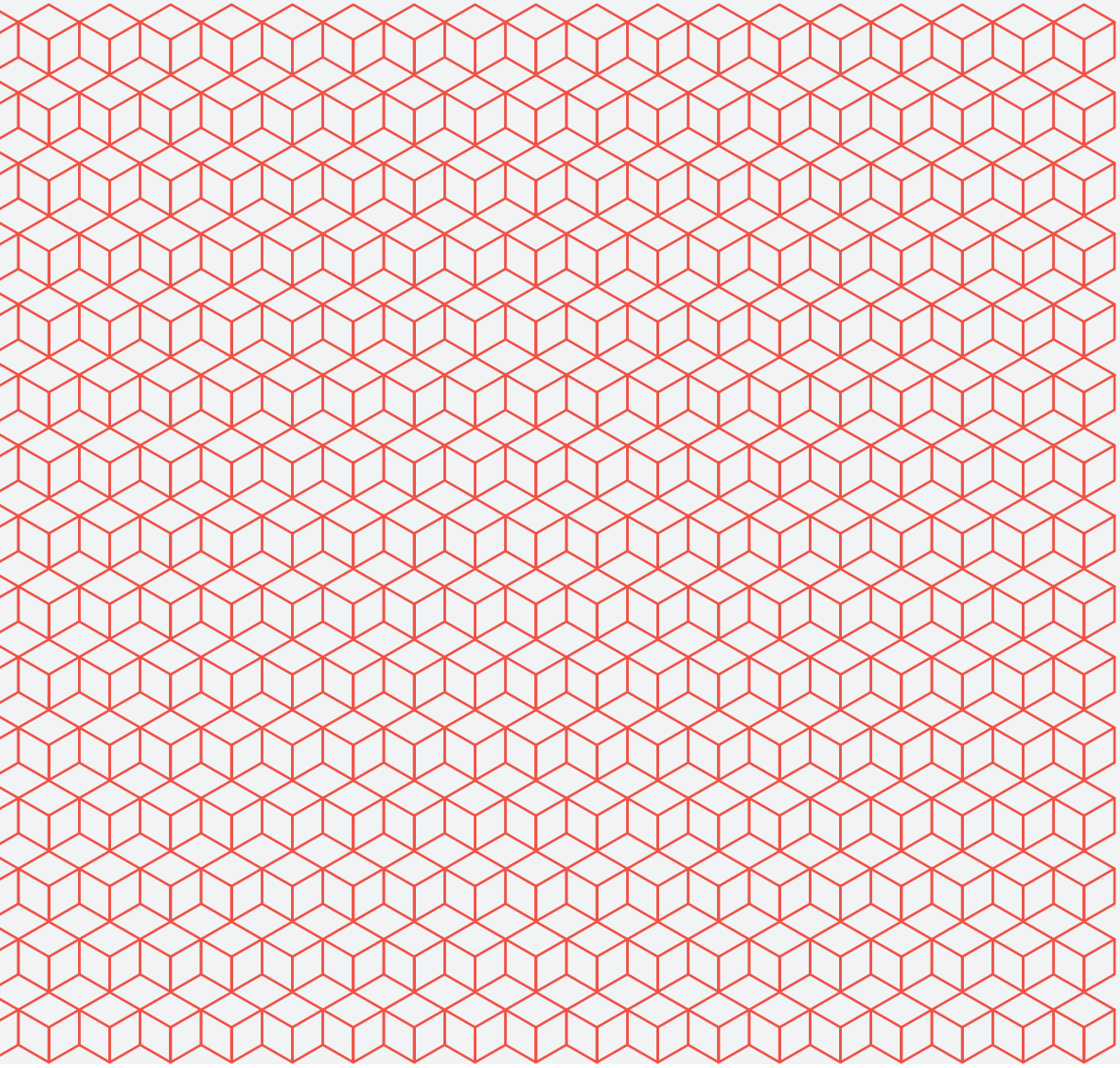
Tokenscope

Introduction to Cryptoassets

Connor DiGregorio



Abstract:

This is a complementary introduction report on the world of cryptoassets. It contains a brief overview of some of the most important aspects in the crypto space. It covers the basics of blockchain technology, explains a few compelling uses cases, and highlights some of the most important tools and resources for new users to get aquainted with.

For more in-depth explaination and analysis of particular cryptoassets or industries, be sure to check out our library of research products at tokenscope.io

CONTENTS

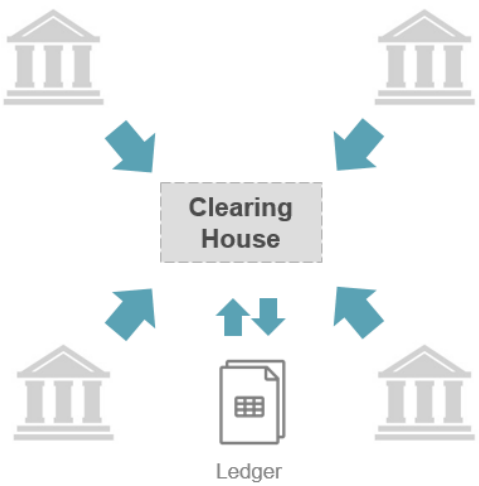
Blockchain Technology

What is blockchain technology?

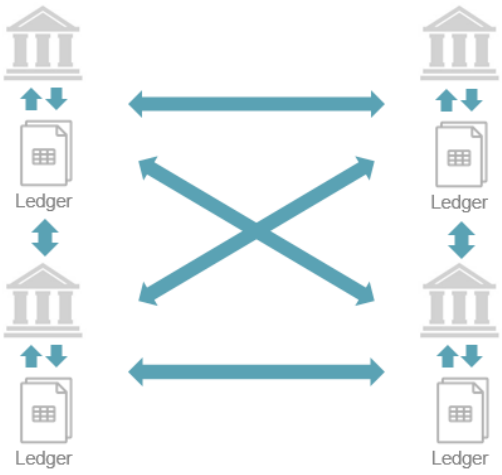
A blockchain is a history of transactions parsed out into segments, or blocks, that are held on a distributed database that is shared by all parties on the network. Every transaction is recorded and stored to create an unchangeable and auditable transaction log. Blockchain can be considered a superior database where data is encrypted. Additionally, data is append-only, meaning once something is recorded on a blockchain, it cannot be erased or tampered with. Additionally, because data is simultaneously shared across a multitude of servers, it is considered more secure and more transparent than traditional data storage systems.

The reason it is called a blockchain is because data, usually in the form of transactions, are organized into batches, or blocks, that are then strung together linearly with each block containing a timestamp and information linking it to the previous block. Thus, a chain of blocks is formed over time. A blockchain is often times used interchangeably with "distributed ledger" or "distributed ledger technology", often shortened to DLT.

Of the many unique features of blockchain, one of the most notable is its decentralized nature. Rather than trusting a single, third party to record transactions and securely hold data, a blockchain allows a network of many different users to come to a consensus on the proper history of the ledger. The innovation here is that this can be done securely among a massive number of users without any users having to know or trust one another. This provides the foundation for digital, trustless, peer-to-peer transactions, which can be done instantly between any two strangers on the globe. Until blockchain technology, that was not possible.



Centralized Model



Decentralized Model

Sources: bits-atoms.net

Advantages of Blockchain

- Less Reliance on Trusted Third Parties
- Increased Security
- More Autonomy
- Time and Cost Savings
- Globally Accessible
- Transparency and Privacy

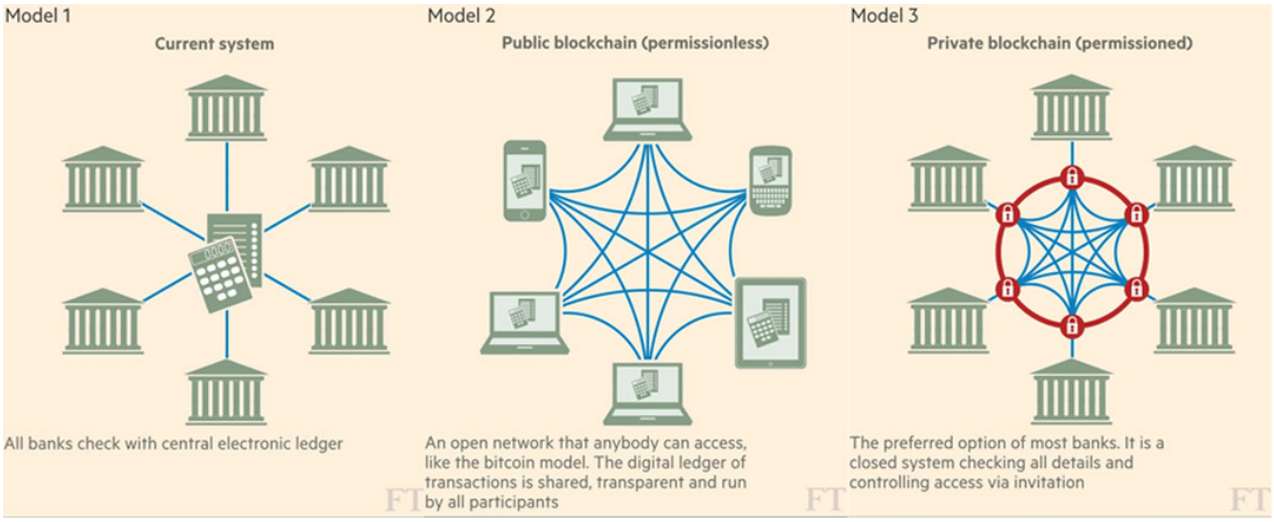
Nuances of Blockchains

There are many iterations of blockchain technology. What was described on the previous page is the backbone of the technology, however it may come in several different forms. For instance, there are notable distinctions between public blockchains and private blockchains.

A public blockchain is one that has a ledger that is openly viewable by anyone. The history of a public blockchain has a complete, transparent history of transactions available for viewing in real time. A private blockchain is the opposite, containing a private ledger and is only viewable to a select group of individuals or entities.

Though there can be exceptions, a public blockchain is typically permissionless, meaning that anyone can participate freely in it. No gatekeeper or group of gatekeepers can prevent an actor from interacting with other actors on the network. A private blockchains is typically also a permissioned blockchain where authorization is required for participation.

It should be noted that development for most applications of blockchain technology is still in its infancy. However, when these projects get fully fledged out, they have the potential to completely upend entire industries. The common thread across the variety of different sectors is blockchain as a disintermediator. Blockchain's real technological leap forward is its ability to cut out the middleman for all types of transactions. In the following sections, we breifly highlight some real use cases of different blockchains.

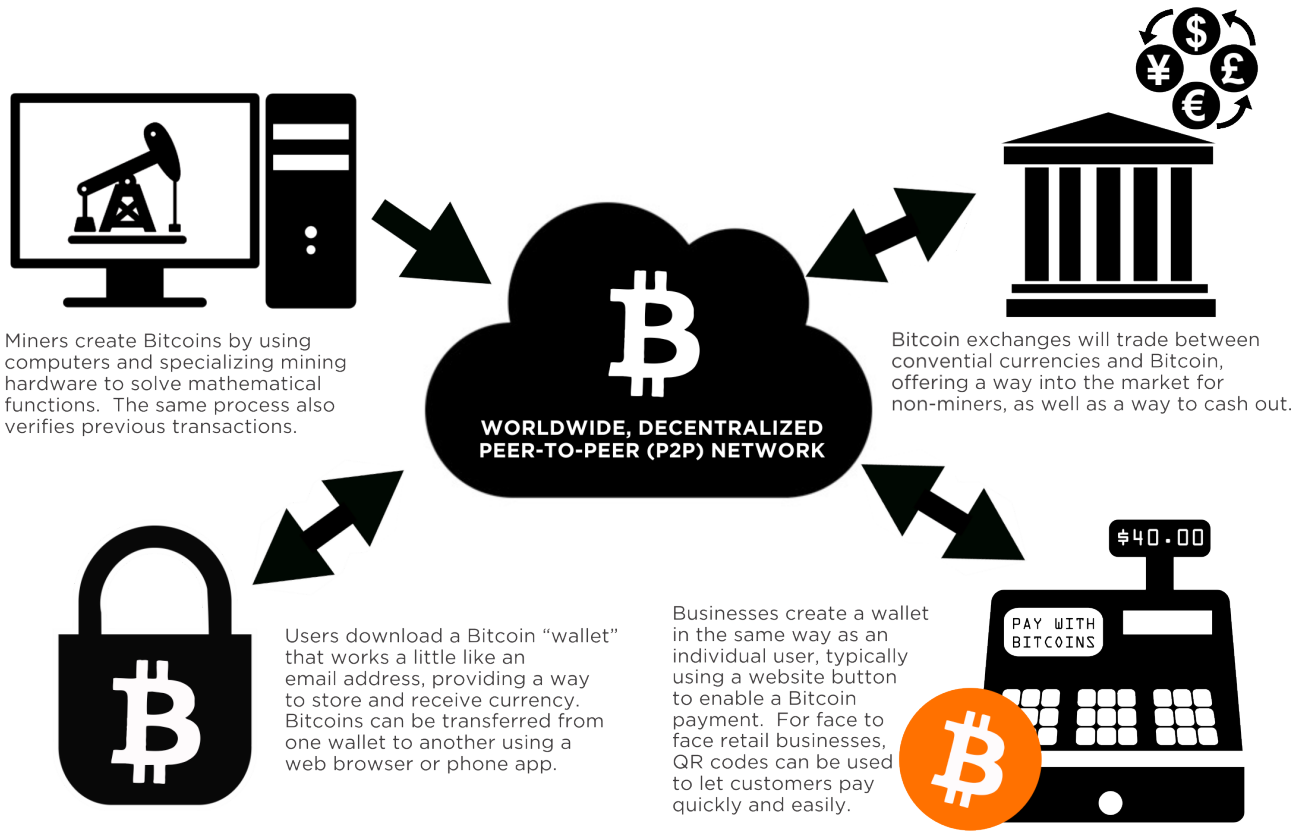


Source: Financial Times

Bitcoin: a cryptocurrency

Bitcoin was the first project to implement blockchain technology and was designed as an electronic peer-to-peer cash system. As such, it provides a way for two people to move money around without having to rely on a third party, which, in our current system, would typically be a bank. In many cases now, when paying over the internet, it relies on multiple third parties, such as Paypal, Venmo, or other payment processors. Bitcoin cuts out any and all middleman, allowing users to directly engage in commerce. Users can have full custody over their money and no singular clearinghouse exists. Rather, the distributed network of miners and other users verify and record all transactions on the network, in effect decentralizing the functions of the traditional banking system.

The potential for Bitcoin becomes most noticeable when transacting across borders. For instance, if an American business is buying a large order of shirts from a textile manufacturer in Mexico. Typically, that payment would involve several different entities, such as a US Bank, a clearinghouse, SWIFT, a correspondent bank, and a Mexican Bank. The process could take over a week and would incur fees along the way. If that same transaction were to take place in Bitcoin, it could be completed within minutes and only cost a few cents in transaction fees. Additionally, the American business and the Mexican business would be the only two parties to ever have handled the money, completely eliminating third-party custodial risk. There are many other instances where using Bitcoin, or other similar cryptocurrencies,



Source: sercuracoin.com

Other Types of Cryptoassets

While Bitcoin functions as a pure currency, there are other cryptoasset that go beyond that. They provide functionality for a variety of scenarios while utilizing the same underlying blockchain technology. Examples of other subclasses of cryptoassets include utility tokens, security tokens, and other tokenized assets.

Utility Tokens

Ether: The native token used on Ethereum, which is a permissionless platform for decentralized applications to run on top of. Sometimes referred to as a decentralized world computer, it enables thousands of other cryptoassets to exists, much in the same manner Windows OS enabled thousands of new apps to function.

Other platforms: EOS, Cardano, NEO, Dfinity, Waves

Binance Coin: A token used on the cryptoasset exchange, Binance. Using this token to trade holds advantages such as cheaper trading fees. Additionally, it will be the main token used in the new decentralized exchange that Binance is building.

Basic Attention Token: A token used in an internet browser called Brave that exchanges value between advertisers, websites and users in a peer-to-peer fashion. Users can earn money paid directly from advertisers for not blocking ads and websites can earn money directly from users' activity on their pages.

Other Tokenized Assets

In theory, there are many assets that can be tokenized. While this is still relatively unexplored in the space, many projects attempting to create these new types of cryptoassets exist. Here are a few examples:

Security Tokens: Tokens that function as a claim to ownership in a company in the same manner as a traditionally regulated security. These tokens follow all compliance by regulatory bodies, such as the SEC, and provide benefits such as dividends and voting rights. The main difference from a tradiotional security is that the token is registered and traded on a blockchain. This is a new type of asset with 2018 being the first year any such type existed.

Tokenized Real Estate: This can come in the form of a simple tokenized deed that is registered and exchanged on a blockchain. Or, this can mean creating fractional ownership with tokens representing minority shares to a property, which can then be traded digitally online.

Tokenized Intellectual Property: This includes assets such as patents, songs, movie scripts, and many other forms of IP. Basically, any idea that holds real value and can be bought and sold can be turned into a token.

Tokenizing these types of assets brings advantages such as greater liquidity, immutable history of ownership, fractional ownership, automated payouts (i.e. rent, royalties), and cutting out expensive middlemen. Of course, there are challenges that come with tokenization, but these are the possibilities that will soon be realities.

Custody & Wallets

One of the innovations of cryptoassets, particularly cryptocurrencies, is the ability to easily self-custody assets. In traditional banking and investment, rarely do you hold your own assets. Typically, a bank will custody your cash and large investment instutions will custody assets like stock, bonds, etc. However, with cryptoassets, there is the option to completely control all the assets that you own. This is done in the form of private wallets. Private wallets are extremely secure and only the person with the unique cryptographic key (i.e. secret password), can access these assets.

Now, self-custody is not always the preferred option for investors. There are more tradition models of custody available, too. Trading on centralized exchanges, such as Coinbase or Bittrex, means that those platforms have complete custody of the assets. Trading on platforms like these may be a better fit for some investors, but it is important they understand the difference between those and private wallets.

Another important concept to understand is the difference between a hot wallet and a cold wallet. Both differ in the type of security and liquidity that they offer. We'll talk in terms of bitcoin for simplicity's sake.

Hot Wallet:

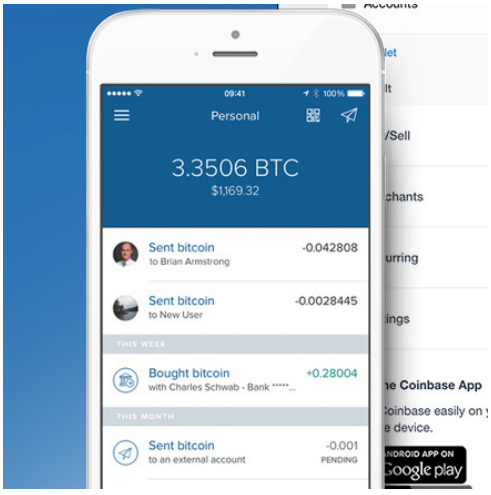
A wallet that is constantly connected to the Bitcoin network. It is connected to the internet and bitcoin can instantly be traded in and out of the wallet. Hot wallets can be both privately controlled, such as My Ether Wallet, or controlled by a third party, such as Coinbase.

Cold Wallet:

A wallet that is not connected to the internet. While bitcoin cannot be sent out of it, it can still receive bitcoin to its address. Cold wallets are used for offline storage. Common examples include hardware wallets, such as a Ledger Nano S, and a paper wallet, which is a piece of paper with the bitcoin address printed on it. Cold wallets are considered the most secure way to store bitcoin.

Wallet Providers

1. Jaxx
2. My Ether Wallet
3. Metamask
4. Trezor
5. Ledger Nano S
6. Exodus



Third-Party Hot Wallet on Coinbase

Personal Cold Wallet with Ledger

References

Top News Outlets:

1. Coindesk.com
2. Cointelegraph.com
3. Bitcoinmagazine.com
4. Ethnews.com

Market Data:

1. Coinmarketcap.com
2. Coincheckup.com
3. Cryptocompare.com

Exchanges:

1. Binance
2. Bittrex
3. Shapeshift
4. Coinbase/GDAX
5. Gemini
6. Kraken
7. Bitfinex (not available to US citizens)

Thought Leaders

- Andreas Antonopoulos
@aantonop
- Chris Burniske
@cburniske
- Nick Szabo
@NickSzabo4
- Vitalik Buterin
@VitalikButerin
- Charlie Lee
@SatoshiLite
- Dan Larimer
@bytemaster7
- Amber Baldet
@AmberBaldet
- Blythe Masters
@BlytheMasters
- Erik Voorhees
@ErikVoorhees
- Michael J Casey
@mikejcasey
- Laura Shin
@laurashin
- Charlie Shrem
@CharlieShrem
- Roger Ver
@rogerkver

Dictionary

Blockchain: a history of transactions parsed out into segments, or blocks, that are held on distributed database that is shared by all parties on the network. Every transaction is recorded and stored to create an unchangeable and auditable transaction log.

Consensus Mechanism: The process in place in distributed systems that allows every node to come to a single conclusion about its shared data. Every blockchain system has consensus mechanism, though there are various models that exist. The most common two are Proof-of-Work and Proof-of-Stake.

Cryptoasset: any digital property that is built on top of blockchain technology. This commonly refers to cryptocurrencies but may also refer to other types of blockchain-based assets. Other examples are tokenized real estate, tokenized intellectual property, unique digital collectibles (i.e. CryptoKitties) and many other forms.

Distributed Ledger: a type of database architecture whereby all nodes within a system cooperate to reach a consensus on the accurate state of a shared data resource, sometimes used interchangeably with the word blockchain.

Initial Coin Offering: a process in which blockchain projects raise funds, usually in the form of cryptocurrency, in exchange for a newly created cryptocurrency that will be native to the blockchain system they are creating.

Miners: The individuals or entities that engage in the processing of using computing power to verify new transactions on the distributed ledger in return for newly "minted" or mined cryptocurrency. Miners are a primary feature in a Proof-of-Work model.

Permissioned Blockchain: a type of blockchain that is limited to a set of approved entities that are able to restrict access from outside parties.

Permissionless Blockchain: a type of blockchain where any party is free to view, transact and wholly participate in without approval or censorship.

Proof of Work: A type of consensus mechanism wherein miners use computing power to solve a complex algorithm and get a mining reward for doing so. In the process of solving the algorithm, the transactions of the distributed system are confirmed, thus creating a single ledger for the network.

Proof of Stake: A type of consensus mechanism that does not require miners to confirm transactions, but rather has nodes that buy into the network with its native currency. The nodes who have put up a "stake" in the network confirm the transactions in this model. Nodes who try to falsely confirm transactions are punished by losing their coins that they put up, thus disincentivizing falsifying data.

Smart Contract: a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract without the need for any third-party involvement. Smart contracts were first proposed by Nick Szabo in 1994.

Disclaimer

Tokenscope

For more reports and research visit
www.tokenscope.io