BITCOIN SECURITY ESSENTIALS

Adonis Pineda

BRIEF HISTORY

Bitcoin, also known as BTC, is a decentralized cryptocurrency. This is a digital currency that is managed and valued by no one and everyone. No one truly controls it or owns it or regulates it more than another individual.

The first ever Bitcoin software was published to the public on an open source software site by an entity known as Satoshi Nakamoto, in 2010.

While the concept was discussed in mailing lists, Bitcoin was the implementation of such a concept.

BITCOIN MINING

With the right software and hardware setup, one can “mine” Bitcoin and generate revenue this way. Bitcoin mining tackles mathematical problems by resolving the data blocks and authenticating the transactions in the blockchain

BLOCKCHAIN

The **blockchain** is the public ledger that keeps track and accounts for all the changes in the bitcoin network, which is user-enforced.

It’s worth it

Bitcoin’s original market price was less than a cent, at about 0.008 USD.

The record peak for a single Bitcoin unit(BTC) was somewhere under $20,000.

Lately, it has been somewhere between $5K-$7K USD, fluctuating

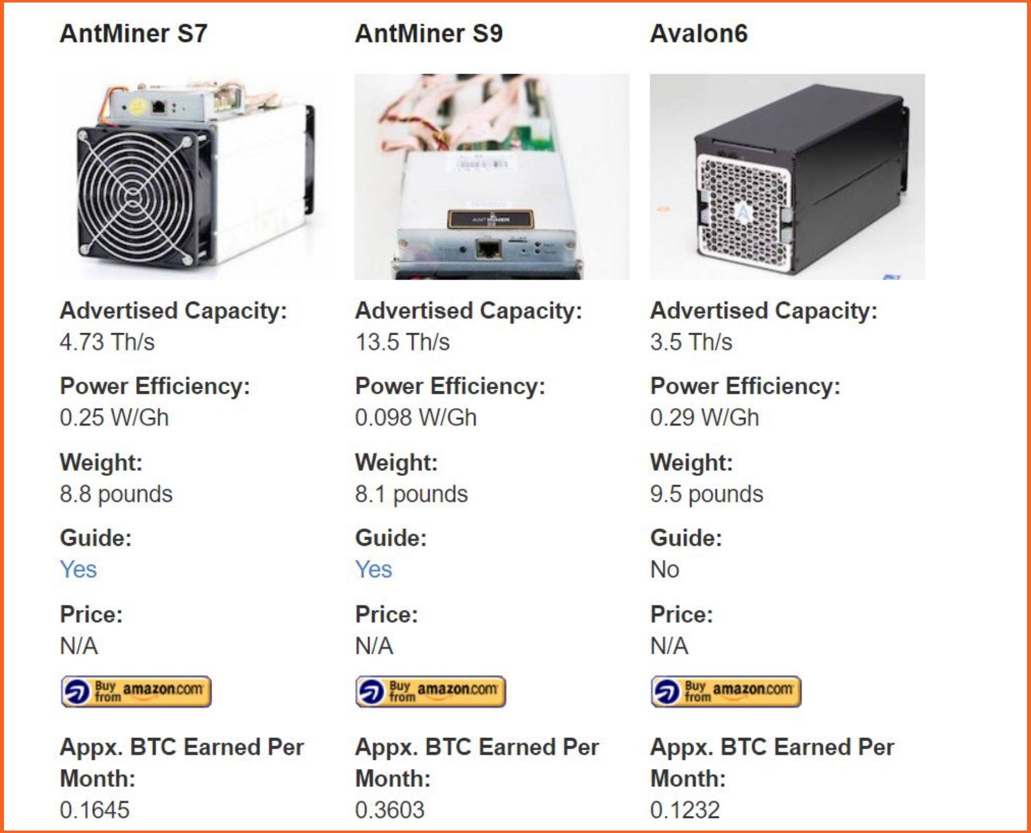
What does this mean?

This means that Bitcoin’s value and efficiency is completely controlled both by those trading and mining.

There are repositories of Bitcoin wallets online, known as cloud wallets, which are technically another layer on top of the actual decentralized network, but they also affect trading and therefore affect value.

Examples of dedicated BTC mining hardware

One should consider other peripheral hardware that will account for cost to operate, as well as the market environment.



	AntMiner S7	AntMiner S9	Avalon6
Advertised Capacity:	4.73 Th/s	13.5 Th/s	3.5 Th/s
Power Efficiency:	0.25 W/Gh	0.098 W/Gh	0.29 W/Gh
Weight:	8.8 pounds	8.1 pounds	9.5 pounds
Guide:	Yes	Yes	No
Price:	N/A	N/A	N/A
	Buy from amazon.com	Buy from amazon.com	Buy from amazon.com
Appx. BTC Earned Per Month:	0.1645	0.3603	0.1232

Source image: bitcoinmining.com

Bitcoin to End User

The Bitcoin address is made of a private key, a private key, and actual address.

The public key is made from the private key.

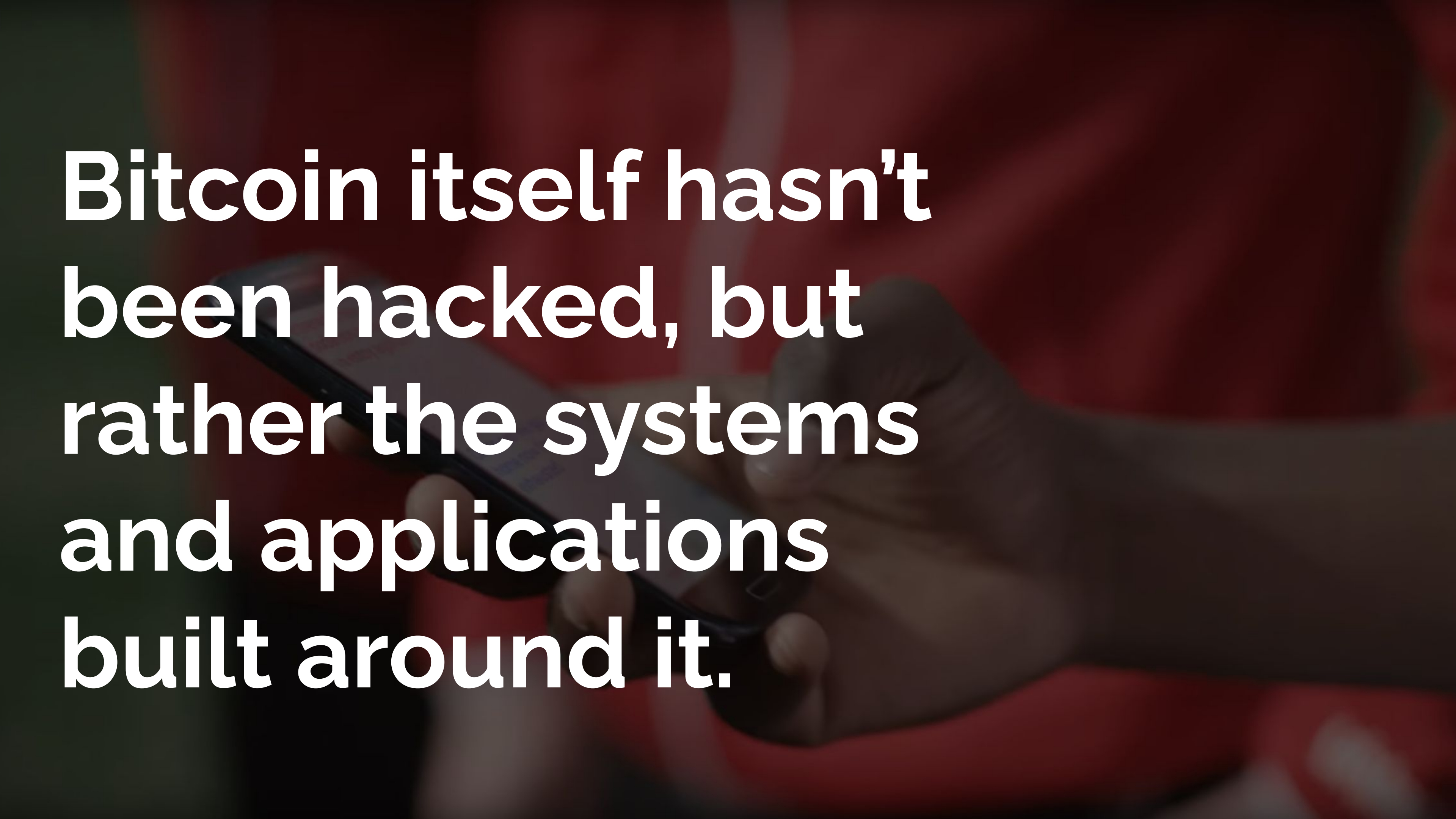
Multiple public keys can be generated from the private key.

Your wallet address is 160 bits long, while the public key is 256 bits long.

Verifying Transactions

There is a way to have transactions fulfilled for free, but these can take substantially longer.

So in some wallets, your transaction can be viewed with the associated fee up front to fulfill them, but the cost is per transaction and does not depend on the amount but the data size of the transaction.
This means that a large amount has a relatively small fee and vice versa.



Bitcoin itself hasn’t been hacked, but rather the systems and applications built around it.

This means that security is dependant on the end-user, regardless of any built-in security.

Types of Bitcoin wallets:

Mobile wallets(iOS, Android)

Web client

Desktop wallets(application on a computer using hard drive space)

Hardware wallet(can operate offline

– New conventions

Because it is decentralized, every new change or update to the behavior of Bitcoin has to be accepted by the majority of holder in order to function. One cannot just create coins out of nothing and expect the network to honor it.

In fact, there are bitcoin address formats that start with 1 and 3, but not some with bc1, known as Bech32, a new benchmark by SegWit. This was made to save space, but is really another platform on top of the actual network. So not everyone with a 1 or 3 address can trade with someone with a Bech32 unless they accept the change.

Method to Secure Your wallet

Use 2FA, or MFA if you must keep your wallet online.

NEVER share your private key unless you are sharing your wallet.

Generate a new key whenever possible, especially for larger amounts.

Multiple parties or large transactions should be handled appropriately with multi-signature options. This means everyone must sign off on the transaction in a digital handshake.

Hardware wallets are usually the most secure, but an air gap must be considered.

Desktop wallets or any software based wallet should have strong passwords and consider having a backup written on paper, or better memorized.

Let’s go to the blockchain!

Questions?