Crypto Club Week 3

Monero and Privacy Coins

Background

- One of the biggest shortfalls of Bitcoin is that all transactions are publicly recorded, stored forever on the blockchain.
- As we enter the Web3 era, it is important that we make sure it does not become a place where we must give up all private information in order to participate in society.

Privacy

Part 1

The importance of privacy

- Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

- Eric Hughes, *A Cypherpunk Manifesto*

The importance of privacy (continued)

- Just because you want privacy does not mean you are doing something illegal. You can reveal yourself if you want, but you should have the ability to choose if you want to reveal yourself.
- A bank (and government/hackers/companies/employers) can see every single transation you make in our current system if they really wanted to. Privacy coins change this dynamic.
- Privacy coins are one of the only answers to the coming Central Bank Digital Currency System.
- https://www.youtube.com/watch?v=M6kxtiKKyMQ

Monero

Part 2

What is Monero? (XMR)

- Monero is **secure, untraceable, electronic cash**.
- It is the single most used and useful cryptocurrency currently in existence. Used for more **day-to-day transactions** than Bitcoin.
- Like Bitcoin, it is open source, decentralized, and freely accessible to all, but with even more advantages than Bitcoin.
- Transactions to and from wallets are not visible, nor are the balances of wallets from any third party or on the blockchain.
- Almost Spanish for "money." (dinero)

The Essentials

- Monero seeks to be **digital cash**, as opposed to digital gold.
- Transactions are always private, others can't tell where you've received Monero from, where you've sent it to, or the amount involved.
- Works as a **tradiational blockchain**, recording payemnts on a digital ledger and storing them in blocks to be verified by other users via mining.
- Blockchain is very similar to Bitcoin, but it is built with privacy in mind.
- **EXAMPLES AHEAD WILL USE "ALICE" AND "BOB" AS TWO USERS AND THEIR WALLETS!!!!!!**

Stealth Addresses

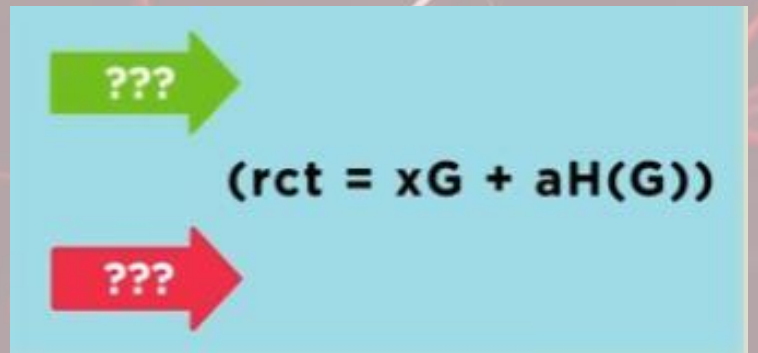
- Stealth addresses are a **one-time public key**, automatically generated and recorded as a part of the transaction to indicate who can spend an output in the later transaction.
- Wallets can prove that Monero was sent to a wallet, keeping the integrity of the blockchain intact.
- This is a great benefit for merchants, because no one can tell how many customers they have, what they are paying for, or how much they are paying for it. All data is private!
- A Monero wallet address is a **95-character string**, consisting of a **public view key**, and a **public spend key**.
- When Alice wants to send money to Bob, Alice's wallet will use Bob's public view key and public send key as well as some random data to create a one-time public key. Everyone can see the one-time public key, but only Alice and Bob know that Alice sent Monero to Bob.
- Bob's wallet scans the blockchain for the output destined for him with his **private view key**. Once the output is detected by Bob, his wallet will generate a **one-time private key** that corresponds with the one-time public key and spend the relavent output with his wallet's **private spend key**.
- This whole process occurs without having Bob's address publicly linked to any transaction. The use of steal addresses is shielded with **ring signatures**.

Ring Signatures

- Ring signatures are a type of digital signature in which a **group of possible signers** are linked together to produce a distinctive signature that authorizes a transaction. Similar is signing a check to a bank account, **but the actual signer is unknown**.
- All members are grouped together in a "ring" where they are all equal and valid. However, the actual signer is a **one-time spend key** that corresponds with the output spent from the sender's wallet.
- The outside signers are **past transaction outputs** pulled from the blockchain to act as **decoys**. To a third party, all the inputs appear to be equally likely to be out output in the spending transaction.
- To protect to blockchain from double-spending, the use of **key images** was implemented. This is a cryptographic key derived from an output being spent and is made part of every ring signature transaction. There can only be one key image for every output on the blockchain.
- A list of all key images are maintained in the blockchain, so miners will be able to verify that no outputs are spent twice!
- Example (2:16): https://www.youtube.com/watch?v=zHN_B_H_fCs

Ring Confidential Transactions

- Ring CT was implemented in July 2017 to **hide transaction amounts**.
- When new Monero is mined, it must be converted from a **pre-RingCT output** into a **RingCT output** before it can be included in a **ring signature**.
- All transactions will have two outputs, one as the actual money being sent, and other being sent back to Alice as "**change**" of the transaction. The sum of the transaction's inputs must equal the sum of the outputs in order to not double-spend.
- RingCT uses the **equation below** to calculate a "**commitment**" from Alice's wallet and how much she is sending to Bob, and how much change she is receiving.
- RingCT's use "**range proofs**," which prevents senders from committing negative values to secure the supply of Monero. It cryptographically proves that the number being sent is above zero.



Kovri: How Monero hides IP addresses.

- Although transactions and wallet addresses can be hidden, personal information can be leaked from security vulnerabilities on the user's computer and internet network level. This is fixed by Kovri.
- Kovri tunnels traffic through the **I2P network** with **"garlic encryption"** and **"garlic routing."** Information travels within a private overlay network by way of messages, which are encrypted each time the message passes along peers in the network.
- Like a **Matryoshka doll**, there is an extra doll added for each computer the message goes through, and with each new doll, there is a lock and a public key to get to the smaller doll.
- Peers in the network are not able to read the messages they are relaying, the only information visible to peers are the instructions to send to the next destination.
- At a slight cost to the network's performance, greater privacy is achieved by allowing users to connect to serval users within the network.
- Kovri can be used in Monero, as well as anonymous internet browsers and email services.

Kovri: visualization

Advantages over Bitcoin

- Bitcoin is often referred to as "**digital gold**." This is good for purposes of storing value, but **terrible** for purposes of privacy.
- Monero is more often called "**digital cash**," because it is so anonymous.
- Unlike with banks and Bitcoin, companies, governments and individuals can keep their customers secret, and hide their activity from nosy people.
- It is pretty much the same thing as digital gold, but it has much more utility in it.

Mining Monero

- In order to avoid a high barrier for entry to mine Monero, the Monero team has avoided the use of ASIC miners (used for Bitcoin) which can be very expensive and price people out of mining and making the network more centralized.
- Monero uses a Proof-of-Work mining algorithm called **RandomX for CPU mining**, but this can vary depending on how you are mining.
- Any standard computer can become a miner. Although not every computer will be efficient at it, and electricity bills and equipment breaking will soon outweigh the reward.
- Most common was is **CPU mining,** the more expensive the CPU the more profitable. (AMD Ryzen Threadripper, AMD Ryzen 9 are currently profitable).
- GPU mining is also an option, being more scalable and powerful than CPU. However, it can get must more expensive.
- You can join **mining pools**, or mine individually. Note that when you are mining, it must be running **24/7**, so use a **Raspberry Pi** instead of an actual computer.
- Mining software might trigger an antivirus warning, make an exception for it. https://xmrig.com/

Illicit Use

- Because of its privacy-oriented features, Monero has been used for all kinds of illicit activities.
- New technology is abused by criminals first because they must be the **most innovative**, but eventually, the technology is made for the general population.
- Monero is the one of most used cryptocurrency on darknet markets, ransomware hacks, and money laundering schemes.
- It is also used by figures like **Russian oligarchs** to avoid US sanctions and other financial barriers places upon countries.

DO NOT UNDER ANY CIRCUMSTANCES VISIT DARKNET MARKETS OR LAUNDER MONEY!!!

- Besides the obvious fact that it could mean **decades in a cage** over something supposedly small.
- You are also operating in the black market, a place where the law cannot protect you.
- The vendors of these services make it their number one priority to know who is visiting their website; and they collect all information that **they can and will use it against you if necessary**.
- Do not make any purchase of illicit items; chances are that you probably don't know what you are doing, and if you don't get caught by the law, **you'll get scammed**.

How to buy Monero

- Monero is blocked from US exchanges, so it **cannot** be purchased on Coinbase or Gemini.
- **Kraken** exchange is a UK-based exchange where you can purchase Monero directly with US dollars.
- Hong Kong exchanges, like **Kucoin and Gate.io** offer Monero in exchange for Bitcoin. Simply purchase Bitcoin from Coinbase, send that Bitcoin to Kucoin, and trade it for Monero.

Monero Wallets

- Non-custodial wallets that offer Monero support.
- https://www.getmonero.org/downloads/
- https://mymonero.com/
- https://www.exodus.com/monero-wallet-xmr
- https://cakewallet.com/ (iOS)

Privacy Coins beyond Monero

Part 3

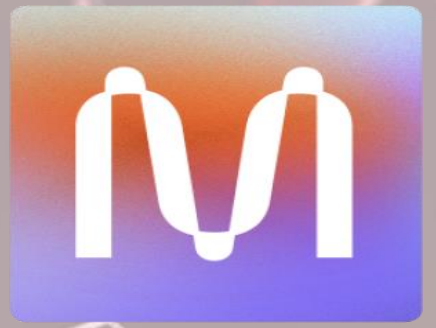
Zcash (ZEC)

- Zcash is a Fork of Bitcoin, PoW consensus model. Built on Bitcoin Core codebase.
- Public blockchain, but sender, recipient, and amount sent can remain private. It offers 4 different types of transactions. **Fully private, deshielding, shielding, and public**.
- Zcash achieves this privacy through an advanced cryptographic technique called a **zero-knowledge proof**.
- It uses a zero-proof construction called a **zk-SNARK**. It creates and maintains a secure ledger of balances. This maintains the integrity of the blockchain, while also keeping information private.
- Zcash has notably active Github of people trying to improve upon the code.
- Can be purchased on most exchanges, including Coinbase.

Dash (DASH)

- Launched in 2014 and a hard fork of Bitcoin. Max supply of 18.9 million coins and PoW consensus model.
- Improves upon Bitcoin by adding faster transaction times and **optional privacy**.
- "**Instant send**" allows a sender to bypass the blockchain and send it directly to the masternodes at cost of a higher gas fee.
- **Masternodes** store data on the blockchain, vote on governance questions, and decide how Dash development fund is distributed. To become a masternode, you must hold 1,000 DASH.
- Dash has a feature called "**private send**" which is basically a built-in coin mixer that combines transactions and send coins to different addresses. Nearly impossible to tell who sent coins to what addresses.
- However, private send is optional, and transactions that are sent privately stand out more because transactions are still visible to anyone.

Mina (MINA)



- Lightest blockchain in existence, only **22kb in total size** (size of two Tweets).
- This makes mining and storing the blockchain much easier because they won't have to download and work through a huge blockchain. (Bitcoin's blockchain is 400gb, with 1mb per block added every ten minutes)
- It uses **zk-SNARKS** as its cryptographic proof instead of brute force computing. Proof-of-stake consensus.
- Capable of running **decentralized applications or "Dapps,"** something that is significantly harder to do on a proof-of-work blockchain like Bitcoin or Monero. These are known as "**zkApps**" and act as a zk-SNARKS smart contract.
- This means that there are now **private smart contracts**, something that is not replicable on networks like Ethereum.
- Every participant is a "**full node**."

Zero-knowledge proofs

- Zero-knowledge proofs are a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.
- This way, a verifier can prove that information is true, without necessarily having to see the details of that proof.

Types of zero-knowledge proofs

- **Ring signature**- outsiders have no idea which key is used for signing.
- **Multi-party computation**- while each party can keep their respective secret, they together produce a result
- **Witness indistinguishable proof**- verifiers cannot know which witness is used for producing the proof
- **Pairing based cryptography**- given f(x) and f(y), without knowing x and y, it is possible to compute f(x×y)
- **Proof of knowledge**- the knowledge is hidden in the exponent like in the example shown above.

Monero use examples (cool edition)

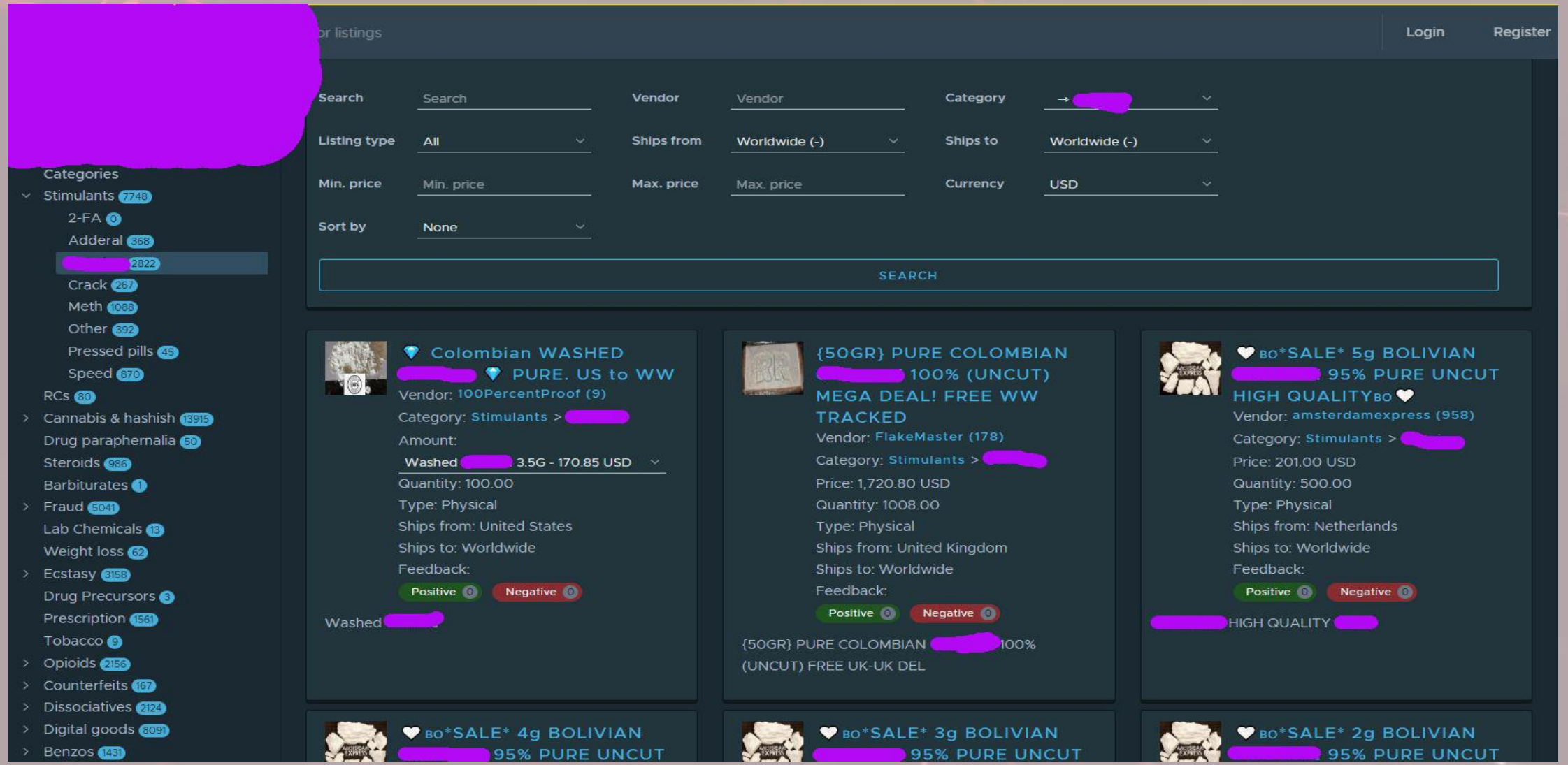
Colonial Pipeline Ransomware Hack (May 2021)

Colonial Pipeline Paid Almost $5M Crypto Ransom Soon After Attack: Report

The company previously said it would not pay the hackers.

By Jamie Crawley May 13, 2021 at 10:12 a.m. CDT Updated Sep 14, 2021 at 7:55 a.m. CDT

Dark market example



Basket > Checkout

BACK TO BASKET

Item	Price	Fee (%)	Amount	Total
McKENNAII CUBENSIS $50 – 7g (1/4 oz) | Rare M...	50 USD	0.50 %	1	50.25 USD
Shipping: First Class Untracked (1.20 USD)	1.20 USD	0.50 %	-	1.20 USD
Fee	0.25 USD	-	-	0.25 USD

Order info

Vendor: OwlSpiral9

Payment currency: XMR

Message to vendor / Delivery info: Message / delivery info

Items price:	50 USD
Shipping:	1.20 USD
Fees:	0.25 USD
Total price:	51.45 USD 0.00252 BTC 0.35383 XMR

qsw7iurcrdwyml5kg4oxbmtqrcnpxiag3iumdarefzeunnyc2dnyljad.onion/product/254 70%

THIEF
World

Search...

EN Sign in Registration

CATEGORIES all | Products | The shops | Open shop | TO BUYERS | SELLERS | Escrow | Track my order | 1 XMR = 162.81 USD

Big Discounts On Weapons

★★★★★ 8+ deals TOP store

Showcase | About Store | Reviews 3 | Complaints 1

Home / Big Discounts On Weapons / Swichblade 300

Swichblade 300

Weapon

from 4 000 USD / 1pcs

24.568515447454 XMR

Київ

Swichblade 300 kamikaze drones
The price per piece is $4,000. A complete set.

9.0
rating

city selection change | INSTANT | PRE-ORDER

That's all!

Any questions?

Monero Resources

Websites

- https://www.getmonero.org/
- https://moneroj.net/
- https://cryptwerk.com/pay-with/xmr/
- https://bit.ly/3BtLvfy- mining calc
- https://miningpoolstats.stream/monero

Youtubers

- https://www.youtube.com/c/MentalOutlaw - Mental Outlaw
- https://www.youtube.com/c/LukeSmithxyz- Luke Smith
- https://www.youtube.com/c/SirSudo/featured- SirSudo
- https://www.youtube.com/watch?v=RiyOv7hKoFA&t=79s- How to start mining