BlockchainHub

Blockchain

A Beginners Guide

Blockchain
Web3
Cryptoeconomics
Tokens
Smart Contracts
DApps
DAOs
ICOs

Date: September 30, 2017
Authors: Shermin Voshmgir, Valentin Kalinov
Publisher: BlockchainHub Berlin, https://blockchainhub.net/

This handbook will not be updated.
A more comprehensive follow up to this handbook has been developed into a textbook:
"Token Economy", by Shermin Voshmgir, 312 pages, 2019

Please note:
Blockchain and other decentralized web technologies are still in their early stages of development. The underlying tech, as well as use cases and players on the market are changing rapidly. While we tried to stay as neutral and general as possible, some information in this document might be outdated shortly after publishing.

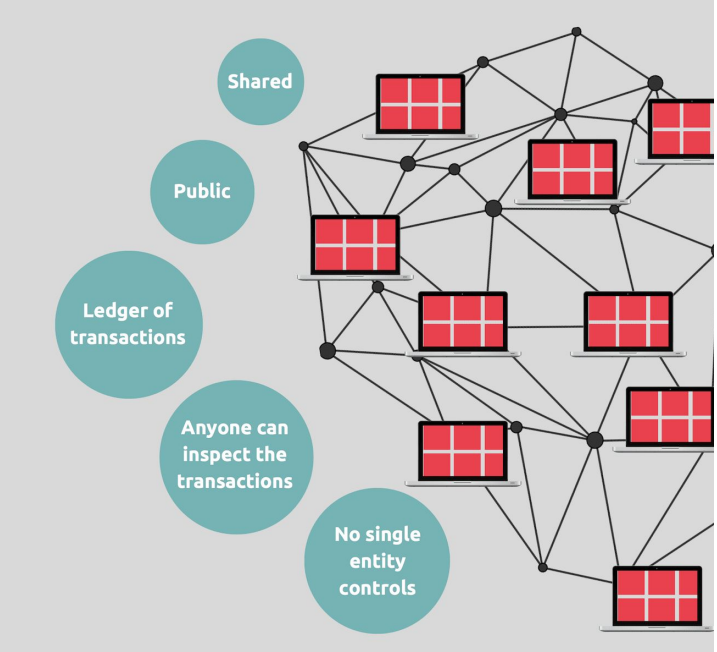
Table of Contents

Blockchain Basics

In this first part we cover the fundamentals of blockchains, smart contracts and the decentralized web. The idea is to give you an overview of how the tech works and why blockchain can be a game changer. In the second part we will focus on some practical “how to” guides.

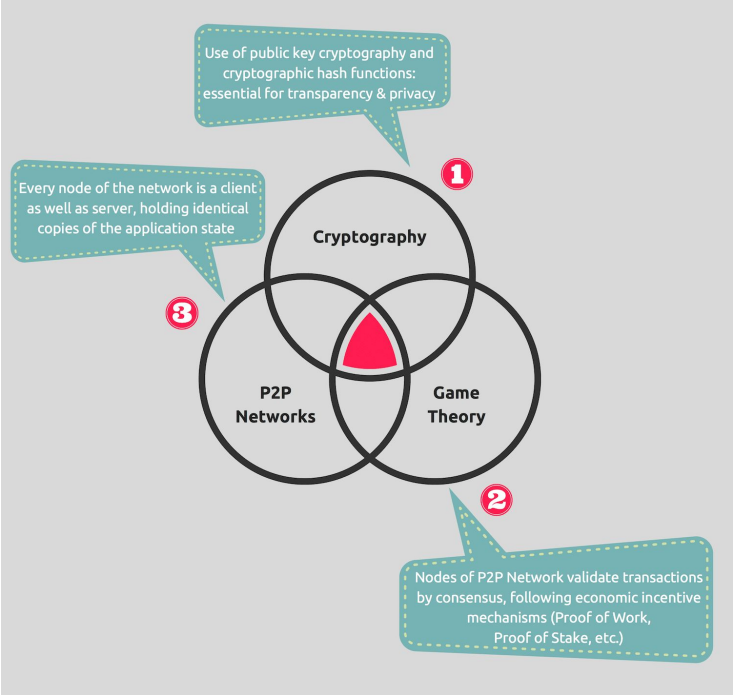
Blockchain

Blockchain, the technology behind Bitcoin, seems to be the driving technology behind the next generation Internet, also referred to the Decentralized Web, or the Web3. The blockchain is a novel solution to the age-old human problem of trust. It provides an architecture for so-called trustless trust. It allows us to trust the outputs of the system without trusting any actor within it.



Blockchain: Like a Spreadsheet in the Sky
Source: Blockchainhub.net

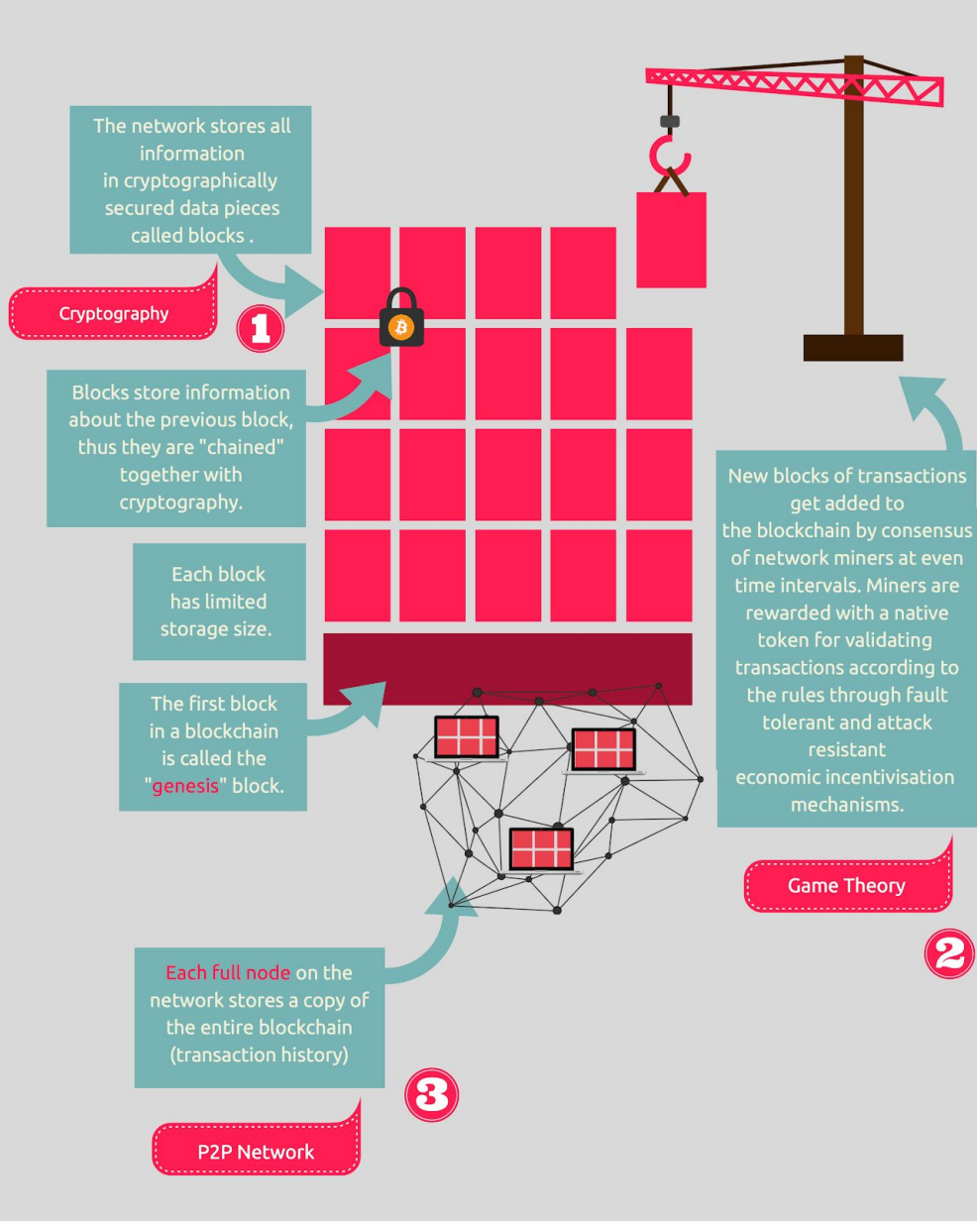
Blockchain is a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls. It is a distributed database that maintains a continuously growing list of transaction data records, cryptographically secured from tampering and revision.



Combination of 3 Technologies
Source: Blockchainhub.net

A Blockchain protocol operates on top of the Internet, on a P2P Network of computers that all run the protocol and hold an identical copy of the ledger of transactions, enabling P2P value transactions without a middleman though machine consensus. Blockchain itself a file - a shared and public ledger of transactions that records all transactions from the genesis block (first block) until today.

The ledger is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a given timespan. The crypto-economic rulesets of the blockchain protocol (consensus layer) regulate the behavioral rulesets and incentive mechanism of all stakeholders in the network.



Why is it called a Blockchain?
Source: Blockchainhub.net

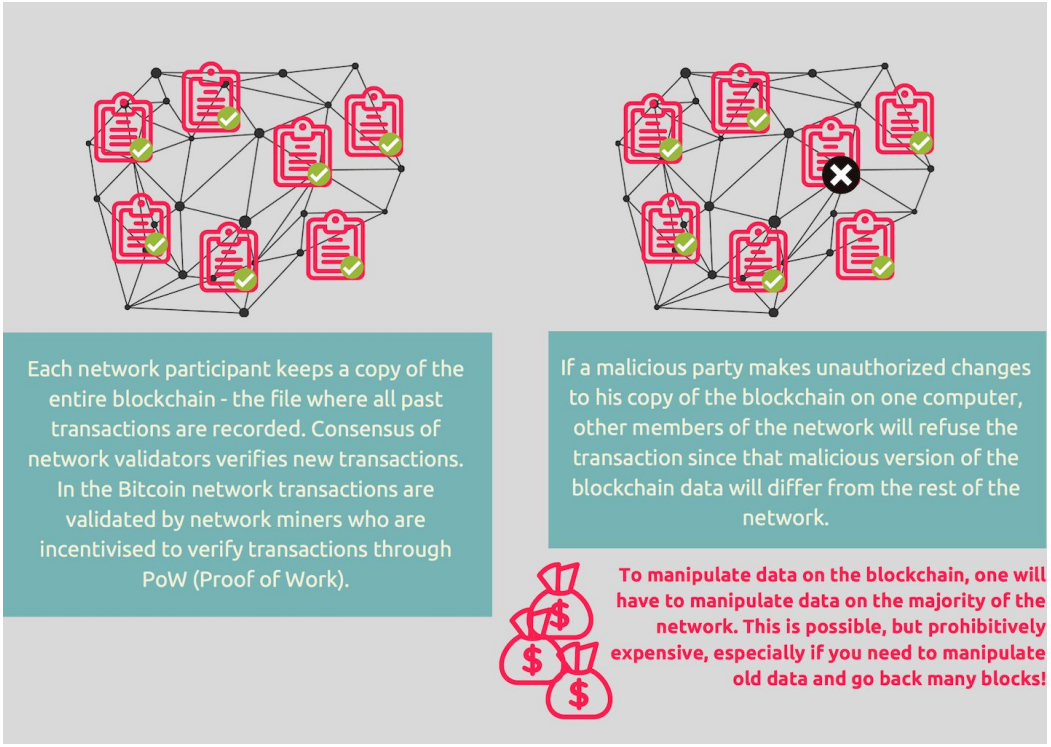
This ledger runs on a Peer-to-Peer (P2P) network of computers. Distributed consensus based on economic incentive mechanisms (game theory) combined with cryptography allows for secure P2P validation of transactions, thus bypassing the need for traditional trusted third parties.

It first came to fame in October 2008 as part of a proposal for Bitcoin, with the aim to create P2P money without banks. All network transactions get stored in the blockchain: Imagine Google Docs: Each person has the latest version of the document, and everybody can inspect it. In order to change the contents of the doc, users need to reach a mutual agreement (consensus).

As opposed to Google Docs the file is not centrally stored, but each node of the network keeps a copy of the blockchain - the distributed ledger recording all transaction history.

Removing the Middleman

Instead of a single trusted third party validating transactions through their servers with authority (single vote), a peer to peer network of computers running the blockchain protocol validates transactions by consensus (majority vote). The blockchain protocol, therefore, formalizes pre-defined consensus rules for approving transactions on the P2P network, as hard-coded governance rules, managing and auto enforcing transactions of all participants in the network.



Why is a Blockchain Tamper Resistant?
Source: Blockchainhub.net

In the case of Bitcoin, instead of a bank validating financial transactions - like sending money from A to B - checking the digital ledger of who owns what stored on their server, a P2P network of computers running the bitcoin protocol confirms transactions by majority consensus. The consensus rules of the Bitcoin network govern how the participants in the network interact with each other. They define:

- ❏ Under which conditions a transaction - sending money from A to B - is valid.
- ❏ Transaction costs related to sending money from A to B.
- ❏ Game theoretic incentive mechanism for validating transactions with a cryptographic token.
- ❏ Rules of how to change current consensus rules.

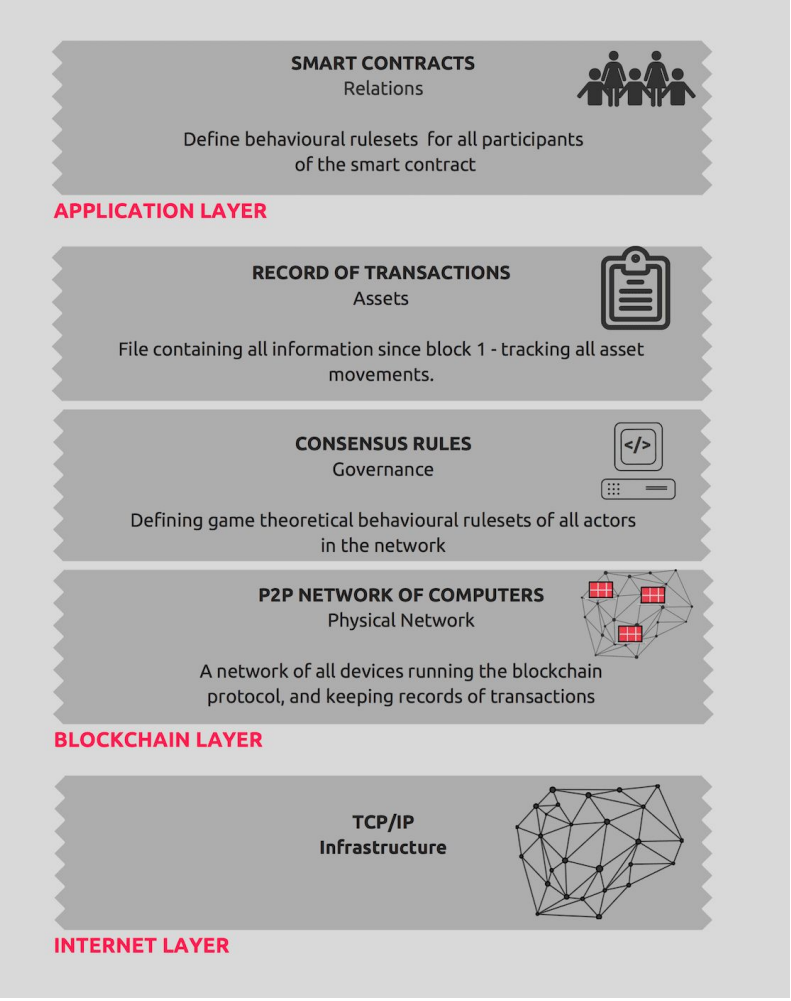
Smart Contracts

Blockchain was initially designed for P2P money only. But it soon showed the potential to be used for any kind of P2P value transaction on top of the Internet. The Ethereum project thus introduced the idea of decoupling the contract layer from the blockchain layer, where the ledger itself is used by smart contracts that trigger transactions automatically when certain pre-defined conditions are met. By decoupling the smart contract layer from the blockchain layer, blockchains like Ethereum aim to provide a more flexible development environment than the Bitcoin blockchain.

These smart contracts are a piece of code running on top of a blockchain network, where digital assets are controlled by that piece of code implementing arbitrary rules. They have properties of contractual agreements but should not be confused with legal contracts. (For more information on legal question around blockchain visit our **Blockchain & Law** page).

If and when all parties to the smart contract fulfill the pre-defined arbitrary rules, the smart contract will auto execute the transaction. These smart contracts aim to provide transaction security superior to traditional contract law and reduce transaction costs of coordination and enforcement.

Smart contracts can be used for simple economic transactions like sending money from A to B. They can also be used for registering any kind of ownership and property rights like land registries and intellectual property, or managing smart access control for the sharing economy, just to name a few. Furthermore, smart contracts can be used for more complex transactions like governing a group of people that share the same interests and goals. Decentralized Autonomous Organizations, DAOs, are such an example for more complex smart contracts.



Blockchain Technology Stack: Ethereum & similar Blockchains
Inspired by Florian Glatz: Source

With blockchains and smart contracts we can now imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision.

In this world every agreement, every process, task and payment would have a digital record and signature that could be identified, validated, stored, and shared.
Intermediaries like lawyers, brokers, and bankers, and public administrators might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction and a fraction of current transaction costs.

Blockchains & smart contracts:

- ❏ Radically reduce transaction costs (bureaucracy) through machine consensus and auto-enforceable code.

- ❏ Bypass the traditional principal-agent dilemmas of organizations, thus providing an operating system for what some refer to as "trustless trust". This means that you don't have to trust people and organizations, you trust code, which is open source and provides transparent processes.

Web3 - The Decentralized Web

In the early 1990's the WWW revolutionized information. Ten years later, the Internet became more mature & programmable. We saw the rise of the so-called Web2, which brought us social media and e-commerce platforms. It revolutionized social interactions, bringing producers and consumers of information, goods and services closer together, and allowed us to enjoy P2P interactions on a global scale.

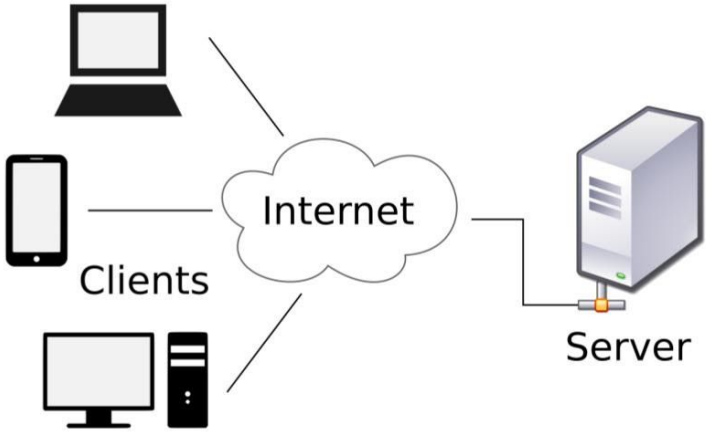
But always with a middleman: a platform acting as a trusted intermediary between A and B who did not know or trust each other. While these platforms have done a fantastic job at creating a P2P economy, with an ever more sophisticated content discovery layer, they also dictate all rules of the transactions, and these platforms own all of our data.

In this context Blockchain seems to be a driving force of the next generation Internet, the Decentralized Web, or Web3. Blockchain can bring us true P2P transactions without intermediaries, and Bitcoin is the first use case. While Bitcoin is P2P money without banks and bank managers, the same technology that brought us Bitcoin could now allow us to build ridesharing without Uber, apartment sharing without Airbnb, and social media without Facebook and Twitter.

Killing the Server: Redesigning Data Structures

We first had the computer, and then we started connecting computers over the internet protocol. In the early days of personal computers, we used to save data on a floppy disc, eject it, walk over to the colleague that needed the file, insert the floppy disc into that person's computer, and copy the file onto their computer so they could use it.

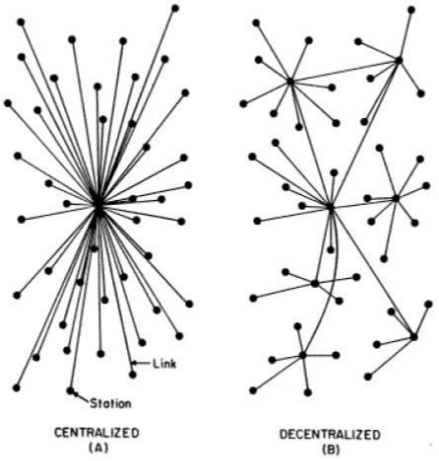
Data was centrally stored one physical device, in order to transfer data, copies needed to be made. The internet made the transfer of these copies faster and massively reduced transaction costs.



The Internet Today: A Client - Server World
Source: Client-Server Model, David Vignoni (2011)

30 years into mass adoption of the internet, our data architectures are mostly still client server based. Which means that our data is centrally stored on one computer, and retrieved via the Internet by another computer over the Internet. Even though we live in an ever more connected world, where every device whether toaster or fridge are also connected to the Internet, data is still centrally stored: on our devices, on the USB stick or even in the cloud.

This raises issues of trust: Can I trust those people and institutions that store my data against any form of corruption: internal or external, man made or machine failure, on purpose or by accident? Such centralized data structures have a unique point of failure points of failure. It's as if we never invented the Internet.



Centralized vs Decentralized
Modified from: On Distributed Communications; Introduction to distributed communications networks
Paul Baran (1964)

From Data Monarchy to Data Democracy

P2P data architectures have existed since the 1990's where they rose to fame with file sharing programs like BitTorrent and Tor browser. In combination with cryptography and game theoretic incentive mechanisms, Blockchain has taken P2P architectures to a new level. We can now start to move from centralized data structures where all data is stored on a central computer to more decentralized or entirely distributed data architectures.

Data Monarchy
Server

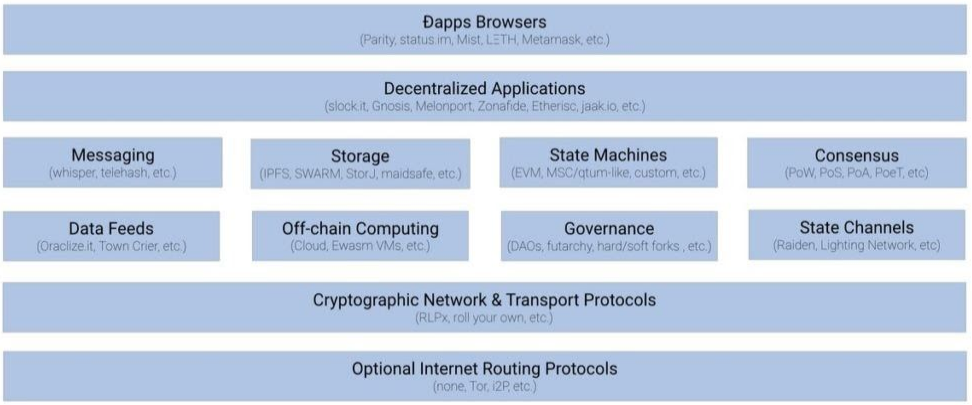
Data Democracy
P2P Networks

In the Web3, we are redefining data structure, given that we live in a connected world. It is important to note that Blockchain is only one of many technologies in this Decentralized Web Stack. While Blockchain is a great P2P way to record who did what and when, it is not ideal for storing large amounts of data, for two reasons: (1) scalability: blockchains are too slow, and (2) doesn't allow privacy by design: never store private data on the Blockchain.

Web3 Technology Stack

Similar to building a standard web or mobile applications, creating a dApp commonly requires a few things: computation, file storage, external data, monetization, and payments. The community has made a lot of progress building the ecosystem in the past four years.

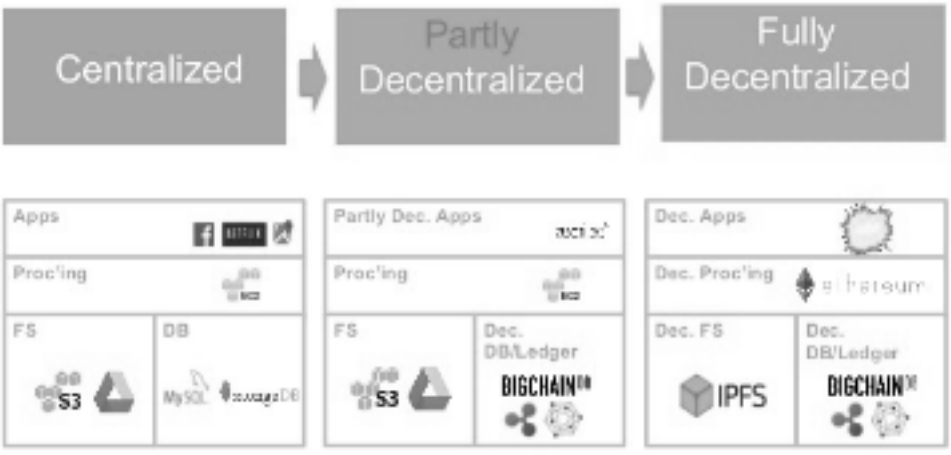
While it was borderline impossible to build a dApp in 2014, in 2017 it's feasible to build a basic dApp that requires minimal computation and file storage. The Web3 ecosystem has come a long way to develop a technology stack that devs can build upon. Here a listing of a few selected graphics:



General Web3 Stack
Source: The Web 3.0 Abstracted Stack by Stephan Tual (2017)

The transition from client-server internet to the decentralized web will be gradual rather than radical. As the decentralized web stack is still maturing, the transition seems to be shifting from centralized to partially decentralized to fully decentralized. Furthermore, it is important to point out that while decentralized architectures are more fault tolerant and attack resistant, they are also slower.

While it is likely that the future of the internet will be more decentralized, this does not mean that we will get rid of centralized systems altogether. Centralized systems also have advantages and will likely prevail, but only for specific use cases.



Decentralization of the Cloud
Source: Weaving the ILP Fabric into Bigchain DB, BigchainDB (2016)

Sources & Further Reading

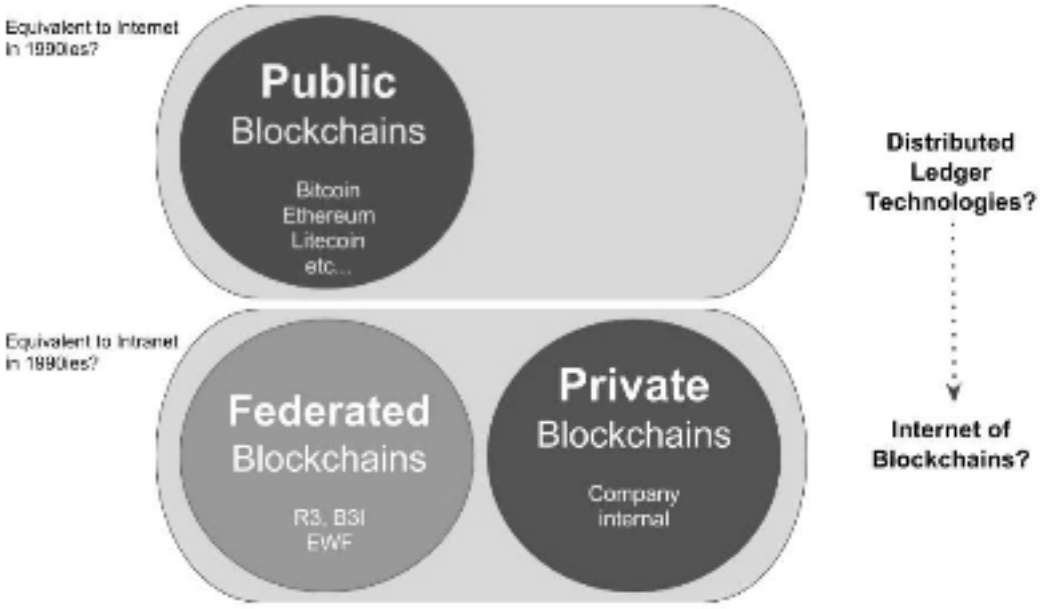
ĐApps: What Web 3.0 Looks Like, Gavin Wood
Ethereum White Paper
Bitcoin White Paper, Satoshi Nakamoto
The dApp Developer Stack: The Blockchain Industry Barometer, by Fred Ehrsam
Blockchain will usher in the era of decentralised computing, Bruce Pon, BigchainDB
Fat Protocols, Joel Monegro
The Shared Data Layer of The Blockchain Application Stack, Joel Monegro
Web 3.0 Revisited — Part One: "Across Chains and Across Protocols", Stephane Tual
Blockchain Infrastructure Landscape: A First Principles Framing, Trent McConaghy

Types of Blockchains

The Bitcoin White Paper was published by Satoshi Nakamoto in 2008; the first Bitcoin block got mined in 2009. Since the Bitcoin protocol is open source, anyone could take the protocol, fork it (modify the code), and start their own version of P2P money. Many so-called altcoins emerged and tried to be a better, faster or more anonymous than Bitcoin. Soon the code was not only altered to create better cryptocurrencies, but some projects also tried to alter the idea of blockchain beyond the use case of P2P money.

The idea emerged that the Bitcoin blockchain could be in fact used for any kind of value transaction or any kind of agreement such as P2P insurance, P2P energy trading, P2P ride sharing, etc. Colored Coins and Mastercoin tried to solve that problem based on the Bitcoin Blockchain Protocol. The Ethereum project decided to create their own blockchain, with very different properties than Bitcoin, decoupling the smart contract layer from the core blockchain protocol, offering a radical new way to create online markets and programmable transactions known as Smart Contracts.

Private institutions like banks realized that they could use the core idea of blockchain as a distributed ledger technology (DLT), and create a permissioned blockchain (private of federated), where the validator is a member of a consortium or separate legal entities of the same organization. The term blockchain in the context of permissioned private ledger is highly controversial and disputed. This is why the term distributed ledger technologies emerged as a more general term.



Types of Blockchains
Source: Blockchainhub.net

Private blockchains are valuable for solving efficiency, security and fraud problems within traditional financial institutions, but only incrementally. It's not very likely that private blockchains will revolutionize the financial system. Public blockchains, however, hold the potential to replace most functions of traditional financial institutions with software, fundamentally reshaping the way the financial system works.

Public Blockchains

State of the art public Blockchain protocols based on Proof of Work (PoW) consensus algorithms are open source and not permissioned. Anyone can participate, without permission. (1) Anyone can download the code and start running a public node on their local device, validating transactions in the network, thus participating in the consensus process – the process for determining what blocks get added to the chain and what the current state is. (2) Anyone in the world can send transactions through the network and expect to see them included in the blockchain if they are valid. (3) Anyone can read transaction on the public block explorer. Transactions are transparent, but anonymous/pseudonumous.

Examples: Bitcoin, Ethereum, Monero, Dash, Litecoin, Dodgecoin, etc.
Effects: (1) Potential to disrupt current business models through disintermediation. (2) No infrastructure costs: No need to maintain servers or system admins radically reduces the costs of creating and running decentralized applications (dApps).

Federated Blockchains or Consortium Blockchains

Federated Blockchains operate under the leadership of a group. As opposed to public Blockchains, they don't allow any person with access to the Internet to participate in the process of verifying transactions. Federated Blockchains are faster (higher scalability) and provide more transaction privacy. Consortium blockchains are mostly used in the banking sector. The consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants.

Example: R3 (Banks), EWF (Energy), B3i (Insurance), Corda
Effects: (1) reduces transaction costs and data redundancies and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms. (2) in that sense it can be seen as equivalent to SAP in the 1990's: reduces costs, but not disruptive.
Note: Some would argue that such a system is not a blockchain. Also, Blockchain is still in it's early stages. It is unclear how the technology will pan out and will be adopted. Many argue that private or federated Blockchains might suffer the fate of Intranets in the 1990's, when private companies built their own private LANs or WANs instead of using the public Internet and all the services, but has more or less become obsolete especially with the advent of SAAS in the Web2.

Private Blockchains

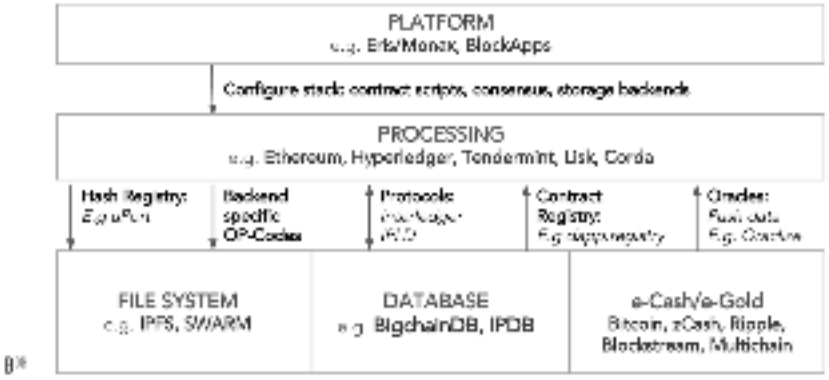
Write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Example applications include database management, auditing, etc. which are internal to a single company, and so public readability may in many cases not be necessary at all. In other cases public audit ability is desired. Private blockchains are a way of taking advantage of blockchain technology by setting up groups and participants who can verify transactions internally. This puts you at the risk of security breaches just like in a centralized system, as opposed to public blockchain secured by game theoretic incentive mechanisms. However, private blockchains have their use case, especially when it comes to scalability and state compliance of data privacy rules and other regulatory issues. They have certain security advantages, and other security disadvantages (as stated before).

Example: MONAX, Multichain
Effects: (1) reduces transaction costs and data redundancies and replaces legacy systems, simplifying document handling and getting rid of semi manual compliance mechanisms. (2) in that sense it can be seen as equivalent to SAP in the 1990's: reduces costs, but not disruptive.
Note: Some would argue that such a system is not a blockchain. Also, Blockchain is still in it's early stages. It is unclear how the technology will pan out and will be adopted. Many argue that private or federated Blockchains might suffer the fate of Intranets in the 1990's, when private companies built their own private LANs or WANs instead of using the public Internet and all the services, but has more or less become obsolete especially with the advent of SAAS in the Web2.

Hybrid/Blockchainified Databases: Example BigchainDB

State of the art public blockchains currently have a scalability issue, which means that the network can only handle a few transactions per second, which makes them unfeasible for large scale applications with high transaction volumes. Bitcoin and Ethereum can only handle less than a dozen transactions per second, yet Visa alone would require 100k transactions per second at peak times. BigchainDB for example combined the scalability power of distributed database with immutable elements of Blockchains to solve this problem on the database side.

Some people would dispute that you can call BigchainDB a blockchain. However it is an important technology in the technology stack of distributed computing and solves the big issue of scalability. We are currently redesigning data structures for the Web3, moving away from centralized computing to decentralized/distributed computing & the decentralized web. In this context, BigchainDB is an important element in the Web3 technology stack (see images below).



Decentralized Stack Interoperability
Source: n.d., BigchainDB (2016)

.

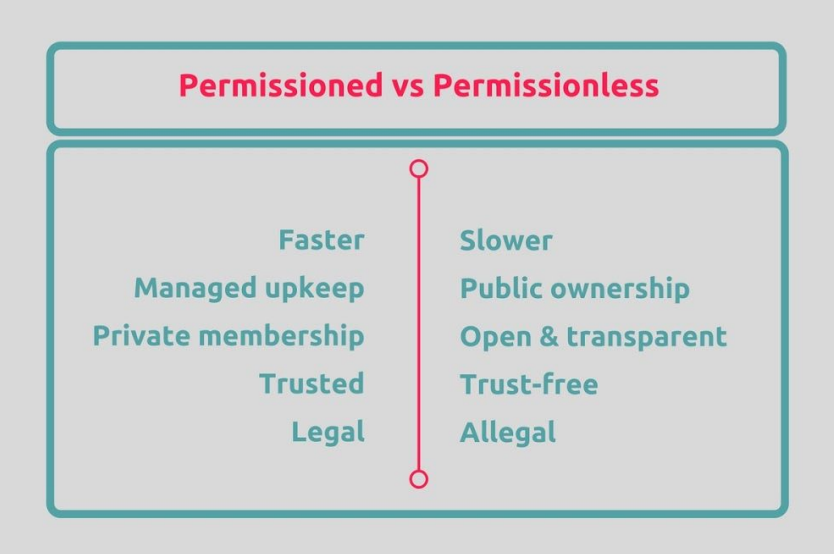
Different Classification Schemes

Many people have tried to classifying blockchains, but there is no consensus on how to accurately distinguish between different types of Blockchains. We have listed a selection of different classification schemes.

	PUBLIC	PRIVATE
Access	Open read/write	Permissioned read and/or write
Speed	Slower	Faster
Security	Proof of Work Proof of Stake Other consensus Mechanisms	Pre-approved participants
Identity	Anonymous Pseudonymous	Know identities
Asset	Native Asset	Any Asset

Public vs Private Blockchains
Source: Chris Skinner's Blog

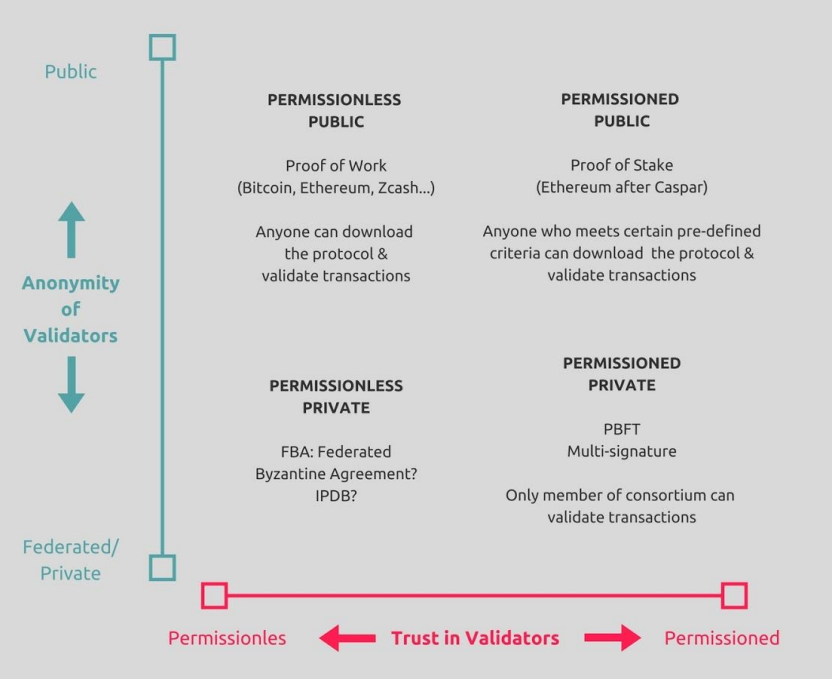
One way to distinguish is between public and private, or permissioned and permissionless. Sometimes these terms are used synonymously, but they refer to different things.



Permissioned vs Permissionless Blockchains
Source: Gavin Wood (2016)

The Bitcoin Blockchain is a game changer, because it is public and permissionless. Anyone in the world can download the open source code, and can start verifying transaction, being rewarded with bitcoin, through a concept called mining.

All stakeholders in the bitcoin network, who do not know and trust each other, are coordinated through an economical incentive framework pre-defined in the protocol and auto enforced by machine consensus of the P2P Network. The smart contract in the blockchain protocol therefore provides an coordination framework for all network participants, without the use of traditional legal contracts. In private and permissioned blockchain, all network participants validating transactions are known. Bilateral or multilateral legal agreements provide a framework for trust, not the code.



Ok, I need a blockchain, but which one?
Adapted and modified from: Pavel Kravchenko (2016)

	Public No centralized management	**Consortium** Multiple Organisations	**Private** Single Organisation
Participants	**Permissionless** - Anonymous - Could be malicious	**Permissioned** - Identified - Trusted	**Permissioned** - Identified - Trusted
Consensus Mechanisms	**Proof of Work, Proof of Stake, etc..** - Large energy consumption - No finality - 51% attack	**Voting or multi-party consensus algorithm** - Lighter - Faster - Low energy consumption - Enable finality	**Voting or multi-party consensus algorithm** - Lighter - Faster - Low energy consumption - Enable finality
Transaction Approval Freq.	**Long** Bitcoin: 10 min or more	**Short** 100x msec	**Short** 100x msec
USP	**Disruptive** Disruptive in the sense of disintermediation. No middle men needed. Unclear what the business models will be	**Cost Cutting** Can radically reduce transactions costs. Similar to SAP in the 1990s. Extreme cost cutting opportunities. Less data redundancy, higher transactions times, more transparency	**Cost Cutting** Can radically reduce transactions costs. Similar to SAP in the 1990s. Extreme cost cutting opportunities. Less data redundancy, higher transactions times, more transparency

Adapted and modified from: Slideshare

Sources & Further Reading

On Public and Private Blockchains, Vitalik Buterin (2015)
Vitalik Buterin: On Public and Private Blockchains, Coindesk
Ok, I need a blockchain, but which one?, Pavel Kravchenko
IBM blockchain explained, Diego Alberto Tamayo
Blockchains What & Why, Gavin Wood

Crypto Economics

Cryptoeconomics refers to as the study of economic interaction in adversarial environments. The underlying challenge is that in decentralized P2P systems, that do not give control to any centralized party, one must assume that there will be bad actors looking to disrupt the system. Cryptoeconomic approaches combine cryptography and economics to create robust decentralized P2P networks that thrive over time despite adversaries attempting to disrupt them. The cryptography underlying these systems is what makes the P2P communication within the networks secure, and the economics is what incentivizes all actors to contribute to the network so that it continues to develop over time.

Before the advent of Bitcoin, it was commonly believed to be impossible to achieve fault tolerant and attack resistant consensus among nodes in a P2P network (Byzantine General's Problem). Satoshi Nakamoto introduced economic incentives to a P2P Network and solved that problem in the Bitcoin White Paper published in 2008. While decentralized P2P systems based on cryptography were nothing new – see Kazaa and BitTorrent – what these P2P systems before Bitcoin lacked was economic incentive layer for coordination of the network of participants. Satoshi's implementation of a Proof of Work (POW) consensus mechanism introduced a new field of economic coordination game, now referred to as cryptoeconomics.

Machine Consensus in a P2P Network

A fundamental problem in distributed computing is to achieve overall system reliability in the presence of a number of faulty or potentially corrupted processes. This often requires entities to agree on some data value that is needed during computation. The consensus problem requires agreement among a number of network participants for a single data value. Some of the processes may fail or be unreliable in other ways, so consensus protocols must be fault tolerant, attack and collusion resistant: (Source)

- **Fault Tolerant**
  Decentralized systems are less likely to fail accidentally because they rely on many separate components.

- **Attack Resistant**
  Decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system.

- **Collusion Resistant**
  It is much harder for participants in decentralized systems to collude and act in ways that benefit them at the expense of other participants, whereas the leadership of corporations and governments collude in ways that benefit themselves but harmless well-coordinated citizens, customers, employees and the general public all the time.

Economic Consensus Rules

In a crypto economic setup, economic incentives are designed to be fault tolerant, attack and collusion resistant. These economic incentives are tied around a cryptographic token. The token is considered to be the least common denominator to align interests in a multi-stakeholder network like a (permissionless) Blockchain. Bitcoin is only the first example for how token governance rulesets align stakeholder interests around economic incentives.

While Satoshi tied Bitcoin's token governance rulesets to PoW incentive mechanisms, other Blockchains that followed have experimented with alternative consensus mechanisms. Here a selection of possible consensus mechanism. Please note that the field of crypto economics is quite new. We will very likely see more consensus mechanisms evolve over time.

- **Proof of Work (PoW):** The Bitcoin blockchain uses electricity to ensure the security of the system. It creates an economic system where you can only participate by incurring costs – Proof of Work (PoW). You do that for the possibility of reward – in this case, Bitcoin tokens. If you spend money, and you play fair by the rules, you get money back. If you cheat, you lose money. The consensus rules are designed in a way that it doesn't pay to cheat. This simple game theoretical equilibrium is the core of the Bitcoin consensus algorithm. Currently, the majority of Altcoins are software forks of the Bitcoin protocol with usually minor changes to the proof of work (PoW) algorithm of the Bitcoin blockchain. Some people argue that Bitcoin's current consensus system is more a Delegated PoW and not a pure PoW as designed by Satoshi, since most miners have formed cartels in form of mining pools.

History: Proof of work is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. The concept may have been first presented by Cynthia Dwork and Moni Naor in a 1993 journal. The term "Proof of Work" was first coined and formalized in a 1999 paper by Markus Jakobsson and Ari Juels. A key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle or CPU pricing function.

- **Proof of Stake (PoS):** is an alternative method by which a cryptocurrency blockchain network aims to achieve distributed consensus. While the proof-of-work (PoW) method asks users to repeatedly run hashing algorithms or other client puzzles, to validate electronic transactions, proof-of-stake asks users to prove ownership of a certain amount of currency (their "stake" in the currency). Peercoin was the first cryptocurrency to launch using Proof-of-Stake. Other prominent implementations are found in BitShares, Nxt, BlackCoin, NuShares/NuBits and Qora. Ethereum has planned a hard fork transition from PoW to PoS consensus. Decred hybridizes PoW with PoS and combines elements of both in an attempt to garner the benefits of the two systems and create a more robust notion of consensus. With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). In the case of Bitcoin, with Proof of Stake, the resource that's compared is the amount of Bitcoin a miner holds – someone holding 1% of the Bitcoin can mine 1% of the "Proof of Stake blocks". Instead of sacrificing energy to mine a block, a user must prove they own a certain amount of the cryptocurrency to generate a block. The higher stake you have, the more likely you are to generate a block. In theory, this should prevent users from creating forks because it will devalue their stake. Proof of Stake sounds like a good idea, but ironically, there is the "Nothing at Stake" problem. Since mining Bitcoins is costly, it is not smart to waste your energy on a fork that won't earn you any money, however with Proof of Stake, it is free to mine a fork.

- **Delegated Proof of Stake:** DPoS uses a reputation system and real-time voting to achieve consensus. To be more specific, a panel of trusted parties has to be established, with all of its members eligible to create blocks and prevent non-trusted parties from participating. Delegates, the parties responsible for creating blocks, are unable to change transaction details. However, they can prevent specific transactions from being included in the next network block. This seemingly requires a fair bit of trust, which makes the concept look far less appealing. However, there is a caveat. Any transaction not included in the next block – or a block failing to create – will mean the next network block is twice the size. In a way, this prevents malicious intent to block certain transactions or blocks being created in the allotted time period. All it does is perhaps slightly delay said transaction or block, but it is seemingly impossible to prevent inclusion and creation in the long run. Moreover, anyone who behaves in a nefarious way will have their behavior exposed to the public. Community members of the DPoS-capable currencies can vote to have said person removed as a delegate altogether. It appears as if cheating under DPoS rules is not only impossible, but it is not in anybody's best interest to do so either. It is equally possible to have more or fewer delegates as part of the network, although that may not necessarily be beneficial either. It is always possible to change the number of delegates, though, which is an important factor to keep in mind.

- **Proof of Burn:** "is a method for distributed consensus and an alternative to Proof of Work and Proof of Stake. It can also be used for bootstrapping one cryptocurrency off of another. The idea is that miners should show proof that they burned some coins – that is, sent them to a verifiably unspendable address. This is expensive from their individual point of view, just like proof of work; but it consumes no resources other than the burned underlying asset. To date, all proof of burn cryptocurrencies work by burning proof-of-work-mined cryptocurrencies, so the ultimate source of scarcity remains the proof-of-work-mined fuel" (Bitcoin Wiki).

- **Proof of Authority (PoA):** A Proof of authority is a consensus mechanism in a private blockchain which essentially gives one client (or a specific number of clients) with one particular private key the right to make all of the blocks in the blockchain.

Upgrading/Changing Consensus Rules

Blockchain protocols are a powerful tool to auto-enforce predefined consensus rules in distributed networks without centralized management. Network members know the transparent and open source ruleset and can opt in and out anytime. Blockchain Protocols are powerful governance tools, as long as the protocol does not need modification.

Over time, as circumstances change, there might be a need for a system upgrade. These upgrades (forks) need majority consensus by all stakeholders in the network. While the protocol can be upgraded through a hard fork or a soft fork and these forks can be highly controversial as we have seen in the Bitcoin block size debate or Ethereum post-TheDAO hard fork.

Example: In the Bitcoin network, developers suggest bitcoin improvements/modifications, small or big, proposals on Github, Bitcointalk, Reddit, mailing lists, etc. Discussion on this level is critical to enable smooth runtime consensus transitions. Modifications with reference implementations get tested on the testnet. After successful testing developers implement the changes into the Bitcoin software. Who has a say in the consensus process? (1) Software Developers (do the reference implementations); (2) Miners (Runtime consensus for mining blocks); (3) Exchanges (They run nodes that validate transactions); (4) Wallet companies (create transactions run on nodes); (5) Merchants (Merchant processing also through nodes).

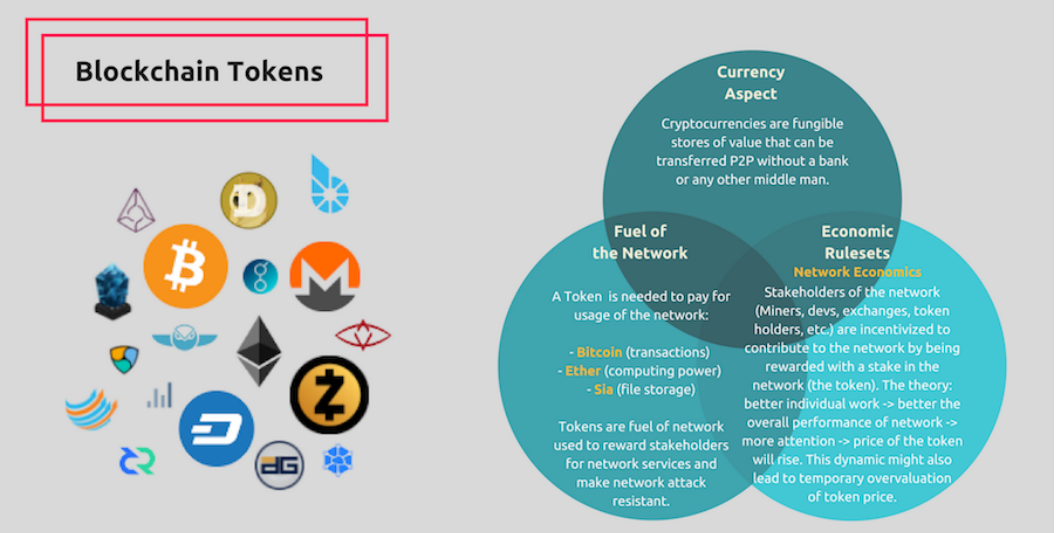
Sources & Further Reading

Cryptoeconomics 101, Nick Tomaino
Making Sense of Crypto Economics, Josh Stark
The meaning of Decentralization, Vitalik Buterin
Understanding Crypto-Economic Security through Game Theory,
Delegated Proof of Stake, Bitshares
Fat Protocols, Joel Menegro
Tokens, Tokens and More Tokens, Nick Tomaino
Crypto Tokens and the Coming Age of Protocol Innovation, Albert Wenger
Crypto Tokens: A Breakthrough in Open Network Design, podcast with Vitalik Buterin, podcast with Olaf Carlson-Wee
Regulatory discussions , Coincenter
A gentle Introduction to Digital Tokens

Tokens

Native tokens of state of the art public & permissionless Blockchains like Bitcoin or Ethereum, are part of the incentive scheme to encourage a disparate group of people who do not know or trust each other organize themselves around the purpose of a specific blockchain. The native token of the Bitcoin Network also referred to as Bitcoin, has token governance rulesets based on **crypto economic incentive** mechanisms that determine under which circumstances Bitcoin transactions are validated and new blocks are created.

These blockchain based cryptographic tokens enable "distributed Internet tribes" to emerge. As opposed to traditional companies that are structured in a top manner with many layers of management (bureaucratic coordination), blockchain disrupt classic top down governance structures with decentralized autonomous organizations (DAOs), where a group of people bound together not by a legal entity and formal contracts, but instead by cryptographic tokens (incentives) and fully transparent rules that are written into the software.

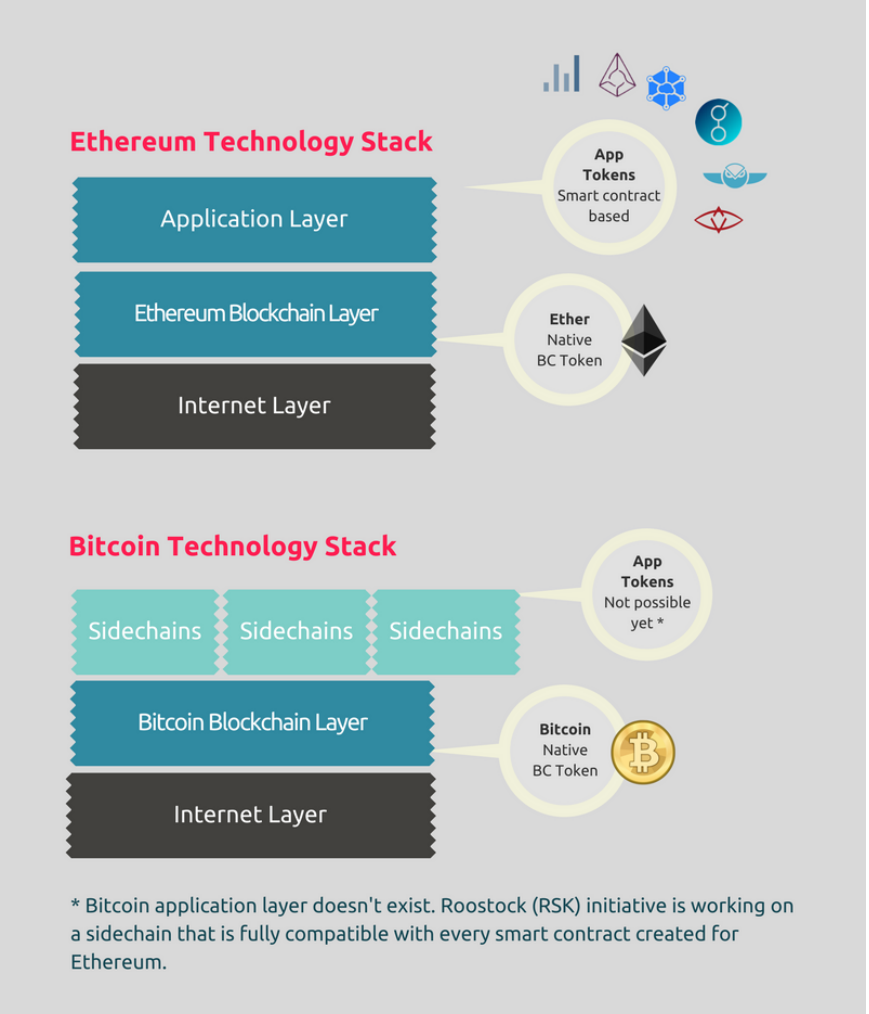


Blockchain Tokens
Source: Blockchainhub.net

The Bitcoin Network can be seen as the first true DAO that provides an infrastructure for money without banks and bank managers and has stayed attack resistant as well as fault tolerant since the first block was created in 2009. No central entity controls Bitcoin. In theory, only a worldwide power outage could shut down Bitcoin.

With the advent of Ethereum however, tokens have moved up the technology stack and can now be issued on the application layer as dApp tokens or DAO tokens. Smart contracts on the Ethereum Blockchain enable the creation of tokens with complex behaviors attached to them. Today, the token concept is central to most social and economic innovations developed with blockchain technology.

Only permissionless ledgers (public Blockchains like Bitcoin or Ethereum), need some sort of incentive mechanism to guarantee that block validators do their job according to the predefined rules. In permissioned (federated/consortium/private) distributed ledger systems, validators and block-creators may be doing their job for different reasons: i.e., if they are contractually obligated to do so. In permissioned environments, validators can only be members of the club and are manually and centrally controlled. Permissioned ledgers, therefore, don't need a token. Also, please note that the term blockchain in the context of such ledgers is highly controversial.



Level of Token
Source: Blockchainhub.net

Type of Tokens

There are different ways to differentiate between tokens. Some of them are outlined below. Please note that Crypto Economics is so new, that we are still in the early stages of exploring different roles and types of tokens. With every new Blockchain and every new application layer we will collectively learn by trial and error of what works and what not.

- **Usage tokens:** A token that is required to use a service. Bitcoin and Ether are the best examples of usage tokens — token ownership does not give you any specialized rights within the network, but it does give you access to the service (the Bitcoin payment network and the Ethereum Virtual Machine in the case of BTC and ETH). Scarce tokens combined with a useful service can create massive value for token holders and entrepreneurs.

- **Work tokens:** A token that gives users the right to contribute work to a decentralized network or DAO (whether on blockchain level or smart contract level) and earn in exchange for their work. That work can be serving as an oracle (in the case of Augur), being the backstop in a collateralized debt system (in the case of Maker), or securing the network (in the case of Ethereum when it switches to proof of stake).

These two types of tokens are not mutually exclusive and some tokens serve as both: usage tokens and work tokens. An example of a token with both characteristics will be ETH when Ethereum transitions from proof of work to proof of stake. Another way to differentiate between tokens is:

- **Intrinsic, Native or Built-in Tokens:** of blockchains like Bitcoin, Ether, etc that serve as: (a) block validation incentives ('miner rewards'); and (b) transaction spam prevention. The logic behind this is that if all transactions are paid, it limits the ability to spam.

- **Application Tokens:** With Ethereum, tokens can now easily be issued on the application layer through smart contracts on the Ethereum Blockchain as so-called complex dApp tokens or complex DAO tokens.

- **Asset-backed tokens:** that are issued by a party onto a blockchain for later redemption. They are the digital equivalent to physical assets. They are claims on an underlying asset (like the gold), that you need to claim from a specific issuer (the goldsmith). The transactions as tokens get passed between people are recorded on the blockchain. To claim the underlying asset, you send your token to the issuer, and the issuer sends you the underlying asset.

Tokens can represent assets	Tokens can be used as...
❏ An hours worth of rooftop solar energy ❏ A currency such as dollar, euro, rupee, or gbp ❏ A promise for a product in a crowdfund ❏ A future download of a song from your favorite artist ❏ An insurance policy ❏ A ticket to an event	❏ Token of ownership ❏ Vouchers ❏ Software license ❏ Stock certificates ❏ Access rental cars or other vehicles ❏ Tickets, access rights ❏ Memberships, subscriptions ❏ Rewards program ❏ Financial Instruments ❏ As a system of voting

Legal Status

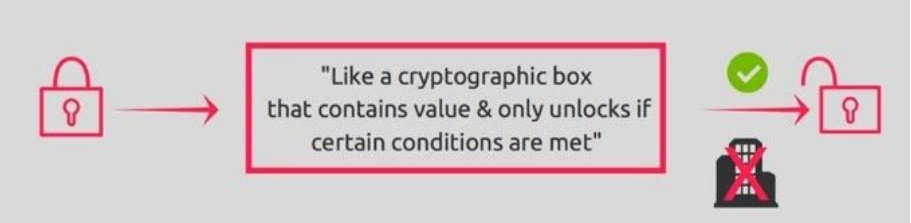
Blockchain tokens embody the full potential of blockchain technology. In order for blockchains to unfold their full potential with regard to reinventing ownership in the digital realm, the technology needs to be recognized de lege ferenda as a system capable of creating an objectively new ontological category. A new kind of thing, which deserves its own regulatory framework that reflects the unique affordances and constraints of blockchain technology.

Sources & Further Reading

Crypto Economics, BlockchainHub
A Blockchain Token Taxonomy, Florian Glatz
Thoughts on Tokens, Balaji S. Srinivasan
ICOs and VCs here, Fred Wilson
Fat Protocols, Joel Menegro
Cryptoeconomics 101, Nick Tomaino
Tokens, Tokens and More Tokens, Nick Tomaino
Crypto Tokens and the Coming Age of Protocol Innovation, Albert Wenger
Crypto Tokens: A Breakthrough in Open Network Design, podcast with Vitalik Buterin, podcast with Olaf Carlson-Wee
Regulatory discussions, Coincenter
A gentle Introduction to Digital Tokens, Bitasonblocks
Tokens on Ethereum, Consensys

Smart Contracts

A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation. It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract and the assets automatically get redistributed among those parties according to a formula based on certain data, which is not known at the time of contract initiation.



Smart Contract
Source: Blockchainhub.net

The term smart contract is a bit unfortunate since a smart contract is neither smart nor are they to be confused with a legal contract:

- A smart contract can only be as smart as the people coding taking into account all available information at the time of coding.

- While smart contracts have the potential to become legal contracts if certain conditions are met, they should not be confused with legal contracts accepted by courts and or law enforcement. However, we will probably see a fusion of legal contracts and smart contracts emerge over the next few years as the technology becomes more mature and widespread and legal standards are adopted.

Slashing Transactions Costs

Would you enter into a contract with someone whom you've never met? Would you agree to lend money to some farmer in Ethiopia? Would you become an investor in a minority-run newspaper in a war zone? Would you go to the hassle of writing up a legal binding contract for a $5 purchase over the internet? For most people the answer would be no, as the transaction costs for these examples exceed the value transferred.

The term smart contract proceeds blockchains and was first proposed by Nick Szabo in 1996. The aim is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting. Auto enforceable code – whether on the protocol level or on the application level – standardizes transaction rules, thus reducing the transaction costs of:

- Reaching an agreement
- Formalization
- Enforcement

A smart contract can formalize the relationships between people, institutions and the assets they own. The transaction rulesets (agreement) of the smart contract define the conditions – rights and obligations – to which the parties of a protocol or smart contract consent. It is often predefined, and agreement is reached by simple opt-in actions. This transaction rule set is formalized in digital form, in machine-readable code (formalization). These rights and obligations established in the smart contract can

now be automatically executed by a computer or a network of computers as soon as the parties have come to an agreement and met the conditions of the agreement (enforcement).

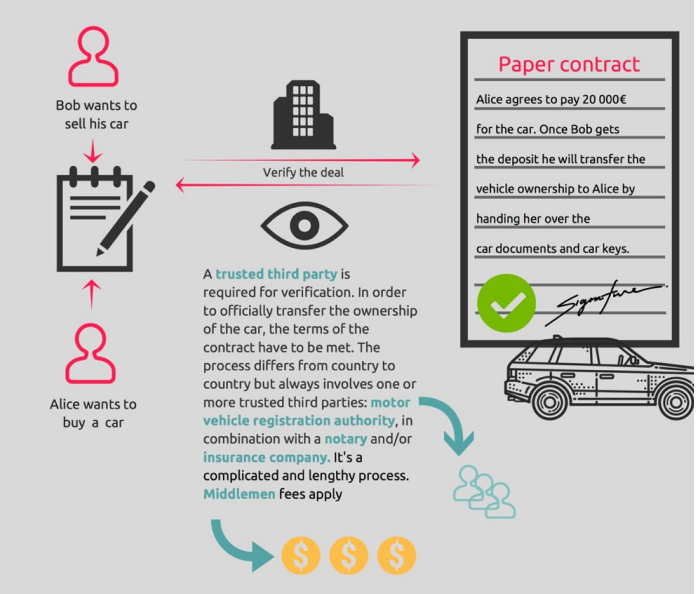
Although the concept of smart contracts is not new, blockchain technologies seem to be the catalyst for smart contract implementation. The most primitive form of a smart contract is a vending machine. The rules of a transaction are programmed into a machine. You select a product by pressing a number related to that product, insert the coins, the machine acts as a smart contract checking whether you inserted enough money. If yes, the machine is programmed to eject the product, and if you inserted too much money, it will also eject the change. If you didn't insert enough money, or if the machine ran out of the money, you will get your change back. Automatic vending machines not only slashed transaction costs by making human vendors obsolete, but they also expanded service, offering 24/7 availability instead of limited opening hours of a kiosk.

Smart Contracts are...	Smart Contracts can...
❏ Self-verifying ❏ Self-executing ❏ Tamper resistant	❏ Turn legal obligations into automated process ❏ Guarantee greater degree of security ❏ Decreasing reliance on trusted intermediaries ❏ Lower transaction costs

Smart contracts are capable of tracking performance in real time and can bring tremendous cost savings. Compliance and controlling happen on the fly. In order to get external information, a smart contract needs information oracles, which feed the smart contract with external information that can trigger transactions.

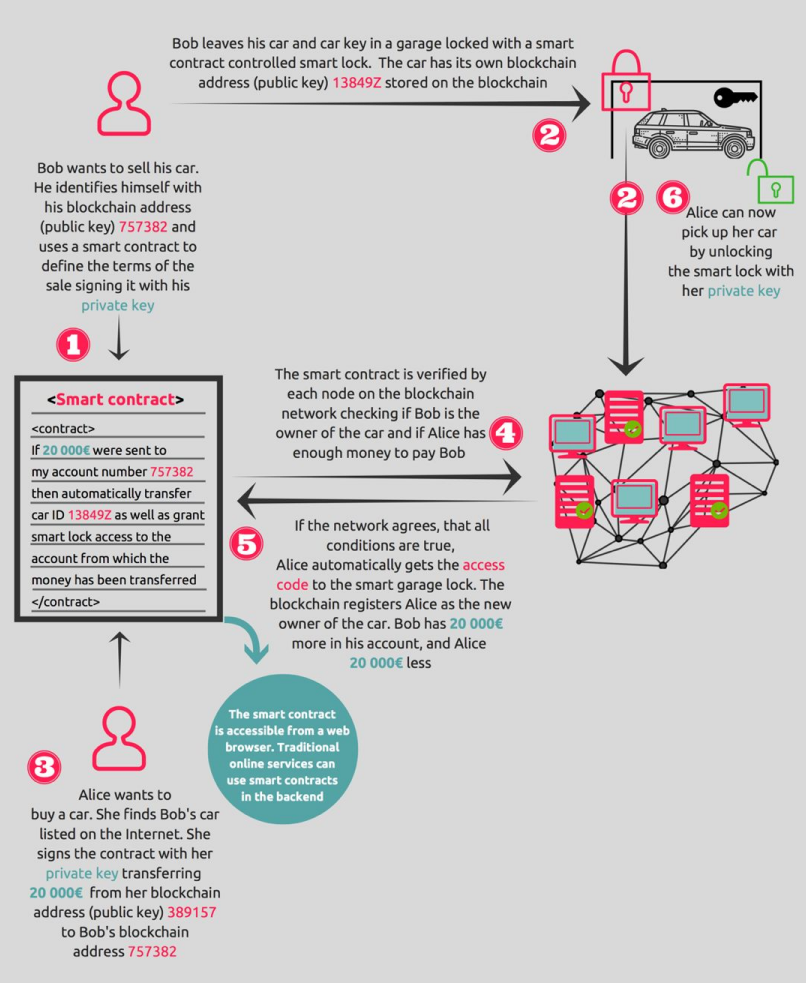
Smart Contract Example

If A and B don't know and don't trust each other, they usually need a trusted third party to serve as an intermediary to verify transactions and enforce them. With smart contracts & blockchains, you don't need those trusted intermediaries anymore for clearing or settlement of your transactions. Take the example of buying and selling a car: If Alice wants to purchase a car from Bob, a series of trusted third parties are required to verify and authenticate the deal. The process differs from country to country but always involves at least one, but usually more, trusted third parties: motor vehicle registration authority, in combination with a notary and/or insurance company. It is a complicated and lengthy process, and considerable fees for these middlemen apply.



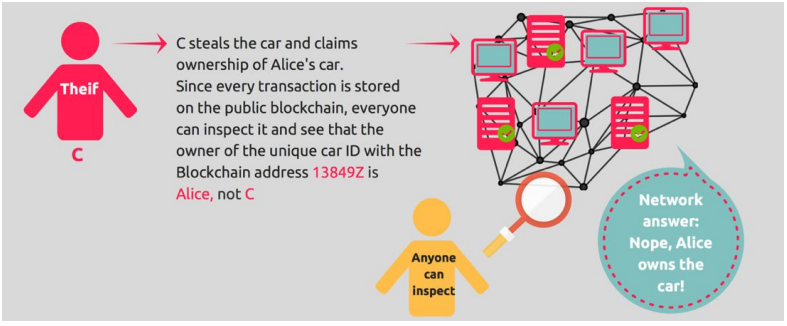
Process of buying a car today
Source: Blockchainhub.net

On the Blockchain, once all involved authorities and companies are on a blockchain, a smart contract could be used to define all the rules of a valid care sale. If Alice wanted to buy the car from Bob using a smart contract on the blockchain, the transaction would be verified by each node in the Blockchain Network to see if Bob is the owner of the car and if Alice has enough money to pay Bob.



Process of buying a car on the Blockchain
Source: Blockchainhub.net

If the network agrees that both conditions are true, Alice automatically gets the access code to the smart lock for the garage. The blockchain registers Alice as the new owner of the car. Bob has € 20,000 more on his account, and Alice € 20,000 less. No middlemen required. On the Blockchain, who owns what is transparent and at the same time anonymous or pseudonymous. This means that every computer running the blockchain protocol could check whether a certain person is the rightful owner of the car or not. Stealing cars won't be as easy as today, especially once we have smart keys granting access control verified on the blockchain, to unlock our future vehicles. As the owner of the car, you could authorize other people to drive it (stating the public key of the respective individual). In such cases opening the car would only be possible with a smart key on the Blockchain.



We we can trust the Blockchain
Source: Blockchainhub.net

Types of Smart Contracts

Blockchain and smart contracts have the potential to disrupt many industries. Use cases can be found in banking, insurance, energy, e-government, telecommunication, music & film industry, art world, mobility, education and many more. Smart contract use cases range from simple to complex.

Time-stamping services like ascribe (art registry) or governmental and semi-governmental registries (land titles, birth certificates, birth certificates, school and university degrees) are examples for simpler technological use cases (the regulatory aspects might be more complex). Decentralized autonomous organizations, on the other hand, are the most complex form of a smart contract. TheDAO in 2016 was an example for such a complex smart contract.

Given the fact that Blockchain is still a new technology, some industries might adopt smart contracts later than others, especially if they are subject to heavy government regulation or if the uses cases require high network effects – like widespread technology adoption along the supply chain, standardization, etc. In general, it's advisable to start out with a small pilot project of a less complex use case to build expertise and understand the technology better and move on to more complex use case at a later stage.

Smart Contract Coding

Solidity is a smart contract programming language. The syntax is similar to that of JavaScript, and it is designed to compile to code for the Ethereum Virtual Machine, to create contracts for voting, crowdfunding, blind auctions, multi-signature wallets and more.

Official Solidity Documentation, Ethereum Foundation
Solidity Tutorial, using Visual Studio
Solidity Code Snippets, useful for Đapp development
Accessing Contracts & Transactions: Interacting with smart contracts
Integrated development platform (IDE) browser based with integrated compiler and solidity runtime environment without server-side components
Ethereum Solidity Gitter chat channel
Remix: IDE that allows developers to build and deploy contracts and decentralized applications on top of the Ethereum blockchain
The Hitchhiker's Guide to Smart Contracts in Ethereum, Manuel Aráoz, Medium
Truffle: The most popular Ethereum development framework, Github

Sources & Further Reading

Nick Szabo, Smart Contracts
Check out our Smart Contract Infographic
Internet of Agreements: Building the Hyperconnected Future on Blockchains - why smart contracts could change the way people do business: by Hexayurt.Capital in collaboration with ConsenSys
Smart Contracts, Florian Glatz
OpenLaw, Consensys

Oracles

An oracle, in the context of blockchains and smart contracts, is an agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts.

Smart contracts contain value and only unlock that value if certain pre-defined conditions are met. When a particular value is reached, the smart contract changes its state and executes the programmatically predefined algorithms, automatically triggering an event on the blockchain. The primary task of oracles is to provide these values to the smart contract in a secure and trusted manner.

Blockchains cannot access data outside their network. An oracle is a data feed – provided by third party service – designed for use in smart contracts on the blockchain. Oracles provide external data and trigger smart contract executions when pre-defined conditions meet. Such condition could be any data like weather temperature, successful payment, price fluctuations, etc.

Oracles are part of multi-signature contracts where for example the original trustees sign a contract for future release of funds only if certain conditions are met. Before any funds get released an oracle has to sign the smart contract as well.

Types of Oracles

There are different types of oracles based on the type of use. We differentiate between software oracles, hardware oracles, consensus oracles and inbound and outbound oracles.

- **Software Oracles**
  Software oracles handle information available online. An example could be the temperature, prices of commodities and goods, flight or train delays, etc. The data originates from online sources, like company websites. The software oracle extracts the needed information and pushes it into the smart contract.

- **Hardware Oracles**
  Some smart contracts need information directly from the physical world, for example, a car crossing a barrier where movement sensors must detect the vehicle and send the data to a smart contract. Another use case is RFID sensors in the supply chain industry. The biggest challenge for hardware oracles is the ability to report readings without sacrificing data security. Oracalize proposes a two-step solution to the risks, by providing cryptographic evidence of the sensor's readings and anti-tampering mechanisms rendering the device inoperable in the case of a breach.

- **Inbound Oracles**
  These provide the smart contract with data from the external world. Example use case will be an automatic buy order if the USD hits a certain price.

- **Outbound Oracles**
  These provide smart contracts with the ability to send data to the outside world. An example would be a smart lock in the physical world which receives a payment on its blockchain address and needs to unlock automatically.

- **Consensus Based Oracles**
  Prediction markets like Augur and Gnosis rely heavily on oracles to confirm future outcomes. Using only one source of information could be risky and unreliable. To avoid market manipulation prediction markets implement a rating system for oracles. For further security, a combination of different oracles may be used, where for example 3 out of 5 oracles could determine the outcome of an event.

Security Challenges

Oracles are third party services which are not part of the blockchain consensus mechanism. The main challenge with oracles is that people need to trust these sources of information. Whether a website or a sensor, the source of information needs to be trustworthy. Different trusted computing techniques can be used as a way of solving these issues. Companies like Oracalize,

for example, have been leveraging Amazon with the TLSNotary-based proofs. Town Crier, another company, is focusing on the utilization of the Intel Software Guard Extensions (SGX). Providing smart contracts with trusted information sources is crucial for the users because in case of mistakes there are no rollbacks.

Sources & Further Reading

Hardware Oracles: bridging the Real World to the Blockchain
Understanding oracles
A visit to the oracle
Smart Contract Oracles
Can oracles send data to smart contracts on multiple blockchains?
How can an Ethereum contract get data from a website?
Why Many Smart Contract Use Cases Are Simply Impossible?
1,749,693 blocks later, Oracalize
SchellingCoin: A Minimal-Trust Universal Data Feed, Vitalike Buterin
Town Crier: An Authenticated Data Feed for Smart Contracts: Scientific paper

Decentralized Applications (dApp)

Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single computer. dApps, have existed since the advent of P2P networks. They are a type of software program designed to exist on the Internet in a way that is not controlled by any single entity.

- ❏ Decentralized applications don't necessarily need to run on top of a blockchain network. BitTorrent, Popcorn Time, BitMessage, Tor, are all traditional dApps that run on a P2P network, but not on a Blockchain (which is a specific kind of P2P network).

- ❏ As opposed to simple smart contracts, in the classic sense of Bitcoin, that sends money from A to B, dApps have an unlimited number of participants on all sides of the market.

DApps vs Smart Contracts

dApps are a 'blockchain enabled' website, where the Smart Contract is what allows it to connect to the blockchain. The easiest way to understand this is to understand how traditional websites operate.

- ❏ **Traditional web application**
  uses HTML, CSS and javascript to render a page. It will also need to grab details from a database utilizing an API . When you go onto Facebook, the page will call an API to grab your personal details and display them on the page.
  Traditional websites: Front End → API → Database

- ❏ **dApps**
  are similar to a traditional web application. The front end uses the *exact same* technology to render the page. The one critical difference is that instead of an API connecting to a Database, you have a Smart Contract connecting to a blockchain.
  dApp enabled website: Front End → Smart Contract → Blockchain

As opposed to traditional, centralized applications, where the backend code is running on centralized servers, dApps have their backend code running on a decentralized P2P network. Decentralized applications consist of the whole package, from backend to frontend. The smart contract is only one part of the dApp:

- Frontend (what you see), and
- Backend (the logic in the background).

A smart contract, on the other hand, consists only of the backend, and often only a small part of the whole dApp. That means if you want to create a decentralized application on a smart contract system, you have to combine several smart contracts and rely on 3rd party systems for the front-end.

dApps can have frontend code and user interfaces written in any language (just like an app) that can make calls to its backend. Furthermore, its front end can be hosted on decentralized storage such as Swarm or IPFS.

dApps Requirements

For an application to be considered a dApp in the context of Blockchain, it must meet the following criteria:

- ❏ **Application must be completely open-source**
  It must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback, but the consensus of its users must decide all changes.

- ❏ **Application's data and records of operation**
  must be cryptographically stored in a public, decentralized blockchain in order to avoid any central points of failure.

- ❏ **Application must use a cryptographic token**
  (Bitcoin or a token native to its system) which is necessary for access to the application and any contribution of value from (miners/farmers) should be rewarded with the application's tokens.

- ❏ **Application must generate tokens**
  according to a standard cryptographic algorithm acting as a proof of the value, nodes are contributing to the application (Bitcoin uses the Proof of Work Algorithm).

dApp development process

- ❏ **Whitepaper & Prototype**
  A whitepaper is published describing the dApp and its features. This whitepaper can outline the idea for dApp development but also entail a working prototype.

- ❏ **Token Sale**
  Initial tokens sale is set up

- ❏ **ICO - Initial Coin Offering**
  Ownership stake of the Dapp is spread

- ❏ **Implementation & Launch**
  Fund are invested to build the dApp and deploy it.

Example: Ethereum dApps

Ethereum intends to create a protocol for building decentralized applications. Ethereum provides developers with a foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats, and state transition functions. In general, there are three types of applications on top of Ethereum.

- ❏ **Financial applications:** providing users with more powerful ways of managing and entering into contracts using their money.

- ❏ **Semi-financial applications:** where money is involved, but there is also a heavy non-monetary side to what is being done.

- ❏ **Governance Applications:** such as online voting & decentralized governance that are not financial at all.

Examples for such dApps:

- **Token Systems:** On-blockchain token systems have many applications ranging from sub-currencies representing assets such as USD or gold to company stocks, individual tokens representing smart property, secure unforgeable coupons, and even token systems with no ties to conventional value at all, used as point systems for incentivization.
- **Financial derivatives and Stable-Value Currencies:** For example, a very desirable application is a smart contract that hedges against the volatility of ether with respect to the US dollar by using the data feed from, e.g., NASDAQ.
- **Identity & Reputation Systems:** A contract stating the name of the owner of a land title can be added to the Ethereum network but not modified or removed. Anyone can register a name with some value, and that registration then sticks forever.
- **Decentralized File Storage:** A Dropbox-like dApp where a smart contract splits the desired data up into blocks, encrypting each block for privacy, and builds a Merkle tree out of it, then the whole data gets distributed across a peer to peer network of computers. However private data does not get stored on the blockchain..
- **Decentralized Autonomous Organizations (DAOs):** A virtual entity that has a certain set of members or shareholders who, perhaps with a 67% majority, have the right to spend the entity's funds and modify its code. The members would collectively decide on how the organization should allocate its resources.

dApp Licences

Operating under open-source license allows dApps to be open for innovation without restrictions of copyright or patent. Also, by being completely open-source, decentralized applications can operate under the legal model of open-source software. Bitcoin, for example, uses the MIT open-source software license.

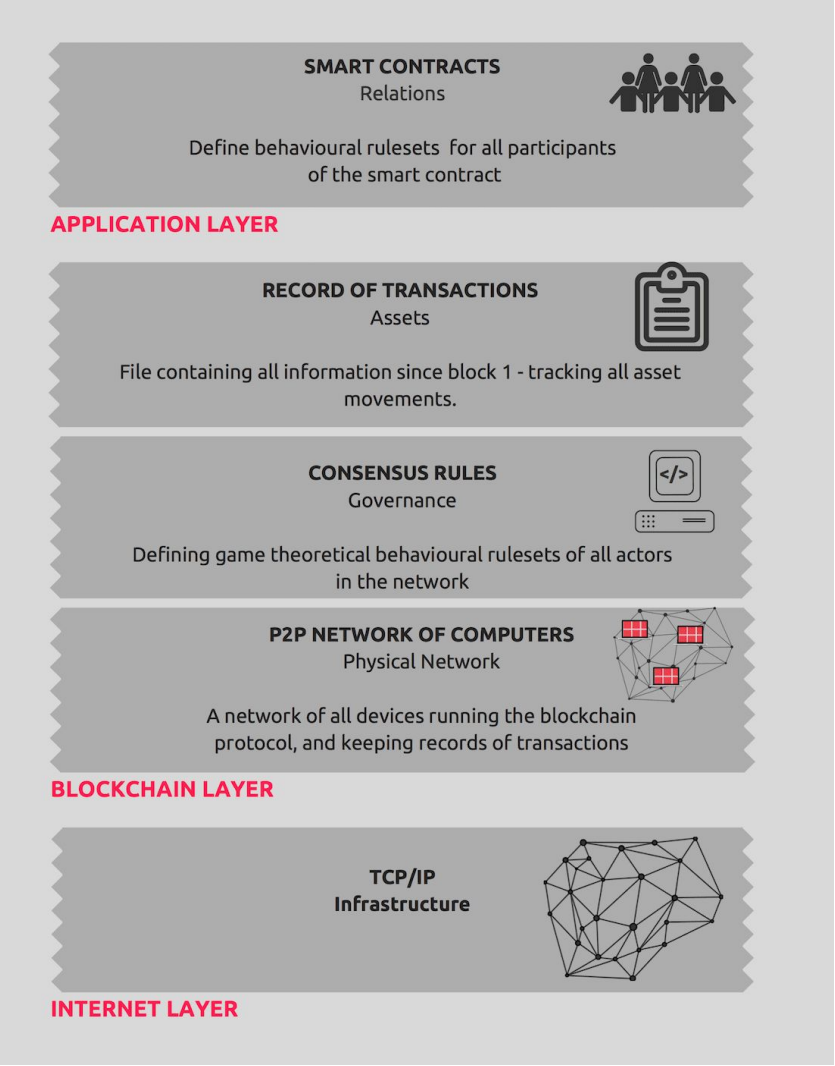
Sources & Further Reading

Ethereum whitepaper is good place to start
Ethereum yellow paper for technical specifications of the blockchain
Pick a language: Solidity the one language that has most extensive documentation
Pick a framework and test rpc: Solidity frameworks Embark and Truffle and use Ethersim as test rpc
Look at example projects: eg. Consensys on Github
dApps basic terminology
ConsenSys dApps tutorial
Ethereum Dapps for beginners
Ethereum reading list for prospective dApp developers
Full stack "Hello World" voting Ethereum dApp tutorial
List of all dApps developed on Ethereum

DAOs

A DAO (Decentralized Autonomous Organization) can be seen as the most complex form of a smart contract, where the bylaws of the decentralized organization are embedded into the code of the smart contract, using complex token governance rules.

Historically, the Bitcoin network was considered the first true autonomous corporation, that was coordinated solely through a distributed consensus protocol, which anybody was free to adopt. Today, DAOs moved up the technology stack, thereby becoming fully virtualized through software. In case of a Bitcoin-style autonomous corporation, a complex stack of technologies and human-machine systems has to be put in place in order to create a functioning autonomous infrastructure.



Blockchain Technology Stack Of Ethereum & similar Blockchains

Inspired by Florian Glatz: Link

At today's evolutionary stage, a DAO materializes as a smart contract – a piece of code – executed on top of an increasingly opaque stack of distributed networking and consensus technology like the Ethereum blockchain or similar blockchains.

Decentralized Organizations (DO)

The idea of a decentralized organization takes the concept of traditional organizations and decentralizes it. Instead of a hierarchical structure managed by a set of humans interacting in person and controlling

property via the legal system, a decentralized organization involves a set of people interacting with each other according to a protocol specified in code and enforced on the blockchain.

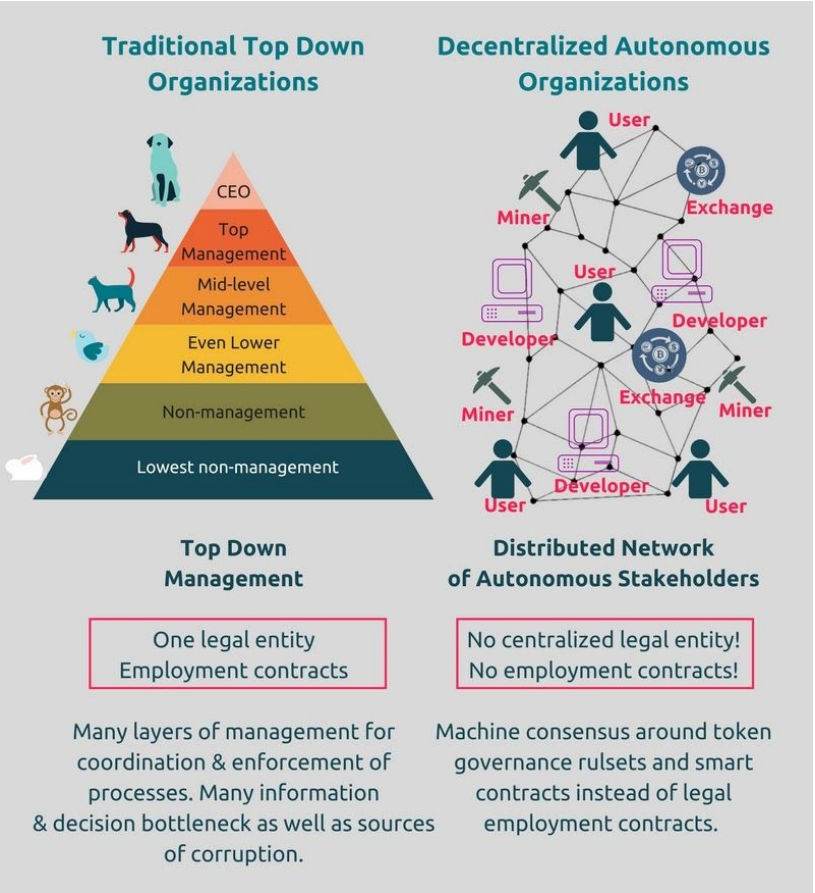
A Decentralized Organization (DO) may or may not make use of the legal system for some protection of its physical property, but even this such usage is secondary. For example, one can take the shareholder-owned corporation above, and transplant it entirely on the blockchain; a long-running blockchain-based contract maintains a record of each individual's holdings of their shares, and on-blockchain voting would allow the shareholders to select the positions of the board of directors and the employees.

Smart property systems can also be integrated into the blockchain directly, potentially allowing DOs to control vehicles, safety deposit boxes and buildings. **DAOs are the holy grail of DOs**: it is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.

Disrupting Governance with DAOs

Governance is the way rules, norms and actions of how people interact with each other are structured, sustained, regulated and held accountable. It regulates the process of decision-making among the actors involved in a collective problem that leads to the creation, reinforcement, or reproduction of social norms and institutions. The degree of formality depends on the internal rules of a given organization and, externally, with its business partners. As such, governance may take many forms, driven by many different motivations and with many different results.

Governance refers to all processes of governing, whether by a government, market or network, family, tribe – formal or informal – through the laws, norms, power or language. Blockchain can disrupt traditional governance structures of all kinds, and challenge the way we currently think about governance.



Disrupting Organizations with Blockchain Tokens
Source: Blockchainhub.net

With large parts of our society traditionally organized in top-down command and control ways, blockchain promises for more decentralized and spontaneous coordination instead of rigid structures by addressing two problems of traditional governance structures (1) Principal-Agent Dilemma, and high (2) transaction costs of coordination.

Smart Contracts in a trustless trust environment – and DAOs are the most complex form of a smart contract – tackle an age-old problem of governance, which in political science and economics is referred to as the principal-agent problem. This dilemma occurs when the agent – a person or entity – is able to make decisions on behalf of, or impacting, a so-called principal – another person or entity. In such setups, moral hazard occurs when one person takes more risks because someone else bears the cost of those risks, usually when there is an underlying information asymmetry in play. If the risk-taking party to a transaction knows more about its intentions than the party paying the consequences of the risk, agents are motivated to act in their own best interests, which are contrary to those of their principals.

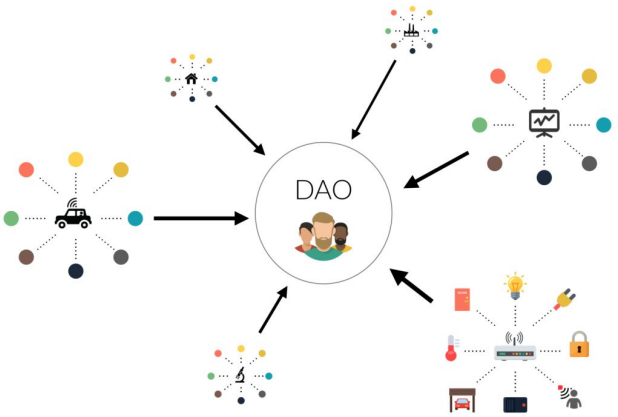
Blockchain and smart contracts reduce transaction costs and levels of bureaucracy and introduce the possibility of finding new ways of aligning interests and governing groups of people in a much more decentral way than we know today.

How DAOs work

Decentralized Autonomous Organisations (DAOs) run through rules encoded as computer programs called smart contracts. It is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.

- **Tokens of Transaction:** In order to exist a DAO needs some kind of internal property that is valuable in some way, and it has the ability to use that property as a mechanism for rewarding certain activities. The funding takes place directly upon creation of the organization. DAOs do not have a hierarchical structure, nor executives or management.
- **Autonomous:** Once deployed the entity is independent of its creators and cannot be influenced by outside forces. DAOs are open source, thus transparent and incorruptible. A DAO's financial transaction record and program rules are maintained on a blockchain. This approach eliminates the need to involve a bilaterally accepted trusted third party in a financial transaction.
- **Consensus:** In order to withdraw or move funds from a DAO, a majority of its stakeholders (this percentage could be specified in the code of the DAO) must agree on the decision. Even if bugs are found in the code, they could not be corrected until a voting procedure has taken place and the majority of voters agreed on it, which could leave known security holes open to exploitation.
- **Contractors:** A DAO cannot build a product, write code or develop hardware. It needs a contractor to accomplish its goals. Contractors get appointed via voting of token holders.
- **Proposals:** Proposals are the primary way for making decisions in a DAO. To avoid people overloading the network with proposals, a DAO could require a monetary deposit to prevent people from spamming the network.
- **Voting:** After submitting a proposal, voting takes place. DAOs allow people to exchange economic value with anyone in the world, like investing, money raising, lending, borrowing, without the need of an intermediary, just by trusting the code.

All cryptocurrencies which use public blockchains are DAOs (Bitcoin, Ethereum, Dash, Digix, etc.). Modern DAOs are complex smart contracts on top of a blockchain. The DAO was an example of a DAO on top of the Ethereum blockchain.

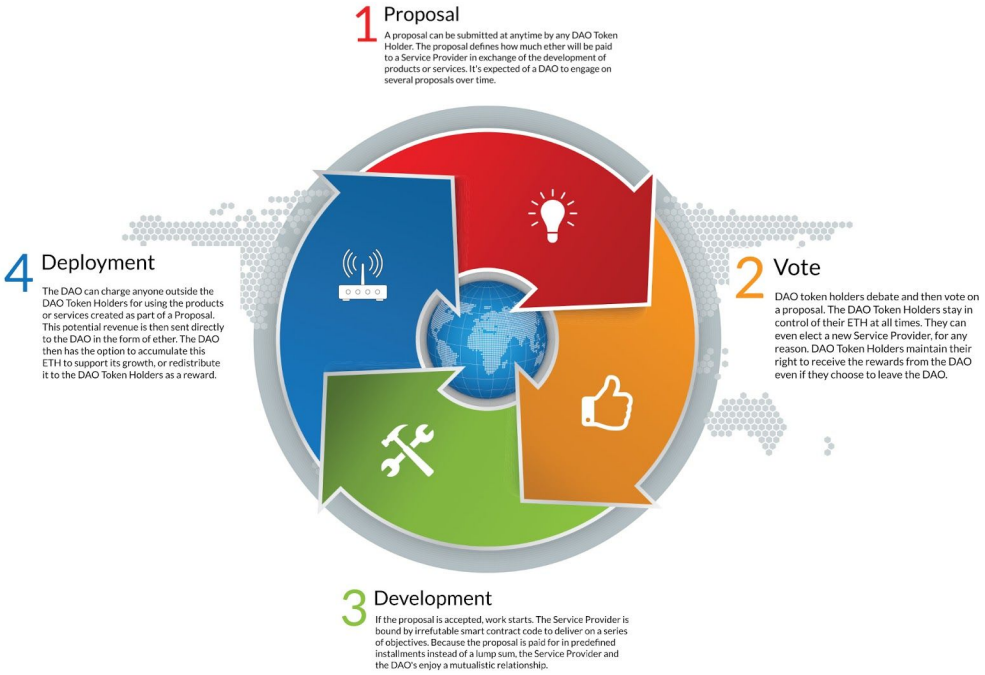


Decentalized Autonomous Organizations
Source: https://daohub.org

DAOs as Crowdfunding Vehicles

Since smart contracts run on top of public blockchain networks such as Ethereum, they can be programmed to collect and manage real economic value in arbitrarily large amounts referred to as ICO. The DAO was an example for such an ICO. Its aim was to be a decentralized autonomous investment fund without fund managers. In the biggest ICO at its time, TheDAO ended up collecting an equivalent of 150m USD in cryptocurrency. Everybody willing to invest was guaranteed a proportional share of the future revenues of the company. Additionally, those shares could be traded for any other asset listed on cryptocurrency exchanges, spanning across both fiat and cryptocurrencies.

Despite The DAO experiment ending prematurely with a spectacular and highly controversial “hack” and a subsequent hardfork of the Ethereum Blockchain, the idea of a new kind of crowdfunding model, based on blockchain token issuance as ownership shares in the funding target’s future success, ignited the minds of entrepreneurs worldwide and has ever since sparked an ICO frenzy.



Voting Process of TheDAO
Source: https://daohub.org

A growing number of startups are beginning to raise risk capital to fund the development of individual products, services or protocols, in a way that shares the future success of the company with its users and investors. Instead of complex, uncertain and strictly-regulated legal contractual relationships between investors and founders, those startups rely fully on DAO-type smart contracts to manage those relationships.

Circumventing legal systems and thereby legality itself, is, however, not the primary interest of most of those startups. Instead, it is the much lower barrier to entry as well as the new untapped market potential that motivates entrepreneurs to go down the route of token crowd sales. Ideals of a new kind of sharing economy, where the users of a service are at the same time its owners, give those startups moral grounds for venturing into legally gray areas.

Need for Legal Certainty

Startups trying to operate as DAOs are in need of a legal framework that allows them to conduct business not only within the closed world of a blockchain network but to interact with the physical world, the world of traditional financial instruments and that of intellectual property. To achieve this goal, two major barriers need to be overcome.

Firstly, startups need to know which kinds of regulations apply in which jurisdiction when selling cryptographic tokens, that may in some form represent a stake in future profits. The potential applicability of contemporary securities regulation is self-evident. Secondly, startups need a workable legal contractual framework, which allows DAOs to be embedded into our current institutional framework around the three above-mentioned fields of physical and intellectual property as well as traditional finance.

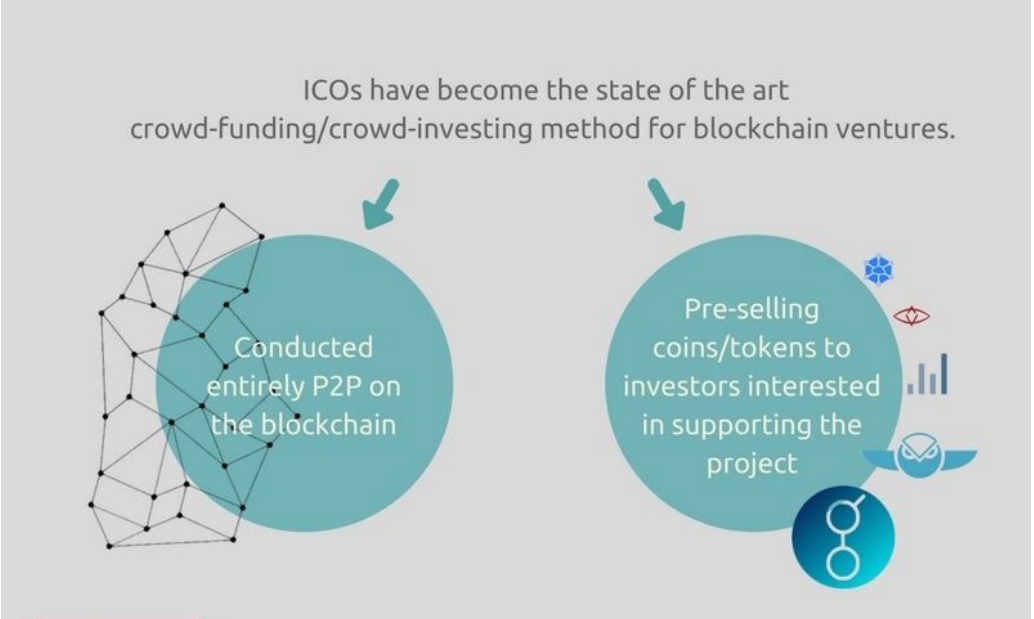
Both of those open problems are tough because they require a lawyer's intuition in a field, that has before only ever been the subject of science fiction literature. To an appreciable extent, however, partial answers may be developed by a suitably staffed entity, that is experienced in solving complex compliance issues arising in areas such as international private, financial, trade, corporate and tax law.

Sources & Further Reading

DAOs, DACs, DAs and More: An Incomplete Terminology Guide, by Vitalik Buterin
On Risks, Rewards and The Evolution Of DAOs, by Maciej Olpinski
Explaining DAOs to a non-technical person in 10 points, by Maciej Olpinski
How to Evaluate an ICO, by Shermin Voshmgir
Resisting the ICO gold rush, Greg McMullen
On Tokens and Crowdsales, Coindesk
Disrupting Organizations with Blockchain & Smart Contracts Journal For Strategic Change, Shermin Voshmgir

Initial Coin Offerings - ICOs

ICOs are a type of crowdfunding or crowd investing tool conducted entirely on the blockchain. Originally, the main idea of an ICO was to fund new projects by pre-selling coins/tokens to investors interested in the project. Entrepreneurs present a whitepaper describing the business model and the technical specifications of a project before the ICO. They lay out a timeline for the project and set a target budget where they describe the future funds spending (marketing, R&D, etc.) as well as coin distribution (how many coins are they going to keep for themselves, token supply, etc.). During the crowdfunding campaign, investors purchase tokens with already established cryptocurrencies like Bitcoin and Ethereum.



Initial Coin Offerings
Source: Blockchainhub.net

As opposed to traditional crowdfunding where the investment is considered to be a donation or a pre-buy of a product, ICOs give the supporters the possibility of a return of investment when selling their coin later at a possibly higher price. ICOs are similar to IPOs only if the token represents a stake in the project.

Crowd Funding or Crowd Investing?

Depending on the white paper, tokens can have very different properties. ICOs are very often compared to crowdfunding or crowdinvesting on the Blockchain. Most cases are hybrid and don't fall into either category. As opposed to crowdfunding where the investment is considered to be a donation, ICOs give the supporters the possibility of a return of investment when selling the token at a later date for a higher price. ICOs could be seen as a mix between a donation, investment or risk capital.

Investors get coins for supporting a startup idea. If a startup is successful, the token will be worth more in the future but is usually not a stake in the system. An ICO is similar to an IPO if the token represents a stake in the project. Unlike IPOs most ICOs that have been conducted in 2016 and 2017 didn't give investors a traditional stake in the startup. These investors can be seen as supporters of a project who are solely motivated by the return of their investment.

TheDAO in 2016 was the token sale closest to an IPO and an exception to that rule. Every token holder had a stake in the TheDAO proportional to the owned number of tokens with attached voting rights.

Please note that depending on the white paper, tokens can have very different properties and value propositions and legal status!

Web2 vs Web3
Source: Blockchainhub.net

Regulation

Until recently, the way an ICO was set up depended entirely on the team behind the blockchain project. Currently, ICOs still lack government regulation or community standards, and this can be regarded as hazardous for uneducated investors.

In most cases, buying the new token does not give investors stake in the company but rather the hope that if the project becomes successful, investors will be able to sell their coins at a much higher price. Critics argue that many current ICOs are based more on FOMO (Fear Of Missing Out) than on rational investor decision giving an advantage to those who understand the system better than others with no kind of investor protection.

The fact that most countries currently lack any type of government regulation for these blockchain based token sales can produce a lot of risks for the stakeholders involved – for entrepreneurs and investors alike. However, the situation is rapidly changing, and more and more governments are starting to regulate or at least look into regulating ICOs. The recent SEC statement regarding The DAO and the fact that China and Korea have recently banned ICOS might bring a different momentum into the current ecosystem.

Types of ICOs

Due to lack of regulation, developers have so far had total freedom on how to run an ICO. There have been different approaches on how these campaigns are set up. Hardly any ICO has been conducted in the same way as another and covering every possible ICO scenario is almost impossible.

However, the price of a token during ICO period often runs through different stages. In general, we can distinguish between four different pricing mechanism:

- **Price increases**
  ICO runs in stages where the team sets a fixed exchange rate for the tokens. The rate could increase incrementally with time. This way early investors who take the biggest risk get the best price per coin ratio. Backers send Bitcoins or Ethereum to the provided addresses and get the new token.

- **Price decreases**
  Another option would be a dutch auction as presented by the Gnosis team for the first time, where the sale starts at the highest price per token proportionally decreases until the end of the auction. Gnosis, for example, used a dutch auction mechanism to raise funds for their project.

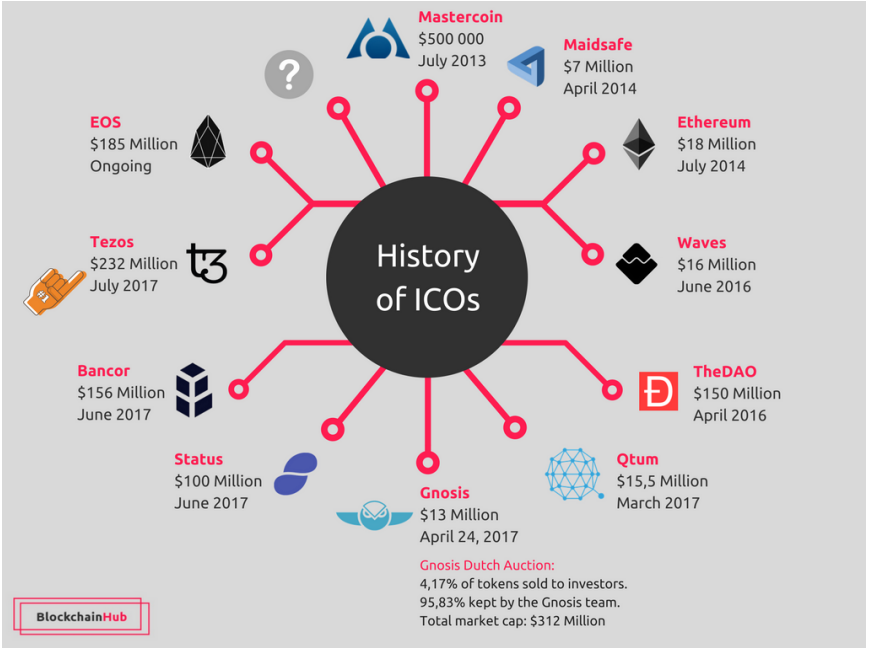
- **Price is fixed**
  If the exchange rate of the issued token is fixed, this gives investors the opportunity to get as many tokens as they like at that fixed price. This mechanism is appealing to large investors because they don't have to worry about influencing the price by purchasing a big number of tokens. After a token sale ends, there is a cool-off period where tokens might be frozen (investors are not allowed to transfer their coins for a certain amount of time) or kept away from exchanges. After the end of the cool-off period, exchanges can start listing the token thus allowing other people to trade it at a market price.

- **Price not determined**
  A developer might decide not to sell his tokens at a fixed exchange rate but rather let people invest in his startup and then distribute the new tokens proportionally by giving each person a percentage of the tokens corresponding to the portion of his investment which is part of total investments. In the EOS token sale, the total money invested got divided by a number of available tokens in order to determine the price. In this case, if a startup gets a single investor he/she will get 100% of the tokens.

As you can see from the examples stated above most token sales so far, have been time capped. However, some startups like Tau-Chain decided to leave their campaign running without a cap and an end date. So before you invest into an ICO make sure you understand how much tokens will be in circulation and what the pricing mechanism will be.

History of ICOs

It all started with the Mastercoin campaign where people could support the Mastercoin project by burning Bitcoin and getting Mastercoin tokens in exchange. This was conducted entirely P2P and inspired other projects that followed to use the Bitcoin blockchain for P2P crowdfunding purposes.



History of ICO
Source: blockchainhub.net

The Ethereum project used the Bitcoin Blockchain in 2014, successfully raising 18 Mio USD in Bitcoin within a four-week period and breaking all crowdfunding records to date, the Ethereum blockchain has become the platform that simplified the process of issuing tokens, sparking a series of record-breaking ICOs in 2016 and 2017.

Initial Coin Offerings are still a relatively new concept and still represent a small amount of the total crowdfunding capital worldwide. Global crowdfunding volume in 2015 was around $34 Billion, whereas the ICO volume was less than a percent of the total volume with $240m raised. The most notable ICO in the blockchain space happened in 2016 where a project called The “DAO” managed to raise $150 Million.

ICO Resources

Coindesk's ICO Tracker
ICO Transparency Monitor
CyberFund
Icoalert
Smith and Crown

Crypto Currency Funds & Fund Management Platforms

Iconomi Melonport
Prism

Sources & Further Reading

How to Evaluate an ICO - Part1 by Shermin Voshmgir
How to Evaluate Initial Coin Offerings by William Mougayar
Cryptoassets: Evaluation & Due Diligence framework
10 Steps for Evaluating Digital Asset Crowdsales, Tokenmarket
Investment Guide To 'Crypto' Coin Offerings Rating Blockchain Startups, Forbes
WeTrust: Lending Circles Going Blockchain, Daniel Zakrisson, WeTrust
ICOs, Token Sales, Crowdfundings, Smith & Crown
What is an initial coin offering?, Blockgeeks
What is an Initial Coin Offering (ICO)?, Ben Dickson
Initial Coin Offering, Investopedia
An Introduction To Initial Coin Offerings (ICO's) - The Venture Capital Disrupters, Tim Lea

Practical Guides

In the first part, we covered the fundamentals of Blockchain to give you an overview of how and why Blockchain be a game changer. In this part, we would like to focus on some practical “How To” guides that might be relevant for Blockchain newbies.

I want to do a Blockchain Project - Where do I start?

There is a wide array of approaches to implementing Blockchain or other Distributed Ledger Technologies. Diverse landscape of players has emerged, including software service providers that offer software capabilities on higher stack levels than the blockchain protocols themselves. Each approach has its own merits and challenges.

	HOW	EXAMPLES
IT Services	Build on request	ConsenSys
Blockchain First	Develop using the tools provided by specific blockchain	Ethereum, Bitcoin
Development Platforms	Tools for IT Professionals	ERIS, Tendermint, Hyperledger
Vertical Solutions	Industry specific	Axoni, Chain, R3, itBit, Clearmatics
Special APIs & Overlays	DIY building blocks	Blockstack, Factom, Open Assets, Tierion

Blockchain Implementation Solutions
Source: Coindesk.com

Blockchain as a Service (BaaS)

Setting up an environment to test and research blockchain requires an ecosystem with multiple systems to be able to develop research and test. The big players in the cloud industry like Amazon(AWS), Microsoft(Azure), IBM(BlueMix) have seen the potential benefits of offering blockchain services in the cloud and started providing some level of BaaS to their customers. Users will benefit from not having to face the problem of configuring and setting up a working blockchain. Hardware investments won't be needed as well. Microsoft has partnered with ConsenSys to offer Ethereum Blockchain as a Service (EBaaS) on Microsoft Azure. IBM(BueMix) has partnered with Hyperledger to offer BaaS to its customers. Amazon announced they would be offering the service in collaboration with the Digital Currency Group. Developers will have a single-click cloud-based blockchain developer environment, that will allow for rapid development of smart contracts.
Examples: Accenture, ConsenSys, Cognizant, Deloitte, IBM, PricewaterhouseCoopers (PWC), Ernst & Young.

Blockchain First

In this case, you work directly with the given blockchain tools and stack. Assembly is required, so this isn't for the faint of heart at this point, as many of the technologies are still developing and evolving. However, working directly with the blockchain provides a good degree of innovation, for example in building decentralized applications. This is where entrepreneurs are creating ambitious end-to-end, peer-to-peer applications, such as OpenBazaar (on Bitcoin), or Ujo Music (on Ethereum).
Examples: Bitcoin, Ethereum, etc.

Development Platforms

Here, you don't start with a preference for a blockchain. Rather, you start with a development approach orientation, and you build an app that backs into a blockchain infrastructure that could be served in the cloud. The goal here is rapid development, and you focus on the blockchain programmability.
Some Choices: BlockApps, Blockstream, Monax
Examples: Parity, Hyperledger, Tendermint.

Vertical Solutions

This segment is where we have seen the most rapid metamorphosis in the past year, mostly in financial services. These solutions are industry-specific and are based on private blockchain or ledger infrastructures. A caveat here is that some of these are not full blockchains. Rather, they are distributed ledgers, which are a subset of blockchain capabilities. And some don't even include a consensus element, which takes the implementation another level down from distributed ledger tech.
Examples: Axoni, Chain, Clearmatics, Digital Asset Holdings, itBit, R3.

APIs & Overlays
This approach uses the blockchain as an asset, ownership or identity-binding infrastructure, and you build applications with a specific focus on chains of proof, ownership rights, title registries or other specific services with a built-in trust-based component.
Examples: Blockstack, Factom, Open Assets, Tierion.

How to find a Blockchain Developer

The shortage of talent in the blockchain space has become a concern for many companies. While this type of shortage is typical in the early phases of every technology there are some differences in this case: many seasoned developers in the crypto community also invested in cryptocurrencies early on and often don't need your money. Furthermore, many of them might prefer to work on their own startup, raising funds through an ICO, rather than working for someone else.

Be more specific!
Before you list your job offer, you need to understand what you are looking for exactly. What do you need or want to build? Saying that you are looking for a blockchain developer is like saying that you are looking for an internet developer.

- ❏ **Do you want to build a new Blockchain?**
  Then you need a Blockchain full stack developer.

- ❏ **Do you want to build an application running on top of a Blockchain?**
  Then you need dapp developers who understand solidity (Ethereum), sidechains (Bitcoin), etc.

- ❏ **Understand the legal challenges that blockchain is facing**
  This will influence your infrastructural decision. Depending on the type of service you want to build you might face more or less legal challenges since some industries are heavily regulated. If your venture is in a highly regulated industry, you might want to consider building on a permissioned blockchain. This might also influence your dev decision or limit/enhance talent you can attract.

Before you hire a full stack blockchain developer consider using already existing blockchain infrastructure like Ethereum. The whole point of a blockchain is that we are crowdsourcing infrastructure. Applications get thinner, simpler and cheaper to code. Building entire blockchain from scratch is time-consuming. Unless you want to invent a new type of Blockchain, which is unlikely if you are not a crypto god yourself because you would not even understand how to build it, it is best to build on top of an existing blockchain. In that case, it would make sense to have an idea about what type of blockchain you want to build on: permissionless or permissioned blockchain, public or private blockchain.

Where to look?
Traditional job portals like LinkedIn might not be the best choice for hunting blockchain devs. Start looking in the relevant crypto communities.

- ❏ **Reddit**
  Note that many people in the cryptocurrency community take their privacy seriously and might not be very active on traditional social media. However many of them are active on Reddit. Look at relevant subgroups on Reddit - This is where many developers discuss their topics of interest and innovation happens. If you approach devs smartly in a way that resonates with their field of interest, you might be lucky to find someone.

- ❏ **Gitter**
  Consider promoting your project on Gitter. Maybe people will come to you. Gitter is the preferred chat app for developers.

- ❏ **Slack/Discord**
  Each crypto project runs its own Slack/Discord channel. Some communities have more than 5000 people in their channels.

- **Ethlance**
  Gives freelancers, including blockchain devs, the opportunity to offer their services online with the help of the blockchain. In order to access the application and view the listings one would need to install a dApp browser like for example MetaMask.

- **Bitcoin Talk forum**
  Bitcointalk forum is a place where new crypto projects get announced. This is also the first Bitcoin forum and it still has a very big community.

- **Meetups**
  Many developers go to local blockchain meetups. Join a local blockchain meetup and talk to the people there.

- **Start up Contents & Hackathons**
  Organize start-up contests in order to draw the attention of blockchain developers or join conferences like the Ethereum Devcon.

Build in-house experience
The lack of blockchain developers could make it very difficult to find & fund talented people from outside, so your best bet is to foster in-house talent. It will take some time but would benefit you most in the long run. Get outside help to train your existing staff.

Understanding the culture around Blockchain & the Decentralized Web
Early blockchain developers are still part of the bitcoin community which leans towards strong libertarianism. Personal freedom is one of the strongest claims. Traditional methods of hiring might not work (i.e., LinkedIn, vacancy announcement on job portals, etc.). Demanding fixed work schedule might not be very tempting either. Blockchains are not only tools for storing value, but they also create a whole economy around a new decentralized world order. If your cultures don't match with that new thinking, or at least, if you don't acknowledge the fact that blockchain is a whole new way of approaching the economy, and that business logic is changing, you might have problems attracting good talent.

How to Buy Bitcoin

Disclaimer! Trading cryptocurrency involves high risks (price volatility), low usability (lacking user experience of tools for non-developers) and bad actors (beware of fraud!). It is not advised for inexperienced investors to invest large sums. Never invest more than you are willing to lose. Only highly skilled people with experience should take such an opportunity. Speculating on the markets could lead to a total loss of funds!

Where to buy Bitcoin & other Cryptocurrencies
There are different places where you can buy bitcoin and other cryptocurrencies (see figure). You can choose between:

- ❏ Cryptocurrency exchanges (online)
- ❏ Bitcoin ATMs (you put money inside and can load your bitcoin wallet)
- ❏ Bitcoin Voucher Cards (ie. Austrian Post Office, House of Nakamoto, Azteco London)
- ❏ Buy it personally from other people

To buy bitcoin you can use standard payment methods including bank transfers, credit cards, cash or Paypal. They all have their pros and cons. Bank transfers are slower compared to other methods; credit cards have high transaction fees, paypal has transaction limits, and cash does not get the best exchange rates. The following figure will give you the brief overview of the ways you could buy cryptocurrency and the possible payment methods.

Cryptocurrency Exchanges
The best way to start buying coins is by opening a wallet with one of the large cryptocurrency exchange websites. To open an account each user needs to provide an official document ID. At the exchange, you can buy most of the popular coins and hold them in the same wallet. It is convenient and will save you a lot of time. The type of wallet is called an online wallet, and people rely on the exchange to keep their funds safe. After you bought your first bitcoin or any other cryptocurrency, you should consider transferring the funds to a more secure wallet, which is controlled only by you. There are different ways you can purchase cryptocurrency. For the sake of simplicity let's concentrate on Bitcoin.

- ❏ **Coinbase** is the most popular Bitcoin online exchange in the US. It operates in a number of European countries as well and provides best in class user experience and usability. It should be pointed out that Coinbase is one of the few exchanges which insures all the funds stored on its platform. In the case of a security breach, the insurance policy should cover the losses. The company offers a mobile app as well. You can purchase Bitcoin via bank wire or a credit card.

- ❏ **Anycoindirect** is a European cryptocurrency exchange. It does not provide a dedicated online wallet. Customers use their bank account to send money to the provider. After the money is received, users get the amount in Bitcoin transferred to the address they have provided.

- ❏ **Cex** allows for buying bitcoins with credit card or bank transfer. The exchange has worldwide coverage and offers a trading* platform with the ability for margin trading as well.

- ❏ **Shapeshift** is a different type of exchange. The platform is aimed at users who hold a portfolio of different cryptocurrencies. The idea behind the exchange is to swap easily coins for other coins, without even needing to register an account. It offers a high degree of privacy. If you own already bitcoin this is a great place to buy other cryptocurrencies.

- ❏ **LocalBitcoins** is a P2P(Peer-to-peer or **Person-to-Person**) Bitcoin exchange. Buyers and sellers agree on trade terms. The exchange connects local people who want to trade bitcoins. Payment methods are determined by the sellers, you can buy coins with Paypal, via bank wire or even with cash. The platform can offer high degree of privacy.

- **Kraken** is US based cryptocurrency exchange and trading* platform. It operates in Europe as well. It offers bitcoin margin trading. Bank transfers are the only way to buy bitcoins from Kraken.

- **Bitrush** is a cryptocurrency exchange that currently operates in Europe. People can buy coins instantly with credit card, iDEAL, Bancontact and MyBank.

- **Bitstamp** is the first regulated and licensed virtual currency exchange in the EU. Users can deposit their funds via bank transfer and buy bitcoins. Bitstamp is also a trading* platform.

- **Gemini** is a cryptocurrency exchange and trading platform. Currently, it operates only in the US. It allows both individual and institutional customers to buy, sell, and store digital assets. Additionally, the platform FDIC-insurees up to $250,000 per beneficial owner(US dollars only). You can buy bitcoins via bank deposit.

- **OkCoin** is one of the biggest Chinese exchanges and trading* platforms.

- **Coinmama** is a Bitcoin broker that specializes in letting you purchase bitcoin with a debit or credit card.

Bitcoin ATMs
ATMs at public places give people the opportunity to buy bitcoins with cash. You will need to install a wallet first in order to transfer the coins to an address of your choice.

Bitcoin Voucher Cards /Gift Cards
Voucher cards could be bought at stores in your area. These look like every other gift card and can be redeemed online. The cards are suitable for small purchases.

Wallets: Where you Manage your Coins
Coins like Bitcoin are stored in the so-called “wallets”. Think of a wallet as your bank account. The difference is that in the crypto world, you don’t have a third party like a financial institution, taking care of your money. In the case of a capital loss or a security breach, there is no rollback. Taking the right steps is vital for securing your funds. Being your own bank requires more caution and responsibility.
To start using Bitcoins or other types of cryptocurrencies, you first need a crypto wallet. The wallet stores the user’s private and public keys, which allows for sending and receiving coins. Different cryptocurrencies offer their own desktop or online wallet, which can be found on their website. A wallet does not store any coins. The only role of the wallet is to keep the user’s private keys safe and to connect to the corresponding blockchain. The private keys allow for the movement of funds between parties. Think of your private key as your home key, if you give it to someone else, he will have as much power as you. Note that coins are never stored in your wallet. Who owns how much Bitcoin is tracked in the Blockchain. There are four types of wallets that differ in usability and security level.

- **Desktop or Mobile Wallet**
  This is the most common type of wallet. An app has to be downloaded on your computer or mobile device. It will store user’s private keys on the device, that’s why it is strongly recommended to make regular backups of the wallet and store them on a different device besides your computer(USB stick, etc.). A mobile wallet could be compared to a real cash wallet. People don’t keep their entire wealth in their back pocket, and you shouldn’t store all of your crypto funds on your smartphone. Mobile wallets can be compared to real cash wallets.
  - Copay.io (Desktop/Mobile)
  - Jaxx.io (Desktop/Mobile)
  - Mycelium.com (Mobile)
  - Electrum.org (Desktop)
  - Exodus.io (Desktop)

- **Online Wallets** are web based wallets, which are hosted on a server. Every online wallet requires a password for login. The upside of these wallets is the usability. They're the most user-friendly

because they require as little setup as possible. The downside is that the wallet owner is dependent on a third party that could be a victim of theft or revoke access to the wallet. It is recommended not to store large values in an online wallet. Enabling 2-factor authentication(2FA) at login is strongly advised. There have been reports of stolen coins from users, despite having 2FA enabled. Hackers are using social engineering techniques to hijack the phone numbers of victims from their carriers. These phone numbers were used as 2FA for their online wallets even for their online banking. Apps like Google Authenticator offer greater security for 2FA and are the preferred way by many people for securing their online profiles.
Blockchain.info
Coinbase.com

- **Hardware Wallet** are a special type of wallet which stores the user's private keys in a secure hardware device (e.g., USB stick). Hardware wallets work by installing a dedicated application on the computer or mobile phone and connecting it with the physical device via USB. This way the private keys are stored offline and are therefore not exposed to viruses or attacks from the internet. The downside is that you have to buy the device first.
Ledgerwallet.com
Bitcointrezor.com
Keepkey.com

- **Paper Wallets:** In this case, people can generate their own private and public keys and print them on a paper for offline storage. This method avoids storing digital data on any device, offering the strongest security possible, but sacrificing usability. Once printed on paper, these wallets have to be kept in a safe place. Losing the piece of paper renders the funds in the wallet unusable. Check:
Bitaddress.org

Paper wallet example:
Left: public address for receiving funds
Right: private key for accessing the funds

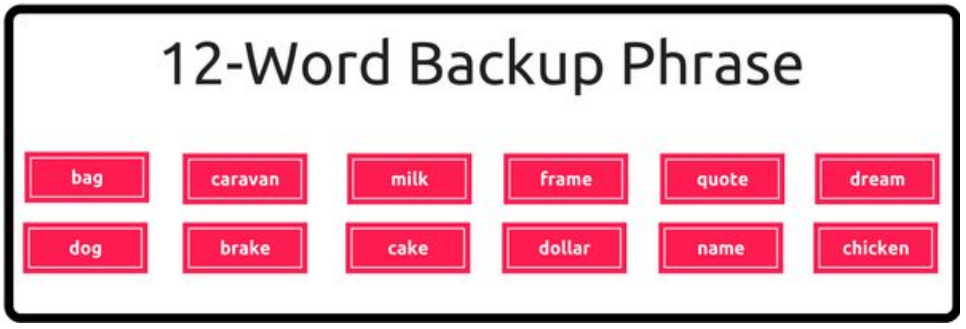
Backups: How to secure your Coins
The first thing you should do after creating a wallet is doing a backup. Losing access to your wallet is equal to burning your money. After you launch your wallet for the first time, you are presented with a 12-word recovery phrase(The phrase may be between 12 and 24 words long). Some wallets display this phrase only once.

Make sure you write down the words and keep them safe. If somebody gains access to these words, he or she may be granted access to your funds(there are different scenarios which won't be covered in this guide, but in general the phrase should be kept secret from other people).

Please consider the possibility of fire and other natural disasters. Having a fireproof storage box is a nice security add-on. If you ever need to recover your wallet from the 12-word phrase, you will only need to install a fresh copy of the wallet program on any device and enter the phrase at launch.

Then magic happens, and your wallet gets restored along with the funds in it. In the case of loss of the 12-word phrase, it is strongly advised to transfer your funds to a new wallet, which is properly backed up. Storing the 12-word phrase on your computer is dangerous because there will always be the danger of a security breach.

There are scenarios in which the 12-word phrase won't be used for backup. The first scenario is online hosted wallets. Users don't own the private keys for these wallets. The exchange owner keeps them. If the website goes down, the keys disappear with it, and access to the user funds wouldn't be possible anymore. The second scenario is paper wallets. The phrase is not needed because all of the information including the private key is printed on paper.



Some wallets still don't use the 12-word backup phrase for backup(example: full node wallets). These wallets are called non-deterministic (Random) Wallets. Such wallet is the Bitcoin Core full node client. These wallets require being backed up manually by the user. This works by copying the files which contain the private keys to a separate storage device (e.g., USB-stick). It is recommended to make multiple copies of these files.

Sending & Receiving Cryptocurrencies

The most important part of your wallet is your address. You use the address for sending and receiving coins. Almost all cryptocurrency addresses look similar to this:
1KDCn9XLVu3xNyr7ox64yjLw3kvKM1bADM.

Think of this as your bank account number. These strings could also be represented via QR-codes.
QR-codes are widely used in the mobile wallets for better convenience. Cryptocurrency transactions have their unique transaction IDs and cannot be reversed. Once you have sent the money to somebody, there is no rollback.

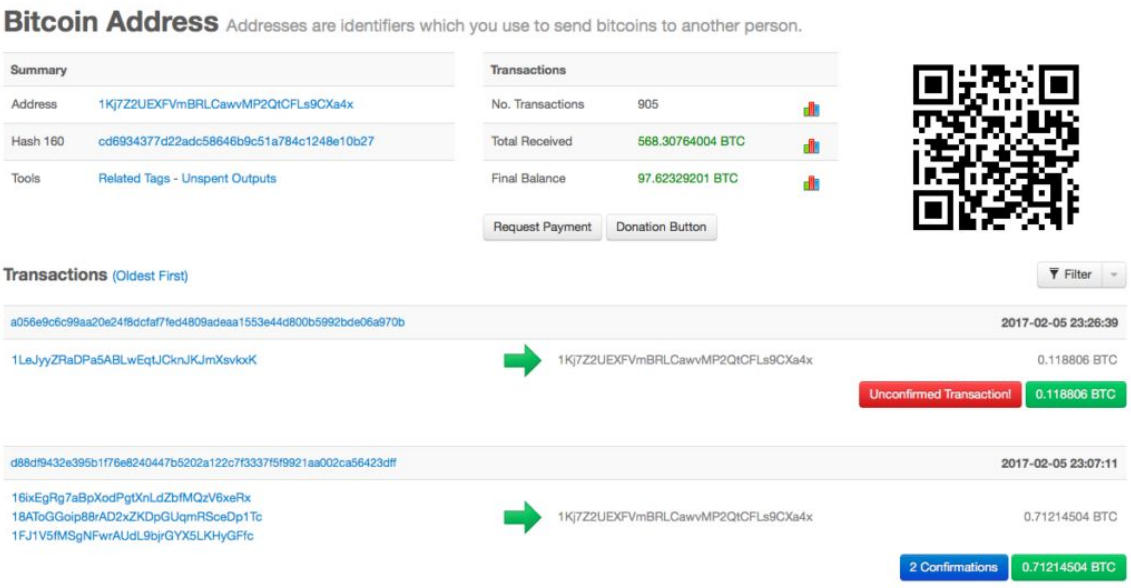
QR-code & string of user address
(mobile wallet)

For a transaction to be valid, it needs to get validated by the network. This process called a “confirmation.” A confirmation could last from a couple of seconds to many minutes, depending on the load of the network. For each transaction, users have to pay a small fee. The fee could range from under 1 cent up to a couple of cents, sometimes even a dollar, and it gets automatically subtracted from your balance.
Many wallets offer the opportunity to see your Bitcoin balance as USD or EUR equivalent. This way you can type the amount of USD or EUR you want to send to somebody, and the wallet will automatically calculate the amount of Bitcoin needed for the transaction.

Tracking Transactions on the Block Explorer
A blockchain is the backbone of any cryptocurrency including Bitcoin. Almost all cryptocurrencies run on public blockchains. Furthermore, each transaction happening on the Bitcoin blockchain gets saved and can be viewed online by anybody, by visiting a so-called block explorer. These explorers are websites which show a live feed of the transactions on the network.

To follow a transaction, you could paste the transaction ID in the search box. These transaction IDs are unique for each transaction and are shown in your wallet. One other way to follow a transaction to or from an address is to paste the address into the search box. This way the block explorer shows all incoming and outgoing transactions associated with this address.

Block explorers could be used for different statistics like for example the number of total transactions on the blockchain or number of unique Bitcoin addresses. (Bitcoin block explorer example: Blockchain.info)



Source: https://blockchain.info

Investing in Bitcoin FAQ

When it comes to investing in Bitcoin for the first time, many questions come up. We will try to address the most common questions people ask in our Bitcoin Investment FAQ.

- **Can I buy less than 1 Bitcoin?**
  Yes!
  Each Bitcoin is divisible to the 8th decimal place.
  You could buy 0.00000001 bitcoins which is worth less than a cent.

- **What is BTC?**
  BTC is the currency code for Bitcoin just like USD for US dollar.

- **What is a Satoshi?**
  Satoshi is the smallest unit of Bitcoin 0.00000001.
  10-8 100 millionth:
  It is named after Satoshi Nakamoto - the inventor of Bitcoin.

- **Is there a Bitcoin supply limit?**
  Yes.
  Bitcoins are created by the process called "mining."
  Bitcoins are created/minded for a fixed rate every time a new block of transactions is created.
  Blocks are created every 10 minutes.
  The block reward started at 50 BTC in 2009, and it gets halved every four years.
  Currently, the block reward is set at 12.5 BTC.
  There mining of Bitcoin - the total supply of Bitcoin is limited to 21 Million.
  This limit is hardcoded into the protocol and cannot be changed.
  Changing the supply by your own is equal to attacking the Bitcoin network.

- **Where can I buy Bitcoin?**
  The most common places where you can buy bitcoins are the online cryptocurrency exchanges. You will need to register with the exchange by providing your government ID. After an approval, you could load your account with fiat currency like USD, EUR, CNY, etc. using your bank account or credit card. For a step-by-step guide on how to buy Bitcoin on an online exchange click here: Link
  Other places where you could buy Bitcoin without registration:

- **What is a Bitcoin wallet?**
  A Bitcoin wallet is a piece of software that stores the user's private keys.
  Your bitcoin wallet allows you to access your Bitcoin.
  These wallets communicate with the Bitcoin network every time you want to send or receive Bitcoin.
  Please note: Bitcoins are not stored in your wallet!
  Only your private key is stored in your wallet.
  If you lose the private key, you lose access to your Bitcoin, and will never be able to access it again, and it will be lost forever.

- **What is a private key?**
  Your wallet never stores any bitcoins.
  The only purpose of a wallet is to keep your private key and communicate with the Bitcoin network. The private key is a long string of random numbers and letters, and it is always paired with a Bitcoin address. It creates signatures that are required to spend your funds by proving that you are the owner of the funds used in the transaction.
  Losing access to the private key is equal setting your cash on fire!
  Back up your private key!

❏ **Which Bitcoin wallets are safe?**
Different types of wallets offer a different level of security.
There is are tradeoffs between usability and accessibility.
The least secure wallets are the online wallets, and the most secure ones are the hardware wallets, and paper wallets also called "cold storage."
More on the topic read here.

❏ **Some Bitcoin exchanges trade BTC against USDT. What is USDT?**
Online exchanges like Poloniex don't use real USD dollars for trading.
Instead of USD they use USDT - a USD token - easily exchangeable P2P just like Bitcoin.
USDT is an asset-backed token which means that every unit of USDT is backed by one real US dollar. The units of USDT are called tethers. Each tether represents one real US dollar.
Some exchanges prefer using USDT because of the easier integration compared to real USD.
As opposed to international bank transfers, Tether tokens can also be transferred internationally at almost no costs.

❏ **How can I start trading Bitcoin?**
Register on online exchanges dedicated to cryptocurrency trading.
Registration on such platforms requires users to send a copy of their government issued ID.
The validation process could take up to few weeks depending on the user influx.
Examples of Bitcoin exchanges: Bitstamp, Gdax, Kraken, Gemini, Bittrex.

❏ **Is there a Bitcoin CEO?**
Bitcoin is a decentralized autonomous organization (DAO) and is governed by the community.
Bitcoin lacks traditional top down structure. Bitcoin is not a company registered in any country.
Bitcoin is a software protocol which lives on the internet.

❏ **What are transaction fees?**
Each time users send bitcoins a transaction fee has to be paid.
These fees are not fixed and depend on the network load.
If there is a huge transaction spike the transaction fees increase accordingly.
Currently, the Bitcoin network can process a handful of transactions, and any usage increase reflects on the fee price.
The Bitcoin community is working towards solving the problem.

❏ **Why are Bitcoin transaction fees so high?**
Bitcoin fees are dynamically adjusted.
When there is a usage increase, the fees increase accordingly.

❏ **What's margin trading?**
Margin trading is essentially trading with borrowed funds instead of your own.
When you place a margin order, all of the money you are using is borrowed from other users offering their funds as peer-to-peer loans.
The funds in your margin account are used only as collateral for these loans and to settle debts to lenders.
Source: Poloniex

❏ **What how do I calculate the Bitcoin Market Cap?**
The market capitalization of a cryptocurrency can give you a perspective on how big the markets for that currency is.
Current Bitcoin market cap is around USD 41 billion.
In order to calculate it, you need to multiply the today's price by the total coin supply.
Market Cap = Price x Circulating Supply
$41 538 444 951 = $2526.85 x 16 438 825 BTC

Check coinmarketcap.com for currenty info]

- ❏ **Where do I find BTC price charts?**
  Bitcoinwisdom
  Coinigy

- ❏ **Is Bitcoin backed by anything?**
  Bitcoin is not backed by anything.
  Its price gets determined by the market.

- ❏ **Why does Bitcoin have value even though it is not backed by anything?**
  What makes Bitcoin valuable are its properties as a digital asset:
  - Limited supply.
  - Easy storage.
  - Easy transfer.
  - It is not controlled by a central bank.
  - People accept it as a currency in exchange for goods.

How to participate in an ICO

Initial Coin Offerings (ICOs) or token sales are gaining a lot of attention, from institutional investors and individuals alike. ICOs are referred to the new IPOs or next generation crowdfunding. But the blockchain ecosystem is still young and lacks standards, thus making token sale participation a hurdle for the average person. In this post, we explain how to participate in a token sale with an easy step by step guide.

Most ICOs today run on top of the Ethereum blockchain through a smart contract that collects Ethereum tokens and automatically exchanges these for a new token presented by the start-up company. The entire process happens entirely P2P without any exchanges or brokers as middlemen. Every ICO has a different pricing mechanism (price decreases, increases, is fixed, non-existent)*. For more info on types of ICOs follow our ICO introduction.

Step 1: Register with a Cryptocurrency Exchange
To participate in an ICO, you need cryptocurrencies, usually Ether or Bitcoin. You cannot participate in an ICO with fiat currency. If you don't own cryptocurrency, you will first need to buy some. The best way to purchase significant amounts of Bitcoin is through online exchanges. Transfer money from your bank account to your newly created account with a cryptocurrency exchange. Please note that the registration process might need some days due to strict KYC and AML regulation. If you don't have a bank account or don't want to give up your privacy by sending your ID to a third party like Coinbase, there are other options like buying Bitcoin/Ether from an ATM or locally from other people. For more info read our tutorial on How to buy Bitcoin & other Cryptocurrencies.

Step 2: Exchange Fiat for Bitcoin or Ether
Once you registered an account with an exchange and the money from your bank account has arrived, you could exchange your EUR, USD, etc. for the cryptocurrency you want to buy. This process takes a few seconds. Your cryptocurrencies will be sent to an online wallet offered by the exchange you registered with. Keeping large amounts of coins online might be dangerous since online exchanges are vulnerable to attacks. In the past money got stolen from online exchanges. Therefore it is highly advised that you send your cryptocurrency to a wallet which is under your control. For more info on how to securely store your coins read our tutorial on How to buy Bitcoin & other Cryptocurrencies.

Step 3: Transfer your Coins from the Exchange to a Blockchain Wallet you Control
Another reason for you to move your coins to a wallet which is under your control is the token sale participation. Unless your exchange offers the explicit possibility to participate in a particular ICO with your online wallet, the general rule is not to send funds from an exchange wallet since you won't have access to the new token. This means that if you use a random online wallet to participate in an ICO and send money to the ICO address, you won't receive the tokens you bought, which is the equal to losing your investment. If this happens to you then you, contact tech support and try resolving the problem. Note that most exchanges are currently overloaded with requests and mostly still have poor customer service. Furthermore, exchanges might not be obliged to process your request depending on the conditions set in their general "Terms of Use ."

Step 4: Set up your Wallet
Most token sales today happen on the Ethereum network. Therefore you will need an Ethereum wallet to participate in the token sale. Not every wallet is suitable for ICOs. The most user-friendly and widely accepted Ethereum wallets are MetaMask and MyEhterWallet. MetaMask is a plugin for the Google Chrome browser. It is not only a wallet but also a lightweight Ethereum dApp browser. MyEtherWallet is a client-side wallet and does not hold your private keys. It also connects with hardware wallets like the Ledger Nano S or Trezor. Depending on the setup and the ICO one of these wallets might be recommended for the participation. If the startup hasn't defined a preferred wallet for the ICO, we recommend using MetaMask.
MetaMask is a desktop type of wallet, and we do not recommend storing large values in it. Use it only for the ICO and then move your funds to a more secure place like a hardware wallet or paper wallet. Don't

forget backing up your wallet. Store your 12-word seed in a safe place (not in the cloud). After your wallet is properly setup & backed up send Ether from your online exchange account to your MetaMask wallet.

Step 5: Buy ICO Tokens
Before you proceed make sure to read the general terms of the ICO and the token purchase agreement. Most start-ups provide step-by-step guides for the token sale participation including screenshots for each step. Make sure you read these. You should also join the social media channels including Slack or Telegram and follow the news around the ICO. Sometimes token sales experience technical problems and staying up to date during the token sale is crucial. Read how the Status ICO managed to clog the Ethereum network. All ICOs start either at a certain time or a previously specified block number. You can use an Ethereum block explorer to check the block numbers. If there is a start time make sure you converted the values for your time zone. Note that some ICOs end in a matter of minutes. Therefore using wallets like Parity that allow for a more advanced setup options might be recommended if you expect the token sale to end quickly. When the token sale starts, you will have to send ETH to the address specified by the team. You will need to set a proper gas limit which is controlled by the MetaMask interface. After you send the transaction there are a couple of scenarios:

- ❏ You receive your tokens right after the token sale ends
- ❏ You need to wait for couple of days for your tokens
- ❏ You will need to redeem your tokens manually (look at eos.io token sale)

Note! In some cases, hackers have manipulated ICO websites, by exchanging the real ETH address with their own ETH address, which means that the address indicated on the ICO website to which investors sent their money was corrupted and the hackers got all the money instead of the team behind the ICO.

Step 6: Secure your Tokens
After you receive your tokens in your MetaMask – or MyEtherWallet, or Parity – address make sure to transfer these to a more secure wallet. You will need to have some extra ETH (small amount) stored in your wallet to pay for transaction costs of sending money from wallet to wallet. Note that this will change once Ethereum updates to Metropolis, but currently it is still something you will need to keep in mind.