Digital Currency Brief

What is cryptocurrency?

Cryptocurrency is the digital equivalent of the US dollar, but instead of using gold or another valued resource to control the creation of units and to verify the transfer of funds, it uses encryption techniques. Bitcoin is the best known and most widely used form of cryptocurrency, and has essentially created a way for people to convert their efforts into a digital token system rather than using physical representation. There are a fixed supply of Bitcoins (21 million) and they function using Blockchain.

A problem presented with the idea of digital currency is false ownership. Real life exchanges are obvious: I say I will give you a Hershey Bar and I either do or don't, this is easy for you to see. On the internet it's more complicated. I can say I will give you a digital Hershey Bar and then just copy it 20 times onto my desktop. This problem of 'double-spending' is solved through the use of Blockchaining.

What is Blockchaining?

Blockchain is a digital decentralized ledger that everyone owns and contributes to. The use of block chaining enables users to have financial exchanges without the use or trust of a third party institution, such as a bank. An important distinction between blockchains and a standard SQL/Oracle database is that it is a consensus system that works peer-to-peer and is maintained by a group rather than a single entity. Blockchaining is what enables cryptocurrency the ability to function on the internet.

Under the Hood Functionality

→ Participant makes a transaction request consisting of amount, recipient, and signature of sender
→ The request is sent to all of the other computers (nodes) within the network
→ The transaction, as well as the user's status, is validated by every node using known algorithms.
→ Specific participants (miners) work to confirm transaction by grabbing all unconfirmed transactions and packing them into a set (block). Once the block satisfies all rules, it is them forwarded to all users in the network who then verify that the work was done correctly.
→ Once satisfied, all users add this transaction to their ledger.
→ Coins from the sender are invalidated, and the recipient now has new coins

Using Cryptocurrency

Benefits

The use of peer-to-peer currency exchange eliminates the need for financial institutions which often come with fees, inefficiency, and potential interference from the third party despite the contractual agreement amongst the two exchanging parties. (ex: My bank declines my abroad purchase because it suspects fraud). The blockchain is designed to be transparent, efficient, and irreversible in regards to individual transactions. The algorithms used within the Bitcoin design are of the highest achievable security, and are therefore impossible to break (as far as we know).

Potential Downsides

The design of Bitcoin specifically does not allow for password recovery. A lost password would result in an unrecoverable wallet. Insecure passwords can lead to bitcoins being stolen, and the irreversible nature of transactions means that stolen bitcoins cannot be reversed and recovered.

Anonymity - Why Criminals use Cryptocurrency

UK Hospital Attack - WannaCry Ransomware

Initially, ransomware attacks consisted of some sort of phishing email with instructions to either transfer or wire money to the attacker — both methods of exchange being easily traceable. Cryptocurrency has allowed attackers to maintain anonymity by operating under false names in order to successfully complete these ransomeware attacks.

Silk Road

An online black market that operated from 2011-2013. Silk Road was an illegal-drug emporium that was operated as a Tor hidden service and used Bitcoin as currency to provide its users, again, with anonymity.