IW WORLD EXCHANGE

65 Court St. 6th Floor
Veritas Place
Hamilton HM12, Bermuda
info@iwwexchange.com
www.iwwexchange.com

in a nutshell

How We Pay For Things Now

We make transactions in three ways:

1) We pay cash,

2) We write checks (or use debit cards),

3) We use credit cards.

The first transaction, a cash exchange, is made between the parties of that transaction and can be completely anonymous. Anonymous transactions are virtually untraceable and, more-often-than not, irreversible.

Transactions 2) and 3) require intermediaries. A check requires a bank account. Credit card transactions require at least two banks one to guarantee the initial transaction and a second to process the payment; in the case of transactions involving foreign currency, it requires a third.

Each intermediary collects fees as compensation for their part of the transaction, whether or not that fee is disclosed. Your bank earns interest on the money you've deposited. It may also charge you a fee to write a check, and another fee if your account balance dips below a set amount. Credit card companies charge retailers and other businesses fees as high as 3% of every transaction. Some charge credit card holders steep annual fees as well. Today, over two-thirds of transactions rely on plastic. Most of these involve credit cards.

To assure these transactions are legitimate, banks and credit card companies (often the same entity) have huge, centralized databases containing critical information about their customers. This information must be kept up-to-date in real time, so they can be shared with other centralized databases to verify transactions. Credit card companies use the fees they charge to maintain these extensive databases and generate a profit.

Centralized Databases Are Extremely Vulnerable to Hacking and Loss of Privacy

The centralized nature of these databases makes them extremely efficient. However, this centralization is vulnerable to hacking and, once hacked, can expose millions of credit card and bank account holders to monetary and identity theft. That’s what happened when the credit rating company Equifax was hacked in 2017 and the Social Security numbers, birth dates and home addresses of up to 143million Americans 44% of the US population were stolen.

Stolen personal data is not the only threat. What these companies do with your data, even when they are not hacked, represents a loss of privacy as well. All of your transactions, including what you bought, how much you bought and where you bought it, are up for sale to companies who use that data to market to you.

Why Bitcoin Is Different

Bitcoin is based on technology known as a Blockchain. This is essentially a database composed of individual blocks of data or in the case of Bitcoin, blocks of transactions. Each block in the Bitcoin Blockchain has a time stamp and is related to the block that comes before it. There are no names, addresses, phone numbers or other personal information associated with Bitcoin transactions. All transactions take place purely in code, which make them completely anonymous.

Once a new block of Bitcoin transactions is added to the chain, its time stamp and relationship to an earlier block means Bitcoin transactions cannot be easily altered or deleted without altering every subsequent transaction in the chain.

Imagine a brick building that is being perpetually constructed as workmen add more and more bricks every day. Every single brick (or block) represents an independent transaction. Every brick has a relationship with the bricks directly surrounding it, yet every brick is also an essential part of the whole structure.

Imagine trying to change or remove a single brick (or block) without knowing where that brick was in the structure or when it was placed there. Now imagine trying to do this without altering the structure as a whole. Any attempt to change any part of the Blockchain would be noticed immediately. It would be like removing a single brick from a wall; it would stick out like a gaping hole.

While an imperfect analogy, this gives you an idea of how difficult it would be to hack the Bitcoin Blockchain. The expense and computing power to attempt such a task would be astronomical and uneconomical. This is one of the reasons why the Bitcoin Blockchain has never been hacked. The bigger the Blockchain, the harder it is to alter any block in the chain, and the more computing power it takes to manage it. This becomes particularly important when it comes to mining bitcoin.

Bitcoin Does Not Need a Centralized Database

Like the bricks in our metaphorical building, bitcoin is made up of individual blocks that when viewed together contain the whole encrypted record of every bitcoin transaction ever made. This eliminates the need for a central database and makes bitcoin extremely mobile. The Bitcoin Blockchain ledger can reside anywhere or everywhere on the web. It is borderless.

Because each block in the chain is only related to a previous block, no one making transactions on the Bitcoin ledger has access to the entire database. Bitcoin users only access those parts of the Blockchain they own by using private encrypted keys.

Private keys (basically, unique pieces of encrypted code) allow a user to rewrite only those parts of the Bitcoin ledger that involve themselves and the entities on the other side of the transaction. Bitcoin keys are used to access addresses that contain units of currency, which can then be transferred directly to a recipient.

Once a private transaction takes place, it is added to the Blockchain and becomes part of the ledger, creating an unalterable and undeletable record. This eliminates the need for centralized record-keeping. The same architecture responsible for facilitating the transaction creates and stores the record. Aside from Bitcoin miners who verify the integrity of the transaction, no middlemen are required to ensure its legitimacy.

The only parties that can access the details of a specific transaction are the parties involved in that transaction who hold the same encrypted key. No names, addresses or other personal data is required. This makes Bitcoin and its other crypto-currency cousins very valuable to those wishing to keep their financial comings and goings on the down low. It is why bitcoin gained its initial notoriety on the dark web as the preferred means of exchange for drug transactions a dubious distinction it still holds