# WHAT CAN BLOCKCHAIN DO?

Financial institutions have financed the disruption of countless industries over the last 30 years; they have an idea of what a revolutionary technology can do to static incumbents.

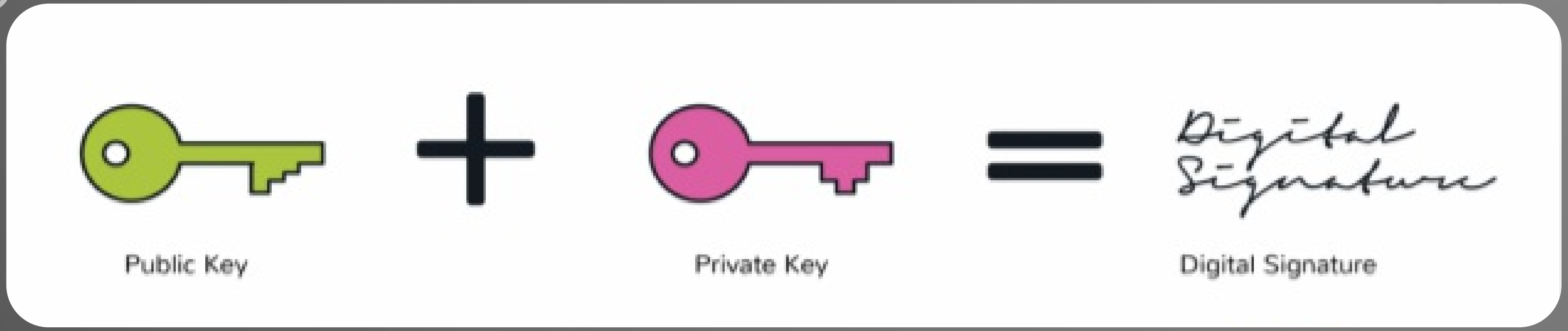
So, to stay ahead of change, banks have been proactive in setting up R&D labs, building test centers and establishing partnerships with blockchain developers to fully understand the revolutionary potential of the technology.

Financial institutions were the first to dip their feet in, but academia, governments and consulting firms have also studied the technology.

All of this work is, of course, in addition to what the entrepreneurs and developers are doing, either by finding new ways to use the bitcoin or ethereum blockchains, or else creating entirely new blockchains.

MorCryp

# ESTABLISH DIGITAL IDENTITY



As discussed in our guide "How Does Blockchain Technology Work?", the identity component of blockchain technology is fulfilled through the use of cryptographic keys. Combining a public and private key creates a strong digital identity reference based on possession.
A public key is how you are identified in the crowd (like an email address), a private key is how you express consent to digital interactions. Cryptography is an important force behind the blockchain revolution

MorCryp

# SERVE AS A SYSTEM OF RECORD

As stated in our guide "What is a Distributed Ledger?", blockchains are an innovation in information registration and distribution. They are good for recording both static data (a registry) or dynamic data (transactions), making it an evolution in systems of record.
In the case of a registry, data can be stored on blockchains in any combination of three ways:

- **UNENCRYPTED DATA** - can be read by every blockchain participant in the blockchain and is fully transparent.

- **ENCRYPTED DATA** - can be read by participants with a decryption key. The key provides access to the data on the blockchain and can prove who added the data and when it was added.

- **HASHED DATA** - can be presented alongside the function that created it to show the data wasn't tampered with. Blockchain hashes are generally done in combination with the original data stored off-chain. Digital 'fingerprints', for example, are often hashed into the blockchain, while the main body of information can be stored offline.
Such a shared system of record can change the way disparate organizations work together.

Currently, with data siloed in private servers, there is an enormous cost for inter-company transactions involving processes, procedures and cross-checking of records.

MorCryp

# PROVE IMMUTABILITY

A feature of a blockchain database is that is has a history of itself. Because of this, they are often called immutable. In other words, it would be a huge effort to change an entry in the database, because it would require changing all of the data that comes afterwards, on every single node. In this way, it is more a system of record than a database.

# SERVE AS A PLATFORM

Cryptocurrencies were the first platform developed using blockchain technology. Now, people have moved from the idea of a platform to exchange cryptocurrencies to a platform for smart contracts.

The term 'smart contracts' has become somewhat of a catch-all phrase, but the idea can actually be divided into several categories:

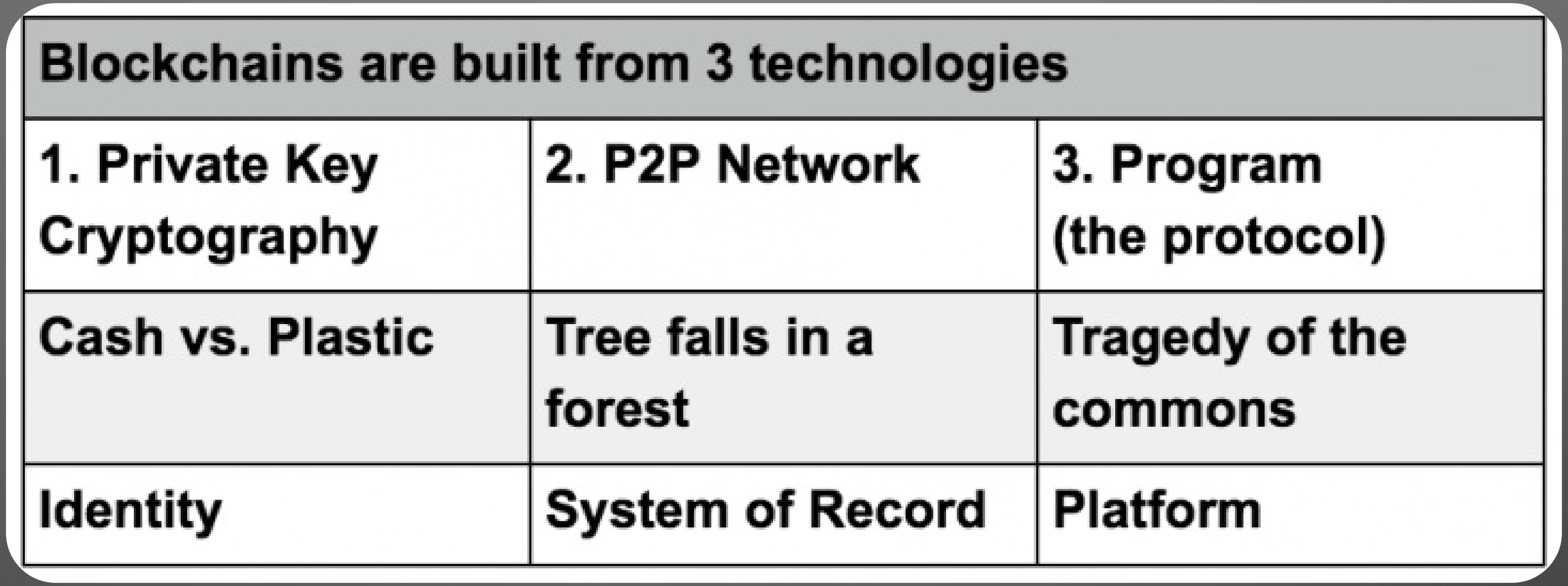
There are the 'vending machine' smart contracts coined in the 1990s by Nick Szabo. This is where machines engage after receiving an external input (a cryptocurrency), or else send a signal that triggers a blockchain activity.

There are also smart legal contracts, or Ricardian contracts. Much of this application is based on the idea that a contract is a meeting of the minds, and that it is the result of whatever the consenting parties to the contract agree to. So, a contract can be a mix of a verbal agreement, a written agreement, and now also some of the useful aspects of blockchains like timestamps, tokens, auditing, document coordination or business logic.

MorCryp

Finally, there are the ethereum smart contracts. These are programs which control blockchain assets, executed over interactions on the ethereum blockchain. Ethereum itself is a platform for smart contract code.

Blockchains are not built from a new technology. They are built from a unique orchestration of three existing technologies.



| Blockchains are built from 3 technologies | | |
|---|---|---|
| 1. Private Key Cryptography | 2. P2P Network | 3. Program (the protocol) |
| Cash vs. Plastic | Tree falls in a forest | Tragedy of the commons |
| Identity | System of Record | Platform |

MorCryp