TITLE SLIDE

Hi, my name is Andrew and today I’m going to be talking to you about virtual currencies and how they work.

WHAT IS IT

Virtual currency or cryptocurrency is a type of digital asset that is designed as a medium of exchange. It’s different from traditional money since it is completely digital and operates independently from any bank or government. Crypto currency has mainly taken off in the last ten years, with bitcoin and Ethereum being the main two that most people talk about. Those are the biggest ones but there are thousands to choose from with more showing up every day. These currencies can be used for anything you would use normal money for as long as the vendor supports it.

HOW DOES IT WORK

Cryptocurrency works by using a digital ledger called a blockchain. A user purchases the currency and it can be stored in a crypto wallet. It can also be purchased through a crypto exchange and stored in the exchange. Once you have a set amount of currency, your actual money value will fluctuate depending on if the price of the cryptocurrency is going up or down.

BLOCKCHAIN TRANSACTIONS

For virtual currency to be moved, it has to be validated on the blockchain. When a transaction is entered, it is sent out to a network of computers all over the world. Those computers solve complex equations that confirm the validity of the transaction. From there it is put into a block. Once a block is filled up, it gets added onto the end of the chain (hence the name). Once it is stored in the blockchain, the transaction is completed. This is part of the reason it can take a little bit of time to confirm a transaction as the block needs to be filled before it can be added onto the chain.

IS CRYPTO ANONYMOUS

Most people think that using cryptocurrency makes you completely anonymous. This is only partially true. Using crypto is pseudo anonymous, meaning you have a fake identity so to speak. When using cryptocurrency your wallet ID is not hidden. It is visible and recorded on the blockchain. But what makes it hard to track is the lack of information connected to that string of numbers and letters that is your wallet ID. To find someone specific by their wallet ID, you would have to know that they made a transaction of a certain amount on a certain day. You could examine the blockchain for that particular day and find the wallet ID that made that transaction. You would need to do this another time with another transaction that you knew happened to truly tie the person to the wallet. It requires a lot of outside information for you to be able to pinpoint these transactions. This is why it is very hard to track someone using crypto, but not impossible.

IS IT SECURE

The use of blockchain makes crypto a secure system. Since it is a peer to peer system, information is stored redundantly on a vast number of computers. Simply editing a transaction on one version of the blockchain and trying to get it recorded would just be flagged by the rest of the systems, and not validated. To really change an entry, one would have to edit a transaction on a majority of the computers on the network, which is virtually impossible. Even then, it would be quickly noticed that something isn’t quite right.

THE BAD SIDE

Since it is harder to track, virtual currency is the main method of payment used on the dark web. The most notable site being The Silk Road. This site was used for multiple different services, such as malware, pirated software, and forged documents. But the primary use was to buy various drugs. Bitcoin was the only payment method used on the silk road, and did a good job at keeping users anonymous. This is obviously a problem for law enforcement. Any time transactions can be conduced without the user being identifiable it will usually be used for mischievous purposes. This goes for more than just crypto currency.

CONCLUSION

In conclusion, virtual currency will always around. New currencies pop up every day trying to be the next bitcoin, or to bring something new to the table.