**BITCOIN**

To use this system, Alice must solve two fundamental problems:

1. Alice needs a way to identify both herself and Bob in the transaction. She can’t employ a trusted authority such as a government registry or email provider because that would create a central point of failure — the very thing Bitcoin was created to eliminate.
2. Alice needs a way to prevent others from changing her transaction and forging transactions in her name.

Bitcoin solves both problems through a system called [public key cryptography](https://bitzuma.com/posts/how-bitcoin-works#public-key-cryptography). This system uses two pieces of information to authenticate messages. A *public key* identifies a sender or recipient, and can be distributed to others. A *private key* creates an unforgeable message signature. Unlike the public keys, the private key must be kept secret. Public and private keys are mathematically linked through a *signature algorithm*, a mathematical procedure for creating identities, signing messages, and validating signatures.

**Public Key Cryptography.** Alice (top) begins by choosing a private key. Using a signature algorithm, Alice obtains a public key from her private key (left). Alice then sends this public key to Bob (bottom) while keeping her private key secret (center-left). Alice signs a message by passing it to **the signature algorithm** together with her private key. The algorithm returns a signature in response (center). Alice attaches this signature to her message and sends both to Bob (center-right). Finally, Bob passes the message, signature, and public key he was given to the signature algorithm. If the message is authentic, the algorithm returns a confirmation (right).

With this overview in mind, here are six things about private keys to keep in mind as you use Bitcoin.

**1. A Private Key is Just a Number**

A Bitcoin private key is simply an integer between one and about 1077. This may not seem like much of a selection, but for practical purposes it’s essentially infinite.

If you could process *one trillion* private keys per second, it would take more than one million times the age of the universe to count them all. Even worse, just enumerating these keys would [consume more than the total energy output of the sun for 32 years](https://www.schneier.com/blog/archives/2009/09/the_doghouse_cr.html). Bitcoin’s entire security model rests on the infeasibility of mapping this vast keyspace.

**In other words, digital signatures are practically impossible to forge.**