Cryptocurrencies...True Anonymity?

**** show coin with BTC taped on it **** Bitcoin! So mysterious to so many people, and so many misconceptions regarding the technology behind it and its capabilities. *Is Bitcoin anonymous? Is it a fad?* And most importantly...*when moon?*

Well with Bitconnect, you can earn 1000% of your investment in as little as 14 days, "what am I gunna do?!" (Play carlos) Here's a promo...

Promotional Spot

Bitcoin is a cryptocurrency, or digital currency, like *donuts in Simpsons Tapped Out, Gold in Candy Crush Saga, or Vbucks in Fortnight.* There are two key differences though. First, Bitcoin is intended to be used as a common-day currency used to purchase common items, replacing modern-day currencies. The second difference is blockchain technology, where every transaction is fully public and verifiable. *This means you can view every transaction taking place on the Bitcoin blockchain. A blockchain is resistant to modification of any data, making them secure by design. They're also decentralized, meaning no one person controls the blockchain, giving power to users, and allowing them to control and send their funds worldwide with no third parties.* There are other benefits...

- *The invention of the blockchain for Bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.*
- There are no banks or other third parties that control how you store and send money, you take full ownership.
- And it's a worldwide currency, which could rid the need for conversions and globalize currency.

So that is Bitcoin, *A) It wasn't created to be anonymous B) It wasn't created for illegal activities C) It wasn't created as a scam D) And it wasn't created as an investment opportunity.*

Now you might be asking: why is it used for illegal activities, if it's not anonymous?

Let me answer that...

1) Bitcoin is being replaced by *Monero for illegal activities, and I'll expand on that in a sec.*
2) Bitcoin is not anonymous, but there are ways to make it very difficult to track where it came from. *For example, you can buy Bitcoin with cash*

in-person using an ATM, and send it to a new wallet, which isn't tied to any previous transactions--giving you decent anonymity. I say decent because *these ATMs typically have cameras built into them,* the malls and stores with ATMs have cameras, and your drive to these stores will face many challenges, like phone-based tracking, license plate monitoring, and other techniques which we'll discuss in section 5 and 6. A better method is buying Bitcoins locally with cash using *a site like LocalBitcoins; I like to call them cryptocraigslist.*

3) Another method of making Bitcoin relatively anonymous is by using a mixer, essentially a laundering service. There are several options but *coinmixer.se seems decent, and bitblender.io seems better since it requires Tor to use. The way these work is you send your Bitcoin into the service, along with many other people, and the service scrambles where the Bitcoin came from and its destination.* Laundering is legal as long as you're not using it to hide illegal activities. You also have to remember the wallet you use to send the BTC should have no information tied to you, as well as the destination wallet.
4) Another method of getting Bitcoin anonymously is by mining it yourself. Mining will require a GPU to mine, using something like Nicehash. *I made a tutorial on mining and how to get started on my channel.*

Alright...so it's a bummer Bitcoin isn't inherently anonymous. Luckily, there are other cryptocurrencies that promise near anonymity by default. *Monero is one of them, which utilizes a private blockchain. This way it's impossible to view transactions on the blockchain. On top of that, your wallet address, which is how you identify your wallet, is never used in the transaction. There are two ghost addresses used to avoid exposing the real addresses.* Monero implements all of this by default, which is great since it eliminates the possibility of human error.

Another project is *ZenCash, based on another private cryptocurrency Zcash. ZenCash utilizes different technology than Monero, but all-in-all accomplishes the similar goal of anonymizing its users.* The main issue with ZenCash is you need to make sure you're using a private address for anonymity benefits, meaning there is a possibility of human error. Privacy is NOT by default.

Before going out and buying cryptos, remember to secure them. This space is very new, there are lots of scams out there, *and people are losing their cryptos left and right.* Avoid leaving your coins on exchanges, transfer them to a wallet where you have control of the private keys. If you want the utmost security, you should go pick up a *Ledger Nano S, which is considered the most secure method of storing cryptocurrencies.*

To recap everything, cryptocurrencies can be used to help anonymize digital purchases. With *Bitcoin,* it's difficult and you'll have to jump some hoops because it's not inherently private. Other technologies like *Monero, Zcash, and Zencash* all offer more private ways of sending money, which are much better than Bitcoin. Remember, as always--do not put full faith in the technology. Create these accounts and send transactions assuming they will be compromised, so even if they are compromised you're personal data is still safe.

Queue Outro Promos

I hope that cleared up some cryptocurrency misconceptions. It is very cool to witness where this technology will go, and only time will tell if cryptos really will take off. The use-case is definitely there. Thanks for watching, and I'll see you in *the next lesson: Auditing.*