Information Security Thought Paper

Cryptocurrency or Digital Currency

Cryptocurrency is a digital or virtual currency that uses cryptography for security purposes, making it difficult to counterfeit. A main feature of a cryptocurrency is that it is not issued by any central authority, which theoretically makes it insensitive to government interference or manipulation. Unfortunately, the anonymous nature of cryptocurrency transactions makes them well-suited for a host of nefarious activities, such as **money laundering**[i], **tax evasion**[ii] and as ransom in Ransomware attacks.

Cryptocurrency first came into existence in the form of Bitcoin, which was launched in 2009 under the pseudonym **Satoshi** Nakamoto[iii]. Bitcoin's success has spawned a number of competing cryptocurrencies, such as Ethereum, Monero and Ripple.

What are cryptocurrencies?

A simple definition of a cryptocurrency is: "***Limited entries in a database no one can change without fulfilling specific conditions.***" Cryptocurrency consists of a network of peers which have a record of the complete history of all transactions and thus of the balance of every account.

How does a transaction flow?

An example of a transaction: "A gives #of Bitcoin to B" and is signed by A's private key (basic public key cryptography). After signed, the transaction is broadcasted in the network, sent from one peer to every other peer (basic p2p-technology). After a specific amount of time it gets confirmed. Confirmation is a critical concept in cryptocurrencies. While the confirmation is pending, transactions can be altered or forged. After confirmation, a transaction cannot be reversed or altered, it becomes part of an irreversible record of transactions called a BlockChain. Confirmation is only carried out by "miners". They confirm transactions as legitimate and spread them to the rest of the network. Every node adds this transaction to its database and thus becomes part of the BlockChain. In compensation for providing these confirmations, miners are paid with a token of the cryptocurrency-system (e.g. Bitcoin).

Details of Crypto Mining

The miner is a crucial part of the cryptocurrency-system. There was a time when anybody was able to mine their own cryptocurrencies using a standard PC, this is no longer a reality. The processing power required to mine effectively increases with the volume of people mining. Requirements have gone from a reasonably powerful processor to a high end GPU to several GPUs working in conjunction. Today, you will need specialized chips specifically configured for crypto mining.

Hardware to mine most modern cryptocurrencies with any success are considerably expensive and the energy consumption can also be quite substantial. Systems will need to run 24/7 so costs are a major consideration. Most miners will spend the majority of their income from mining on paying to maintain and run the equipment. Today the

Bitcoin network can process 5.5 quintillion hashes per second, unless you have the equipment that can handle this volume, it would probably be best to leave the mining to **industrialized cryptocurrency installations.**[iv]

Security Considerations with Cryptocurrencies

Authorities are approaching this problem by enabling cryptocurrency holders to convert cryptocurrencies to U.S. Dollars or other currency. Large exchanges comply with strict requirements in terms of "Know-your-customer" and the fight against money laundering by collecting identification data from their users. This makes it much more difficult for criminal groups to anonymously convert their cryptocurrency into conventional currency. In 2015, the **BlockChain Alliance**[v] as a public-private partnership was established by exchange providers, technologists, and law enforcement officials and regulators. The organizations purpose is to enable the BlockChain community and law enforcement to battle criminal activities together. The U.S. and **EUROPOL**[vi] are collaborating on using BlockChain to analyze and track criminal and terrorist activity. By aligning with IT and industry experts, law enforcement will be better able to combat cryptocurrency related criminal activity.

Recommendation

Government is unlikely to accept cryptocurrency in payment for services in the near future. It is therefore recommended that government be mindful of cryptocurrency as it evolves, continue to investigate, and be prepared to adopt when the time is right.

Resources:

Bitcoin: A Peer-to-Peer Electronic Cash System; Satoshi Nakamoto, (satoshin@gmx.com, www.bitcoin.org)
https://bitcoin.org/bitcoin.pdf

Know Your Customer (KYC)
https://en.wikipedia.org/wiki/Know_your_customer

BlockChain Alliance
http://blockchainalliance.org/

U.S. Authorities & Europol focus on combating the abuse of virtual currencies
https://www.europol.europa.eu/newsroom/news/us-authorities-europol-focus-combating-abuse-of-virtual-currencies

End Notes:

[i] Money laundering is the process of creating the appearance that large amounts of money obtained from criminal activity originated from a legitimate source. The money from the illicit activity is considered dirty, and the process "launders" the money to make it look clean.
[ii] Tax evasion is an illegal practice where a person, organization or corporation intentionally avoids paying their true tax liability.
[iii] Satoshi Nakamoto's, true identity has yet to be verified.
[iv] Large warehouses packed with floor-to-ceiling racks of expensive graphics cards, working towards the sole aim of mining new units of cryptocurrencies.
[v] BlockChain Alliance : https://digitalchamber.org/initiatives/blockchain-alliance/
[vi] EUROPOL : https://www.europol.europa.eu/