology to create the Dark Web was initially created (and still funded) by US Military Researchers in the mid-1990s to allow spies and intelligence agencies to anonymously send and receive messages. Named "The Onion Router", it was quickly coined with the shorter "Tor" with its name coming from application layer encryption within a communication protocol stack; many layers representing the layers of an onion.

If the US Military built it, why is it accessible to anyone with the right tools? The strategy was

to release Tor into the public domain with simple logic; you can't hide messages if there is nothing to hide them behind therefore if more people had access to send anonymous messages, the harder it would be for counter-intelligence to discover their messages. Another perceived benefit was to help people in nations where they are seen to be oppressed, with impossible freedom of speech laws, to allow them to voice themselves freely where they cannot be tracked and punished. A good idea in theory however it has primarily been filled with crime and the ability to find these criminals is extremely difficult - the whole point of the original Tor project was to be impossible to find.





## Summary

### **Surface Web**

- Accessible
- Indexed for Search Engines
- Little illegal activity
- Relatively small in size

### Surface Web

The Surface Web has been part of the World Wide Web since the first browser was first invented in 1990 by Tim Berner-Lee and is the part of the web you will be most familiar with, as it anything that can be discovered through your internet browser using any of the main search engines (Google, Bing, Yahoo etc.). This is what you use when you read the news, buy something on Amazon, or visit any of your usual daily websites, and is also the area of the web that is under constant surveillance by governments across the world.

Making up under 5 percent of the total World Wide Web content that is known to exist is a figure that is already miniscule, but estimates suggest that the Deep Web could be anywhere from 500 to 5000 times larger. In perspective, there are roughly twenty terabytes (TB) of data and roughly one billion documents on the surface web compared to 7,500 terabytes (TB) of discovered data and almost 600 billion discovered documents on the deep web.



## Deep Web

- Accessible by password, encryption, or through gateway software
- Not indexed for Search Engines
- Little illegal activity outside of Dark Web
- Huge in size and growing exponentially

The Deep Web was also part of the web at its conception, and in basic terms it is the opposite of the surface as it anything that search engines cannot find. This is the key difference between the two in real data terms; sites on the surface internet are indexed for search engines to find, but the deep web is not indexed. However both are also accessible by the public, they just require different methods to access them - usually a specific password encrypted browser or a set of log in details.

Despite containing the Dark Web, it isn't actually so bad and without it we wouldn't be able to use the internet as we do today: the Deep Web contains all of our medical records, financial records, social media files, and plenty other important information we want and need to keep secure. It is this need to keep secure files that gave rise to the need to keep a portion of the web secured away from being "Googled" at the whim of anybody at any time.

A good example is when you have to either generate a pin number or have memorable information to enter to access your bank accounts online. This information is stored on the Deep Web and you have to use your details to allow you special access, but as you can see

you can (and do) still have relative access to the Deep Web, and it isn't the entirely illicit, dangerous part of the web it is often confused with.



### **Dark Web**

- Restricted to special browsers
- Not indexed for Search Engines
- Large scale illegal activity
- Unmeasurable due to nature

### **Dark Web**

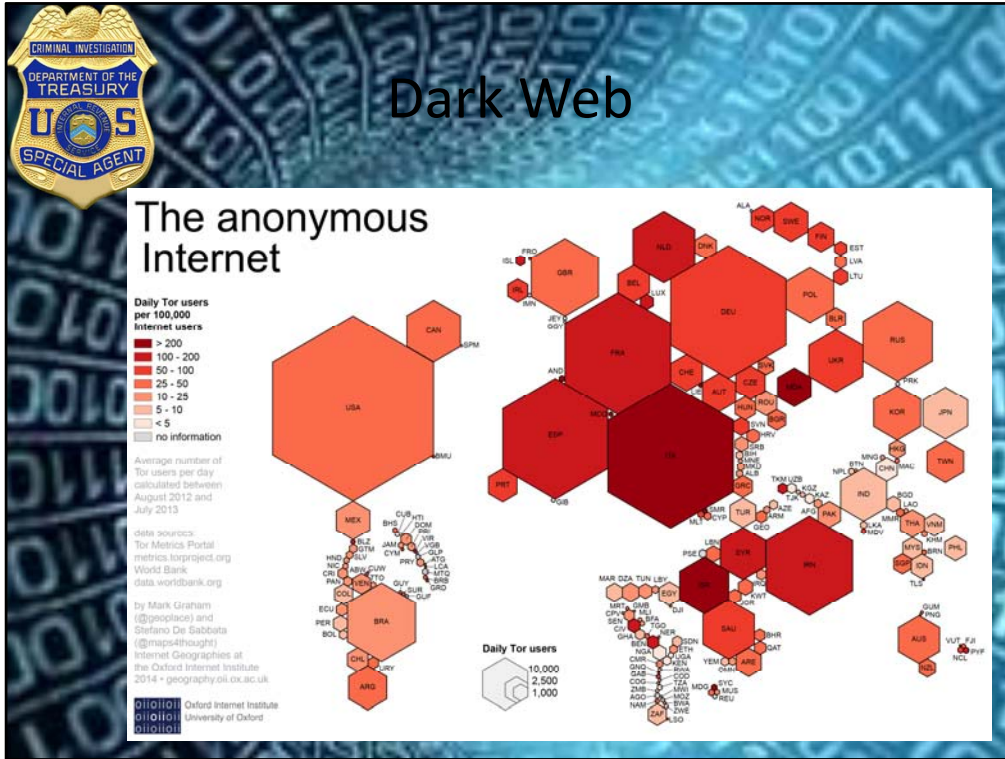
The Dark Web IS part of the Deep Web, but it has one major difference in that it has been intentionally hidden and is inaccessible to normal web browsers. The technology to create the Dark Web was initially created (and still funded) by US Military Researchers in the mid-1990s to allow spies and intelligence agencies to anonymously send and receive messages. Named "The Onion Router", it was quickly coined with the shorter "Tor" with its name coming from application layer encryption within a communication protocol stack; many layers representing the layers of an onion.

If the US Military built it, why is it accessible to anyone with the right tools? The strategy was to release Tor into the public domain with simple logic; you can't hide messages if there is nothing to hide them behind therefore if more people had access to send anonymous messages, the harder it would be for counter-intelligence to discover their messages.

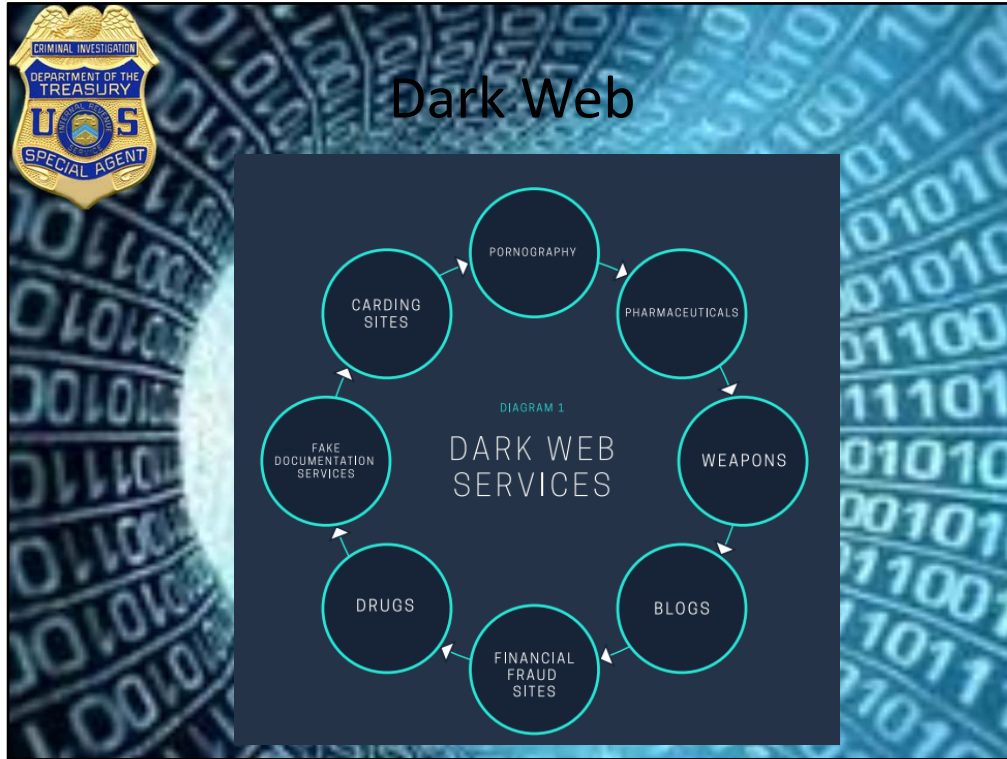
Another perceived benefit was to help people in nations where they are seen to be oppressed, with impossible freedom of speech laws, to allow them to voice themselves freely where they cannot be tracked and punished. A good idea in theory however it has

primarily been filled with crime and the ability to find these criminals is extremely difficult - the whole point of the original Tor project was to be impossible to find.





Use of the dark web by country






Examples of criminal activity on the dark web

**Accessing the Dark Web**

- Requires software running on computer or Tails and usb
  - The Onion Router (Tor) is most popular
  - Others include: 1P2 and Freenet
- Uses encryption and proxies/relays to conceal a user's location and usage
  - More than 2.5 million daily users

The remainder of this presentation will focus on Tor; however, the same concepts apply to the others



Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".

Tails relies on the Tor anonymity network to protect your privacy online:

- all software is configured to connect to the Internet through Tor
- if an application tries to connect to the Internet directly, the connection is automatically blocked for security.

Tor is an open and distributed network that helps defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Tor protects you by bouncing your communications around a network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Using Tor you can:

- be anonymous online by hiding your location,
- connect to services that would be censored otherwise;
- resist attacks that block the usage of Tor using circumvention tools such as bridges.

To learn more about Tor, see the official Tor website, particularly the following pages:

- Tor overview: Why we need Tor
- Tor overview: How does Tor work
- Who uses Tor?
- Understanding and Using Tor — An Introduction for the Layman

To learn more about how Tails ensures all its network connections use Tor, see our design document.

Use anywhere but leave no trace

Using Tails on a computer doesn't alter or depend on the operating system installed on it. So you can use it in the same way on your computer, a friend's computer, or one at your local library. After shutting down Tails, the computer will start again with its usual operating system.

Tails is configured with special care to not use the computer's hard-disks, even if there is some swap space on them. The only storage space used by Tails is in RAM, which is automatically erased when the computer shuts down. So you won't leave any trace on the computer either of the Tails system itself or what you used it for. That's why we call Tails "amnesic".

This allows you to work with sensitive documents on any computer and protects you from data recovery after shutdown. Of course, you can still explicitly save specific documents to another USB stick or external hard-disk and take them away for future use.

State-of-the-art cryptographic tools

Tails also comes with a selection of tools to protect your data using strong encryption:

Encrypt your USB sticks or external hard-disks using LUKS, the Linux standard for disk-encryption.

Automatically use HTTPS to encrypt all your communications to a number of major websites using HTTPS Everywhere, a Firefox extension developed by the Electronic Frontier Foundation.

Encrypt and sign your emails and documents using the de facto standard OpenPGP either from Tails email client, text editor or file browser.

Protect your instant messaging conversations using OTR, a cryptographic tool that provides encryption, authentication and deniability.

Securely delete your files and clean your disk space using Nautilus Wipe.

TOR and Tails are available on the TOR Project website. Access download links directly from <https://www.torproject.org>. Insert your USB drive and follow the instructions on <https://tails.boum.org>.

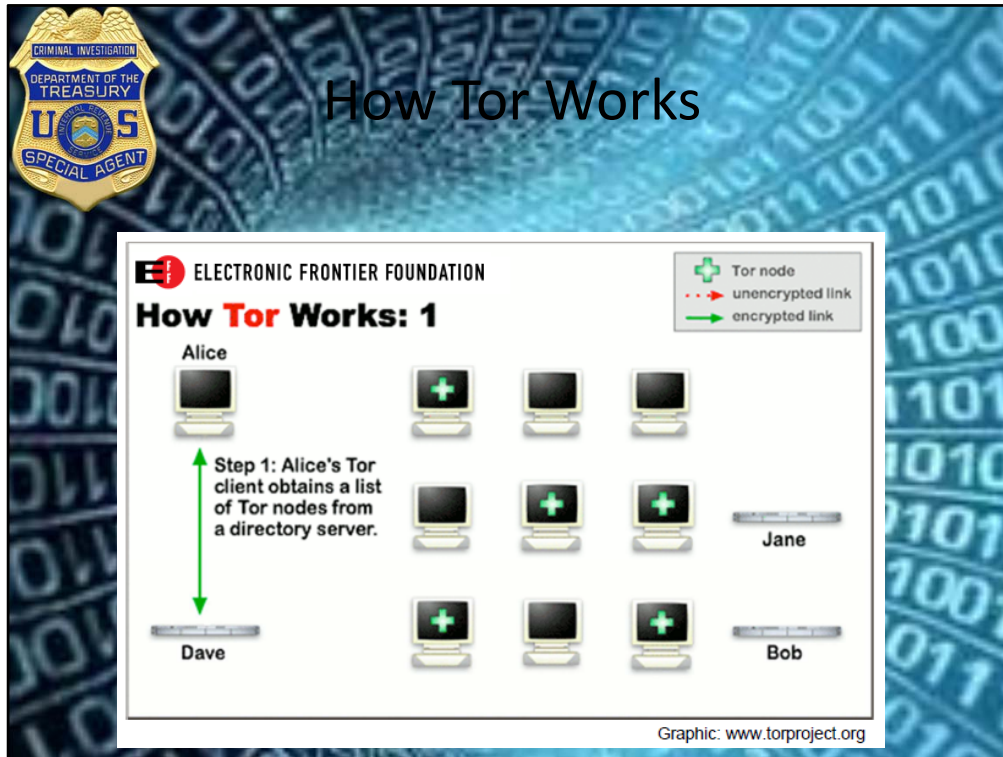
Browse safely.

Common portals and search engines:

- DuckDuckGo
- The Hidden Wiki
- Onion.link
- Ahmia.fi
- Grams
- Torch

Encryption is strong, but not impenetrable. The FBI discovered and exploited vulnerabilities in the TOR network. Though the agency refused to disclose the source code used to penetrate the network, undoubtedly law enforcement agencies around the world monitor and operate on the Deep Web. Members of the TOR project vowed to patch network holes and strengthen the protocol.



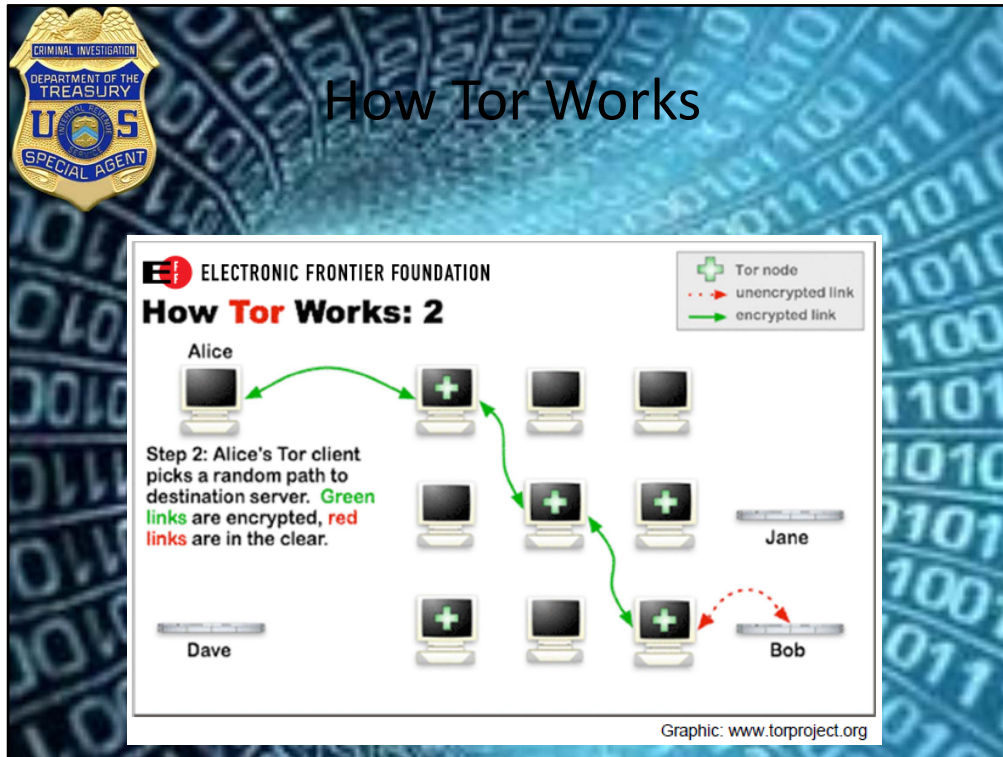


Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". The intent for Tor's use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Tor does not prevent an online service from determining when it is being accessed through Tor. Tor protects a user's privacy, but does not hide the fact that someone is using Tor. Some websites restrict allowances through Tor. For example, the MediaWiki TorBlock extension automatically restricts edits made through Tor, although Wikipedia allows some limited editing in exceptional circumstances.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network


surveillance that relies upon knowing its source and destination.



Tor aims to conceal its users' identities and their online activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe. These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location. That anonymity extends to the hosting of censorship-resistant content by Tor's anonymous hidden service feature. Furthermore, by keeping some of the entry relays (bridge relays) secret, users can evade Internet censorship that relies upon blocking public Tor relays.

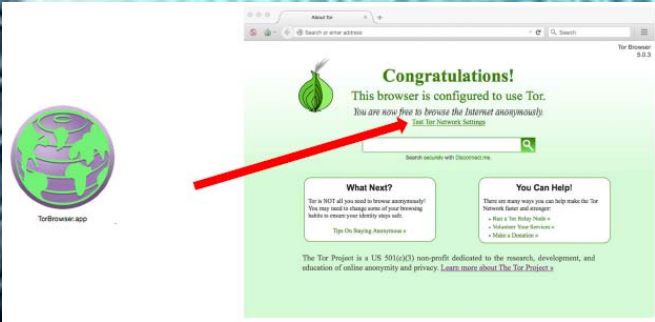
Because the IP address of the sender and the recipient are not both in cleartext at any hop along the way, anyone eavesdropping at any point along the communication channel cannot directly identify both ends. Furthermore, to the recipient it appears that the last Tor node (called the exit node), rather than the sender, is the originator of the communication.





# Tor Browser

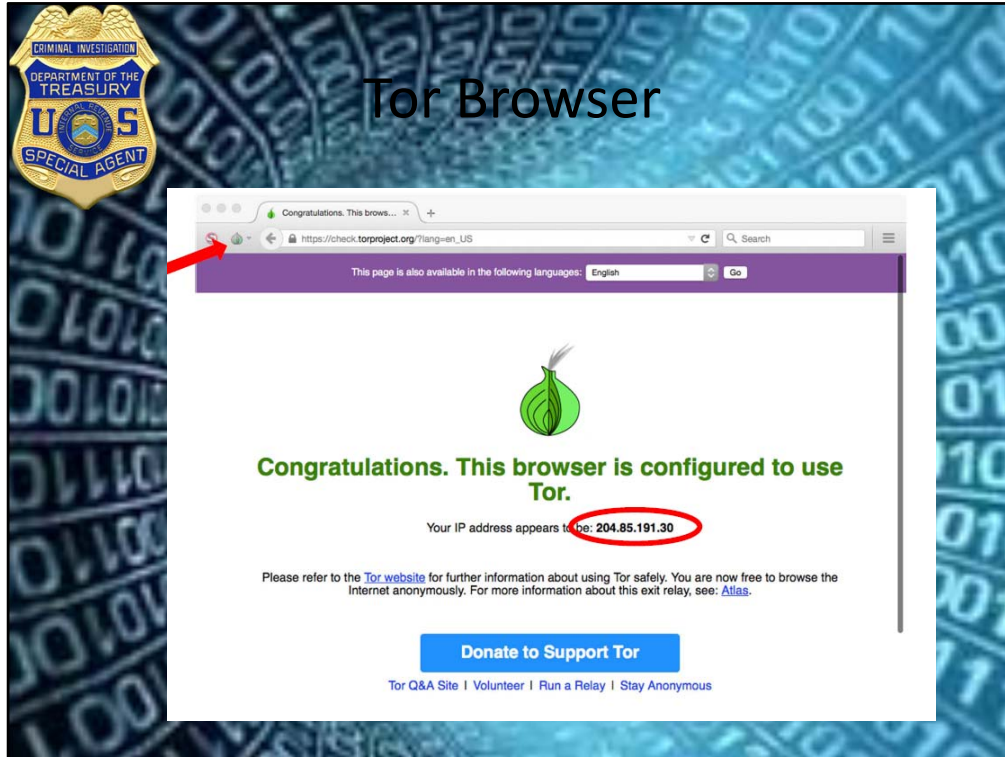
- Web browser based on Mozilla Firefox and pre-configured to protect your anonymity (Tor, scripting disabled, plugins, etc.)



- Note: does not protect your computer from malware, viruses, etc.

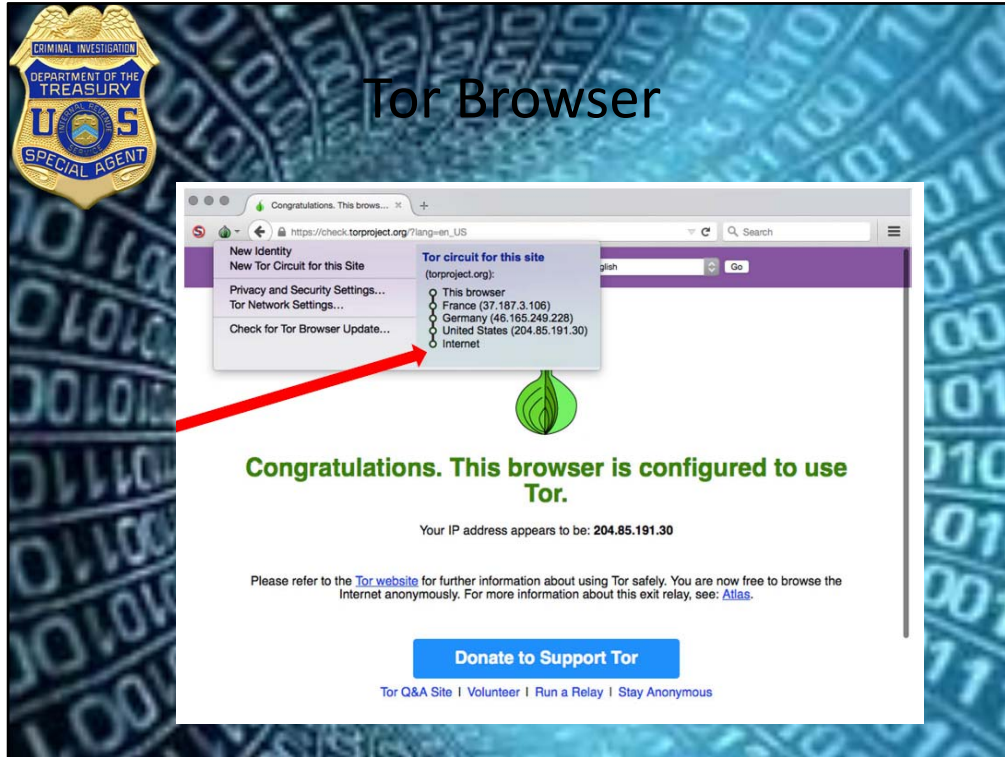
How to use the Tor Browser – Click on the link by the arrow





How to use the Tor Browser – Notice the current identified IP Address. This will be different then the IP Address of a connection made used a standard browser

Click on the link by the arrow



How to use the Tor Browser – Notice the connections that are made prior to going to the site the user requested. One way to get a new list of connections – just close Tor and re-open.



Examples of some search engines used in the dark web. {Not an all inclusive list – and new sites come up and go down often}

- Onion URL Repository -<http://32rfckwuorlf4dlv.onion/> The Onion URL Repository has a massive index of over a million page results and does not have limits on what information it holds.
- Uncensored Hidden Wiki -<http://zqktlwi4fecvo6ri.onion/> Uncensored Hidden Wiki is an uncensored collection of links and articles that, over the site's history, have included links to information on criminal activities from drugs to child pornography. The site has cleaned up its act considerably, but there are still links to graphic content and possibly illegal sites to be found.
- notEvil - <https://hss3uro2hsxfogfq.onion.to> This search engine the users can skip all the clutter and distraction from surfing the web with no ads. It's clean and mimics the look of Google.
- ParaZite -<http://kpynyvym6xqi7wz2.onion/li...> ParaZite is a search engine that gamifies the deep web. It offers basic, and useful, search features, and in addition also offers up the chance to gamble by taking you to a random site on the deep web. It's the deep web equivalent of Google's "Feeling Lucky" feature.

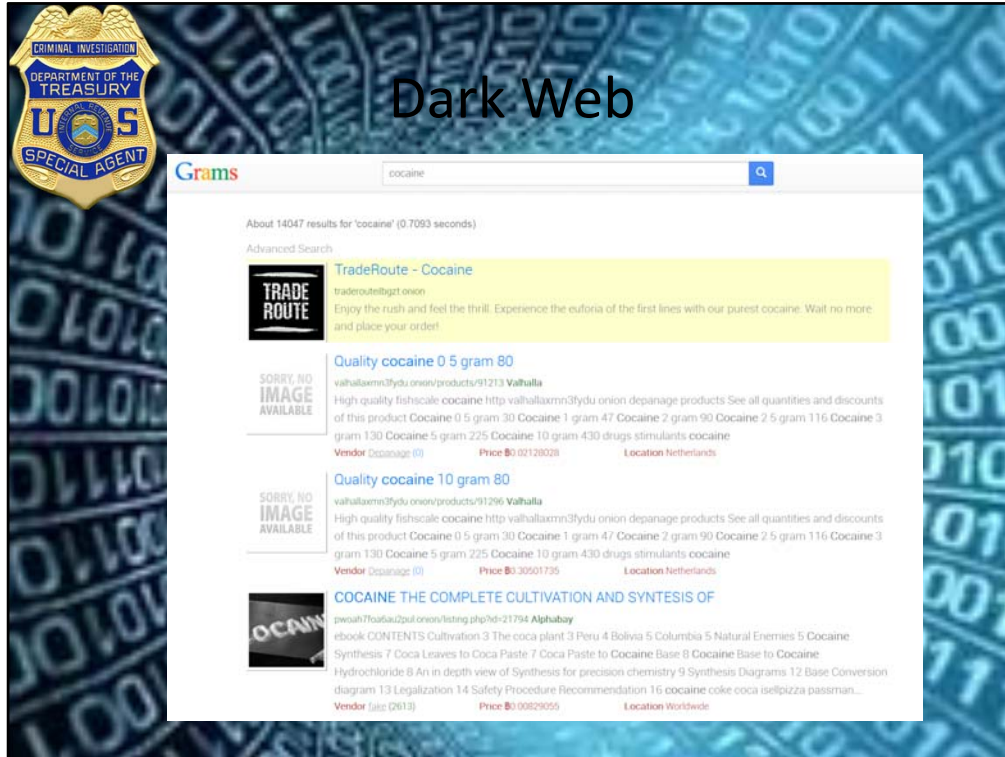
#### **Why is a Deep Web search not available from Google?**

The primary reason Google doesn't provide deep web content is that this content doesn't index in the regular search engines. Hence, these search engines will not show results, or

crawl to a document or file which is unindexed by the world wide web. The content lies behind the HTML forms. Regular search engines crawl, and the searches are derived from interconnected servers.

Interconnected servers mean you are regularly interacting with the source, but when it comes to the dark web this does not happen. Everything is behind the veil and stays hidden internally on the Tor network; which ensures security and privacy.

Only 4 percent of Internet content is visible to the general public, and the other 96 percent is hidden behind the deep web.



Search result examples look and feel like a google search return. These are onion addresses and can only be accessed using Tor or other dark web browser.



## Dark Web

**DEEPPDOT.WEB**  
Official Hidden service:  
DeepDot35Wmeyd5.onion

**MARKETS LIST & AVAILABILITY STATUS**

**TOP MARKETS!**

Dream market - 98.02%
Point / T*chka Free Market - 88.53%
Wall Street Market - 97.19%

**INVITE / REFERRAL MARKETS**

Olympus Market - 99.98%
Libertas Market (Monero Only) - 86.35%

**MARKETS**

The Majestic Garden - 96.34%
Zion Market - 89.61%
CGMC - 91.04%
Berlusconi Market - 95.24%

**VENDOR SHOPS**

Gammagoblin - 96.17%
The French Connection - 98.37%
CharlieUK - 95.56%
ToYouTeam - 78.35%
EuroPills - 46.24%
Fight Club - 46.17%
ElHerbolario - 98.19%
I33TER - 45.48%

DeepDotWeb is a news site dedicated to events in and surrounding the dark web featuring in-depth interviews and reviews about darknet markets, Tor hidden services, legal actions, privacy, bitcoin and related news.

Exclusive coverage has included darknet market drug busts, pedophile crowdfunding, the details of hacking of darknet markets. as well as the diversification of markets such as TheRealDeal selling software exploits.


Site features include blacklisted markets, comparisons and reviews.




The FBI has seized DeepDotWeb, a comparison search system and news site about dark web markets, accusing the outfit of money laundering.

Police in five countries arrested the alleged operators – including two Israelis and moderators in France, Germany, and the Netherlands – in a sweeping international raid disclosed Tuesday and took down the .com and .onion sites, replacing them with notices of seizure.

The site rose in prominence after larger dark web sites like Silk Road fell to government crackdowns. DeepDotWeb offered a number of services including cryptocurrency news related to privacy and dark web selling. The site also listed dark web markets for buying and selling cryptocurrency.



# Dark Web



**Must Read**


[Is the Tor network really that safe?](#)

[Easy ways to buy crypto-currencies worldwide](#)

[Multisig vs Escrow vs Finalize Early, and what they mean.](#)

["What PGP is" and how to use it in a few easy steps.](#)

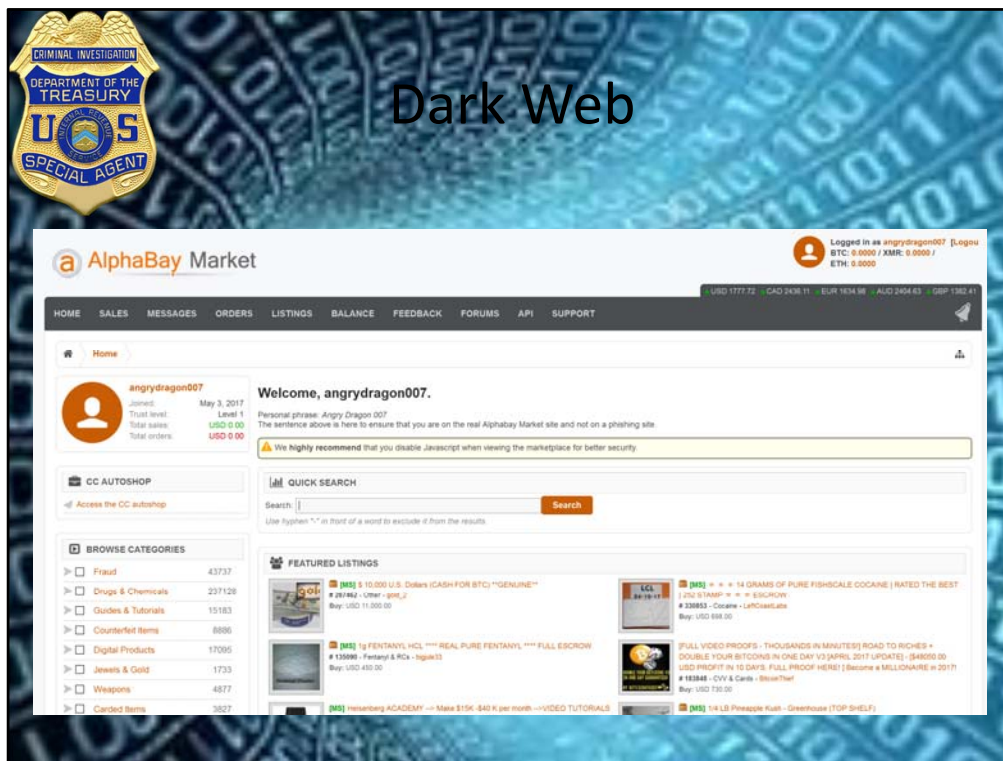
[PGP messaging tutorial for Windows \(GPG4WIN – Kleopatra\) Detailed and simple!](#)



NEWS MAY 10, 2019

**International Law Enforcement Seizes DeepDotWeb, Arrests Admin**

Onion List & Availability Status	
<b>Markets</b>	
Dream Market	Show URLs <a href="#">↗</a>
Wall Street Market	Show URLs <a href="#">↗</a>
Tochka / Point Market	Show URLs <a href="#">↗</a>
Nightmare Market	Show URLs <a href="#">↗</a>
Empire Market	Show URLs <a href="#">↗</a>
Berlusconi Market	Show URLs <a href="#">↗</a>
Cannazon Market	Copy URL <a href="#">📄</a>
Rapture Market	Copy URL <a href="#">📄</a>
The Majestic Garden	Copy URL <a href="#">📄</a>
CG & M Cooperative	Copy URL <a href="#">📄</a>
<b>Vendor Shops</b>	
RechardSport	Copy URL <a href="#">📄</a>
The French Connection	Copy URL <a href="#">📄</a>
ElHerbolario Shop	Copy URL <a href="#">📄</a>
Dutch Magic Shop	Copy URL <a href="#">📄</a>
Gammagoblin Shop	Copy URL <a href="#">📄</a>
CharlieUK Shop	Copy URL <a href="#">📄</a>
DutchDrugz Shop	Copy URL <a href="#">📄</a>
ToYouTeam Shop	Copy URL <a href="#">📄</a>
AltBay Shop	Copy URL <a href="#">📄</a>
<b>Forums</b>	
Dread Forum	Show URLs <a href="#">↗</a>

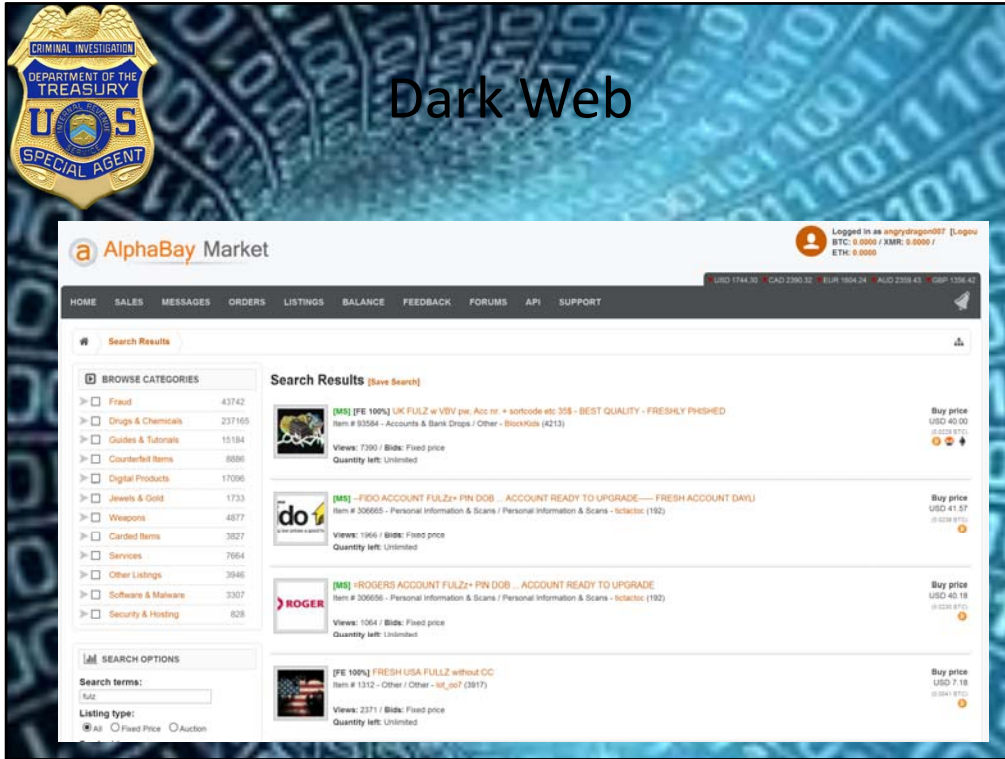


Example of Dark Net Market – Alphabay [No longer active – taken down by law enforcement - On July 20, “after a globally coordinated operation” between law enforcement agencies worldwide, the United States Department of Justice announced the takedown of Alphabay and Hansa marketplace.]

AlphaBay was a darknet site and you could only access the AlphaBay URL via the Tor network. It offered all sorts of listings, but mostly illicit drugs, firearms, stolen personal information, etc. The payment was regulated by bitcoins.

AlphaBay Market transactions were processed through a centralized Escrow system to protect buyers at all times.

When a transaction was started, the funds are temporarily held in the Escrow system until the buyer marks that he has received the goods.

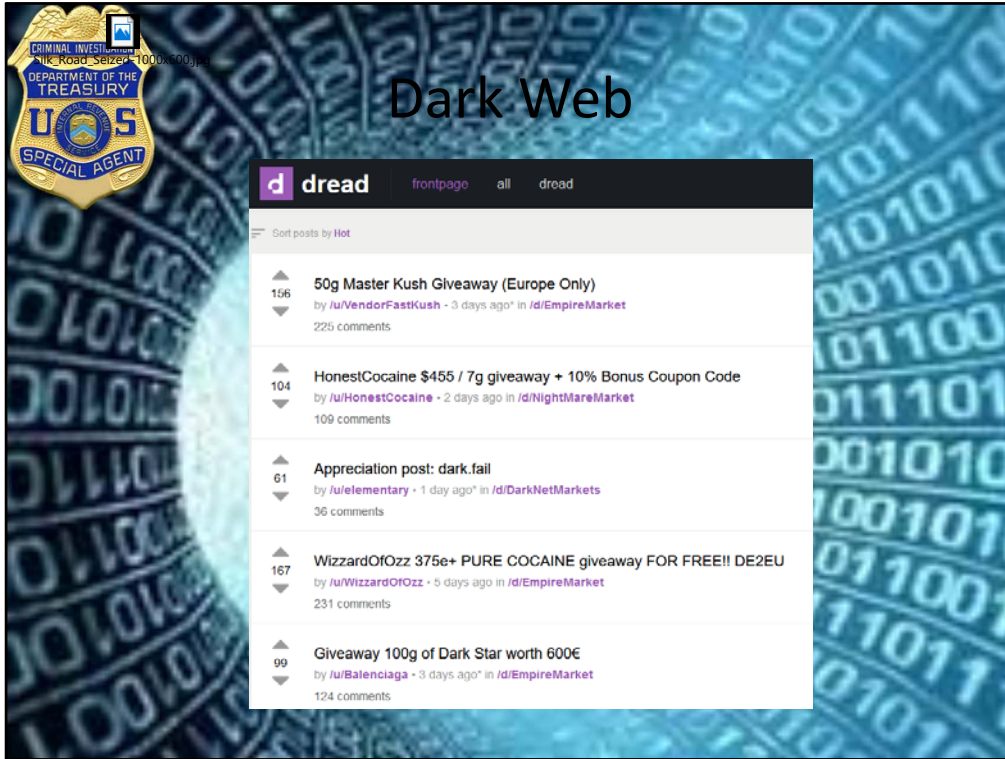


Example of search results from Alphabay





Seized Alphabay screen



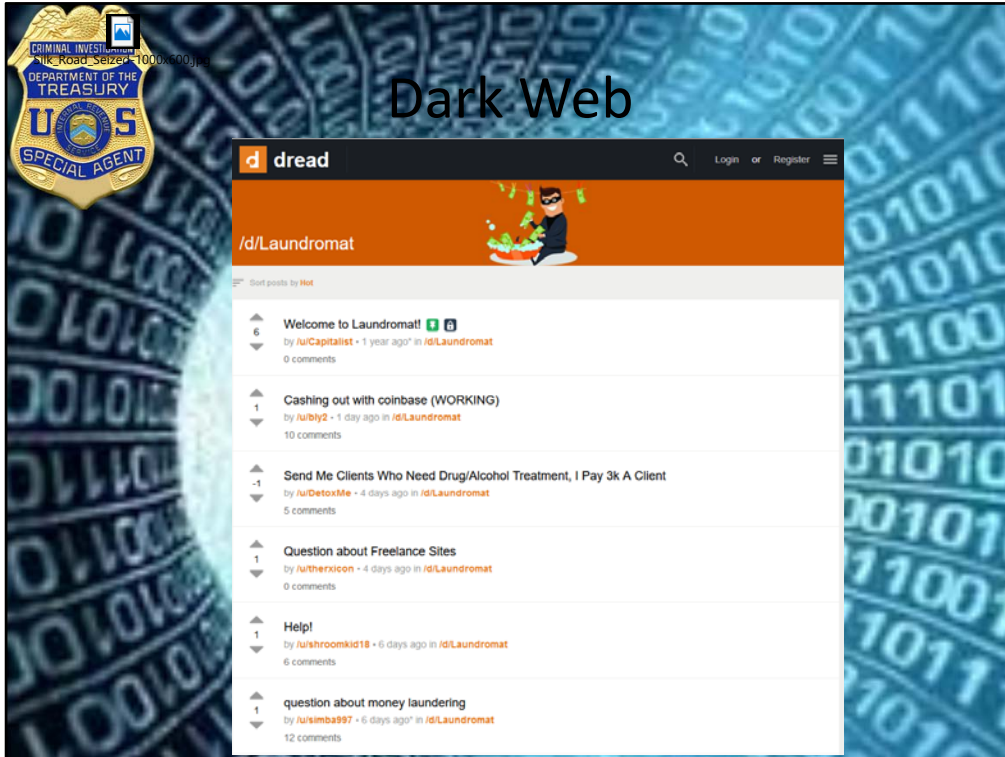
The image shows a screenshot of a forum post on the 'dread' website. The background is a blue-tinted image of binary code (0s and 1s) arranged in a circular pattern. In the top left corner, there is a logo for the U.S. Customs and Border Protection (CBP) with the text 'CRIMINAL INVESTIGATION', 'DEPARTMENT OF THE TREASURY', 'U.S. CUSTOMS AND BORDER PROTECTION', and 'SPECIAL AGENT'. The forum post itself is titled 'Dark Web' and lists several items for sale or giveaway. The items are sorted by 'Hot'.

Score	Title	Author	Time	Location	Comments
156	50g Master Kush Giveaway (Europe Only)	/u/VendorFastKush	3 days ago	/d/EmpireMarket	225
104	HonestCocaine \$455 / 7g giveaway + 10% Bonus Coupon Code	/u/HonestCocaine	2 days ago	/d/NightMareMarket	109
61	Appreciation post: dark.fail	/u/elementary	1 day ago	/d/DarkNetMarkets	36
167	WizzardOfOzz 375e+ PURE COCAINE giveaway FOR FREE!! DE2EU	/u/WizzardOfOzz	5 days ago	/d/EmpireMarket	231
99	Giveaway 100g of Dark Star worth 600€	/u/Balenciaga	3 days ago	/d/EmpireMarket	124

## Dark Web

**Discover**

Subreddit	Subscribers	Description
<a href="#">/d/Dread</a>	71,251	The official community for Dread announcements, discussion and f...
<a href="#">/d/FakeID</a>	1,202	Your new safe, secure, and growing Fake ID community.
<a href="#">/d/WallStreetMarket</a>	15,848	[b][color=red]WSM HAS EXIT SCAMMED!
<a href="#">/d/LibertasMarket</a>	12,399	Market link
<a href="#">/d/murderhomelesspeople</a>	1,727	Learn, teach & discuss the fine art of dealing drugs offline.
<a href="#">/d/Forgeries</a>	697	Forgery at its Finest
<a href="#">/d/HarmReduction</a>	610	You're looking for /d/DNSTARS next door!
<a href="#">/d/RaptureMarket</a>	611	[b]OFFICIAL MARKET URLS [!b]
<a href="#">/d/DarkNetAustralia</a>	1,537	
<a href="#">/d/Opiates</a>	902	Tell us about all your darknet experiences or in real life experience...
<a href="#">/d/DarkNetMarkets</a>	19,006	Discussion about the DNMs and Vendors.
<a href="#">/d/FakeIDUK</a>	193	Home of discussions for all things Fake ID in the UK
<a href="#">/d/TochkaFreeMarket</a>	12,792	Official mirrors.
<a href="#">/d/HiddenService</a>	1,311	Post all your !2p, freenet, and darknet links here. A reddit style dire...
<a href="#">/d/DankNation</a>	2,608	Before you purchase or post reviews. Please review /d/darknetmar...
<a href="#">/d/Lean</a>	268	#Legalz0L.ean
<a href="#">/d/DarkDotFail</a>	573	PGP-verified onion links because I got sick of using DNStats.
<a href="#">/d/TheMajesticGarden</a>	769	A subread for TMG
<a href="#">/d/EmpireMarket</a>	4,252	[b]Empire Market is the #1 market[!b]
<a href="#">/d/DNMIUK</a>	1,943	A place to discuss harm reduction & UK darknet activity.



The image shows a screenshot of a dark web forum post on the Dread platform. The background is a blue and black pattern of binary code (0s and 1s). In the top left corner, there is a gold badge for the U.S. Department of the Treasury, Office of the Inspector General, Criminal Investigation Division, with the text 'SPECIAL AGENT'. The main title of the post is 'Dark Web' in large white font. The forum post itself is titled '/d/Laundromat' and features a profile picture of a person in a black hoodie and mask. The post content includes several entries:

- Welcome to Laundromat!** by /u/Capitalist • 1 year ago in /d/Laundromat (6 upvotes, 0 comments)
- Cashing out with coinbase (WORKING)** by /u/bly2 • 1 day ago in /d/Laundromat (1 upvote, 10 comments)
- Send Me Clients Who Need Drug/Alcohol Treatment, I Pay 3k A Client** by /u/DetoxMe • 4 days ago in /d/Laundromat (-1 downvote, 5 comments)
- Question about Freelance Sites** by /u/theixicon • 4 days ago in /d/Laundromat (1 upvote, 0 comments)
- Help!** by /u/shroomkid18 • 6 days ago in /d/Laundromat (1 upvote, 6 comments)
- question about money laundering** by /u/simba997 • 6 days ago in /d/Laundromat (1 upvote, 12 comments)



Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as Ukash and Bitcoin are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the "WannaCry worm", traveled automatically between computers without user interaction.

Starting from around 2012 the use of ransomware scams has grown internationally.





The attack began on Friday, 12 May 2017, with evidence pointing to an initial infection in Asia at 7:44am UTC. The initial infection was likely through an exposed vulnerable Server Message Block (SMB) port, rather than email phishing as initially assumed. Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.

Organizations that had not installed Microsoft's security update from April 2017 were affected by the attack. Those still running unsupported versions of Microsoft Windows, such as Windows XP and Windows Server 2003 were at particularly high risk because no security patches had been released since April 2014 (with the exception of one emergency patch released in May 2014). A Kaspersky Lab study reported however, that less than 0.1 percent of the affected computers were running Windows XP, and that 98 percent of the affected computers were running Windows 7. In a controlled testing environment, the cybersecurity firm Kryptos Logic found that they were unable to infect a Windows XP system with WannaCry using just the exploits, as the payload failed to load, or caused the operating system to crash rather than actually execute and encrypt files. However, when executed manually, WannaCry could still operate on Windows XP.

The worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or

were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems.

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

One of the largest agencies struck by the attack was the National Health Service hospitals in England and Scotland, and up to 70,000 devices – including computers, MRI scanners, blood-storage refrigerators and theatre equipment – may have been affected. On 12 May, some NHS services had to turn away non-critical emergencies, and some ambulances were diverted. In 2016, thousands of computers in 42 separate NHS trusts in England were reported to be still running Windows XP. NHS hospitals in Wales and Northern Ireland were unaffected by the attack.

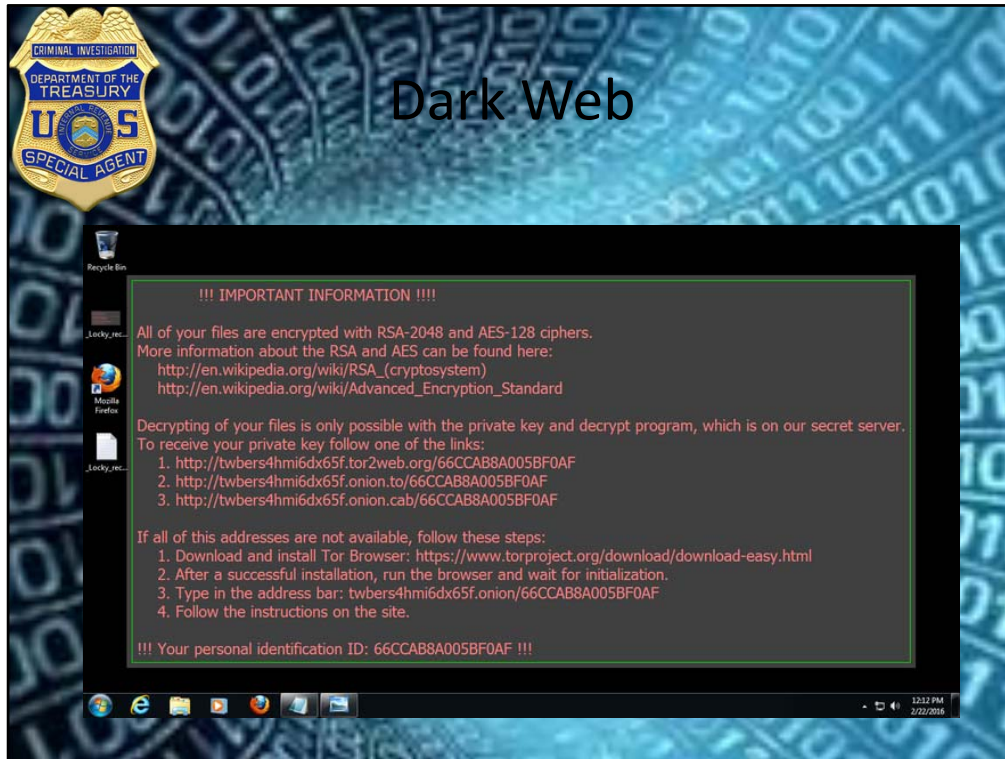
Nissan Motor Manufacturing UK in Tyne and Wear, England, halted production after the ransomware infected some of their systems. Renault also stopped production at several sites in an attempt to stop the spread of the ransomware. Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide.

In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.



Example of what a user would see when their computer is infected with ransomware .

Notice the bitcoin address at the bottom of the screen – this can be used to track on the blockchain or one of the bitcoin tracing software programs



Another example of an infected computer





In the last half of 2017, cryptojacking became popularized. This led to an eventual and predictable shift from cyber criminals not only cryptojacking, but also installing malware with the sole purpose of using an endpoint that isn't theirs to mine cryptocurrency. It's a smart strategy if you're a cyber criminal. Why try and ransom someone's system and wait for them to pay you when you can just print money?

Consider cryptojacking to be just one more illicit use of an endpoint you are supposed to control. There are a number of ways to actually do this but one of the more pervasive models comes in the form of a script created by CoinHive. If you think of the normal web-based marketing model, it serves ads on webpages to generate revenue for the site and drive customers to whomever the advertiser wants. This model, as annoying and pervasive as it is, has helped fuel the growth of the Internet. What CoinHive did was change that model. Instead of serving ads while watching content or visiting websites the script would run and use your browser as a cryptocurrency miner. This actually presents an upside and allows people who opt in to donate to charities by monetizing their CPU. Think of this as a newer version of SETI @home with a reward mechanism built in.

The problem begins to show up when one looks at how easy it is to inject malicious code into websites. Cyber criminals quickly started using these types of scripts and piggybacked on existing injection techniques. This has occurred for legitimate websites as well as for malicious ones. It got so pervasive it actually started to damage people's mobile devices.

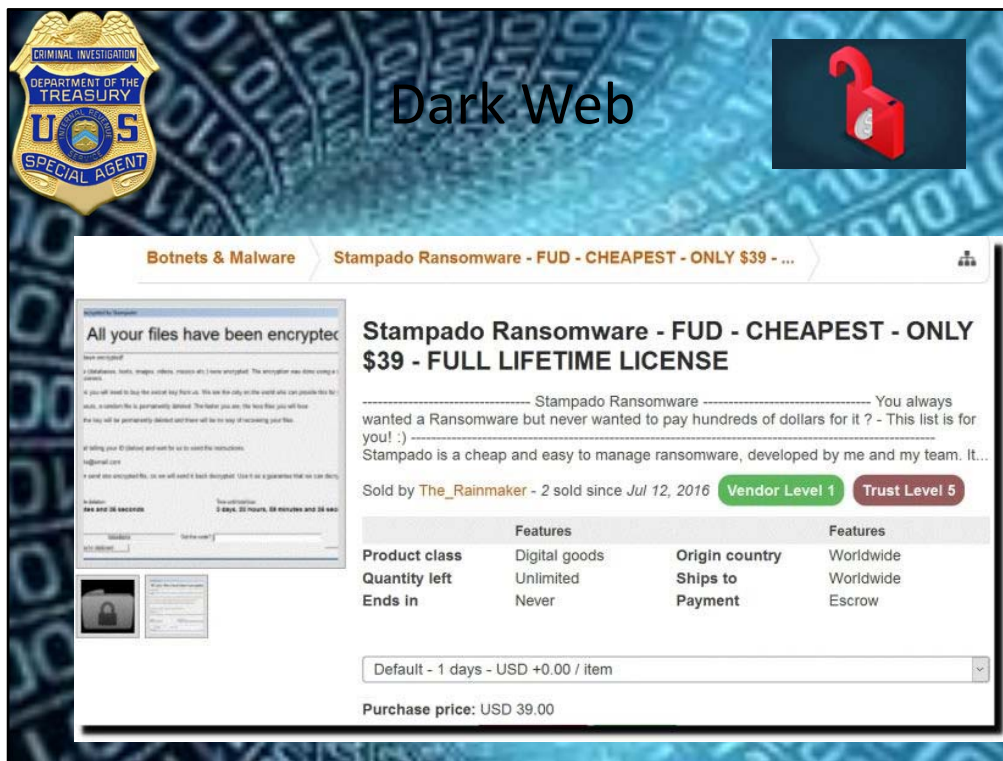
Cryptomining malware grew from there. In January 2018, researchers identified 250 unique



pieces of cryptomining malware alone. As with any other profitable malware model, the cyber criminals will continue to innovate, obfuscate, and try and evade existing endpoint prevention capabilities. The problem will persist until the model no longer becomes profitable.

Ransomware and cryptomining malware will continue to be a thing. As long as there is a profit, the cyber criminals will continue to use it as an avenue of attack. I would expect to see the same innovation and evasion we have seen from ransomware continue to evolve this next form of extortion.

Stopping this form of malware requires the same approach we've always taken to stop other pieces of malware. The intention of the malware may be different, but prevention, detection, and response remain the same.



Ransomware has become so popular, you can try it on your friends.

Users on several English and Russian language hacking forums are advertising a new twist on the practice of infecting people's computers, encrypting their files, and demanding a payment to unlock them. Instead of limiting their spread of that kind of malicious file to the people they can directly infect, some criminal software developers are now offering to custom-build a modified ransomware for you, which you would then distribute as you see fit.


Calling itself Shark Ransomware, it seems to work in principle like most ransomware, in that it affects a Windows computer, locks some files, and demands a bitcoin payment to receive a key to get them back. The software itself is free, but when someone pays, the developer automatically takes a 20 percent cut of the ransom.

The ransomware, named Stampado, gives the victim 96 hours to pay to have their computer unlocked. After 96 hours, data starts disappearing. And it's fully undetectable at this point. Until the owner pays to access his personal information, the ransomware will start deleting files at random. Eventually, if the bounty is never paid, there won't be any files left to recover.



An Internet Bot, also known as web robot, WWW robot or simply bot, is a software application that runs automated tasks (scripts) over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering (web crawler), in which an automated script fetches, analyzes and files information from web servers at many times the speed of a human. More than half of all web traffic is made up of bots.

Efforts by servers hosting websites to counteract bots vary. Servers may choose to outline rules on the behavior of internet bots by implementing a robots.txt file: this file is simply text stating the rules governing a bot's behavior on that server. Any bot interacting with (or 'spidering') any server that does not follow these rules should, in theory, be denied access to, or removed from, the affected website. If the only rule implementation by a server is a posted text file with no associated program/software/app, then adhering to those rules is entirely voluntary – in reality there is no way to enforce those rules, or even to ensure that a bot's creator or implementer acknowledges, or even reads, the robots.txt file contents. Some bots are "good" – e.g. search engine spiders – while others can be used to launch malicious and harsh attacks, most notably, in political campaigns.



**Contact Information**

**James Daniels**  
**Program Manager – Cyber Crimes**  
**IRS-Criminal Investigation**  
**James.Daniels@ci.irs.gov**  
**360-905-1142**

The background of the slide features a blue-toned tunnel of binary code (0s and 1s) receding into the distance, creating a sense of depth and digital connectivity.