

Blockchain

Technology Primer

Version 1.0 | July 2018

Executive Summary

Blockchain technology has seen an almost unprecedented hype in recent years. Starting as a bitcoin network to manage financial transactions, it has been attributed as a panacea to solving every problem from managing refugee crises to energy to tracking food supplies.

This document is a dive into blockchain technology to understand the history and basics as well as explain its various components and commercially available implementations.

The objective is to educate the reader about the technology details so they can develop:

1. A perspective about its application to specific Advertising Technology use cases
2. An understanding of the technology choices available
3. An understanding of business and operational implications of implementing a blockchain solution

This document is accompanied by the IAB Tech Lab Resources Wiki, a curated collection of resources available on the web for further reading to learn more and dive deeper into specific topics.

About IAB Tech Lab

The IAB Technology Laboratory is an independent, international, research and development consortium charged with producing and helping companies implement global industry technical standards. Comprised of marketers, advertising agencies, digital publishers and ad technology firms, as well as other companies with interests in the interactive marketing arena, IAB Tech Lab's goal is to reduce friction associated with the digital advertising and marketing supply chain, while contributing to the safe and secure growth of the industry. Learn more about IAB Tech Lab [here](#).

More information available at: <https://www.iabtechlab.com>

THE STANDARDS, THE SPECIFICATIONS, THE MEASUREMENT GUIDELINES, AND ANY OTHER MATERIALS OR SERVICES PROVIDED TO OR USED BY YOU HEREUNDER (THE “PRODUCTS AND SERVICES”) ARE PROVIDED “AS IS” AND “AS AVAILABLE,” AND IAB TECHNOLOGY LABORATORY, INC. (“TECH LAB”) MAKES NO WARRANTY WITH RESPECT TO THE SAME AND HEREBY DISCLAIMS ANY AND ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, ERROR-FREE OR UNINTERRUPTED OPERATION, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. TO THE EXTENT THAT TECH LAB MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THE PRODUCTS AND SERVICES DO NOT CONSTITUTE BUSINESS OR LEGAL ADVICE. TECH LAB DOES NOT WARRANT THAT THE PRODUCTS AND SERVICES PROVIDED TO OR USED BY YOU HEREUNDER SHALL CAUSE YOU AND/OR YOUR PRODUCTS OR SERVICES TO BE IN COMPLIANCE WITH ANY APPLICABLE LAWS, REGULATIONS, OR SELF-REGULATORY FRAMEWORKS, AND YOU ARE SOLELY RESPONSIBLE FOR COMPLIANCE WITH THE SAME, INCLUDING, BUT NOT LIMITED TO, DATA PROTECTION LAWS, SUCH AS THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (CANADA), THE DATA PROTECTION DIRECTIVE (EU), THE E-PRIVACY DIRECTIVE (EU), THE GENERAL DATA PROTECTION REGULATION (EU), AND THE E-PRIVACY REGULATION (EU) AS AND WHEN THEY BECOME EFFECTIVE.

Blockchain Working Group

The Blockchain Technology Primer has been developed by a subgroup of the IAB Tech Lab Blockchain Working Group. Key contributors to this subgroup were:

Michael Freyberger	AppNexus
Christopher Beach	Receptiv
Ezgi Cengiz	Twitter
Breaux Walker	Kochava Inc.
Alexei Furs	Optimatic
Archie Sharma	OpenX
David Jung	Meredith Digital
Pooja Nayak	Starcom Worldwide
Adrian Domek	Parsec Media
Ryan Gauss	AerServ
Demitri Nikolaou	Spectrum Reach
Miguel Morales	Lucidity
Amit Shetty	IAB
Jeremy Stanton	Amino Payments
Dustin Suchter	SRAX

*As of June 26, 2018

Table of Contents

Executive Summary	1
About IAB Tech Lab	1
Blockchain Working Group	3
Introduction	6
Distributed Ledger Technologies	8
Decentralized Database and Applications	8
Private vs public	9
Public	9
Private	10
Consensus	12
Consensus Methods	12
Proof of Work	12
Proof of Stake	12
Proof of Burn	13
Proof of Activity	13
Proof of Elapsed Time (PoET)	13
Simplified Byzantine Fault Tolerance (SBFT)	14
Mining	15
Smart Contracts	16
What is a Smart Contract?	16
Implications of Smart Contracts	17
Cryptography and Hashing	18
Cryptography in Blockchain	18
Digital Signature	19
What if I lose my private key?	20
Multisig	21
Wallet	21
Hashing	22
Blockchain Data Structure/ Merkle Tree	23
Blockchain Technology Stack	25
Shared Data	26
Protocols	26

Platforms	26
Products	27
Fat Protocols	27
Advertising Use cases	29
Fraud Prevention	31
Identity, Data and Privacy	31
Measurement	31
Transparency	32
Settlement	32
Appendix 1: A brief history of Blockchain	33
Appendix 2: Lexicon	36

Introduction

“Blockchain is a solution looking for a problem” is frequently the title of many articles today as Blockchain technology has evolved from Bitcoin to Ethereum to several other protocols and applications addressing not just financial services, but several other industries including media and advertising technology.

Blockchain was developed to solve a very specific problem—storage and transfer of digital assets between two peers without the need for an intermediary. As the world transitions to digital representation of assets, there are only two ways to manage the digital transactions—either through third party intermediaries e.g. banks or credit card processors, which is what we do today, or bitcoin-like networks with well defined protocols to authenticate the entities, validate their asset holdings, and verify transactions between two entities.

How does blockchain technology enable error-free digital transactions without an intermediary to perform the required check and balance?

As an intermediary, a bank processes transactions in the order they occur and thus, at any time knows the value that is held by an entity in their system. It is therefore able to perform an authorization of funds without errors.

In a blockchain, this task is performed by users of the blockchain solving a cryptographic puzzle and adding a transaction to a previous set of transactions in the right order. This set of transactions is a ‘block’.

A majority of users must agree to the validity of this block by adding other blocks to this ‘chain’ of blocks. Since future blocks are dependent on previous blocks, it is impossible to alter or delete a block. This is why a blockchain is ‘immutable’.

Every transaction is visible to everyone so users can verify if the sender has the assets they claim to have, thus eliminating a third party. This is done by the sharing of a database or ledger and every user can theoretically have a copy of all the transactions. Hence a blockchain is a 'distributed' ledger.

Although many people like to understand blockchain as a database, It is much more than a database. It is a combination of distributed or shared databases with public or private permission to store and access transactions, consensus methods to approve and record a transaction, clever use of cryptography to authenticate an entity, currency to pay for the system upkeep and reward those who provide the resources to maintain the system, as well as store of value of an asset, and with smart contracts, a way to enforce a condition or automate a process to be followed.

It is because of these components that blockchain technology can be applied to many use cases beyond money or bitcoin e.g. Ethereum protocol adds abilities to run peer-to-peer programs or contracts and applications that allow it to be applied to diverse operations beyond a money transfer use case.

In this document we will explore all the different components and concepts of blockchain technology and operational elements.

Distributed Ledger Technologies

Distributed ledger technologies (DLT) were a precursor to blockchain and understanding DLT is a good starting point. We could even consider blockchain an implementation of DLT.

A ledger or register by definition is a process by which a record is kept for all the transactions of a company or organization. Since the dawn of civilization, ledgers have been used for keeping economic transactions to record asset holdings, contracts, and payments for goods and services. A centralized ledger is governed by a single entity that is entrusted with proper maintenance of checks and balances. A distributed ledger operates as a 'network' in which users approve record of transactions. The data is replicated with multiple users and there is no one database.

Every user or computer on the DLT network has to make its own determination and then the users 'vote' on the correct version of the record of transactions. With an approved consensus, the ledger is updated with the transaction details. All the users or computers within the network maintain their own copy of the ledger. There is no central owner or administrator of the distributed ledger. The data is stored and shared between everyone on the large network irrespective of their location or institution. Any change to the record is immediately registered in all copies of the distributed ledger. It can be electronic, financial, legal, or physical. The security and accuracy of the distributed ledger are maintained through an encryption (cryptography).

Decentralized Database and Applications

Decentralized databases and applications have been around for a long time. Popular implementations of decentralized applications include Bittorrent and IPFS¹ as well as

¹ "IPFS is the Distributed Web." <https://ipfs.io/>.

others like emule² for music and other media sharing applications. Common attributes among distributed systems include the ability to scale by adding new nodes, load balancing of data among nodes, and ability to verify content which is replicated among many nodes.

Private vs public

Who can be part of a DLT?

Each DLT network has its own protocol that governs the rules for participation, verifying the record of transactions and maintaining the ledger. Participation can be public or private. In public DLT anyone can join the network whereas in a private DLT, there is a permission mechanism on who can be allowed into the network.

Public

Popular examples of public distributed ledgers include Bitcoin and Ethereum. The advantages of a public chain is that an entity or consortium of entities cannot easily take control of the ledger and inject fraudulent transactions. Part of the security of public ledgers comes from the ability of anyone to be able to verify current and historical transactions without relying on third-party intermediaries.

Another family of public ledgers include zCash and Monero. These ledgers, while public and auditable, are completely private. Only the entities that participated in a transaction are able to view the contents of those transactions.

Both families of public ledgers use highly distributed consensus mechanisms such as Proof of Work or Proof of Stake. These types of consensus mechanisms require tokens or coins to create the economic incentives to protect the network. However, due to the

² <https://www.emule-project.net/home/perl/general.cgi?l=1>

large distribution of nodes, the number of transactions public ledgers can handle is currently capped at ~15/sec³.

Private

A third family of distributed ledgers is private ledgers such as Quorum and HyperLedger. Private ledgers provide unique properties such as being completely secure from non-authorized participants and keeping all transaction data private and only accessible by ledger participants. However, due to the smaller number of participating verification nodes, it is more vulnerable to 51% attacks.

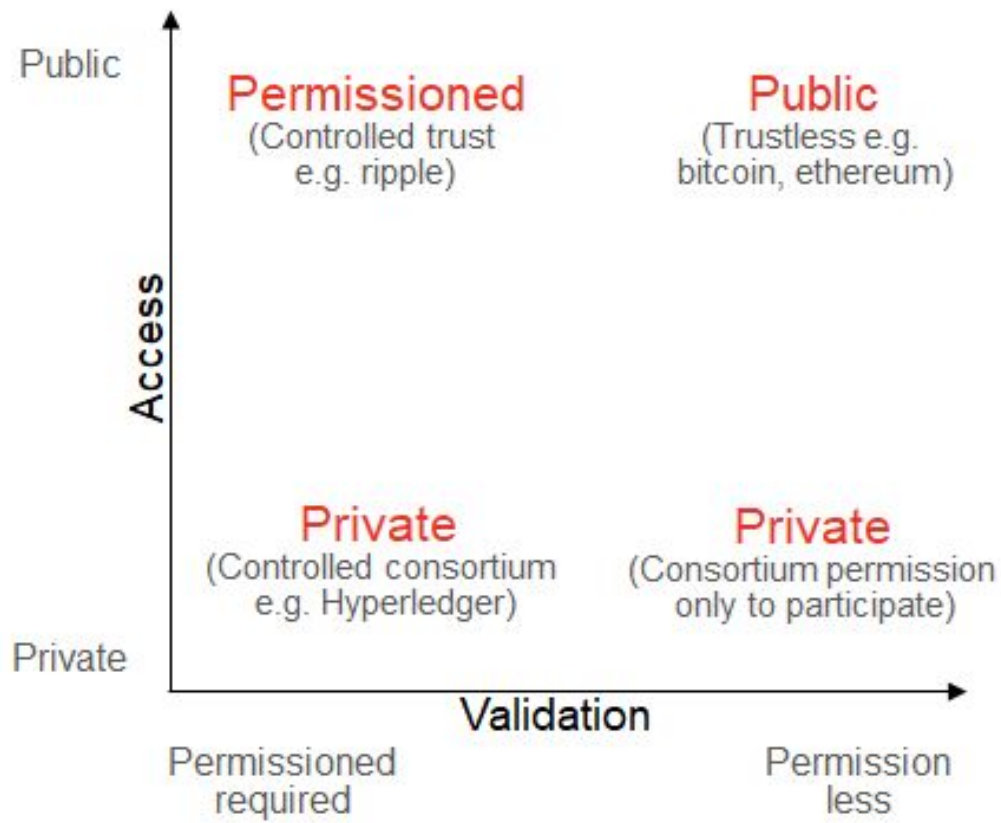
Private ledgers tend to employ low-distribution consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT), Raft, or Paxos. Due to the limitations inherent in these consensus mechanisms, only a limited number of nodes may participate in them. These family of consensus mechanisms do not require tokens or coins to operate. Due to the limited number of nodes, the number of transactions of private ledgers is much higher than current public ledgers and may be capped at ~20k/sec⁴ depending on the number of participating nodes.

³ "Performance and Scalability of Blockchain Networks and Smart ... - DiVA."

<https://umu.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf>

⁴ "Performance and Scalability of Blockchain Networks and Smart ... - DiVA."

<https://umu.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf>. Accessed 9 Feb. 2018.



Consensus

Blockchains are peer-to-peer networks with no central administrator or authority. It is crucial to ensure that the network participants reach consensus on the state of the ledger i.e. the uniqueness and order of records. This is done through consensus algorithms that apply different methods to ensure that the right order and uniqueness of transactions has been determined and validated by enough users to be added to the ledger.

Consensus Methods

Some consensus methods are:

Proof of Work

Proof of Work describes a system that requires a substantial but feasible amount of effort in order to deter malicious uses of computing power, such as sending spam emails or launching denial of service attacks. The concept was adapted to a peer-to-peer network by Hal Finney in 2004 through the idea of "reusable proof of work." Bitcoin became the first widely adopted application of Finney's idea. Proof of work forms the basis of many other cryptocurrencies as well. In bitcoin, the proof of work requires that the miner has correctly identified and verified the previous block, verified the list of transactions correctly since the previous block, and guessed a special number called a nonce.

Proof of Stake

Proof of Stake (PoS) concept states that an individual can mine or approve a transaction based on how many coins he or she holds through voting. This implies that the more Bitcoin or altcoin held by a wallet, the more voting power the user will have.

Besides the number of coins held other factors such as age or minimum balance of address may also be included to determine stake.

Proof of Burn

Proof of Burn is a method of consensus in which a miner is required to burn or waste a proof of work coins usually different than the proof of burn coin which is being verified by making it unspendable. This is done by sending it to an eater address. This 'burn' transaction is recorded and verified and the user that 'burnt' the coin gets rewarded with the coins of its own blockchain currency. The main idea behind proof of burn is that the user is demonstrating long term commitment by taking a short term loss. The more coins a user can burn the more rewards they get so it can create a rich get richer problem. The advantages of proof of burn are more stability as users are betting on long term as well as fair distribution and decentralization.

Proof of Activity

Proof of Activity is a crossover approach that combines both Proof of Work and Proof of Stake. First, Proof of Work is performed to identify a winning block and then a chosen set of users perform the validation, thus achieving consensus.

Proof of Elapsed Time (PoET)

Chipmaker Intel's Proof of Elapsed Time (PoET) is another consensus algorithm aimed at reaching consensus using secure instructions placed within Intel's widely available computer chips. PoET exploits features of computer chips (of nodes) to safely, and with a high degree of randomness, select a leader (node) to create a new block. PoET is similar to Simplified Byzantine Fault Tolerance (SBFT) in that it eliminates the requirement of costly computational resources. Each validating node or validator requests a wait time from a Trusted Execution Environment (TEE), which refers to a specially designated area within an Intel chip, also called a Software Guard Extension

(SGX). The leader among a pool of validating nodes is elected through a lottery system in which the node with the shortest wait time is claimed to be the winner. The protocol instructions within SGX produces an attestation (proof of waiting) for the winning node, which can be verified by other nodes in the network.

Simplified Byzantine Fault Tolerance (SBFT)

Main drawbacks of using Proof Of Work (PoW) consensus is its huge power consumption and limited capacity to process transactions quickly. Thus, PoW is unsuitable for enterprise applications that need to scale and provide speedy transactions.

Since all network participants are trusted and known to each other in a permissioned blockchain, all stakeholders can agree on a custom architecture with a consensus protocol that can meet the scalability and performance requirements of business applications. Simplified Byzantine Fault Tolerance (SBFT) is one such consensus algorithm and was specifically designed for scalability and speed. Unlike in PoW, where all nodes are identical to each other, SBFT's specialized nodes have different roles to achieve consensus and manage the state of ledger.

SBTF is computationally more efficient than PoW because nodes do not compete against each other and expend large amounts of computing resources trying to solve a puzzle. Instead, one generator node (master replicator) is preselected to create a new block, which contributes to both the speed and scalability needs of business applications. The modular nature of the network facilitates for defective and malicious nodes to be quickly identified and removed, adding an extra layer of network security.

Mining

Just like we dig deep into earth for valuable material like gold, copper, or other minerals and commodities of utility like coal, mining in blockchain is performed to obtain coins or currency of the network.

Mining for coins in blockchain is different than mining for gold. Besides obtaining coins (e.g. bitcoin), the miners also perform a service for the blockchain network, i.e. they validate and record transactions in a decentralized fashion using any of the consensus methods described above and as enforced by the network protocol.

Blockchain networks rely on miners to perform tasks that an intermediary may typically do in business transactions, e.g. in the case of the Bitcoin network, miners perform tasks similar to bank tellers—checking that a particular transfer of bitcoins is between two valid accounts, validating that the sender's signatures are authentic, and the sender owns the coins that are being transferred.

Thus, mining enables decentralization in a blockchain network.

Smart Contracts

What is a Smart Contract?

A smart contract is a concept introduced by the Ethereum blockchain network. It is a computer program that is capable of running a set of predefined functions when a specified condition or set of conditions occurs. The program is stored on the distributed ledger and is capable of writing the resulting change to the distributed ledger.

A “smart” contract is a relationship that may be established through the interaction of electronic agents and/or which may be performed or enforced, in whole or in part, upon satisfaction of a set of pre-programmed conditions. Nick Szabo provided the initial example of a “smart” contract, which was simply a vending machine that dispenses goods upon payment of a specified sum.

A “smart” contract may, but need not, involve employment or deployment of a blockchain. When using a “smart” contract incorporating blockchain technology, the underlying algorithm is based on a consensus among the parties or through contract methodology⁵.

A further example of a “smart” contract that does not employ a blockchain is where one uses an electronic agent to determine when to purchase an item. For example, ABC, Inc. uses an electronic agent to determine when to purchase a discrete item based on need combined with available prices and how many discrete items to purchase. XYZ, Inc. sells this discrete item and uses an electronic agent to negotiate its contracts based on its available supply and the market in general. ABC needs 1 million discrete items and is willing to pay up to \$1/item; XYZ has 100 million discrete items, which it can sell

⁵ Craig A. de Ridder, Mercedes K. Tunstall, Nathalie Prescott, Recognition of Smart Contracts <https://www.pillsburylaw.com/en/news-and-insights/recognition-of-smart-contracts.html>

and is willing to sell at \$0.50/item. ABC and XYZ enter into negotiations using electronic agents that have been programmed to establish delivery terms, volumes, and price based upon established parameters. In this manner, ABC and XYZ reach an agreement through the interaction of the electronic agents; ABC receives the needed discrete item and pays XYZ the agreed upon amount. At no point during the transaction, after the electronic agents were programmed and deployed, was there any human intervention in the contract for review, negotiation, or agreement, nor was there a necessity to use blockchain to execute or perform said transaction⁶.

Implications of Smart Contracts

Disintermediating contracts entirely: Blockchain currency disintermediates by eliminating middlemen for reconciliation and distribution of funds. Therefore, smart contracts could eliminate contractual middlemen^[8].

Self enforcing programs: Smart contracts could contain code providing for remedies or enforcement mechanisms that automatically occur based on certain conditions, thereby creating self-enforcing contracts.

Flexible contracts: Further, smart contracts and blockchain could mark the return of consumer commercial contracts with boilerplate provision. Currently, contracts such as digital terms of service have no provision to alter or decline certain contractual provisions. But with smart contracts that self-execute and self-enforce, the possibility for programmed-in conditions might enable variable price structures for goods or services, depending on a number of terms that are accepted or rejected. Consumer or entity choice could be effectuated by automated agents programmed into the blockchain to behave according to set preferences.

⁶ Max Raskin, The Law and Legality of Smart Contracts, April 2017, Georgetown Law Review <https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/>

Cryptography and Hashing

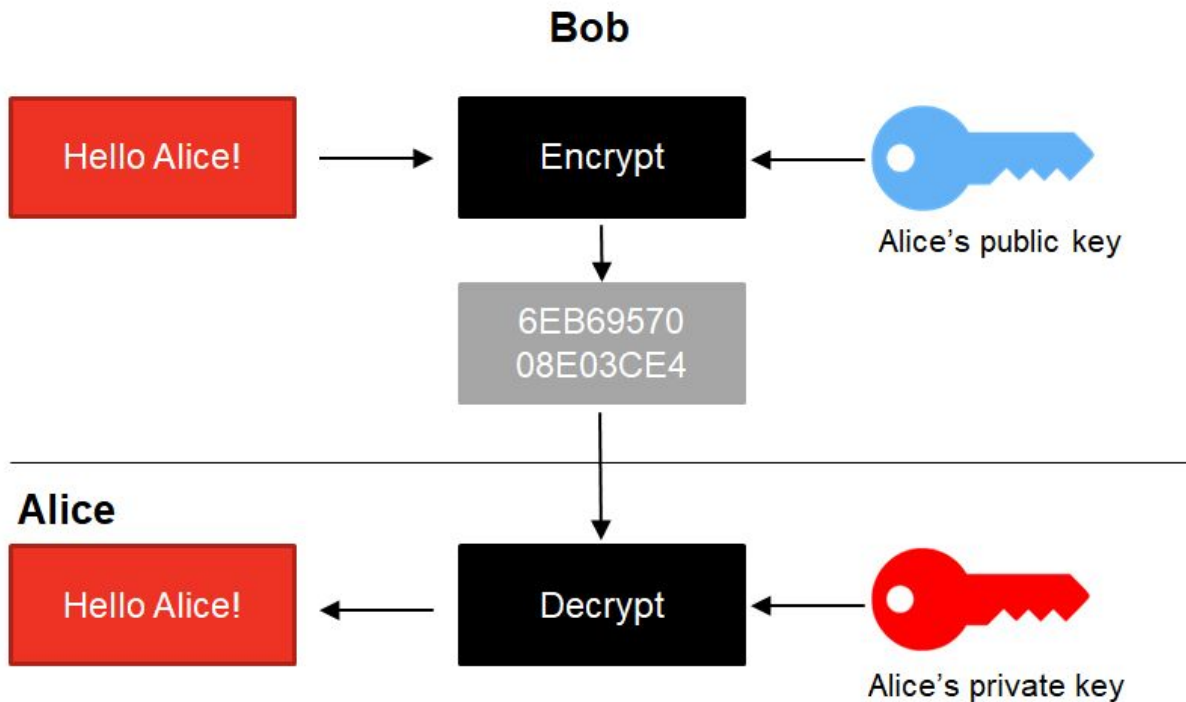
Cryptography is a way to disguise and reveal—more commonly known as encrypting and decrypting data or content of messages. It is constructing and using rules that prevent external parties or the public from reading encrypted messages for information security. In cryptography, data or a piece of information is converted in to a useless or nonsensical piece of text based upon mathematical rules. This is usually done using what is called a key, commonly referred to as a private key. To decrypt or bring the message back to its original form, either the private key or a public key issued by the private key owner is required. This ensures the security of information.

Cryptography in Blockchain

In blockchain, cryptography is used for the following two purposes:

1. Securing the identity of the sender of transactions
2. Ensuring that past records cannot be tampered with

Blockchain uses a form of cryptography known as public key or asymmetric cryptography. This form uses a combination of a sender's private key and recipient's public key to encrypt the transaction and recipient's private key and sender's public key to decrypt the message. A user can share their public key with anyone without fear of revealing their private key. This ensures the security of information as well as the identity of sender and recipient.



7

Public key cryptography can also produce a digital signature—a combination of a user's identity and the data they wish to secure.


Digital Signature

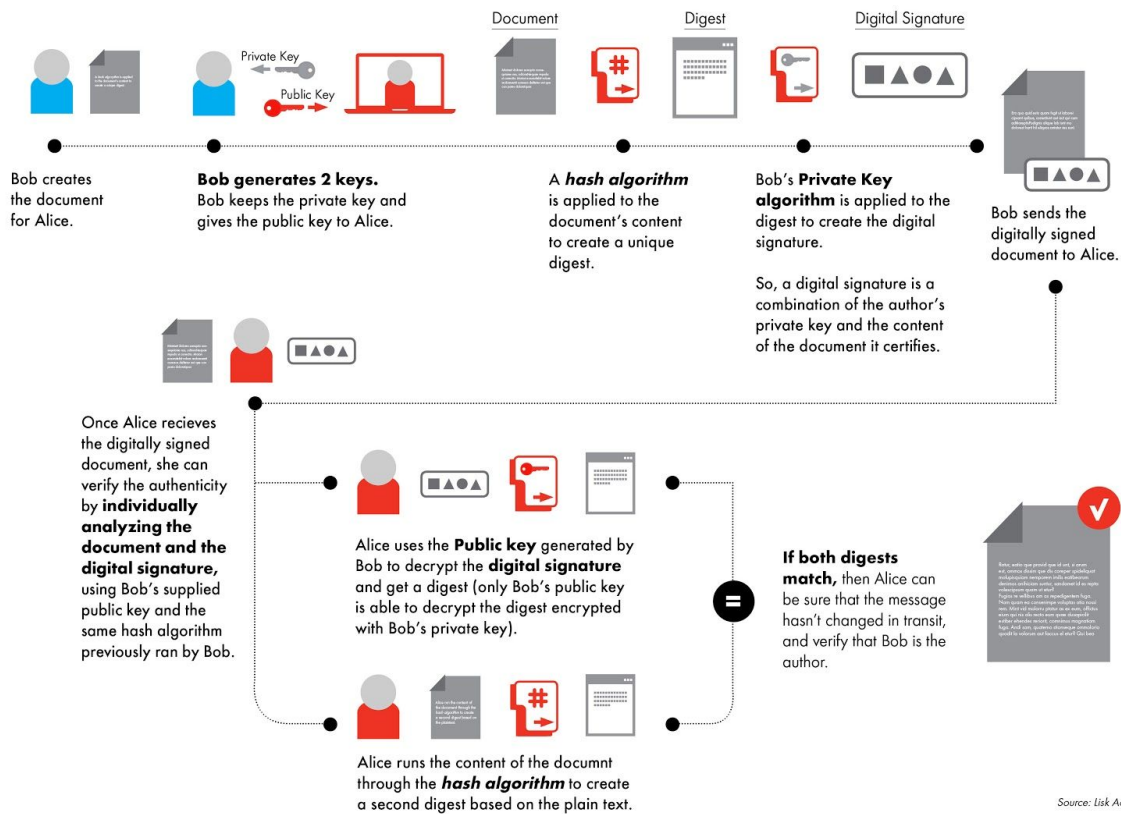
Digital signatures are the key to security and integrity of data recorded on blockchain. Digital signatures guarantee security by encryption and integrity by ensuring that if the data is changed, then the signature will also change. This is what ensures immutability in blockchain. They also ensure authenticity as they can only be bound to one user. Digital signatures are unique to a signer and based on three algorithms:

- Private and public key owned by the user
- A signing algorithm that combines the private key and data being signed

- An algorithm that verifies and determines whether the message is authentic or not based on message or data, the public key, and the signature.

HOW A DIGITAL SIGNATURE IS CREATED?

 The Digital Signature **doesn't encrypt the message**.
In the following example, Bob is sending a non-encrypted document to Alice.



What if I lose my private key?

In public key cryptography, think of public key as the username visible to everyone and private key as the password. If you lose private key there is no reset password option. If you lose your private key, you lose everything and all capabilities controlled by that

private key. If someone steals the private key, they get access to control everything controlled by that private key.

It is very important to keep your private key safe and managed in a way that cannot be destroyed or hacked. It is done through hardware wallets or paper copies locked in a safe place.

Multisig

Usually the blockchains work on single signature, i.e. a user creates a private key to control all their transactions.

But most blockchains, including Bitcoin, allow multiple network participants to control transactions together. This makes the system safer and helps recovery from a disaster or accidental loss of private key.

This is called a multi-signature system or 'multisig'. In this, a predetermined set of participants agree to sign all their signatures. It is usually a set of potential signees and minimum required signatures for a valid transaction. It's like a board of directors of three maintaining funds for an organization. Unless at least two directors sign, the funds cannot be spent. Or a husband & wife bank account where both signatures are required.

Wallet

A wallet is a secure way to store the private and public key. Through the private key, the wallet allows you to perform routine transactions like sending and receiving coins or checking the overall balance. It is like an account number to which all the blockchain activity of participants is attached.

Wallets can be as simple as a private key written on a piece of paper or they can be sophisticated storage gadgets that store private keys and connect to the internet when the user wants to perform a transaction.

Software applications are available to install on your computer or in the cloud, and mobile apps are available as wallets.

Hashing

Hashing is a technology at the center of maintaining the reliability of data in blockchains. It is a method which takes any input and converts it to a fixed length encrypted output. Any changes in the input completely changes the output. Hashing increases the security and integrity of data many times over. It is done using hash functions with the following characteristics:

- Impossible to produce the same value for different inputs
- Same input always produces the same output
- Quick to produce a hash for any given input
- Impossible to determine input based on hash value
- Slightest change to input completely alters the hash

Hashing provides certainty that the data has not been tampered with. You could run a file received through a hashing algorithm, calculate the hash of that data, and compare it to the one shown by whoever sent you the data. If the hashes don't match, you can be certain that the file was altered before you received it.

In blockchain, hashing is used to represent the current state of the blockchain. Any new input or transaction creates a new hash or new state of the world but includes the previous state. Changing any previous record would require all hashes to be changed, making it near impossible to alter or tamper with any records as the data is shared by all

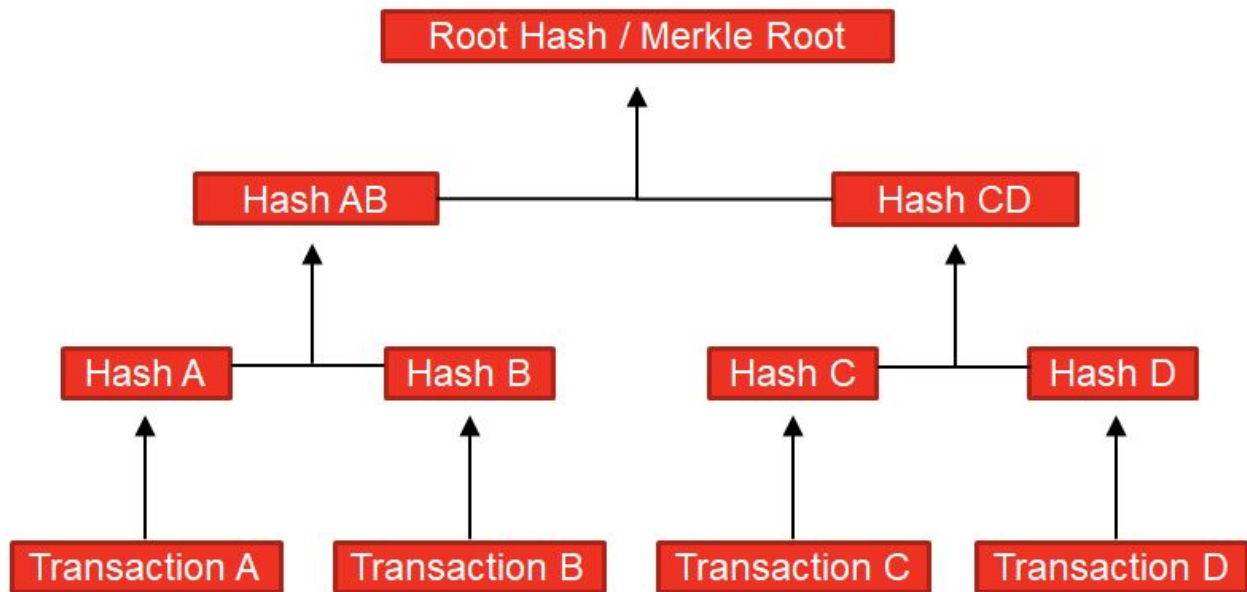
participants and changes will be visible to everyone and not pass the consensus verification.

Blockchain Data Structure/ Merkle Tree

Blockchain data structure is a linked list of transactions connected back to one another by hashed links. Actually, it is a sequence of blocks (or hashes of blocks) and each block contains many transactions, or hashes of transactions.

Blockchains use Merkle Tree—a method that uses hashes of all transactions, then the hash of the whole set of transactions, or the block itself until, only one transaction is left. The last transaction is called the Merkle root. This provides the following key features:

- Ability to verify whether a transaction is included in a block
- Light-clients (since we don't have to download the entire chain)
- Overall performance and scalability
- Simplified Payment Verification (or SPV) verifying transactions in a block without downloading the entire block



In the above, the root hash can provide information for transactions A, B, C, and D. If any of the transaction changes, or another transaction is added, then the root hash will also change.

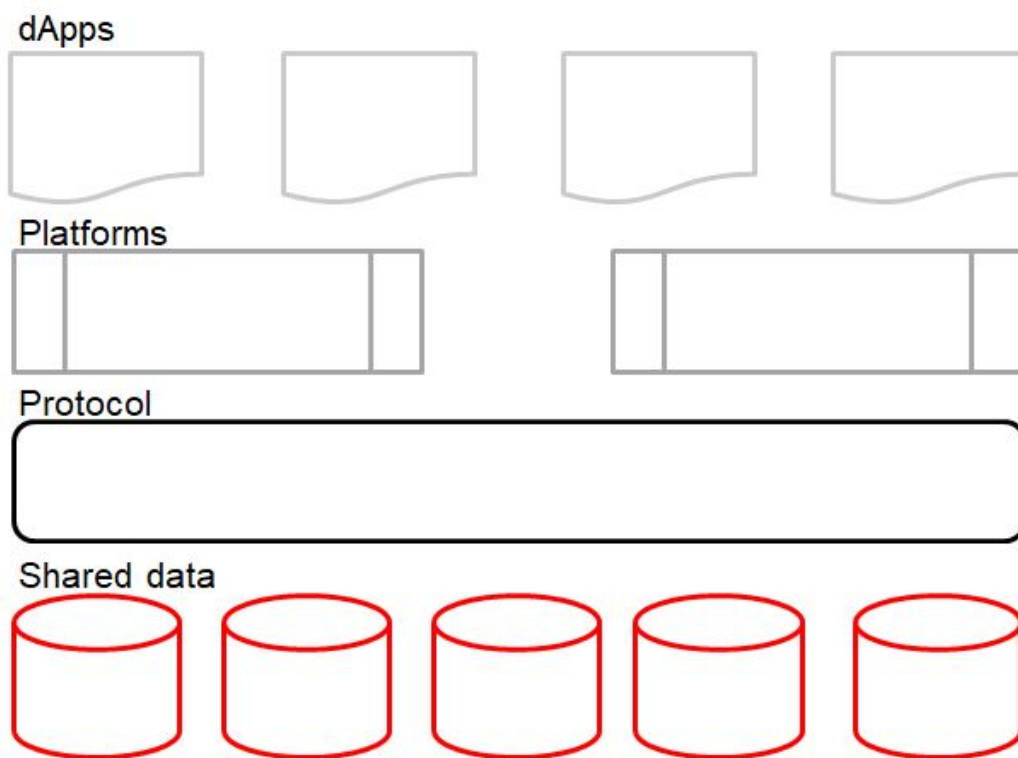
Together, cryptography, digital signatures, and hashing provide blockchain with immutability, security, and reliability while Merkle Tree adds efficiency, performance, and scalability.

Blockchain Technology Stack

How does it all work together? How do the different technology components stack together to make a complete usable application?

The Blockchain technology stack can be viewed as four layers of components:

- Shared Data
- Protocol
- Platforms
- Products / dApps / Smart Contracts



Shared Data

This is the decentralized database that stores all the transactions in hashed format. Refer to the “Distributed Ledger Technologies” section for more details.

Protocols

Examples of existing protocol infrastructure on the web today include TCP/IP, SMTP, HTTP, and HTTPS. Protocols are essentially the infrastructure that everyone who is part of the blockchain ecosystem must adhere to. Blockchain protocols implement rules for consensus, validation, incentive, and participation. Bitcoin and Ethereum are examples of protocols. Bitcoin, being the first and largest example, has protocols in place to prevent a "double-spend" attack, allow for peer-to-peer payments, and ensure a strong and verified settlement layer. Other types of protocols incorporate other aspects to allow for more features and address different problem sets.

Platforms

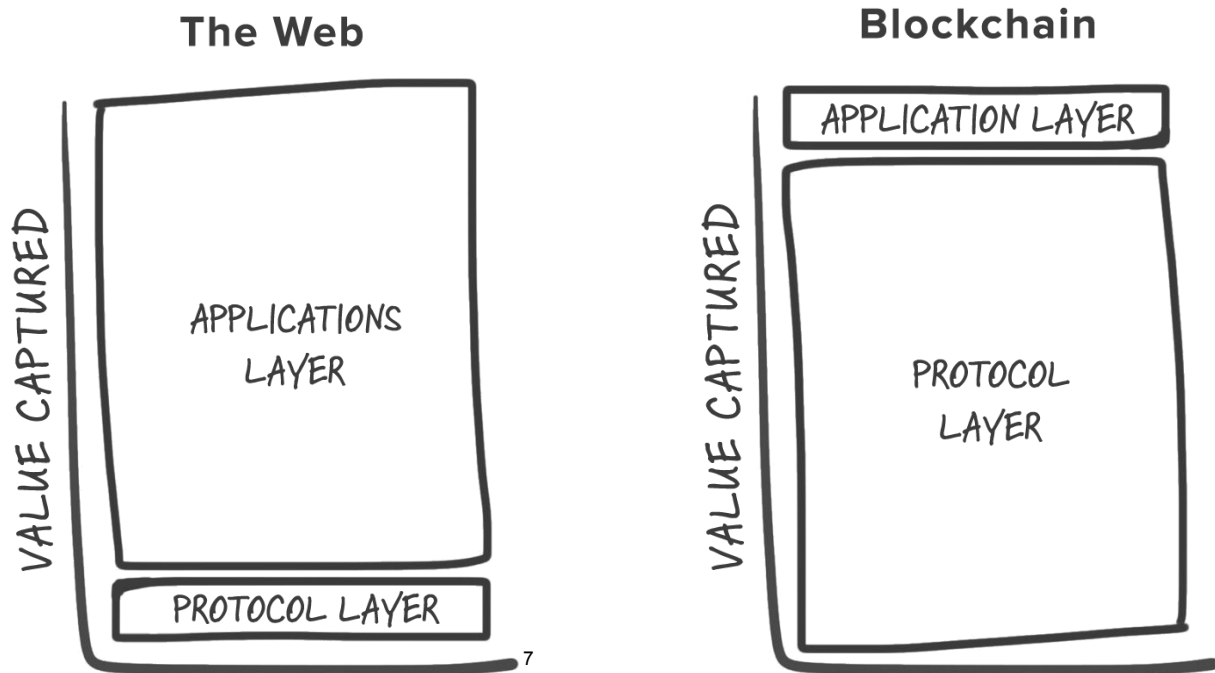
Platforms are a kind of middleware. They allow developers to build applications on top of protocols. Blockchain platforms (Blockchain 2.0) take the concepts introduced by Bitcoin’s blockchain protocol and try to expand it to become universal and “turing complete.” Platforms seek to act as a “universal computer” that allow the development of applications on top of their protocol layer. Examples of known blockchain platforms include Ethereum, NEO, and EOS. Each utilize the technology pioneered by Bitcoin and aim to expand on the protocol by incorporating "smart contracts." This new advancement in the blockchain protocol allows for the use of universal functions to be built on the blockchain infrastructure.

Products

Products are the interface to the protocols and platforms. They allow users to interact with the protocol and shared data. Developers use platforms to build products. Examples of products are dApps (Decentralized Applications). These "dApps" utilize blockchain technology alongside platform capabilities like "smart contracts" to provide not only the security of the blockchain, but also the ability to self execute operations. "dApps" are the thin application layer built on top of a blockchain protocol layer and allow for trustless, peer-to-peer, decentralized applications.

Fat Protocols

Examples of existing protocol infrastructure on the web today include TCP/IP, SMTP, HTTP, and HTTPS. They exist as the fundamental building blocks of today's internet, but that being said, are relatively "thin" protocol layers. While they do provide guidance and structure for utilization of the internet, they are not robust enough to handle a majority of the actions that today's online environment requires. As a result of this "thin" layer, a "fat" layer of application has been built to create viable ecosystems and infrastructure by which all participants adhere. A majority of the value is therefore captured in this "fat" layer of applications whereby the applications can collect and utilize the data as they see fit.

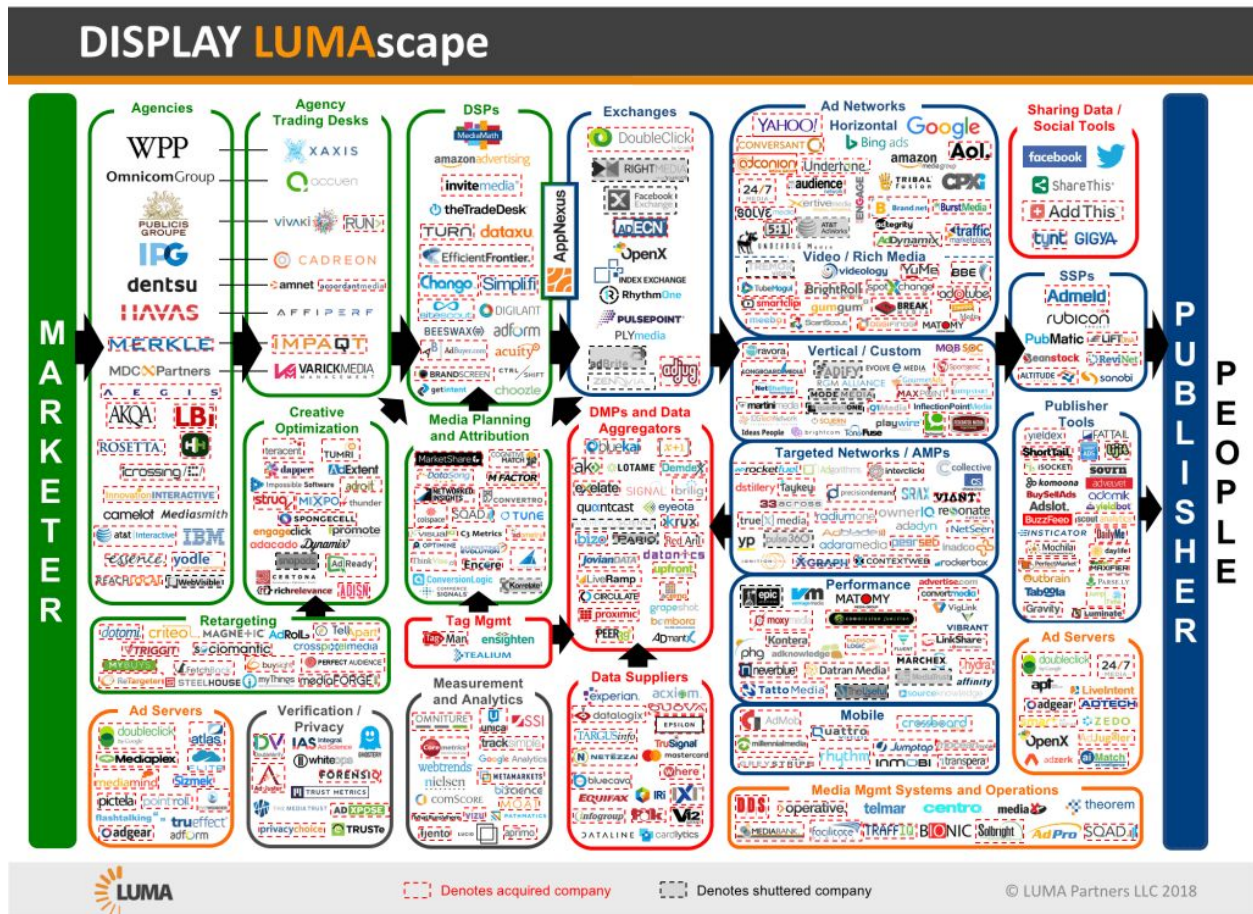


Blockchains flip this distribution between the application layer and the protocol layer. Blockchains allow for the creation of "fat" protocol layers with very specific functions and guidelines in place. This new protocol layer can handle governance, communication, and settlements that were previously reserved for the application layer. Conversely, by building robust protocol layers, applications can be very "thin" and can benefit from a trustless, decentralized, network without being dependent on centralized entities.

⁷ <https://www.usv.com/blog/fat-protocols>

Advertising Use cases

The digital advertising supply chain involves multiple parties—advertiser, agency, trading desk, DSP, data management platform, exchange, SSP, ad network, measurement provider, and publisher—in just one transaction. The LUMAScape⁸ below depicts this complexity.

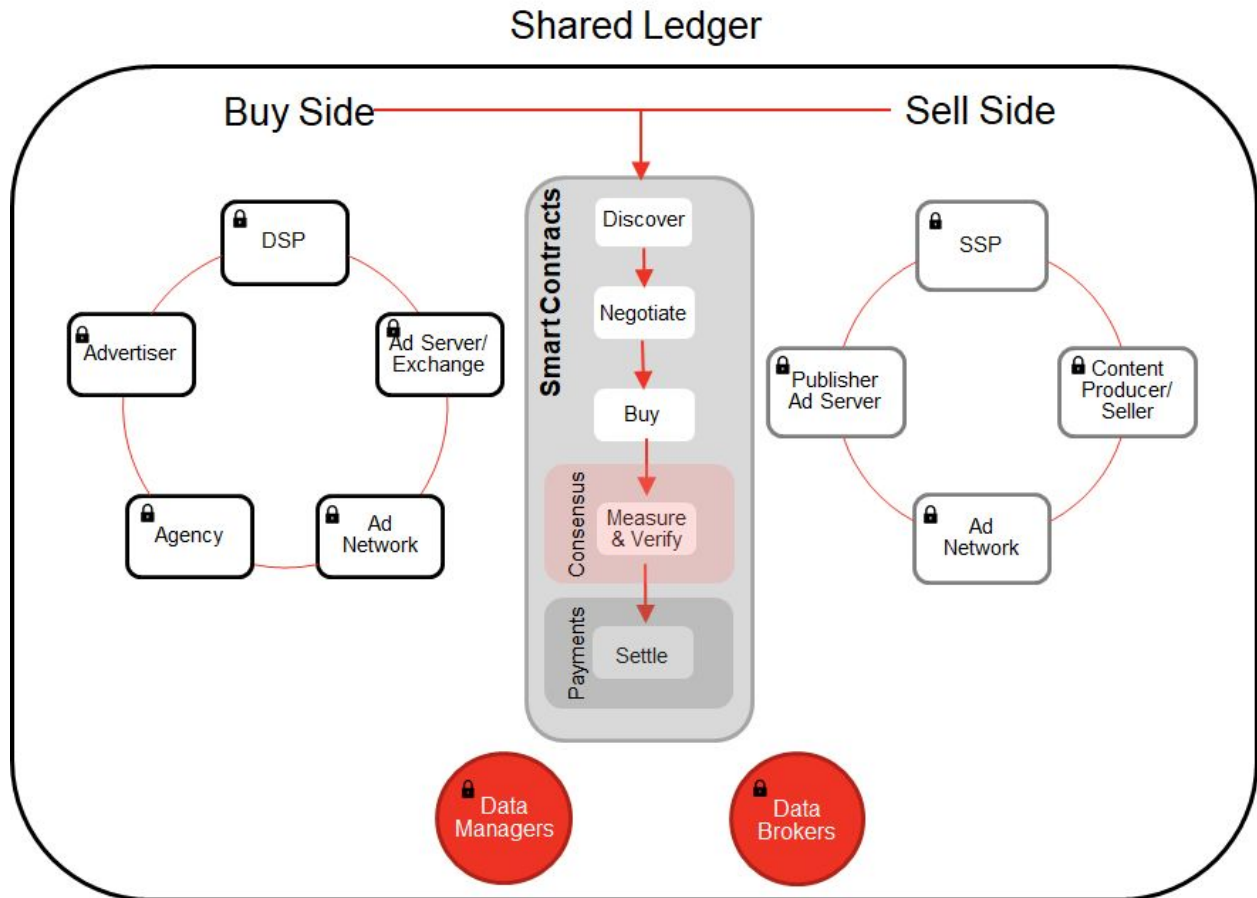


To discover, match, negotiate, measure, and perform settlements requires sharing of data across multiple partners in a transaction. Given the key features of blockchain technology:

- Shared database

⁸ <https://www.lumapartners.com/luma-institute/lumascape/display-ad-tech-lumascape/>

- Protocol governance
- Smart contracts
- Immutability
- Cryptography and digital signatures



It can be an enabling technology that can help enforce the rules and agreements required to complete the transaction, as well as usher in a new era of redefining the currency of transaction for digital advertising.

Blockchain technology is in the early stages of evolution and several industries are in initial development and adoption cycles. There are some areas where more work is

needed, e.g. speed of transaction is limited on blockchain, though work is being done to overcome these challenges with advanced concepts like off-chain or side-chain processing.

Some immediate areas where IAB Tech Lab Blockchain Working Group envisions application of blockchain technology are:

Fraud Prevention

Strong cryptography-based authentication and immutability of data can ensure verification of entities participating in a network or transactions and consensus-driven public records can be maintained by sellers and buyers.

Identity, Data and Privacy

Given the new regulations around privacy and the need for consumer identity and data to be shared among multiple parties, shared ledger with cryptographic permissions can enable elegant solutions for propagating consumer consent and secured identity, as well as PII (Personally Identifiable Information).

Measurement

With multiple parties involved in a typical ad impression, it requires validation and reconciliation between all the business partners and can be a very time-consuming, inefficient, and ineffective process. Shared databases and smart contracts, together with protocol enforced consensus, can provide a much more efficient reconciliation of ad impression measurement among business partners.

Transparency

Clever uses of cryptography, shared data, and consensus can help build a transparent system for negotiating and matching the entities participating in a transaction.

Settlement

The first blockchain network, Bitcoin, was built for payments so blockchain can definitely help deliver a payment system that can disburse payments to all partners involved in a transaction with accuracy, precision, and speed.

Appendix 1: A brief history of Blockchain

Satoshi Nakamoto is almost ubiquitously acknowledged as one of the founding figures of bitcoin, and therefore, of blockchain. Yet many experts, such as Jim Robinson, assert that the history of blockchain stretches back further than Nakamoto's 2008 White Paper that first delved into the details of the bitcoin protocol.

The origins of cryptocurrency

Internet technology connects individuals to one another directly, opening a vast range of possibilities. By dissolving pre-existing physical and political boundaries, the entire planet gained access to the same information for the first time in history. This level of access is guaranteed by the internet's decentralized design. In the absence of a centralized hub, there is no single point of failure or control.

Digital currencies

Satoshi Nakamoto wrote the 2008 White Paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*.

First key idea: Peer-to-peer electronic cash mechanisms do not need an intermediary bank to transfer payments between peers. Bitcoin is built on decades of cryptographic research, including that conducted on Merkle Trees, hash functions, public-key cryptography, and digital signatures.

David Chaum: Blind signatures and e-cash (1982)

Early proposals to create digital cash date as far back as the early 1980s. In 1982, David Chaum proposed a scheme that used blind signatures to build untraceable digital currency. In this scheme, a bank would issue digital money by signing a blind and random serial number presented to it by the user. The user could then use the digital token signed by the bank as currency. The limitation to this scheme was that the bank

had to keep track of all the serial numbers used for this purpose. This was a central system by design and required the trust of the users.

Adam Back: Hashcash (1997)

Hashcash, introduced in 1997, was originally proposed to thwart unwanted, unsolicited, or spam email. The idea behind hashcash was to solve a computational puzzle that was easy to verify, but comparatively difficult to compute.

Wei Dai: B-money (1998)

The concept and idea of using Proof of Work to create money.. A major weakness in the b-money system was that an adversary with higher computational power could generate unsolicited money without allowing the network to adjust to an appropriate difficulty level. This system lacked details on the consensus mechanism between nodes and some security issues, such as Sybil attacks, were also not addressed.

Nick Szabo: Bit gold (1998)

Despite being based on the Proof of Work mechanism, Bit gold had the same problems as b-money (with the exception that the network difficulty level was adjustable). Tomas Sander and Ammon TaShama introduced an e-cash scheme in 1999 that, for the first time, used Merkle Trees to represent coins and zero-knowledge proofs to prove the possession of coins. In the e-cash scheme, a central bank was required to keep a record of all used serial numbers. This scheme allowed users to be fully anonymous, albeit at a computational cost

Hal Finney: RPoW (2004)

RPoW (Reusable Proof of Work) was introduced by Hal Finney in 2004 and used the hashcash scheme by Adam Back as a proof of computational resources spent to create the money. This was also a central system that kept a central database to keep track of all used Proof of Work tokens. Additionally, this was an online system that used remote

attestation, made possible by a trusted computing platform (also referred to as Trusted Platform Module, or TPM, hardware).

Bitcoin (2008)

Satoshi Nakamoto leveraged current network technology to implement a P2P system for exchanging virtual cash. All the peers on the network operate as equal actors participating through the same protocol. The monetary policy of Bitcoin is defined and self-regulated by its open network of computers. Thus, through bitcoin, the world witnessed the emergence of a new phase of money.

Appendix 2: Lexicon

Smart contract: Computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger.

Smart legal contract: A smart contract that articulates and is capable of self-executing, on a legally-enforceable basis, the terms of an agreement between two or more parties.

Distributed ledger: Computer software that employs a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed digital record of transactions or data. Distributed ledgers maintain the security and accuracy of transactions by deploying cryptographic keys and signatures to control access and permissions in the shared ledger. Access control rules are usually agreed on and enforced by the network (Crown, 2016:5).

Blocks: Blockchain, transactions are bundled together into blocks Each block is linked by cross-referencing a cryptographic hash of the previous block in the header and thus providing traceability back to the first or genesis block. The cryptographic linkage between blocks results in the “tamper-proof” (or append-only) property of the ledger, because if a malicious actor tries to add, remove, or change a transaction in any one block, this will affect all the blocks that follow. In a bitcoin blockchain, a block typically contains 500 transactions and Merkle trees are used to link them together to improve efficiency.

Blockchain: A blockchain is a special type of distributed ledger that underpins bitcoin or any other protocol layer (Ethereum, Eos, etc). A blockchain's key characteristic is that it employs a data structure where transactions are organized and bundled into a block. Every block is bound or linked ("chained") together with a previous block using a cryptographic hash function (Crown, 2016:17).

Consensus: Blockchains are decentralized or based on a P2P network, the fact that there is no central authority means that reaching consensus on the state of the ledger (the order and uniqueness of transactions) is a crucial matter

Hash functions: Technique where data sets of varying length and size are converted into fixed lengths. This is necessary for verification purposes to compare different data inputs. Cryptographic hash functions are useful when determining if two objects are equal.

Merkle trees: Special data structures that guarantee the integrity of the ledger This final hash at the top is the Merkle root and it provides proof of validity for all the transactions added to the tree

Mining: Mining can be defined as the process in which a node finds a valid block by solving a computational puzzle called proof-of-work. Proof-of-work is often misunderstood as proof that something works; rather, it indicates proof that the miner did the work on the blockchain.

Public blockchain: A blockchain that allows anyone with the appropriate computing capability to submit messages for processing, be involved in the process of reaching consensus, or otherwise participate in the network. The Bitcoin blockchain is an example of a public blockchain.

Private blockchain: A blockchain whose participants are pre-selected or subject to gated entry based on satisfaction of certain requirements or on approval by an administrator.

Blockchain-based asset: An asset that consists solely of a token on a blockchain.

Tokenized asset: An asset that consists of intangible or tangible property apart from a blockchain, such as real or chattel property or a legal interest in some asset, but which is represented by a token on a blockchain.

Virtual currency: A medium of exchange and that operates like a currency in some environments, but that does not have all the attributes of fiat currency, in particular that it does not have legal tender status in any jurisdiction.

Virtual currency wallet: A means (software application or other mechanism/medium) for holding, storing, and transferring a virtual currency.

Public/private key signature: A method of ensuring data integrity and origin authenticity that uses a party's private key to sign and its corresponding public key to verify the validity of its signature