Cryptocurrency Cheat Sheet

www.LMGsecurity.com

Cryptocurrency is deeply intertwined with the rise of the dark web and cybercrime. It is also the basis for many legitimate transactions. Here are the key things you need to know about cryptocurrency, as well as the latest criminal trend, cryptojacking.

What is a Blockchain and How Does it Work?

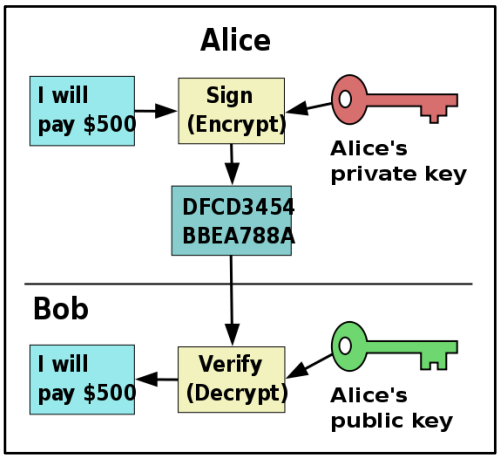
A blockchain is simply a digital ledger that is used to record and distribute information. Instead of a single entity controlling the ledger, anyone can have a copy of it. Cryptography is used to verify changes.

Here is how the blockchain works:

- Everyone has a public/private *key pair*.
- Anyone in the world can run a server which hosts a copy of the full blockchain.
- With cryptocurrency, every transaction is an update to the currency's blockchain.
- Want to update the blockchain? Use your private key to *sign* an update.
- Send the update to the blockchain network.
- Anyone can use your public key, plus the agreed-upon cryptographic algorithm, to verify that it really was you that signed the update.
- Once a blockchain server verifies your update, it adds your update to its official ledger.
- The blockchain servers communicate and soon the entire network has been updated.

Making a Cryptocurrency Payment

- Alice wants to pay the plumber Bob $500 in Bitcoins.
- She writes up the transaction, attaches Bob's public key so we know who the money is going to, and then signs it with her private key.
- Alice uploads this signed note to the Bitcoin network, where it is added to the blockchain ledger.
- From that point on, Bob owns the Bitcoin.



Cryptojacking Tips

Cryptojacking has become the newest cybersecurity epidemic. Criminals break into computers around the world to steal their processing power and mine digital coins that hold real world value.

Cryptojacking is a concern because it:

- Steals your computing resources
- Slows down your systems
- May also be a data breach

Protect yourself and your clients:

- Strong, WRITTEN policies
- Software patch management
- Training
- Resource monitoring

Cryptocurrency Cheat Sheet

www.LMGsecurity.com

Glossary

Here are important terms to understand regarding cryptocurrency:

Algorithm - A set of steps used to accomplish a task. For example, an encryption algorithm consists of steps taken to encrypt data.

Blockchain – A distributed digital transaction ledger which stores a record of all transactions.

Cryptocurrency – A digital asset in which cryptography is used to regulate creation of new units and transfer of funds.

Cryptojacking - When criminals steal your computer's resources in order to mine *cryptocurrency*.

Digital coin – A chain of digital *signatures*.

Encryption - The process of scrambling information so it cannot be accessed by anyone except authorized parties.

Key - A long string of numbers used as input when encrypting or decrypting data. Keys are commonly stored in files on a computer.

Key Pair - A pair of keys consisting of a *public key* and a *private key*. The keys are used together, so what one key encrypts, the other will decrypt, and vice versa.

Miner – Software which searches for the answer to a complex mathematical puzzle. Once the miner finds the answer, it submits it to the blockchain network, which creates a new "coin" by updating the ledger.

Private Key - A key which is kept secret, held only by the owner.

Public Key - A key which is distributed to the world.

Signature – A long string of numbers, which is the result of a process where a message and a *private key* are used as input to an *algorithm*. The purpose of the signature is to allow other people to verify the sender's identity, and confirm that the message has not been altered in transit. The sender's corresponding *public key* is used to confirm that they sent the message.

Wallet – Software that stores your public and private *keys*.