



WHAT ARE THE APPLICATIONS AND USE CASES OF BLOCKCHAINS?

Blockchain technology is a revolution in systems of record. Bitcoin is history's first permanent, decentralized, global, trustless ledger of records. Since its invention, entrepreneurs in industries around the world have come to understand the implications of this development. The nature of blockchain technology has got imaginations running wild, because the idea can now be applied to any need for a trustworthy record. It is also putting the full power of cryptography in the hands of individuals, stopping digital relationships from requiring a transaction authority for what are considered 'pull transactions'. For sure, there is also a lot of hype. This hype is perhaps the result of how easy it is to dream up a high-level use case for the application of blockchain technology. It has been described as 'magic beans' by several of the industry's brightest minds. There is more on how to test whether blockchain technology is appropriate for a use case or not in our guide "Why Use a Blockchain?". For now, we turn to a discussion of the development of blockchain technology for *how* it could be useful.

AS A SYSTEM OF RECORD

DIGITAL IDENTITY

Cryptographic keys in the hands of individuals allow for new ownership rights and a basis to form interesting digital relationships. As we've discussed in our guides "What is Blockchain Technology?", "How Does Blockchain Technology Work?" and "What Can a Blockchain Do?", blockchains provide an opportunity to establish a strong system for digital identity.

Because it is not based on accounts and permissions associated with accounts, because it is a push transaction, and because ownership of private keys is ownership of the digital asset, this places a new and secure way to manage identity in the digital world that avoids exposing users to sharing too much vulnerable personal information.

TOKENIZATION

For the purposes of authenticating a unique physical item, the items are paired with a corresponding digital token. This essentially means tokens are used as to bind the physical and digital worlds. These digital tokens are useful for supply chain management, intellectual property, and anti-counterfeiting and fraud detection



MorCryp

INTER-ORGANIZATIONAL DATA MANAGEMENT

As stated in our guide "What is a Distributed Ledger?", blockchain technology represents a revolution in how information is gathered and collected. It is less about maintaining a database, more about managing a system of record.

FOR GOVERNMENTS:

Governments have an interest in all three aspects components of blockchain technology. Firstly, there's the ownership rights surrounding cryptographic key possession, revocation, generation, replacement, or loss.

They also have an interest in who can act as part of a blockchain network.

And they have an interest in blockchain protocols as they authorize transactions, as governments often regulate transaction authorization through compliance regimes (eg stock market regulators authorize the format of market exchange trades).

For this reason, regulatory compliance is seen as a business opportunity by many blockchain developers.

FOR AUDIT TRAILS:

Using the client-server infrastructure, banks and other large institutions that help individuals form digital relationships over the internet are forced to secure the account information they hold on users against hackers.

While banks can spend the billions of dollars to keep information secure, the system is currently asking businesses to do the same. We are sharing the same information with these businesses as we are with the banks, after all. Yet, businesses are under attack and have been hacked, resulting sometimes in the exposure of customers' intimate financial details.

Blockchain technology offers a means to automatically create a record of who has accessed information or records, and to set controls on permissions required to see information.

This also has important implications for health records.



MOFCRYPT

AS A PLATFORM FOR SMART CONTRACTING

Blockchains are where digital relationships are being formed and secured. A consortium of the largest banks in the world, as well as several insurance companies, led by a startup, is seeking to build a platform to establish new digital relationships between banks themselves. Their approach to securing these new digital relationships is a combination of Ricardian contracts and coded business logic.

In short, this version of smart contracts seeks to use information and documents stored in blockchains to support complex legal agreements.

Other startups are working on sidechains - bespoke blockchains plugged into larger public blockchains. These 'federated blockchains' are able to overcome problems like the block size debate plaguing bitcoin. It is thought these groups will be able to create blockchains that authorize super-specific types of transactions.

Ethereum takes the platform idea further. A new type of smart contracting was first introduced in Vitalik Buterin's white paper, "A Next Generation Smart Contract and Decentralized Application Platform". This vision is about applying business logic on a blockchain, so that transactions of any complexity can be coded, then authorized (or denied) by the network running the code.

As such, ethereum's primary purpose is to be a platform for smart contract code, comprising of programs controlling blockchain assets, executed by a blockchain protocol, and in this case running on the ethereum network.



МорСгуп

FOR AUTOMATED GOVERNANCE

Bitcoin itself is an example of automated governance, or a DAO (decentralized autonomous organization). It, and other projects, remain experiments in governance, and much research is missing on this subject.

FOR MARKETS

Another way to think of cryptocurrency is as a digital bearer bond. This simply means establishing a digitally unique identity for keys to control code that can express particular ownership rights (eg it can be owned or can own other things). These tokens mean that ownership of code can come to represent a stock, a physical item or any other asset. Rules on how these instruments can be transacted can be coded by a blockchain protocol.

FOR STREAMLINING OF CLEARING AND SETTLEMENT

In the world of stock trading, we often hear the term 'T+3'. This means, a trade (T) is followed by three days before the trade is accepted (settled). There are non-blockchain ways to get this number down, but not without compromising security and risk.

With blockchain technology, however, trade is settlement, and we have a T+0 equation.



Beyond just being a trusted repository of information, blockchain technology could enable regulatory compliance in code form - in other words, how blocks are made valid could be a translation of government legal prose into digital code.

In the case of banks, for example, this could mean improving efficiency in anti-money laundering (AML) compliance. Blockchain technology can be calibrated to do different things - permit transactions or report transactions of a certain type according to exact rules.

This means that banks could automate regulatory reporting or transaction authorization.

IN SHORT

All of this work is allowing people to secure digital relationships that were impossible before. Data is being disclosed differently, secured differently and recorded differently.

This is changing digital relationships, creating the ability for them to be automated in code via 'smart contracts'.



МорСгуп