Mining

The SHA-256 and Scrypt algorithms serve as "proof-of-work" algorithms for cryptocurrencies and other cryptographic problems. These algorithms verify that a miner has donated enough processing power to the network to deserve a cryptocurrency reward. Miners verify transactions on the network and earn bitcoin or other currencies. Both algorithms serve the same purpose, but there are several differences between the two.

The SHA-256 algorithm serves as proof-of-work for the most popular and well known cryptocurrency, bitcoin. This algorithm is more complex and results in longer transaction times, measured in Gigahashes per second (GH/s). However, the security of the SHA-256 algorithm is greater than others. Due to the complexity and greater required processing power, cryptocurrencies using SHA-256 more often use ASIC mining equipment (Application specific integrated circuits). The price of ASIC equipment and high energy consumption makes SHA-256 mining impractical for most individuals.

Scrypt mining is much less complex than SHA-256, and therefore requires significantly less processing power. Transaction times for cryptocurrencies using Scrypt are shorter, measured in MH/s or KH/s. The processing power required for Scrypt mining is much more practical for the average user, and a CPU or GPU can be used for mining. Several alternative coins use the Scrypt algoritm for mining and are branded as "lighter" alternatives to the processing-intensive bitcoin. A noticeable example, Litecoin, uses this algorithm to allow the average user to mine with a GPU.

P2P Network

The network that powers bitcoin encompasses several layers of cryptography of peer-to-peer processes. A user new to the bitcoin currency must create a digital “wallet”. The wallet software generates and stores encryption keys that give the user power to send and receive currency across the network. The wallet stores the user's “private key”, an essential encryption key that verifies ownership of the user's bitcoin. The private key must be kept secure so that a malicious user cannot spend another user's money. The wallet software generates public addresses that allow users to exchange funds over the network.

Transactions use these cryptographic keys to complete exchanges without the need for a third party to manage the transaction fairly. If a user wishes to send bitcoin to another, he or she must have the other user's public address. The spender uses his or her wallet software to specify the address of the recipient and the amount of bitcoin. The wallet “signs” the transaction using the private key. Signing prevents any modification to the transaction once initiated. Miners using a specialized software donate processing power to the bitcoin network to verify transactions using cryptography. Miners solve the mathematics required to confirm the peer-to-peer exchange of coins, eliminating the need for a third party such as a bank or credit card network.

A public ledger known as the “blockchain” stores a record of every bitcoin transaction. This cryptographically-enforced ledger maintains fairness in the system and prevents malicious users from modifying transactions or wallet balances to their benefit. The blockchain record allows wallet software to determine a user's spendable balance as well.

The system's revolutionary use of cryptography eliminates the standard third-party verification that credit card and debit cards use. However, the system does contain flaws that users must exercise caution to avoid. Failed online wallet service and exchange Mt. Gox demonstrated a flaw in the private-

key ownership system of the bitcoin network. This exchange went bankrupt and froze or lost user's digital wallets. Without access to their private keys, users effectively lost ownership of their bitcoin. Some users lost upwards of $30,000 worth of digital currency. One user commented on the loss of his private key in *The Wall Street Journal,* “I didn't think that they were going to be completely destroyed. Fortunately, a user that stores his or her own wallet can ensure secure ownership of bitcoin. Users of machine-local wallets such as Multibit can back up copies of the “wallet.dat” file that stores the private key. This file can be stored on a cloud service such as Dropbox or stored on a removable drive to ensure ownership even if the hard drive containing the wallet is stolen or destroyed. Users can also save bitcoin by printing a physical copy of his or her private key known as a paper wallet. Wallet software can easily import the private key from this paper wallet so that an owner may spend bitcoin over the network.

The peer-to-peer exchange system of bitcoin contains some flaws. However, astute users' may take steps to ensure the security of their funds and avoid these security flaws. The use of cryptography to enforce fairness in the network allows for a revolutionary new system that avoids traditional third-party involvement in transactions.

Sources

https://www.coinpursuit.com/pages/bitcoin-altcoin-SHA-256-scrypt-mining-algorithms/

http://www.coindesk.com/scrypt-miners-cryptocurrency-arms-race/

https://bitcoin.org/en/how-it-works

The Wall Street Journal Monday, March 3, 2014