Welcome to Tech Talks

Glen Maxson
Center for Learning in Retirement
Spring 2018 – Session 7 of 8
Seniortechadvisor.com

What we'll cover in 6 weeks

1) ~~Computers & Operating Systems~~
2) ~~Applications & The Cloud~~
3) ~~The Internet, The Web & Social Media~~
4) ~~Security & Privacy~~
5) ~~Entertainment & Education~~
6) ~~Blogging, Self-Publishing & Internet of Things (IoT)~~
7) Cryptocurrency
8) Tech Book Reviews

Cryptocurrency – What is it?

- A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.
- Cryptocurrencies are a type of digital currencies, alternative currencies and virtual currencies.
- Cryptocurrencies use decentralized control as opposed to centralized electronic money and central banking systems.
- The decentralized control of each cryptocurrency works through a blockchain, which is a public transaction database, functioning as a distributed ledger.

Bitcoin

- Bitcoin, created in 2009, was the first decentralized cryptocurrency. Since then, numerous other cryptocurrencies have been created. These are frequently called **altcoins**.
- The aim of Bitcoin was to create a **cryptographically secure currency that could be used as a form of universal cash** and replace all forms of fiat currency in the world.
- What was not expected was that because Bitcoin code was open source, people could create their own version of Bitcoin by replicating and tweaking the code to suit their own needs, in essence starting a new cryptocurrency.

How does it work - the basics?

- **Cryptocurrency can be thought of as a digital currency like PayPal or bank credit**
- **There are many other cryptocurrencies beyond Bitcoin**
- Unlike bank credit, **cryptocurrency is decentralized and thus not centrally controlled**.
- **Instead of a central power controlling cryptocurrency, an algorithm and users themselves control cryptocurrency**.
  - The algorithm dictates how transactions work and how new coins are created, users create peer-to-peer transactions, which are recorded on a public digital ledger.
- **Those who confirm transactions by breaking cryptographic codes are called miners**. Mining is a process that creates new coins.
- **But all you really need to do is set up a Coinbase account and use that to buy and sell Bitcoin, Ether, or Litecoin and to send and receive cryptocurrency**.
  - And remember to pay your taxes.

How does cryptocurrency work?

- Transactions are sent between peers from “cryptocurrency wallets” by matching up public codes which relate back to user-held private passwords (cryptographic “keys”).
- Transactions made between peers are recorded on a public ledger of transactions called a “blockchain.” All users of a given cryptocurrency have access to the ledger if they choose to download a “full node” wallet (as opposed to holding their coins in a third party wallet like Coinbase).
- The transaction amounts are public, but who sent the transaction is encrypted. Each transaction leads back to a digital “cryptocurrency wallet.” Whoever owns the password (or key) to the wallet, owns the amount of cryptocurrency denoted on the ledger.
- When someone sends or receives cryptocurrency, when they send from one wallet to another wallet using a set of private and public passwords, that transaction is queued up to be added to the ledger. Many transactions are added to a ledger at once.
- These “blocks” of transactions are added sequentially. That is why the ledger and the technology behind it are called “block” “chain.” It is a “chain” of “blocks” of transactions.

How does blockchain work?

- When a peer-to-peer cryptocurrency transaction is made, that transaction is sent out to all users with “full node” wallets.
- Specific types of users called miners then try to solve a cryptographic puzzle (using software) which lets them add a “block” of transactions to the ledger. Whoever solves the puzzle first gets a few “newly mined” coins as a reward. Sometimes miners pool computing power and share the new coins.
- The algorithm relies on consensus. If the majority of users trying to solve the puzzle all submit the same transaction data, then it confirms that the transactions are correct.

What is cryptocurrency mining?

- People who are running software and hardware aimed at confirming transactions to the digital ledger are cryptocurrency miners.
- Solving cryptographic puzzles (via software) to add transactions to the ledger (the blockchain) in the hope of getting coins as a reward is cryptocurrency mining.

- Cryptocurrency mining in Iceland is using so much energy, the electricity may run out

Where did it come from?

- There have been many attempts at creating a digital currency during the 90s tech boom, with systems like Flooz, Beenz and DigiCash emerging on the market but inevitably failing. There were many different reasons for their failures, such as fraud, financial problems and even frictions between companies' employees and their bosses.
- Notably, all of those systems utilized a Trusted Third Party approach, meaning that the companies behind them verified and facilitated the transactions. Due to the failures of these companies, the creation of a digital cash system was seen as a lost cause for a long while.
- Then, in early 2009, an anonymous programmer or a group of programmers under an alias Satoshi Nakamoto introduced Bitcoin. Satoshi described it as a 'peer-to-peer electronic cash system.' It is completely decentralized, meaning there are no servers involved and no central controlling authority. The concept closely resembles peer-to-peer networks for file sharing.

Who is Satoshi Nakamoto?

- ***Satoshi Nakamoto*** *is the name used by the unknown person or people who designed bitcoin and created its original reference implementation. As part of the implementation, they also devised the first blockchain database. In the process they were the first to solve the double-spending problem for digital currency.*
- *The 'creator' of Bitcoin,* ***Satoshi Nakamoto****, is the world's most elusive billionaire (worth more than $7B as of November 2017). Very few people outside of the Department of Homeland Security know Satoshi's real name. In fact, DHS will not publicly confirm that even THEY know.*
- WIRED has obtained the strongest evidence yet of **Satoshi Nakamoto's** true identity. The signs point to Craig Steven Wright, a man who never even made it onto any Nakamoto hunters' public list of candidates, yet fits the cryptocurrency creator's profile in nearly every detail.

[Interview]

Interesting Note: The ***satoshi*** *is currently the smallest unit of the bitcoin currency recorded on the block chain. It is a one hundred millionth of a single bitcoin (0.00000001 BTC). The unit has been named in collective homage to the original creator of Bitcoin,* ***Satoshi*** *Nakamoto.*

What can I do with it?

- In the past, trying to find a merchant that accepts cryptocurrency was extremely difficult, if not impossible. These days, however, the situation is completely different.
- There are a lot of merchants - both online and offline - that accept Bitcoin as the form of payment. They range from massive online retailers like Overstock* and Newegg to small local shops, bars and restaurants. Bitcoins can be used to pay for hotels, flights, jewelry, apps, computer parts and even a college degree.
- Other digital currencies like Litecoin, Ripple, and Ethereum aren't accepted as widely yet. But things are changing, with Apple having authorized at least 10 different cryptocurrencies as a viable form of payment on App Store.
- Users of cryptocurrencies other than Bitcoin can always exchange their coins for BTCs. Moreover, there are Gift Card selling websites like Gift Off, which accepts around 20 different cryptocurrencies. Through gift cards, you can essentially buy anything with cryptocurrency.

The Overstock Problem

- Retailer Overstock mixed up bitcoin and bitcoin cash, letting customers buy items at a steep discount

  Bitcoin vs. Bitcoin Cash: What's the Difference?

  - Bitcoin is a cryptocurrency that exists within a network of computers, within the blockchain. This is ledger-recording technology. The problem with this technology is that it's slow.
  - Bitcoin Cash is a hard fork from Bitcoin and is effectively a new currency. It has an increased block size of 8mb to accelerate the verification process, with an adjustable level of difficulty to ensure the chain's survival and transaction verification speed, regardless of the number of miners supporting it.
  - As of 3/23/2018, Bitcoin is worth $8896 and Bitcoin Cash is worth $1010 per coin.

Where can I get some?

How to Buy Your First Cryptocurrency Coin

- Buying cryptocurrency is confusing for a lot of people. It's not a stock or a typical "investment." It's not like anything most people have ever seen or experienced. You don't get shares; instead you get digital coins or tokens.
- For most people in the U.S., Coinbase would be the easiest option to buy Ethereum, Bitcoin, or Litecoin. After verifying your account, you can add a number of payment methods including credit or debit cards, U.S. bank accounts, or even wire transfers of funds. Other options for exchanges that will take U.S. dollars for coins are Kraken, and Gemini in the U.S
- If you are looking for some of the newer coins like NEO that are making big movement but haven't made their way to the aforementioned exchange sites, you can look into Bittrex, Poloniex or Livecoin. You can transfer Bitcoin or Ethereum to these platforms from Coinbase and then exchange it for any other digital currency that you want.

Buying Cryptocurrency With Coinbase

- If you're interested in buying Bitcoin or one of the other better-known cryptocurrencies your best bet is CoinBase, which also supports Bitcoin Cash, Ether, and Litecoin. The popular digital exchange is easy to use and widely trusted, though it does go offline occasionally when trading is particularly frenzied.
- You can download the Coinbase app on your phone or create an account at coinbase.com. Agree to the terms and you'll be greeted by a chart showing the recent rise and fall of Bitcoin and other currencies. The next thing you'll need to do is add a way to make purchases by tapping the "Buy" button on the app or clicking over to the Buy/Sell tab on the website. From here, you can connect a debit or credit card for quick small investments, or add a direct line to your bank account for larger purchases.
- Hit the Buy button again. Pick the type of cryptocurrency you're buying and enter the amount of money you want to spend in U.S. Dollars. You'll see how much that comes to in Bitcoin (or whatever cryptocurrency you're buying) along with a small fee from Coinbase. Finally, confirm the transaction by hitting the Buy button and you're done. (If this is the first time, you may get a call from your bank asking to verify the purchase before it goes through.)

Buying Cryptocurrency Without Coinbase

- If you want to buy Ripple or one of the other up-and-coming cryptocurrencies, you'll have to look beyond Coinbase. One popular option is Kraken, which supports Bitcoin and Ether, along with smaller currencies like Ripple and Stellar.
- Using Kraken is a little more complicated than Coinbase, and you'll want to do it through the website. The first thing you need to do is setup an account here. Once it's active, click on Account and pick Get Verified. You'll need to provide your name, phone number and address by selecting Tier 2 at the very least. You may also need a valid government-issued photo ID and proof of residence (that's Tier 3) to actually withdraw money from the exchange, depending on where you and your bank are located:
- Next, you'll need to deposit money into your Kraken account. To do this, go to Account, then Funding, and then Deposit. From here, follow the directions on Kraken's website to activate a wire transfer before sending the money over from your bank account.
- Now you're ready to buy. Click on Account, then Trade, and then New Order. Then pick the cryptocurrency you want and the government-backed currency you're using to buy it from the drop down menu in the top right corner (you can also use Bitcoin to buy smaller currencies like Ripple). Select Simple and under that click on Buy. Then enter the amount you want of whatever cryptocurrency you're buying and hit the green button to confirm.

Where can I store it safely?

- Unlike most traditional currencies, cryptocurrencies are digital, which entails a completely different approach, particularly when it comes to storing it. Technically, you don't store your units of cryptocurrency; instead it's the private key that you use to sign for transactions that need to be securely stored.
- There are several different types of cryptocurrency wallets that cater for different needs. If your priority is privacy, you might want to opt for a paper or a hardware wallet. Those are the most secure ways of storing your crypto funds. There are also 'cold' (offline) wallets that are stored on your hard drive and online wallets, which can either be affiliated with exchanges or with independent platforms.
- *Bitcoin Wallets for Beginners: Everything You Need to Know*

What is a wallet?

- Cryptocurrency wallets are software programs that store your public and private keys and interface with various blockchain so users can monitor their balance, send money and conduct other operations.
- When a person sends you Bitcoins or any other type of digital currency, they are essentially signing off ownership of the coins to your wallet's address.
- To be able to spend those coins and unlock the funds, the private key stored in your wallet must match the public address the currency is assigned to. If public and private keys match, the balance in your digital wallet will increase, and the senders will decrease accordingly.
- The transaction is signified merely by a transaction record on the blockchain and a change in balance in your cryptocurrency wallet

Different types of wallets

- Wallets can be broken down into three distinct categories – software, hardware, and paper.
- (Software) **Desktop** wallets are downloaded and installed on a PC or laptop. They are only accessible from the single computer in which they are downloaded.
- (Software) **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 and theft.
- (Software) **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.
- **Hardware** wallets differ from software wallets in that they store a user's private keys on a hardware device like a USB dongle. Although hardware wallets make transactions online, they are stored offline which delivers increased security. Users simply plug in their device to any internet-enabled computer or device, enter a pin, send currency and confirm.
- **Paper** wallets are easy to use and provide a very high level of security. The term refers 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. Or 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 is referred to as **'sweeping.**'

Oops

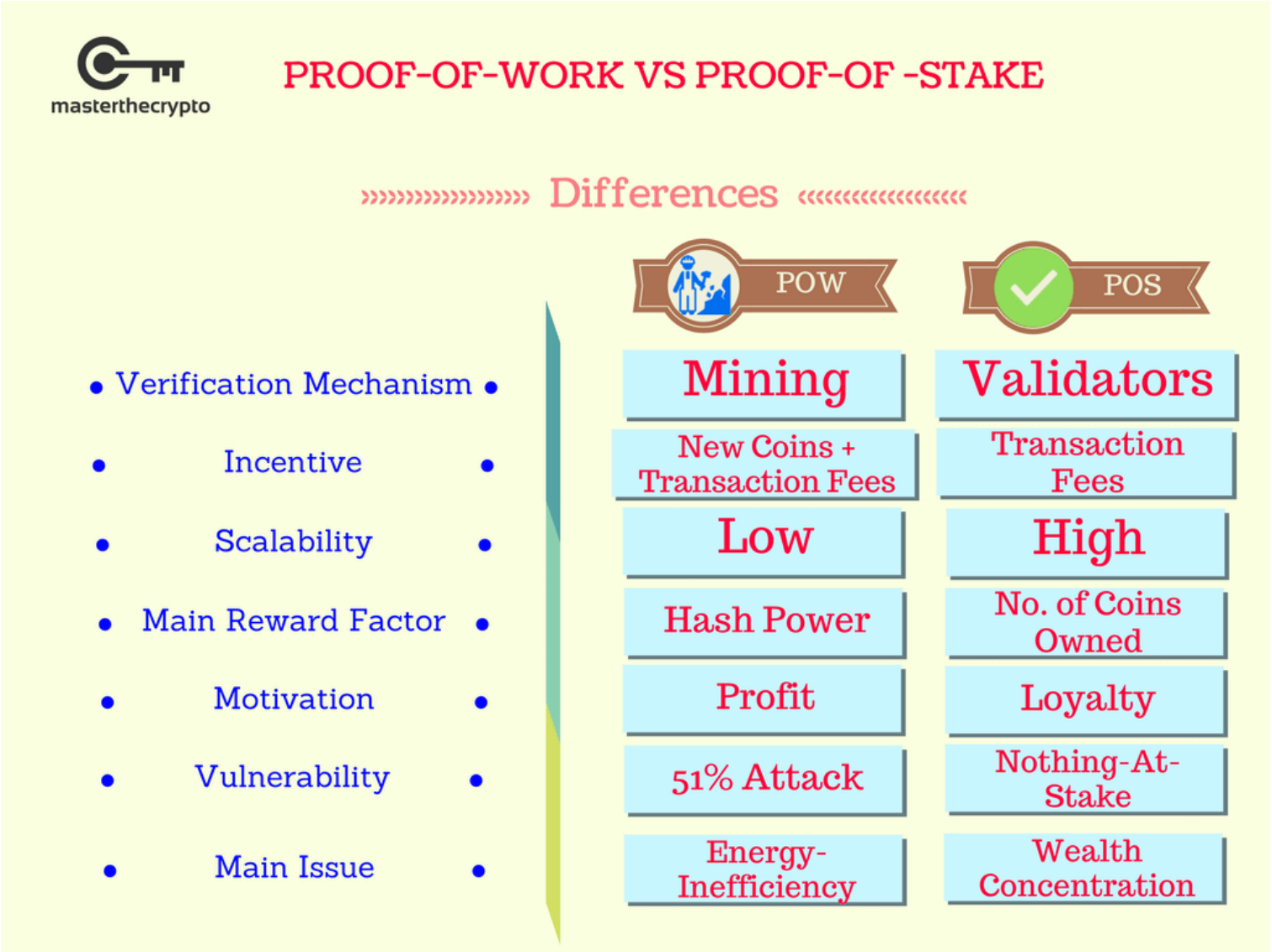
- *A British man says he accidentally threw away over $80 million (now $65 mil) worth of bitcoin.*
  - *James Howells, an IT worker from Newport, claims to have unintentionally dumped 7,500 bitcoin in mid-2013.*
  - *He is now planning to find them, but isn't sure how, as he believes the hard drive he saved them to is currently buried in a landfill site.*
  - *The value of the cryptocurrency was around $130 at the time Howells claims to have thrown the hard drive away. It is currently worth $8,631*.*
  - *That means the bitcoin stored on the hard drive would have been worth around $975,000 at the time the device is said to have been ditched. Today, they would be worth $64,732,500.00.*

*Price-check 3/23/18 – his Bitcoin was worth $143,811,750 at its peak on Dec. 17, 2017

Trends

- **The rise of stablecoins** – pegging the value to the US dollar
- **Consumer accessibility and participation increase in the crypto market** – ex. Cointal
- **Application to traditional B2B markets** – ex. NewEra
- **Inflow of institutional money into crypto** – Goldman trading desk
- **More forks** (IFOs – Initial Fork Offerings) – ex. Bitcoin Cash*
- **More ICOs** (Initial Coin Offerings), reduction in 'scamcoins'
- **Major players enter** – Square, Microsoft Azure, IBM
- **More regulation and taxes** – think FIFO*
- **Privacy coins** – Monero, Zcash, Dash, Verge and PIVX
- **Advertising** – 'in-browser mining', new advertising platforms like BAT
- **Banks scramble to catch up** – people storing wealth in crypto
- **Rise of DEX** (Decentralized Exchange) like GDAX, Bittrex, and Poloinex. Supports 3rd party-less transaction.
- **The DApp Revolution -** "decentralized apps" for Ethereum and other platforms build on craze CryptoKitties started.
- **POW To POS -** shift from Proof of Work (requires lots of power) to Proof of Stake.

PoW vs PoS


masterthecrypto
PROOF-OF-WORK VS PROOF-OF -STAKE
Differences
POW
POS
Verification Mechanism
Mining
Validators
Incentive
New Coins + Transaction Fees
Transaction Fees
Scalability
Low
High
Main Reward Factor
Hash Power
No. of Coins Owned
Motivation
Profit
Loyalty
Vulnerability
51% Attack
Nothing-At-Stake
Main Issue
Energy-Inefficiency
Wealth Concentration

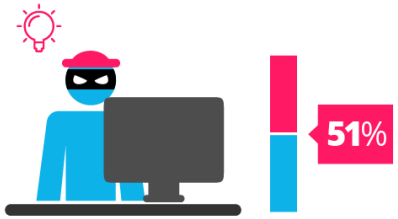
PoW vs PoS

The Ethereum community and its creator, Vitalik Buterin, are planning to do a hard fork to make a transition from proof of work to proof of stake.

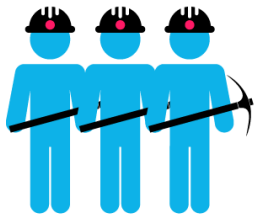
Reason: Miners need a lot of energy. One Bitcoin transaction requires the same amount of electricity as powering 1.57 American households for one day (data from 2015).

Proof of Work vs Proof of Stake

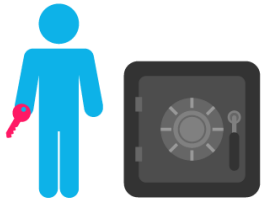
proof of work is a requirement to define an expensive computer calculation, also called mining



A reward is given to the first miner who solves each blocks problem.



Network miners compete to be the first to find a solution for the mathematical problem



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

The PoS system there is no block reward, so, the miners take the transaction fees.

Proof of Stake currencies can be several thousand times more cost effective.

Issues (to list just a few)

- **Bitcoin blockchain size problem** – limits # of transactions the network can process
- **Price manipulation/collusion** – "whales" contribute most to excessive volatility
- **Pump and dump ICO schemes** – token speculation at ICO drives prices up then cash out
- **Cybercrime** – defending against hackers and heists adds inefficiency, and loss has little chance of recovery
- **Lack of price uniformity** – price charting across exchanges is problematic, volatility doesn't help
- **Transaction delays** – delays from opening a trading account through to making deposits and withdrawals
- **Spoofing payment information and phishing** – malware and phishing work much as they do with e-money
- **Hacking a payment gateway** - Ethereum Classic Web wallet example
- **User address error** - with Ethereum, if the last digit of the address wasn't copied, the money would disappear into thin air
- **Loss of wallet file*** - wallet files on computers can be stolen using malware or lost if the hard disk crashes
- **Insecure ICOs** – no market regulation, no guarantee of RoI
- **Cryptojacking** – use of botnets to mine cryptocurrency with your browser, computer, router, security camera…
- **Anonymity and criminal activity** – cryptocurrency allows bad guys to collect in ways that make them less likely to be identified

The 'Everything' problem -*Welcome to the new cryptocurrency boom, a roiling, boiling mess of speculation, broken transactions, and confusion. And that's just how the crypto lovers like it.*

Tips for cryptocurrency holders and crypto-investors

- Always verify a Web wallet's address, and don't follow links to an Internet bank or Web wallet.
- Before sending, double-check the recipient's address, the amount being sent, and the associated fee.
- Write down a mnemonic phrase that allows you to recover a cryptowallet if you lose it or forget your password.
- Keep a cool head and make informed decisions when crypto-investing, and don't panic or hurry.
- Always remember that crypto-investment is very risky. Do not invest more than you're ready to lose at any moment. Diversify.
- Use cryptocurrency hardware wallets.
- Run high-quality antivirus protection to protect the devices you use to access cryptowallets, trade on crypto-exchanges.
- Backup your wallet. Store only small amounts of currency for everyday use online, on your computer or mobile. Use offline storage options for backup like Ledger Nano or paper or USB.
- Update software. Keep your software up to date so that you have the latest security enhancements available. You should regularly update not only your wallet software but also the software on your computer or mobile.
- Add extra security layers. The more layers of security, the better. Setting long and complex passwords and ensuring any withdrawal of funds requires a password is a start. Use wallets that have a good reputation and provide extra security layers like two-factor authentication and pin code requirements every time a wallet application gets opened. You may also want to consider a wallet that offers multisig transactions like Armory or Copay.

Futures

- Bill Gates, co-founder of Microsoft, investor and philanthropist:
  - *"Bitcoin is exciting because it shows how cheap it can be. Bitcoin is better than currency in that you don't have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient." [SOURCE]*
- Richard Branson, founder of Virgin Galactic and more than 400 other businesses:
  - *"Well, I think it is working. There may be other currencies like it that may be even better. But in the meantime, there's a big industry around Bitcoin. — People have made fortunes off Bitcoin, some have lost money. It is volatile, but people make money off of volatility too." [SOURCE]*
- Al Gore, former Vice President of the United States:
  - *"When Bitcoin currency is converted from currency into cash, that interface has to remain under some regulatory safeguards. I think the fact that within the Bitcoin universe an algorithm replaces the function of the government …[that] is actually pretty cool." [SOURCE]*
- Eric Schmidt, executive chairman of Google:
  - *"[Bitcoin] is a remarkable cryptographic achievement… The ability to create something which is not duplicable in the digital world has enormous value…Lot's of people will build businesses on top of that." [SOURCE]*
- Peter Thiel, co-founder of PayPal:
  - *"PayPal had these goals of creating a new currency. We failed at that, and we just created a new payment system. I think Bitcoin has succeeded on the level of a new currency, but the payment system is somewhat lacking. It's very hard to use, and that's the big challenge on the Bitcoin side." [SOURCE]*

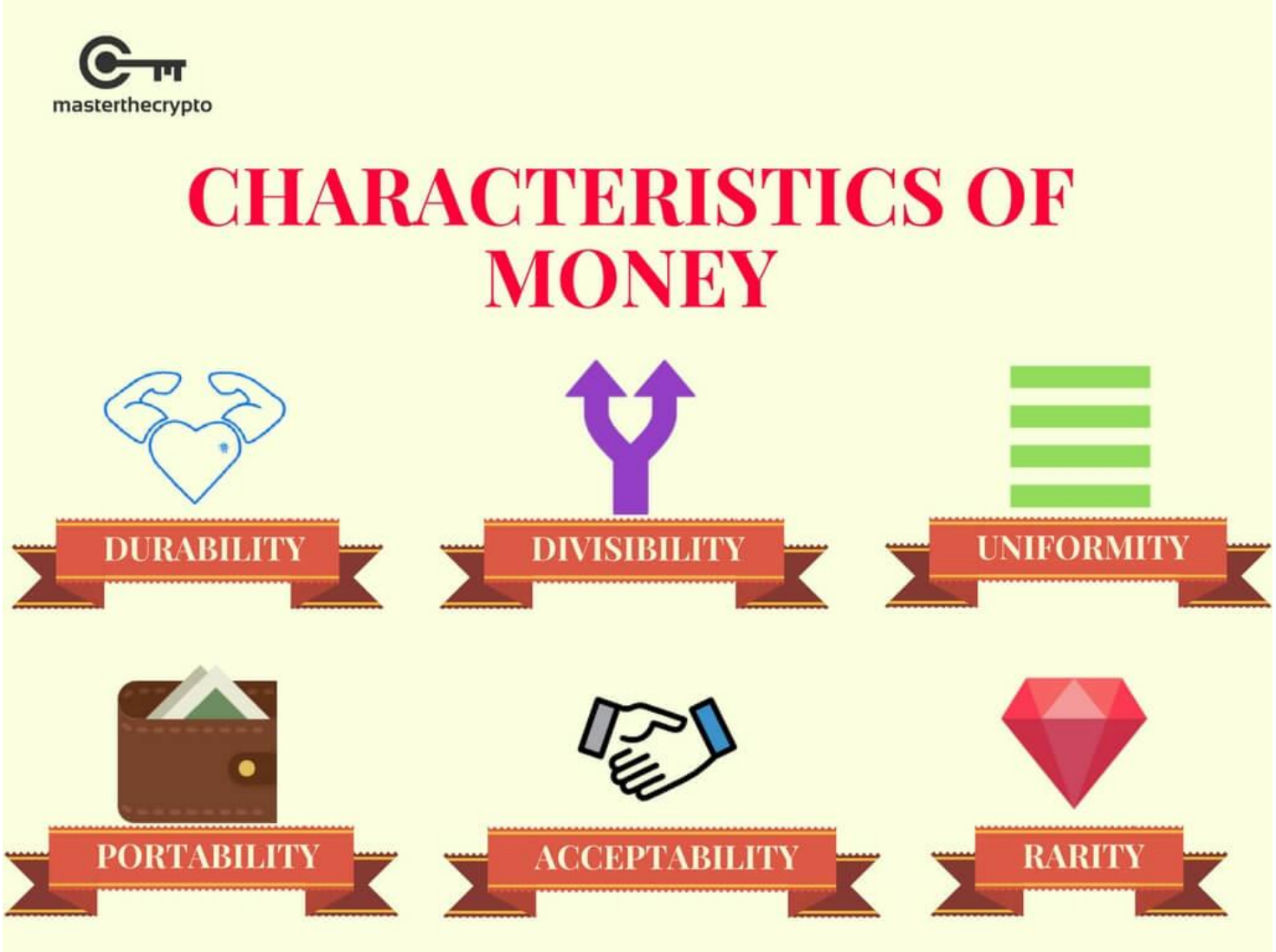
Legality

- As cryptocurrencies are becoming more and more mainstream, law enforcement agencies, tax authorities and legal regulators worldwide are trying to understand the very concept of crypto coins and where exactly do they fit in existing regulations and legal frameworks.
- With the introduction of Bitcoin, the first ever cryptocurrency, a completely new paradigm was created. Decentralized, self-sustained digital currencies that don't exist in any physical shape or form and are not controlled by any singular entity were always set to cause an uproar among the regulators.
- A lot of concerns have been raised regarding cryptocurrencies' decentralized nature and their ability to be used almost completely anonymously. The authorities all over the world are worried about the cryptocurrencies' appeal to the traders of illegal goods and services. Moreover, they are worried about their use in money laundering and tax evasion schemes.
- As of November 2017, Bitcoin and other digital currencies are outlawed only in Bangladesh, Bolivia, Ecuador, Kyrgyzstan and Vietnam, with China and Russia being on the verge of banning them as well. Other jurisdictions, however, do not make the usage of cryptocurrencies illegal as of yet, but the laws and regulations can vary dramatically depending on the country.

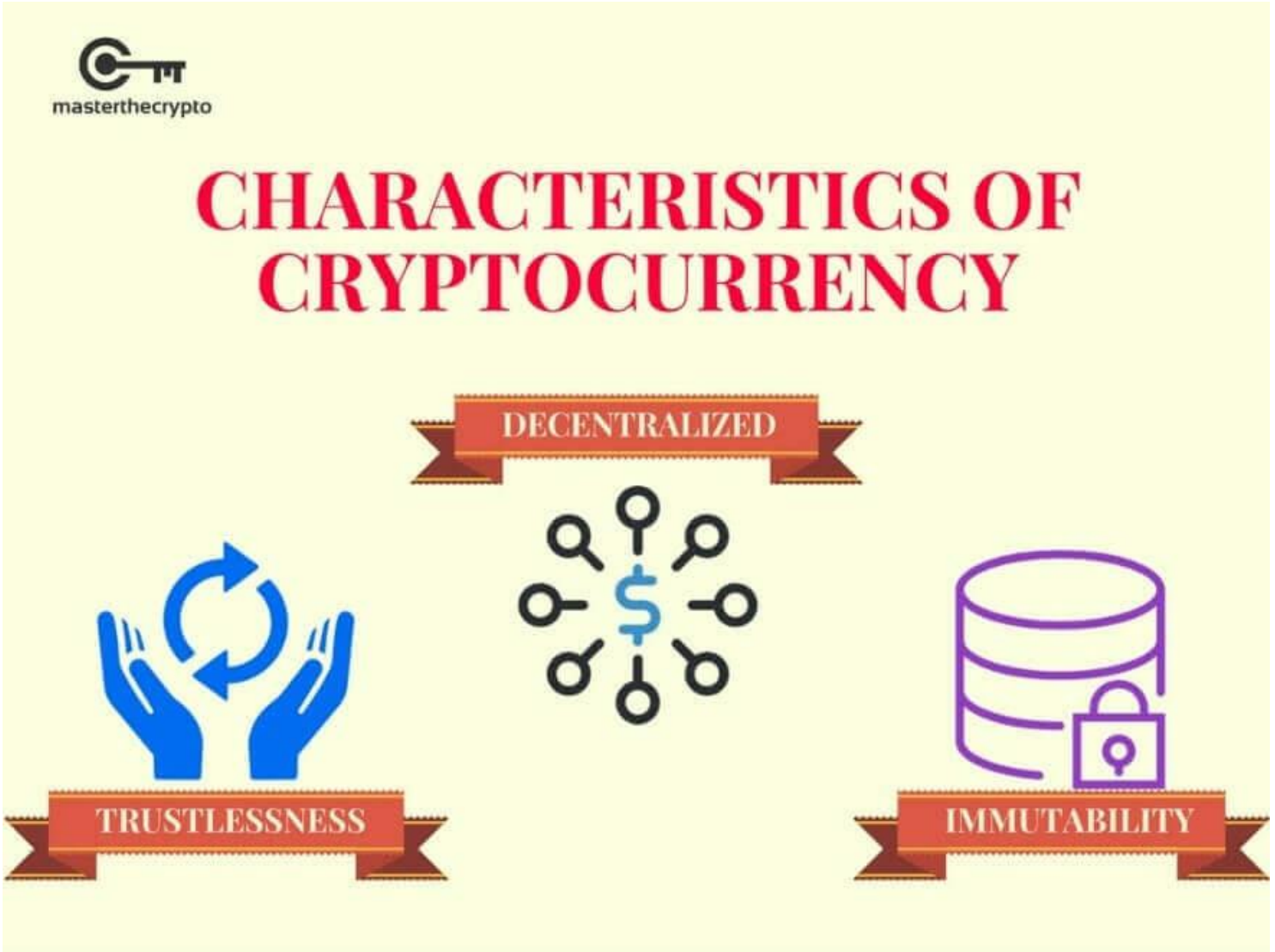
Taxes (get complicated)

- **No free lunch -** If you earn money by investing in cryptocurrencies, you likely have to pay taxes. Like it is with everything else.
- **The Good News -** Like with every other financial product you don't need to pay VAT when selling Bitcoin. And in some jurisdictions you have to pay nearly no taxes. Amazingly Germany, a country usually known for very high tax rates, has become a tax haven for cryptocurrencies. Like the USA and many other countries, Germany considers Bitcoin not a financial product, but a property. This means that if you earn money by trading it, you don't pay a flat tax for financial income – which is 25 percent, for example for bank account interest – but you have to tax the profit of buying and selling cryptocurrencies like income.
- However, there is a loophole. If you hold your coins for more than 1 year, you don't need to pay taxes at all when you sell it. This rule was added to dis-incentivize day trading of other properties and stabilize prices by incentivizing holders. For cryptocurrencies it made Germany, and also the Netherlands, which apply the same rules, to tax havens. Some countries might have similar rules.
- One problem the one year rule poses is that you need to prove that you hold the crypto for this timeframe. Usually, exchanges can help you with prints of your trade history. Also, you can use the public blockchain as a proof of storage. In most cryptocurrencies, it is transparent when coins are received and spent by a particular address. But not in all. For example, Monero uses Ring Signatures and Confidential Transactions, which are great tools to maintain anonymity. But the downside is that they make it more or less impossible to prove that you hold coins more than one year. Maybe you take this into account when selecting coins for your portfolio.
- **The Bad News -** If you use a good exchange and keep track of your trades, taxing Bitcoin is possible, but also a pain. You need to calculate every single profit, not just from trading, but also from using Bitcoins to pay for things.
- But that's just the beginning. Things become really a complicated nightmare if it comes to Altcoins. For the tax authorities, an Altcoin counts like Bitcoin. In most countries, this means it is not a financial product, but a property. If you buy it with Bitcoin and sell it for Bitcoin, you have to tax the difference, but not in Bitcoin, but in Dollar or your national paper money. This means, you not only need to keep track of all your Altcoin trades, but you also need to take into account the price of Bitcoin when buying and selling.

Money


masterthecrypto
CHARACTERISTICS OF MONEY
DURABILITY
DIVISIBILITY
UNIFORMITY
PORTABILITY
ACCEPTABILITY
RARITY

Crypto


masterthecrypto
CHARACTERISTICS OF CRYPTOCURRENCY
DECENTRALIZED
TRUSTLESSNESS
IMMUTABILITY

Crypto Features

- **Trustlessness:** In the case of fiat, you need to trust a third party to guarantee the value of your money by not debasing it. The buyer or seller of goods and services in the transaction must make the same assumptions you do. Cryptocurrency removes this need to trust someone by incentivizing every actor in the network to not debase the currency and not commit fraud.
- **Decentralization:** With banks and governments, the supply and creation of money through mints and interest rates are at their sole discretion. Users of the currency they control are at their mercy. With cryptocurrency no individual or consortium is able to affect the supply of currency or exert significant influence over it without the approval of the majority. Even if there is majority approval, minorities are free to “fork” away and administer their own version of the currency.
- **Immutability:** When we want to check how money has been removed from our bank accounts, we are able to refer to our transaction history with the bank. However, doing so implies a few things:
  - That we trust the bank does not fabricate false transactions and manipulate our money
  - That we trust the bank delivers outgoing transactions to our intended recipients
  - That the bank employs sufficient security to ensure that other parties are not able to make these transactions on our behalf. When the element of trust and centralization is removed from the equation, however, there is no longer any party to trust to do this. As a result, records need to be made public and unchangeable. The cryptographically secure nature of cryptocurrency ensures that while it is not impossible to change the transaction ledger, it is extremely difficult and would require you to oppose the entire network of cryptocurrency users.

Videos

- Bitcoin: How Cryptocurrencies Work – YouTube
- Top 3 Cryptocurrency to Invest in 2017 – YouTube
- The Biggest Opportunity In Cryptocurrency – Video
- How to Play Bitcoin & Cryptocurrency in Your Trading Strategy
- Bitcoin, Blockchain & Cryptocurrency Videos
- Long Live Dogecoin: Why Developers Won't Let the Joke Currency

Sources

- What is Cryptocurrency. Guide for Beginners
- Cryptocurrency
- 10 Incredible Uses for Cryptocurrency and Blockchain You Probably Haven't Thought of
- How Does Cryptocurrency Work?
- How Does Cryptocurrency Work? (for Beginners)
- Cryptocurrency and E-money: How does the transaction work?
- How to Buy Cryptocurrency
- How to Buy Your First Cryptocurrency Coins (Ethereum, Bitcoin, Litecoin, and NEO)

Sources

- How To Invest in Cryptocurrencies: The Ultimate Beginners Guide
- Cryptocurrency Wallet Guide: A Step-By-Step Tutorial
- Evolution of Cryptocurrency: The Problem With Money Today
- Evolution of Cryptocurrency: What is Cryptocurrency?
- What are the regulatory issues facing cryptocurrency developers?
- Cryptocurrencies have an everything problem
- Major Problems in the Cryptocurrency Market
- Problems and risks of cryptocurrencies
- 4 Cryptocurrency Trends to Watch in 2018

Sources

- How Two Unexpected Factors Will Drive What's Next In Cryptocurrency Trends
- Looking Ahead: 12 Cryptocurrency Trends Ready To Explode In 2018
- Cryptocurrency like bitcoin is easy money for criminals
- Misc References https://charts.bitcoin.com/
  - bitcoin and blockchain: what math puzzle do miners actually solve? example with real transactions
  - Cryptocurrency mining in Iceland is using so much energy, the electricity may run out
  - Scientists at Russian nuclear research facility arrested for mining cryptocurrency
  - South Korea Responds To Cryptocurrency Petition
  - 'Satoshi' Craig Wright Is Being Sued for $10 Billion
  - Uber co-founder Garrett Camp is creating a new cryptocurrency
  - Bitcoin Resources

Recent Articles

- Wyoming Takes Another Step To Become the Cryptocurrency Capital of America
- President Trump Prohibits US Exchange of Venezuelan Cryptocurrency Petro
- Cryptocurrencies Featured In Congressional Report
- No, The Mt. Gox Sell-Off is Not to Blame for Market Dip
- This year's SXSW was all about blockchain dreamers, cryptocurrency scammers, and everything in between
- BlockCAT Launches "Error-Proof" Ether Transactions With Tabby Pay
- Bitcoin Drops to Month Low After Google Bans Crypto Advertisements
- PayPal CEO Says Cryptocurrencies Are Just an Experiment for Now
- Reaction to Turbulent Week in Crypto Markets
- Japan to punish several cryptocurrency exchanges: sources
- Want To Make Millions? Copy Someone's Cryptocurrency Project
- This Is What Happens When Bitcoin Miners Take Over Your Town
- Bitcoin Is Ridiculous. Blockchain Is Dangerous
- Japan to punish several cryptocurrency exchanges: sources
- CryptoKitties Come of Age With $12 Million in Venture Funding
- Santander Partners With Ripple to Create a New Cross-Border Payment App

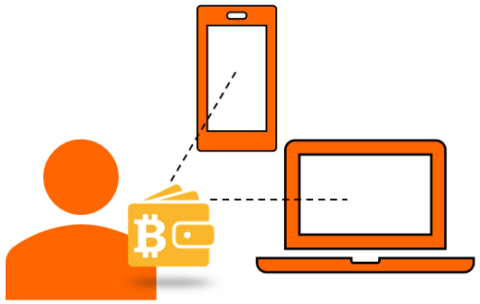
Wallets

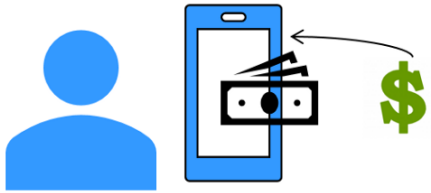
- As with any other investment, you need to pay close attention to the cryptocurrencies' market value and to any news related to them. **Coinmarketcap** is a one-stop solution for tracking the price, volume, circulation supply and market cap of most existing cryptocurrencies.
- Depending on a jurisdiction you live in, once you've made a profit or a loss investing in cryptocurrencies, you might need to include it in your tax report. In terms of taxation, cryptocurrencies are treated very differently from country to country. In the US, the Internal Revenue Service ruled that Bitcoins and other digital currencies are to be taxed as property, not currency. For investors, this means that accrued long-term gains and losses from cryptocurrency trading are taxed at each investor's applicable capital gains rate, which stands at a maximum of **15 percent.**

Terms

- **Public Ledger**: All confirmed transactions from the start of a cryptocurrency's creation are stored in a public ledger. The identities of the coin owners are encrypted, and the system uses other cryptographic techniques to ensure the legitimacy of record keeping. The ledger ensures that corresponding "digital wallets" can calculate an accurate spendable balance. Bitcoin calls this public ledger a "transaction block chain."
- **Transaction**: A transfer of funds between two digital wallets is called a transaction. That transaction gets submitted to a public ledger and awaits confirmation. When a transaction is made, wallets use an encrypted electronic signature (an encrypted piece of data called a cryptographic signature) to provide a mathematical proof that the transaction is coming from the owner of the wallet. The confirmation process takes a bit of time (ten minutes for bitcoin) while "miners" mine. Mining confirms the transactions and adds them to the public ledger.
- **Mining**: Mining is the process of confirming transactions and adding them to a public ledger. To add a transaction to the ledger, the "miner" must solve an increasingly-complex computational problem (like a mathematical puzzle). Mining is open source so that anyone can confirm the transaction. The first "miner" to solve the puzzle adds a "block" of transactions to the ledger. Once a block is added to the ledger, all correlating transactions are permanent, and they add a small transaction fee to the miner's wallet (along with newly created coins). The mining process is what gives value to the coins and is known as a proof-of-work system.

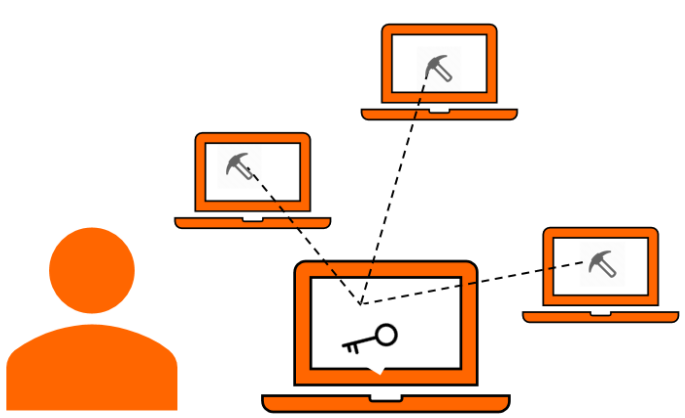
Transaction begins: Bitcoin vs E-money

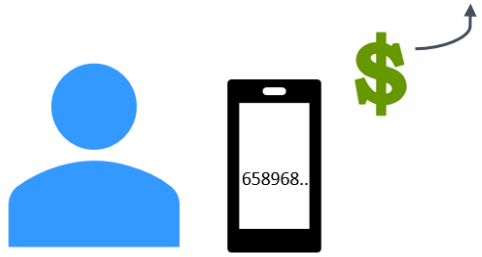




- Bitcoin — User goes to an online exchange to convert fiat currency for Bitcoin and stores them in a Bitcoin wallet.
- E-money — User exchanges e-money for an equal amount of e-value stored, for example in a mobile wallet.

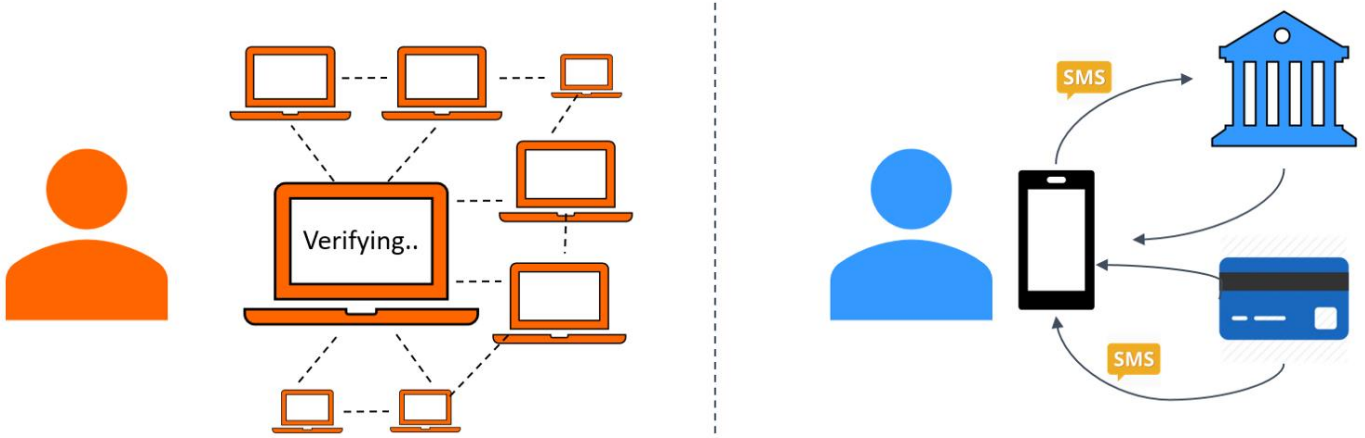
Submitting Payments: Bitcoin vs E-money





- Bitcoin — A request is sent to the Bitcoin network in order to make a purchase. Currently, there are many online merchants accepting Bitcoin such as overstock.com, Expedia, Newegg, Microsoft...
- E-money — The value of money to be transferred and the recipient's phone number are entered. The money transfer is sent.

Verifying Transactions: Bitcoin vs E-money



- Bitcoin — Bitcoin's decentralized peer-to-peer network of "miners" maintains a master ledger- a blockchain, to verify every transaction. It takes an average of 10 minutes to verify. Upon verification, data is broadcast to all users and the ledger is updated.
- E-money — User receives an SMS to verify the mobile transaction. The e-money issuer maintains records of all transactions and customer balances.

Investing

- Many people believe that cryptocurrencies are the hottest investment opportunity currently available. Indeed, there are many stories of people becoming millionaires through their Bitcoin investments. Bitcoin is the most recognizable digital currency to date, and in 2016 BTC was valued at $800. This year (2018) it's settled out around $11,000 per bitcoin, after hitting a peak of $19,200 December 2017and a recent low of $7000 on Feb. 6, 2018.
- **What's the current value of Bitcoin?**
- Ethereum, perhaps the second most valued cryptocurrency, has recorded the fastest rise a digital currency ever demonstrated. Since May 2016, its value increased by at least 2,700 percent. When it comes to all cryptocurrencies combined, their market cap soared by more than 10,000 percent since mid-2013. May 2016 Ethereum was valued at around $12 USD, and today is ~$900 after hitting a peak close to $1400 in January 2018.
- Cryptocurrencies are high-risk investments. Their market value fluctuates like no other asset's. Moreover, it is partly unregulated, there is always a risk of them getting outlawed in certain jurisdictions and any cryptocurrency exchange can potentially get hacked.
- If you decide to invest in cryptocurrencies, Bitcoin is obviously still the dominant one. However, in 2017 its share in the crypto-market has quite dramatically fallen from 90 percent to just 40 percent. There are many options currently available, with some coins being privacy-focused, others being less open and decentralized than Bitcoin and some just outright copying it.
- While it's easy to buy Bitcoins - there are numerous exchanges in existence that trade in BTC - other cryptocurrencies aren't as easy to acquire. Although, this situation is slowly improving with major exchanges like Kraken, BitFinex, BitStamp and many others starting to sell Litecoin, Ethereum, Monero, Ripple and so on. There are also a few other different ways of being coin, for instance, you can trade face-to-face with a seller or use a Bitcoin ATM.
- Once you bought your cryptocurrency, you need a way to store it. All major exchanges offer wallet services. But, while it might seem convenient, it's best if you store your assets in an offline wallet on your hard drive, or even invest in a hardware wallet. This is the most secure way of storing your coins and it gives you full control over your assets.
-

Investing

- **Why Invest in Cryptocurrencies And Why Not?**
- Besides what was already said, there are three major good reasons to invest in cryptocurrencies. First, because you want to hedge your net-worth against the fall of the Dollar imperium, which is assumed by many people to inevitably happen at some time. Second, because you support the social vision behind cryptocurrencies – that of a free and hard money for the whole world. Third, because you understand and like the technology.
- However, there are also very bad reasons to invest in cryptocurrencies. Many people fall victim to the hype surrounding every cryptocurrency-bubble. There is always somebody captured by FOMO (fear of missing out), buying massively in at the peak of a bubble, just in hope to make quick money, while not understanding cryptocurrencies at all. That's a bad reason. Don't do this. Learn before you invest.
- **What Cryptocurrencies Should I buy? Building your Portfolio.**
- The former only crypto has been Bitcoin. Up until late 2016 Bitcoin was the cryptocurrency, and there was not much besides it. If you wanted to invest in the success of cryptocurrencies, you bought Bitcoin. Period. Other cryptocurrencies – called "Altcoins" – have just been penny stocks on shady online-markets, mostly used to keep miner's GPUs working, pump the price and dump the coins.
- However, this has changed. While Bitcoin is still the dominant cryptocurrency, in 2017 it's share of the whole crypto-market has rapidly fallen from 90 to around 40 percent. Many people saw this coming as a result of the growing popularity of Ethereum and the ongoing self-tearing of the Bitcoin community over the blocksize issue. This again shows that it is important to keep your eyes open and listen to what the communities say.
-