

Key Terminology:

The Goal:

1. DESIGN THE TEMPLATE: The Main Key Term Page Should be a framework (template) for the rest of the definitions so that when you choose a word from the list it propagates seamlessly into the wiki page template. All definitions should follow this template. The template should have a section for general definitions and a section for a deeper dive. A footer section can house reference information.
2. DEFINE TERMS -Search and combine definitions. All the terms in the outline need to be examined and completed.

Contributors		
Name	Email	Definitions

[New York Times](#), [New York Magazine](#)

Bitcoin

Created in 2009 by the pseudonymous Satoshi Nakamoto, Bitcoin is the world's largest cryptocurrency by market capitalization, though it's gone through several cycles of booms and busts since its inception.

Blockchain

A blockchain is a distributed database shared across a large number of computers comprising a computer network. Information is stored and verified on these shared databases in a cryptographically secure way, by keeping data in groups known as blocks that are connected by chains of data. This structure chains data together irreversibly in chronological order and in a decentralized manner, leading some to see it as a more secure and open option for information storage and exchange.

Blockchain ETF

Exchange-traded funds invest in a specific bundle of specific stocks. Therefore, a blockchain ETF invests in a specific bundle of exclusively blockchain-based companies.

Block header

A block header is used to identify individual blocks in a blockchain. Each contains three sets of block metadata along with other individual components.

Block height

Block height is the number of confirmed blocks preceding a particular block in the blockchain. It's representative of the blockchain's current size or time in existence.

Consensus mechanism

A consensus mechanism is used in computer and blockchain systems to validate single data or single states of a distributed computer network. It encompasses any methodology that is used to achieve agreement, trust and security across a decentralized computer network. The two most common in the crypto world right now are proof of work and proof of stake.

Cryptocurrency

Cryptocurrencies are a form of digital currency that is secured via cryptography, most typically through decentralized networks on blockchain technology. That means that it's distributed across a large number of computers outside of any central authority control. Cryptocurrency is often lauded for its decentralization, as it makes it impossible to counterfeit or double-spend transactions and has faster and cheaper money transfers. However, it has so far come with extreme price volatility, high energy consumption and use for criminal activities.

Decentralized applications (dApps)

dApps are digital applications that operate on a blockchain network of computers rather than on one computer alone. Examples of dApps are BitTorrent, Tor and more that allow for participants to consume, feed and seed content, or do all at the same time. Their decentralized nature makes them free from the control of a single authority, thereby increasing user privacy and offering flexible development.

Decentralized autonomous organizations (DAOs)

Simply put, a DAO is an organization built with blockchain technology, though they've been described as "crypto co-ops," "financial flash mobs" and "group chats with a bank account." Essentially, it's an organization that forms with a specific end goal, most commonly to make big investments or purchases. Because of the involvement of blockchain technology, members of a DAO use crypto tokens to manage member rights, a common treasury and voting on certain decisions within the group. All of the important decisions from the group will appear on a permanent blockchain ledger shared by all members, making DAOs more democratic than traditional non-crypto organizations.

Decentralized finance (DeFi)

Decentralized finance, or DeFi, is an evolving realm of the crypto world that aims to use blockchain technology to replace traditional intermediaries and trust or permission mechanisms with an internet-native financial system — essentially a crypto Wild West version of Wall Street. It's been valued at around \$77 billion, with trading activity that's [grown by over 550%](#) in the last year. Overall, DeFi is still a very much emerging part of the crypto world, and it remains largely unregulated at this point.

Distributed ledger technology

Another term for blockchain technology, distributed ledger technology describes a method for securely and accurately storing information using cryptography.

EOS

EOS is a blockchain-based platform launched in 2018 that allows for the development of dApps. Specifically, it has capabilities to support authentication, permissioning, data hosting, usage management and communication between dApps built on its platform and the internet. EOS also has its own cryptocurrency, the EOS token. Ethereum is its main competitor.

Ethereum

Known best for its cryptocurrency ETH, Ethereum is a blockchain-based platform that allows for public creation and maintenance of secure digital ledgers. Its cryptocurrency is the second largest in the world by market capitalization, only behind that of Bitcoin. While known for its cryptocurrency, Ethereum is notably different from Bitcoin in its long-term goals of using blockchain technology for a diverse range of applications. Notably, both Bitcoin and Ethereum operate on proof of work protocols, but Ethereum is working to transition to a proof of stake protocol.

Hard fork

A hard fork is an overhaul of a network's protocol that can validate previously invalid blocks and transactions in a blockchain, or vice versa. Notable examples have occurred with Bitcoin to create Bitcoin Cash and Bitcoin SV, for instance. For a hard fork to succeed, all nodes must upgrade and agree on the new version.

Hash

A hash is a function that solves for a blockchain computation by converting an input of arbitrary length into an encrypted output of a fixed length. Hash functions are one-way, making it impossible to reverse-engineer the input from the output. They are considered a backbone of the blockchain network as their fixed length makes it impossible to guess and crack the blockchain.

Hashgraph consensus mechanism

The hashgraph consensus mechanism is based on the use of information about information, called "gossip," and virtual voting to create consensus in verifying new blocks. The crypto community has yet to widely adopt it.

Hyperledger fabric

Launched by Linux in 2015, Hyperledger Fabric is an open-source enterprise-grade private permissioned blockchain. It was designed by IBM for industrial enterprise use and has features for faster transactions, smart contract technology and streamlined data sharing, in particular.

Hyperledger Iroha

Hyperledger Iroha is a platform of business blockchain frameworks intended to support infrastructure projects that require blockchain technology. Notably, its capabilities include the potential to build an identity management system, as well as software apps that can help unbanked people have access to financial services.

Nonce

An abbreviation for "number used only once," a nonce is the first number a blockchain miner needs to find before it can solve for a block in the blockchain. They are notoriously difficult to find and miners are rewarded with cryptocurrency after identifying them. Examples of nonces outside of crypto include two-factor authentication, purchase authentication and other form of account recovery and identification.

Nonfungible tokens (NFTs)

It's easiest to understand this concept by breaking it down in two parts. "Nonfungible" describes something that is not easy to exchange or mix with other similar goods or assets, per the Cambridge Dictionary. Meanwhile, a "token" is a thing serving as a visible or tangible representation of a fact, quality or feeling, according to Oxford Languages. By those definitions, a nonfungible token is a visible or tangible representation of something that cannot be easily exchanged for something similar. And that's actually kind of how NFTs really work.

The key here is: These tokens can't be easily exchanged because they are unique cryptographic assets, on a blockchain with unique identification codes and metadata that can't be replicated. Unlike cryptocurrencies, which are fungible tokens, NFTs can't be traded or exchanged at equivalency. They're most commonly represented by artwork or real estate at present, but they have the potential to represent any real-world asset that would benefit from a more efficient buying, selling and trading process (with a reduced probability of fraud for identities, property rights and more).

Permissioned blockchain

A permissioned blockchain is a blockchain that is not publicly accessible and can only be accessed by users that have permission to do so. This access control offers increased security of blockchain systems like Bitcoin, as users are only able to take actions that blockchain administrators allow and must identify themselves digitally.

Proof of stake

Proof of stake is a decentralized consensus mechanism that requires coin owners to offer their own coins up as collateral (in other words, staking their coins) for a chance to validate blocks in a blockchain. Validators are selected randomly, instead of via the competition mechanism used in proof of work. To have the chance to be a validator, coin owners must stake a certain amount of their coins (i.e. Ethereum's requirement of 32 ETH). Multiple validators must verify the new block before it can be finalized and closed. Proof of stake is known for being far less energy-consuming than proof of work.

Proof of work

Proof of work is a decentralized consensus mechanism that requires all members of a network (i.e. computer nodes in a blockchain) to complete a significant but feasible amount of work to solve an arbitrary mathematical puzzle. It's widely used to validate transactions and mine new tokens in cryptocurrency mining, as it doesn't require the need for a trusted third party. However, despite its benefits, proof of work is notorious for requiring huge amounts of energy.

Rug pull

A rug pull is a scam where software developers raise a huge sum of money in order to fund a crypto project, then take advantage of the nature of DeFi by using the lack of financial gatekeepers or verified third parties to disappear with that money.

Smart contracts

A smart contract involves the use of self-executing lines of code to outline the terms of agreement in the contract, which exists on a decentralized and distributed blockchain network. Smart contracts allow for agreements between two separate and even anonymous parties, without the need for any third party authority or system. Smart contracts are trackable and irreversible.

Soft fork

A soft fork is a change in software protocol for blockchain technology that only makes previously valid transactions invalid. For a soft fork to succeed, only a majority of nodes need to upgrade and agree on the new version.

Stablecoins

Stablecoins are a type of cryptocurrency that is tied to a reserve asset, like the dollar. They're an attempt to create a more stable option, akin to fiat currencies, while also taking advantages of instant processing and privacy offered by cryptocurrency.

Tron

Tron is a blockchain-based digital platform founded in 2017 with the goal of hosting a global entertainment system digital content sharing. As of August 2021, it had over 50 million accounts. Tron also has its own cryptocurrency, Tronix, and was founded by BitTorrent CEO Justin Sun.

Web1

This describes the earliest iteration of the internet. Most internet users were consumers, rather than content creators, and most available websites were static informational pages such as Britannica Online, [mp3.com](#) and personal websites.

Web2

This describes the current state of the internet. The shift from Web1, which first began at the turn of the 21st century, indicated an increase in users creating content and more actively engaging with the internet, as opposed to simply consuming information on it. The move from Web1 to Web2 was not signified by any specific technical advancement, but rather a change in internet usage that demonstrated an increase in user information-sharing and interconnectedness.

Web3

This describes an idea of a future state of the internet. A marked advancement in usage style from Web2, Web3 is "the internet owned by the builders and users, orchestrated with tokens," [according to](#) investor Packy McCormick. At the core of Web3 predictions is the idea of a decentralized and open internet with greater user utility. Though the definition of what this will actually look like is still taking shape, experts agree that Web3 will be marked by decentralization, trustless and permissionless interactions, wider use of artificial intelligence and machine learning and, finally, increased connectivity and ubiquity across applications and devices.


0x Protocol

The 0x protocol allows for peer-to-peer exchanges of assets on Ethereum's blockchain. It was launched in 2017 by 0x Labs and is intended to create the infrastructure for new financial applications using blockchain technology.

Sophie Burkholder is a 2021-2022 corps member for Report for America, an initiative of The Groundtruth Project that pairs young journalists with local newsrooms. This position is supported by the Heinz Endowments.
Series: [Web3 Month 2022-30-SUBSCRIBE TO OUR NEWSLETTERS](#)

- Need Graphic to show level of difficulty

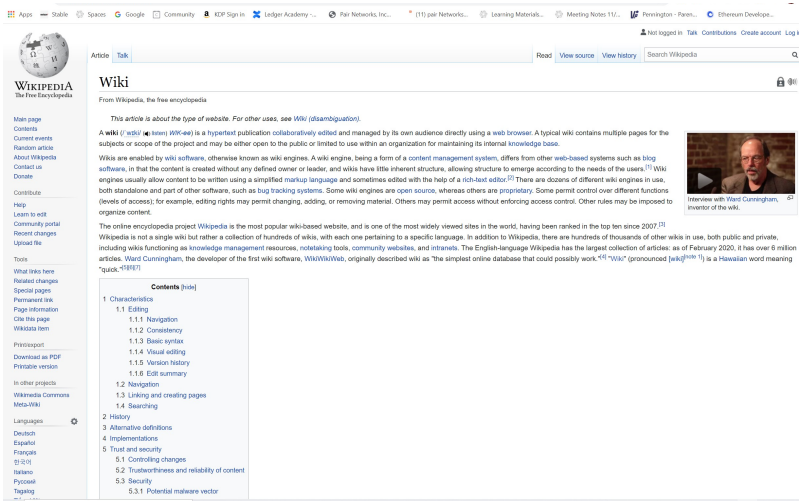
	Definition	Key Concepts	Level	Reference	Sponsor
--	------------	--------------	-------	-----------	---------

Anti Money Laundering (AML)	<p>Anti-money laundering (AML) refers to the laws, regulations and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income. Though anti-money laundering laws cover a limited range of transactions and criminal behavior, their implications are far-reaching. For example, AML regulations require banks and other financial institutions that issue credit or accept customer deposits to follow rules that ensure they are not aiding money-laundering.</p> <p>Anti -laundering (AML) refers to the activities intended to prevent individuals from transferring value obtained illegally into a legitimate sources of income.</p> <ul style="list-style-type: none"> • AML regulations require financial institutions to monitor customers' transactions and report on suspicious financial activity. 	<ul style="list-style-type: none"> • Anti Money Laundering (AML) seeks to deter criminals by making it harder for them to hide ill-gotten money. • Criminals use money laundering to conceal their crimes and the money derived from them. • AML regulations require financial institutions to monitor customers' transactions and report on suspicious financial activity. 		https://www.investopedia.com/terms/a/aml.asp	
Application	An application is software that runs on your computer or cell phone that allows you to perform certain tasks. Me ntion Dapps?				
Blockchain	<p>"A blockchain is a peer-to-peer distributed ledger forged by consensus, combined with a system for "smart contracts" and other assistive technologies". hyperledger.org</p> <p>A blockchain is a chain of blocks each containing transaction (transition) data. Each block, except the first block, is linked with the previous block together forming a chain. Once a block has entered the blockchain, it can not be altered resulting in data immutability .</p> <p>A blockchain is a continuously growing list of records, which are ordered and combined/grouped into blocks. Such blocks are linked (or "chained") using cryptography. The first block in a blockchain is called the genesis block, and each following block is appended after the last block in the chain.</p> <p>Each block typically contains a cryptographic hash of the previous block. Since each new block contains a hash of the previous block, a blockchain is inherently resistant to modification of historical data. In typical blockchain implementations, the records that are grouped into a block are referred to as transactions that take place between parties and are added to the about-to-be-written block after they have been verified.</p> <p>For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.</p>	<ul style="list-style-type: none"> • Money laundering is the illegal process of making "dirty" money appear legitimate instead of ill-gotten. • Criminals use a wide variety of money laundering techniques to make illegally obtained funds appear clean. • Online banking and cryptocurrencies have made it easier for criminals to transfer and withdraw money without detection. • The prevention of money laundering has become an international effort and now includes terrorist funding among its targets. 		https://www.investopedia.com/terms/m/moneylaundering.asp LFS272	

Byzantine Fault Tolerant	<p>Byzantine Fault Tolerant Consensus</p> <p>Byzantine Fault Tolerance (BFT) is defined as the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information.</p> <p>An important consideration to be aware of while setting up a blockchain network is the requirements of Byzantine Fault Tolerant (BFT) consensus, compared with the Crash Fault Tolerant (CFT) one. Due to the underlying complexity of BFT consensus algorithms, a best practice is for the community to leverage the latest academically-proven consensus algorithms based on rigorous and peer-reviewed demonstrations of the safety and liveness properties. Such algorithms include the Tendermint, Algorand, Mir-BFT and HotStuff. There is also some on-going work on Golang-based implementation of the BFT-SMART algorithm for Hyperledger Fabric. These are important reference points for blockchain architects and developers interested in adopting BFT consensus in the future. At Oracle, we are actively exploring the available options to ensure they meet the rigorous proof requirements as well as deliver operational characteristics, including performance and resilience required in enterprise applications.</p>				
Certificates of Authority	<p>Certificate Authority</p> <p>In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. Wikipedia</p> <p>The Certificate Authority (CA) provides a number of certificate services to users of a blockchain. More specifically, these services relate to user enrollment, transactions invoked on the blockchain, and TLS-secured connections between users or components of the blockchain. This guide builds on either the fabric developer's setup or the prerequisites articulated in the fabric network setup guide.</p>				
Chain	A block contains an ordered set of transactions. It is cryptographically linked to the preceding block, and in turn it is linked to be subsequent blocks. The first block in such a chain of blocks is called the genesis block . Blocks are created by the ordering service, and then validated and committed by peers.				
Chaincode	<p>Chaincode - Smart contracts in Hyperledger Fabric. A smart contract defines the executable logic that generates new facts that are added to the ledger. A chaincode is typically used by administrators to group related smart contracts for deployment, but can also be used for low level system programming of Fabric,.</p> <p>that manages access and modifications to a set of key-value pairs in the World State via Transaction. In Hyperledger Fabric, smart contracts are packaged as chaincode. Chaincode is installed on peers and then defined and used on one or more channels.</p> <p>A chaincode definition is used by organizations to agree on the parameters of a chaincode before it can be used on a channel. Each channel member that wants to use the chaincode to endorse transactions or query the ledger needs to approve a chaincode definition for their organization. Once enough channel members have approved a chaincode definition to meet the Lifecycle Endorsement policy (which is set to a majority of organizations in the channel by default), the chaincode definition can be committed to the channel. After the definition is committed, the first invoke of the chaincode (or, if requested, the execution of the Init function) will start the chaincode on the channel.</p>				
Consensus	<p>A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.</p> <ul style="list-style-type: none"> Coming to an agreement: The mechanism gathers all the agreements from the group as much as it can. Collaboration: Every one of the group aims toward a better agreement that results in the groups' interests as a whole. Co-operation: Every individual will work as a team and put their own interests aside. 				
ERC20 Standards Tokens	<p>ERC20 Standards Token is the Ethereum token system, which is used for Ethereum smart contracts platform. Developed in 2015, ERC-20 defines a common list of rules to function within the Ethereum ecosystem.</p> <p>The Ethereum community created these standards with six mandatory and three optional rules.</p> <p>Mandatory</p> <ul style="list-style-type: none"> totalSupply balanceOf transfer transferFrom approve allowance <p>Optional</p> <ul style="list-style-type: none"> Token Name Symbol Decimal (up to 18) <p>Other ERC Token standards for Ref.</p> <ol style="list-style-type: none"> ERC-20 Token Standard. https://eips.ethereum.org/EIPS/eip-20 ERC-165 Standard Interface Detection. https://eips.ethereum.org/EIPS/eip-165 ERC-173 Owned Standard. https://eips.ethereum.org/EIPS/eip-173 ERC-223 Token Standard. https://github.com/ethereum/EIPS/issues/223 ERC-677 transferAndCall Token Standard. https://github.com/ethereum/EIPS/issues/677 ERC-721 Non-Fungible Token Standard https://eips.ethereum.org/EIPS/eip-721 ERC-827 Token Standard. https://eips.ethereum.org/EIPS/eip-827 ERC-1155 Multi-Token Standard https://eips.ethereum.org/EIPS/eip-1155 				
Digital Government	<p>Digital government is the state-of-art concept from public administration science, a successor of e-government paradigm. The former model simply indicated the digitalisation of the public administration.</p> <p>Digital government refers to the creation of new public services and service delivery models that leverage digital technologies and governmental and citizen information assets. The new paradigm focuses on the provision of user-centric, agile and innovative public services. Blockchain absolutely is the one of the most innovative digital technologies that has to be considered under the new paradigm of governmental policy making and service delivery.</p>			Ref: Blockchain for Digital Governments (europa.eu)	

Digital Identity	<p>A decentralized identifier (DID) is a pseudo-anonymous identifier for a person, company, object, etc. Each DID is secured by a private key. Only the private key owner can prove that they own or control their identity. One person can have many DIDs, which limits the extent to which they can be tracked across the multiple activities in their life. For example, a person could have one DID associated with a gaming platform, and another, entirely separate DID associated with their credit reporting platform.</p> <p>In one example, users sign up to a self-sovereign identity and data platform to create and register a DID. During this process, the user creates a pair of private and public keys. Public keys associated to a DID can be stored on-chain in case keys are compromised or are rotated for security reasons. Additional data associated with a DID such as attestations can be anchored on-chain, but the full data itself should not be stored on-chain to maintain scalability and compliance with privacy regulations.</p> <p>A decentralized identifier (DID) is a pseudo-anonymous identifier for a person, company, object, etc. Each DID is secured by a private key. Only the private key owner can prove that they own or control their identity. One person can have many DIDs, which limits the extent to which they can be tracked across the multiple activities in their life. For example, a person could have one DID associated with a gaming platform, and another, entirely separate DID associated with their credit reporting platform.</p>			Blockchain for Digital Identity: Real World Use Cases ConsenSys	
Ethereum	Ethereum 2.0 (Eth2) is the next phase in the evolution and improvement of the public Ethereum network. With a shift from a Proof of Work to Proof of Stake consensus algorithm, Ethereum 2.0 will result in improved scalability, security, and usability for the network.				
Genesis Block	<p>The Genesis Block is the first block or block zero in any blockchain-based system, It is the prototype of all other blocks in the blockchain network. Based on this which additional blocks are added to form a chain of blocks, hence we call them blockchain. In theory, there is no real need for a Genesis Block. However, it is necessary to have a starting point that everyone can trust.</p> <p>The hash of genesis block is added to all new transactions in a new block. This combination is used to create its unique hash. This process is repeated until all the new blocks are added to a blockchain. Without Genesis Block, it would be really difficult for the participant to trust a blockchain and to know how and when it started.</p> <p>Note : Every block in a blockchain stores a reference to the previous block. In the case of Genesis Block, there is no previous block for reference.</p> <p>Technically it means that the Genesis Block has it's "previous hash" value set to 0. Which means that no data was processed before the Genesis Block. All other blocks will have sequential numbers starting by 1, and will have a "previous hash" set to the hash of the previous block.</p>				
Ledger	A ledger holds facts about the current and historical state of a set of business objects.				
Proof of Stake	Proof of Stake (PoS) is a class of consensus algorithm that selects and rewards validators as a function of a validator's economic stake in the network. Unlike PoW , the probability of creating a block in a PoS network is not a result of hash power from burning energy, but rather the result of economic value-at-loss. Proof of Stake will be the consensus mechanism that Ethereum 2.0 uses to maintain the network. Unlike Proof of Work networks, Proof of Stake networks can achieve finality . (consensys)				
Proof of Work	Proof of Work (PoW) is a class of consensus algorithm that rewards miners who expend computational energy to solve mathematical problems to propose new blocks. With PoW, the probability of mining a block and thus receiving block rewards is a function of how much computational energy (known as hash power) a miner expends. Popular blockchains such as Bitcoin, Ethereum (1.0), and Litecoin are all Proof of Work blockchains. (consensys)				
Stablecoin	<p>What is Stablecoins and how many and how they work?</p> <p>The way Stablecoins achieves by collateralizing other real-world assets and pairing the value to them. As such, the value of stablecoins should never exceed the collateral in reserve, and therefore can (in most cases) be exchanged to the assets they're pegged to at any time.</p> <p>It's important to know that staple coins or non-mined ones and non pre-mined. Instead, their total supply is always changing and reacting to the movements in the market. In order to control inflation, coins are burned when exchanged to the pegged asset. Likewise, when an asset is collateralized, newly created stablecoins enter the market.</p> <p>Several different types of stablecoins currently exist. Even though the underlying principle is the same, the main difference is how a particular stablecoin maintains its value.</p> <ol style="list-style-type: none"> 1, FIAT- backed Stable Coins , ex : USD \$\$ 2, Commodity backed Stable coins , ex : GOLD 3, Cryptocurrency-backed stable coins, ex: bitcoin/ethereum 4, Seigniorage/Algo backed Stable coins , ex , : no proven example. <p>Ref : https://blog.knowledgesociety.tech/what-is-stablecoins-and-how-do-they-work/</p>				
Verifiable Credential	<p>A Credential is a set of one or more claims made by an issuer. A Verifiable Credential is a tamper-evident Credential that has authorship that can be W3C Verifiable Claims Working Group cryptographically verified.</p>				

NEED GRAPHICS TO REPRESENT USER LEVEL.....



Concepts vs. interpretations vs natural lang.

Term	Definition	Status	Owner
AML	Anti -laundering (AML) refers to the activities intended to prevent individuals from transferring value obtained illegally into a legitimate sources of income. <div><ul style="list-style-type: none">• AML regulations require financial institutions to monitor customers' transactions and report on suspicious financial activity.</div>	IN PROGRESS	
Application	An application is software that runs on your computer or cell phone that allows you to perform certain tasks. Mention Dapps?	IN PROGRESS	
Blockchain	"A blockchain is a peer-to-peer distributed ledger forged by consensus, combined with a system for "smart contracts" and other assistive technologies". hyperledger.org A blockchain is a chain of blocks each containing transaction (transition) data. Each block, except the first block, is linked with the previous block together forming a chain. Once a block has entered the blockchain, it can not be altered resulting in data immutability .		
Byzantine Fault Tolerant	Byzantine Fault Tolerant Consensus Byzantine Fault Tolerance (BFT) is defined as the feature of a distributed network to reach consensus (agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information.An important consideration to be aware of while setting up a blockchain network is the requirements of Byzantine Fault Tolerant (BFT) consensus, compared with the Crash Fault Tolerant (CFT) one. Due to the underlying complexity of BFT consensus algorithms, a best practice is for the community to leverage the latest academically-proven consensus algorithms based on rigorous and peer-reviewed demonstrations of the safety and liveness properties. Such algorithms include the Tendermint, Algorand, Mir-BFT and HotStuff. There is also some on-going work on Golang-based implementation of the BFT-SMART algorithm for Hyperledger Fabric. These are important reference points for blockchain architects and developers interested in adopting BFT consensus in the future. At Oracle ,we are actively exploring the available options to ensure they meet the rigorous proof requirements as well as deliver operational characteristics, including performance and resilience required in enterprise applications.	IN PROGRESS	
Certificate s of Authority	Certificate Authority In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. Wikipedia The Certificate Authority (CA) provides a number of certificate services to users of a blockchain . More specifically, these services relate to user enrollment, transactions invoked on the blockchain, and TLS -secured connections between users or components of the blockchain. This guide builds on either the fabric developer's setup or the prerequisites articulated in the fabric network setup guide.	IN PROGRESS	
Chain	A block contains an ordered set of transactions. It is cryptographically linked to the preceding block, and in turn it is linked to be subsequent blocks. The first block in such a chain of blocks is called the genesis block . Blocks are created by the ordering service, and then validated and committed by peers.	IN PROGRESS	
Chaincode	Chaincode - Smart contracts in Hyperledger Fabric. A smart contract defines the executable logic that generates new facts that are added to the ledger. A chaincode is typically used by administrators to group related smart contracts for deployment, but can also be used for low level system programming of Fabric.. that manages access and modifications to a set of key-value pairs in the World State via Transaction . In Hyperledger Fabric, smart contracts are packaged as chaincode. Chaincode is installed on peers and then defined and used on one or more channels. A chaincode definition is used by organizations to agree on the parameters of a chaincode before it can be used on a channel. Each channel member that wants to use the chaincode to endorse transactions or <i>query</i> the ledger needs to approve a chaincode definition for their organization. Once enough channel members have approved a chaincode definition to meet the Lifecycle Endorsement policy (which is set to a majority of organizations in the channel by default), the chaincode definition can be committed to the channel. After the definition is committed, the first invoke of the chaincode (or, if requested, the execution of the Init function) will start the chaincode on the channel.	IN PROGRESS	
Consensus	A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block. <div><ul style="list-style-type: none">• Coming to an agreement: The mechanism gathers all the agreements from the group as much as it can.• Collaboration: Every one of the group aims toward a better agreement that results in the groups' interests as a whole.• Co-operation: Every individual will work as a team and put their own interests aside.</div>	IN PROGRESS	

Verifiable Credential A Verifiable Credential is a set of one or more claims made by an issuer. A Verifiable Credential is a tamper-evident Credential that has authorship that can be W3C Verifiable Claims Working Group cryptographically verified.			
<ul style="list-style-type: none"> ERC Token Standards 	<p>ERC20 Standards Token is the Ethereum token system ,which is used for Ethereum smart contracts platform. Developed in 2015, ERC-20 defines a common list of rules to function within the Ethereum ecosystem.</p> <p>The Ethereum community created these standards with six mandatory and three optional rules.</p> <p>Mandatory</p> <ul style="list-style-type: none"> totalSupply balanceOf transfer transferFrom approve allowance <p>Optional</p> <ul style="list-style-type: none"> Token Name Symbol Decimal (up to 18) <p>Other ERC Token standards for Ref.</p> <ol style="list-style-type: none"> ERC-20 Token Standard. https://eips.ethereum.org/EIPS/eip-20 ERC-165 Standard Interface Detection. https://eips.ethereum.org/EIPS/eip-165 ERC-173 Owned Standard. https://eips.ethereum.org/EIPS/eip-173 ERC-223 Token Standard. https://github.com/ethereum/EIPs/issues/223 ERC-677 transferAndCall Token Standard. https://github.com/ethereum/EIPs/issues/677 ERC-721 Non-Fungible Token Standard https://eips.ethereum.org/EIPS/eip-721 ERC-827 Token Standard. https://eips.ethereum.org/EIPS/eip-827 ERC-1155 Multi-Token Standard https://eips.ethereum.org/EIPS/eip-1155 	IN PROGRESS	
Ethereum	Ethereum 2.0 (Eth2) is the next phase in the evolution and improvement of the public Ethereum network. With a shift from a Proof of Work to Proof of Stake consensus algorithm, Ethereum 2.0 will result in improved scalability, security, and usability for the network.	IN PROGRESS	
Genesis Block	<p>The Genesis Block is the <i>first block</i> or <i>block zero</i> in any blockchain-based system. It is the prototype of all other blocks in the blockchain network. Based on this which additional blocks are added to form a chain of blocks, hence we call them blockchain. In theory, there is no real need for a Genesis Block. However, it is necessary to have a starting point that everyone can trust.</p> <p>The hash of genesis block is added to all new transactions in a new block. This combination is used to create its unique hash. This process is repeated until all the new blocks are added to a blockchain. Without Genesis Block, it would be really difficult for the participant to trust a blockchain and to know how and when it started.</p> <p>Note : Every block in a blockchain stores a reference to the previous block. In the case of Genesis Block, there is no previous block for reference.</p> <p>Technically it means that the Genesis Block has it's "previous hash" value set to 0. Which means that no data was processed before the Genesis Block. All other blocks will have sequential numbers starting by 1, and will have a "previous hash" set to the hash of the previous block.</p>	IN PROGRESS	
Ledger	A ledger holds facts about the current and historical state of a set of business objects	IN PROGRESS	
Proof of Stake	Proof of Stake (PoS) is a class of consensus algorithm that selects and rewards validators as a function of a validator's economic stake in the network. Unlike PoW , the probability of creating a block in a PoS network is not a result of hash power from burning energy, but rather the result of economic value-at-loss. Proof of Stake will be the consensus mechanism that Ethereum 2.0 uses to maintain the network. Unlike Proof of Work networks, Proof of Stake networks can achieve finality . (consensus)	IN PROGRESS	
Proof of Work	Proof of Work (PoW) is a class of consensus algorithm that rewards miners who expend computational energy to solve mathematical problems to propose new blocks. With PoW, the probability of mining a block and thus receiving block rewards is a function of how much computational energy (known as hash power) a miner expends. Popular blockchains such as Bitcoin, Ethereum (1.0), and Litecoin are all Proof of Work blockchains. (consensus)	IN PROGRESS	

Stablecoin	<p>What are Stablecoins and how many and how do they work?</p> <p>The way Stablecoins achieves by collateralizing other real-world assets and pairing the value to them. As such, the value of stablecoins should never exceed the collateral in reserve, and therefore can (in most cases) be exchanged to the assets they're pegged to at any time.</p> <p>It's important to know that staple coins or non-mined ones and non pre-mined. Instead, their total supply is always changing and reacting to the movements in the market. In order to control inflation, coins are burned when exchanged to the pegged asset. Likewise, when an asset is collateralized, newly created stablecoins enter the market.</p> <p>Several different types of stablecoins currently exist. Even though the underlying principle is the same, the main difference is how a particular stablecoin maintains its value.</p> <ol style="list-style-type: none"> 1, FIAT- backed Stable Coins , ex : USD \$\$ 2, Commodity backed Stable coins , ex : GOLD 3, Cryptocurrency-backed stable coins, ex: bitcoin/ethereum 4, Seigniorage/Algo backed Stable coins , ex, : no proven example. <p>Ref : https://blog.knowledgesociety.tech/what-is-stablecoins-and-how-do-they-work/</p>	IN PROGRESS	
Cryptocurrencies			
Cryptography	Process for protecting data from theft or modifications. It uses an algorithm and a secure key to allow only the sender and the intended recipient of a message to view its contents.		Félix
Dapp	Short for "decentralized app". Software applications that run on a distributed peer-to-peer decentralized network. Dapps are not controlled by any single authority.		Félix
DeFi	Short for "decentralized finance". Merger of traditional financial services with decentralized technologies, using smart contracts.		Félix
Digital Identity	<p>A digital identity arises organically from the use of personal information on the web and from the shadow data created by the individual's actions online. A digital identity may be a pseudonymous profile linked to the device's IP address, for example, a randomly-generated unique ID. Data points that can help form a digital identity include usernames and passwords, drivers license number, online purchasing history, date of birth, online search activities, medical history, etc. Biometrics, Behavioral, Biographic are the modals that make up a person's identity.</p> <p>In one example, users sign up to a self-sovereign identity and data platform to create and register a DID. During this process, the user creates a pair of private and public keys. Public keys associated to a DID can be stored on-chain in case keys are compromised or are rotated for security reasons. Additional data associated with a DID such as attestations can be anchored on-chain, but the full data itself should not be stored on-chain to maintain scalability and compliance with privacy regulations.</p> <p>A decentralized identifier (DID) is a pseudo-anonymous identifier for a person, company, object, etc. Each DID is secured by a private key. Only the private key owner can prove that they own or control their identity. One person can have many DIDs, which limits the extent to which they can be tracked across the multiple activities in their life. For example, a person could have one DID associated with a gaming platform, and another, entirely separate DID associated with their credit reporting platform.</p> <p>Blockchain for Digital Identity: Real World Use Cases ConsenSys</p>		Phumza
Digital Government	<p>Digital government is the state-of-art concept from public administration science, a successor of e-government paradigm. The former model simply indicated the digitalisation of the public administration.</p> <p>Digital government refers to the creation of new public services and service delivery models that leverage digital technologies and governmental and citizen information assets. The new paradigm focuses on the provision of user-centric , agile and innovative public services. Blockchain absolutely is the one of the most innovative digital technologies that has to be considered under the new paradigm of governmental policy making and service delivery.</p> <p>Ref: Blockchain for Digital Governments (europa.eu)</p>		Phumza
Distributed Ledger			
	<ul style="list-style-type: none"> • D • OA • Fo • rk • Ha • sh • Hy • per • led • ger • Co • m • mu • nit • y • Ter • mi • nol • og • y • /Gl • os • sary • Im • mu • tab • ility • Me • rkl • e • tree • Mi • ning • Mu • lti • Sig 		

- No
de
- No
n
Fu
ngi
ble
To
ken
- Or
acle
- Pe
er
co
m
mit
tin
g/
en
dor
sing
- Pe
rmi
ssi
on
ed
Le
dg
er
- Pri
vat
e
Blo
ck
ch
ain
- Pri
vat
e
Key
- Pr
oof
of
Au
tho
rity
-
-
- Pr
oto
col
- Pu
bli
c
Key
- Pu
bli
c
Blo
ck
ch
ain
- S
ma
rt
Co
ntr
act
- Sc
ala
bili
ty
- Sh
ard
- St
ate
-
- To
ken
- Tr
an
sa
cti
on
Blo
ck
- Tu
rin
g
Co
mp
lete
- Val
ida
tor
- W
all
et
- ZK
P
Ze
ro
Kn
ow
led
ge
Pr
oofs
- 51
%
Att
ack

- Consortium
- Membership Service Provider
- Digital Identity

September 21,2020

Ethereum: Decentralized open-source blockchain that features smart contract functionalities.

Genesis Block: First block of a blockchain. It is sometimes referred to Block Zero (0)

Proof of Stake: Consensus mechanism used to add new blocks to the blockchain. In Proof of Stake, validators lock up some assets as a stake, and then vote on the blocks that they believe will be added next to the chain. When the block gets added, they get a reward proportional to their stake.

Proof of Work: Consensus algorithm used to add new blocks to the blockchain. In Proof of Work, participants (miners) compete against each other, trying to validate transactions by solving complex cryptographic puzzles. Miners who solve the cryptographic puzzle get asset rewards.

Stable Coin: Assets designed to limit their market price fluctuation.

Byzantine Fault Tolerant Consensus

NIST considers standard terms

<https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8301-draft.pdf>

Terminology

A *project* is an active entity that has project member(s) and produces project result(s). Its member(s) use project sites to coordinate and disseminate result(s). A project does not need to be a formal legal entity. Key terms relating to project are:

- Project *members* are the group of one or more people or companies who work together to attempt to produce project results. Some FLOSS projects may have different kinds of members, with different roles, but that's outside our scope.
- Project *results* are what the project members work together to produce as their end goal. Normally this is software, but project results may include other things as well. Criteria that refer to "software produced by the project" are referring to project results.
- Project *sites* are the sites dedicated to supporting the development and dissemination of project results, and include the project website, repository, and download sites where applicable (see [sites_https](#)).
- The project *website*, aka project homepage, is the main page on the world wide web (WWW) that a new user would typically visit to see information about the project; it may be the same as the project's repository site (this is often true on GitHub).
- The project *repository* manages and stores the project results and revision history of the project results. This is also referred to as the project *source repository*, because we only require managing and storing of the editable versions, not of automatically generated results (in many cases generated results are not stored in a repository).

blockchain; cryptoasset; cryptocurrency; data portability; decentralized governance; digital asset;
 106 digital token; distributed ledger; fintech; off-chain scaling; self-hosting; smart contract; state
 107 channel; tokenization; transaction confidentiality; verifiable data; wallet; zero-knowledge proof.

Consensus Layer - Responsible for generating an agreement on the order and confirming the correctness of the set of transactions that constitute a block.

- **Smart Contract Layer** - Responsible for processing transaction requests and determining if transactions are valid by executing business logic.
- **Communication Layer** - Responsible for peer-to-peer message transport between the nodes that participate in a shared ledger instance.
- **Data Store Abstraction** - Allows different data-stores to be used by other modules.
- **Crypto Abstraction** - Allows different crypto algorithms or modules to be swapped out without affecting other modules.
- **Identity Services** - Enables the establishment of a root of trust during setup of a blockchain instance, the enrollment and registration of identities or system entities during network operation, and the management of changes like drops, adds, and revocations. Also, provides authentication and authorization.
- **Policy Services** - Responsible for policy management of various policies specified in the system, such as the endorsement policy, consensus policy, or group management policy. It interfaces and depends on other modules to enforce the various policies.
- **APIs** - Enables clients and applications to interface to blockchains.
- **Interoperation** - Supports the interoperation between different blockchain instances

Keywords

blockchain; cryptoasset; cryptocurrency; data portability; decentralized governance; digital asset; digital token; distributed ledger; fintech; off-chain scaling; self-hosting; smart contract; state channel; tokenization; transaction confidentiality; verifiable data; wallet; zero-knowledge proof.

Acronyms

APIs = application program interface, no apostrophe

BFT = Byzantine Fault-Tolerance or Tolerant

BFTP = Byzantine Fault-Tolerant Protocol

CA = certificate authority

CRL = certificate revocation list

DID = decentralized identity

DLT = distributed ledger technology

DLTs = distributed ledger technologies, no apostrophe

MOU = memo of understanding

NIZK = Non-Interactive Zero Knowledge

PBFT = Practical Byzantine Fault Tolerant

PII = personally identifiable information

PoC = proof of concept, plural PoCs = proofs of concept, not proof of concepts

PoET = proof of elapsed time

PoS = proof of stake

PoW = proof of work

RBAC = role-based access control

RPS = reads per second

TPS = transactions per second

SDKs = software development kits, no apostrophe unless possessive = SDKs' version number

SNARK = Succinct Non-Interactive Argument of Knowledge

UXTO = unspent transaction output

ZK = zero knowledge

August 24, 2020

TERMS	Under Review	Working	Approved
AML	X		
Application		X	
Block		X	
Chain		X	
Chaincode		X	
ERC Token Standard	X		
Genesis Block	X		
Stablecoin		X	
BFT consensus		X	

- **Business process flows:** These are the commons steps in a business process, or supply chain process. In the [solar project finance example](#) page, these are **Identify** a project, **Originate** a project, **Raise** the Funds, **Build** the project, and **Run** the project. The application environment is specifically aligned with the processes since they provide services across
- **Governance Framework:** This pertains to the Governance Frameworks in common [Trust Over Ip](#) stacks.
- **DIDs and Agent Credentials:** Common ID layer and verifiable credential layer that determined who is who in the common network, and what data can be shared between each agent. Tools for this are provided from [Hyperledger Indy](#) (DID) and [Hyperledger Aries](#) (Agent Credentials).
- **Common DLT Data Layer:** This can be a permissioned ledger that stores data from the network that applications can use for their specific services across the business process flow, granted that they have access from the other applications and the underlying agentes (eg. the user). Such a layer can use [Hyperledger Fabric](#).
- **Business Protocols and Taxonomies:** The common language use by the business process flows can be understood as a shared taxonomy, which defines common schemas and methods. This is business specific.
- **Client Layer:** This layer is a common entry point for every application in the network, it makes it easy for applications to interact with the network and even integrate their own set of network solutions, since application may be leveraging tools from other DLT environments.
- **Application Environment:** These are the actual applications and platform of applications using the network and providing different concrete services to the end-user for their processes. Applications in this model can be proprietary or open source, but require using the open source network to establish the trusted interactions across them.

Term	Status	Definition
AML	ACTIVE	NEEDS REVIEW
Application	ACTIVE	NEEDS REVIEW

BLOCK	ACTIVE	<p>A block contains one or more transactions stored within the blockchain. Blocks are created by the ordering service, and then validated and committed by peers.</p> <p>Analogy: A block is similar to a page of a ledger.</p>
Blockchain	ACTIVE	<p>A block contains an ordered set of transactions. It is cryptographically linked to the preceding block, and in turn it is linked to be subsequent blocks. A blockchain is a list of records (blocks), linked (or chained) chronologically. The first block in such a chain of blocks is called the genesis block.</p> <p>Analogy: a blockchain is similar to a book of records that keeps a log of all transactions ("blocks"), in chronological order.</p>
Chain	ACTIVE	<p>The ledger's chain is a transaction log structured as hash-linked blocks of transactions. Peers receive blocks of transactions from the ordering service, mark the block's transactions as valid or invalid based on endorsement policies and concurrency violations, and append the block to the hash chain on the peer's file system.</p>
Chaincode	ACTIVE	<p>Embedded logic that encodes the rules for specific types of network transactions.</p>
DApp	ACTIVE	<p>Decentralized application - Whole or part of logic on a decentralized network; built on a peer-to-peer network like a blockchain; May have their own blockchain.</p>
Initiatives	ACTIVE	<p>Groups of stakeholders collaborating to educate, develop pilots, & set policy.</p>
Blockchain Platform	ACTIVE	<p>A decentralized, distributed, immutable ledger.</p>
Project	ACTIVE	<p>Implementation of an Application, DApp, or Intermediary System.</p>
Intermediary System	ACTIVE	<p>Standard or specification for data and procedure that may include libraries, protocols, applications; is not a blockchain in and of itself.</p>
Private Consortium	ACTIVE	<p>Organization members collaborating to set standards, governance, development, and hosting of a private blockchain and its related applications.</p>
Public Permissioned Consortium		<p>Organization members collaborating to set standards, governance, development, and hosting of a public permissioned blockchain and its related applications.</p>
Channel		<p>Private blockchain overlay that allows for data confidentiality and isolation. Channels are defined by a Configuration Block</p>
Configuration block		<p>Block that contains the configuration data that defines members and policies for a system chain or channel.</p>
Consensus		<p>General agreement that allows to confirm the correctness and the order of the set of transactions of a specific block.</p>
Smart contract		<p>Decentralized, immutable and deterministic protocols that provide automation in blockchain solutions and allow to remove third-parties and let peer-to-peer interactions. Smart contract activities can be verifiedOnce agreed between the parties and deployed on a distributed ledger, their activities and outcomes can be verified, so they can be trusted by all stakeholders.</p>
Genesis block		<p>First block of a block chain, that initializes the ordering service.</p>
Transaction		<p>A transaction is created when a chaincode is invoked from a client application to read or write data from the ledger.</p>
Smart contract		<p>Code – invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the latest values for all keys included in the chain transaction log via transactions.</p>

Person	A human being, alive or deceased, as recognized by each jurisdiction's legal definitions.
--------	-------------------------------------------------------------------------------------------

Organization	An organized group of one or more people with a particular purpose.
Role	People have roles in Organizations for specific periods of time.
Resource	Anything could be a resource, depending on its context defined in metadata.
Event	People and Organizations have events with each other and with resources on or over specific periods of Time.
Relationship	Organizations, Resources, and Events all can have standard association types
Identity	The unique fact of being who or what a person or thing is
Digital Identity	A unique fact of being who or what a person is IN the digital world. It may be connected to a real world Identity (thus being a digital twin) or may not (alias/persona)
Digital Identifier	Unique information used to identify people, organizations, or things within a context. For example: SSN, e-mail, SASID, LASID. A digital identity can have more than one digital identifier.
PII	Personally Identifiable Information is any item, collection, or grouping of information about an individual that is maintained by an organization, including identifying information, education, financial transactions, medical history, Social Security Numbers, and criminal or employment history.
Personal Information	PII, demographics, and linked event information. Some information becomes personal in context (such as small group size aggregates).
Learner Information	Information about a learner.
Privacy Rights	Rights of a person to control access to and use of their personal information. More formal definition: "the right of a person to be free from intrusion into or publicity concerning matters of a personal nature"
Authentication	Actions and mechanisms that can authenticate the identity of a person that includes information about an authentication provider, the login identifier used to authenticate a person's identity, and other information related to authentication of a person's identity.
Authorization	The authority to access to data or services to authorized entities.
Access Control	The protocols in a system that limit access to data or services to authorized entities. Information about a data system or application that an authenticated person or system may access
Self-sovereign identity	An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Identifiers together with the usage of the associated Identity Data
Information Security	Systems of controls designed to enforce privacy access controls and operational continuity.
Data Stewardship /Processor	Responsibility to have proper security for privacy access controls.
Trust	A person or systems ability to rely on something from another. Fiduciary trust can be delegated from one entity to another.
Competency Definition	An information resource that includes a statement that describes a capability or behavior that a person may learn or be able to do within a given situation and environment along with definitions of the potential levels of mastery and metadata related to that statement
Competency Assertion	Event data that includes an Assertion by an Issuer about a Person regarding their competency as of a certain date.
Credential Definition	An information Resource that defines a competency or qualification, achievement, personal or organizational quality, experience, attribute, or aspect of an identity typically used to indicate suitability
Credential Award	Event data that includes an Assertion by an Agent/Issuer that documents a Person or Organization's qualification, achievement, personal or organizational quality, experience, attribute, or aspect of an identity as of a certain date or date range.

Hyperledger Glossary for marketing

- [Save for later](#)
- [Watch](#)
- [Share](#)

1. [Dashboard](#)
2. [Community Architects Team](#)
3. [Works in Progress](#)

[Skip to end of banner](#)[Go to start of banner](#)[Skip to end of metadata](#)

- Created by [Ry Jones](#), last modified by [Silona Bonewald](#) on [Mar 22, 2019](#)

[Hyperledger Glossary for marketing](#)

[Marketing](#)

- **What is a project?**
 - **A project is a top-level DLT or component that has been ratified by the TSC.**
 - **Projects should ship**
 - **The bar for new projects is high.**
 - **Burrow**
 - **Fabric**
 - **Indy**
 - **Iroha**
 - **Sawtooth**
 - **GRID (should be a sub-project of Sawtooth, or a lab)**
 - What are the benefits?
 - What kind of Support does it get?
- **What is a sub-project?**
 - What are the benefits?
 - What kind of Support does it get?
 - What is the relationship to the Project?
- **What is a tool?**
 - **A tool is a project that works with one or more of the DLT projects, as ratified by the TSC.**
 - **Tools should ship**
 - **The bar for new tools is lower than projects, but still high**
 - **Caliper**
 - **Cello (should be a sub-project of Fabric)**
 - **Composer (should be sub-project of Fabric, or a lab)**
 - **Explorer (probably a sub-project of Fabric)**
 - **Quilt (should be a lab)**
 - **URSA**
- **Proposed Current State of the World**
 - **Projects**
 - **Burrow**
 - Burrow is a top-level DLT designed to bring support for the Ethereum smart contract standard to permissioned blockchains.
 - Burrow is interoperable with Sawtooth and has planned interop with Fabric.
 - **Fabric**
 - **Cello**
 - Cello is a tool for provisioning DLT networks. Currently it can only provisions Fabric networks.
 - Cello plans to support provisioning other DLT networks by supporting Kubernetes.
 - **Composer**
 - Composer is a tool for designing business logic and translating it into DLT smart contracts.
 - **Explorer**
 - **Indy**
 - **Ursa**
 - **Iroha**
 - **Sawtooth**
 - **Grid**
 - **Labs**
 - **Quilt**
- **What is a Library?**
- **What is a framework?**
- **What is a Platform?**
- **How a sub-project can graduate into top-level project?**
 - Demonstrate interop across multiple existing top-level projects.
- **Different Levels of interop for each?**
 - Platform have a ready SDK
 - Full support for API across multiple platforms
 - Information exchange level VS asset exchange level
 - Different levels?
 - Level 1 – show roadmap and/or prototype code for talking to multiple DLT platforms (not necessarily Hyperledger)
 - Level 2 – demonstrate working code.
 - Level 3 – active tracking of API changes with automatic detection via routine CI/CD compatibility testing.
 - Different types of interop
 - Interfacing with one only one DLT at a time, but capable of talking to multiple DLTs.
 - Example: Explorer should be able to talk to all DLTs but it's purpose is to talk to one at a time.
 - Example: Caliper should be able to measure perf of multiple DLTs (not exclusive to HL) but it's purpose is to talk to one at a time.
 - Interfacing across multiple DTLs at the same time.

- Example: Quilt needs to talk to multiple DLTs at the same time to lock an asset in one DLT and create it in another at the same time.
- What are the interop requirements for Tools and Libraries?
- Can we reward platforms for being interop with other platforms?
- **What is a SIG?**
 - **A SIG is a group of people that want to discuss a particular area where blockchains may be useful.**
 - **They may produce white papers, use cases, or code.**
 - **SIGs may or may not ship**
 - **SIGs consist of SMEs for the vertical of the SIG**
 - **SIGs are governed by ECO**
 - Healthcare
 - Public Sector
 - Social Impact
 - Telecom
 - Trade Finance
- **What is a WG?**
 - **A WG is focused on guiding development in specific areas**
 - **A WG may or may not ship**
 - **A WG develops guidelines and frames the expertise of the SMEs more broadly so they can work in a wider scope than an individual project**
 - Architecture
 - Identity
 - Learning Materials
 - Perf & Scale
 - Smart Contracts
 - TWGC is probably a sig? It's somewhere between a WG and a SIG. It is a Technical group because of the great firewall issues and translation issues.
- **What is a lab?**
 - **Labs were created to provide a low-impact to LF staff incubation ground for code to be tried out and try to build momentum.**
 - **The lab must find a sponsor on the TSC or among lab stewards.**
 - **Labs start with code first.**
 - **The roles and responsibilities of stewards is unclear.**
 - **The goal is to allow projects to graduate from a lab to a project or tool without a lot of handholding by LF staff.**
 - **Labs are not really expected to ship anything**
 - **No blog posts about labs, no PR, etc. The bar is low.**
- **What is SEMVER?**
 - **SEMVER, Semantic Versioning, is how all projects and tools are supposed to be versioned.**
- **What is FMR?**
 - **FMR, First Major Release, is tied to a gate for having SEMVER 1.0.0**
- **Who governs FMR?**
 - **FMR is a gate governed by the TSC.**
- **Who cares?**
 - **It is expected that projects and tools that pass FMR will have some level of support as they move forward.**
- Community Maturity
- Vendor Diversity
- What is Incubation, active, inactive?
 - If this is a measure of community maturity, how do we described the attributes of the community maturity such that being "immature" doesn't harm the marketing of the project.
 - The "Status" seems to be too prominent in our marketing and too visible in our wiki.
 - What we want outsiders to see is our technical readiness and the opportunities that exist for getting involved.
 - What we want insiders to see is the maturity metrics of the communities associated with each project.
- CII badge
- Policy on Websites, twitter etc.

Silona Wrote

1.

hey I'm thinking we should either move this to the marketing part of the wiki or give it to the Learning materials group. [Ry Jones](#) what do you think?

[Reply](#)
[Like](#)
 Jan 06, 2020

a.

[Ry Jones](#)

probably the latter - if they want it. If LMG doesn't want to maintain it, then marketing

Term	Definition
Block	<p>A block contains one or more transactions. The contents of the block are not encrypted in the blockchain. A block, in general, contains valid and invalid transactions. However invalid transactions have no effect on the State.</p> <p>A block usually contains three sections: a blockheader, the payload (with at least the transactions) and the metadata section (containing the valid/invalid indicator per transaction).</p> <p>Fabric: A block in Fabric contains both valid and invalid transactions.</p> <p>Sawtooth: A block in Sawtooth contains only valid transactions.</p> <p>Burrow: A block in Burrow contains only valid transactions.</p> <p>Iroha: A block in Iroha contains only valid transactions.</p> <p>Block - A set of transactions that are bundled together and added to the chain at the same time.</p>
Blockchain	<p>According to hyperledger.org,</p> <p><i>"A blockchain is a peer-to-peer distributed ledger forged by consensus, combined with a system for "smart contracts" and other assistive technologies".</i></p> <p>Smart contracts are simply computer programs that execute predefined actions when certain conditions within the system are met.</p> <p>Consensus refers to a system of ensuring that parties agree to a certain state of the system as the true state.</p> <p>A blockchain is a chain of blocks each containing transaction (transition) data. Each block, except the first block, is linked with the previous block and each block, except the last block, is linked with the next block, together forming a chain.</p> <p>Once a block has entered the blockchain, it is 'chiselled in granite'. This characteristic delivers the immutability of the data in the blockchain, also referred to as practically tamper-resistant data or virtually incorruptible data. This aspect is one of the main reasons for the broad interest in blockchain technology.</p> <p>[For those with software development experience: In computer science language a blockchain is an append-only data structure; a blockchain (instance) consists at any moment in time of a number of blocks. If the chain has N blocks, then it has N-1 links, valid for N>=1. The blockchain contains all the transitions, while the World State is derived from all transitions (there is a better optimization as World State (N) = valid transactions in block N applied to World State (N-1).]</p>
Chain	<p>Each block header contains, besides its identifier within the scope of the blockchain, a hash of the data in the block. It also contains a copy of the hash of the previous block. Because of this relationship, the a copy of the hash of the previous block, the term chain is used. This is the basis for the tamper-resistant characteristic of a blockchain.</p> <h2>Chain</h2> <p>blocked URL</p> <p>Blockchain B contains blocks 0, 1, 2.</p> <hr/> <p>The ledger's chain is a transaction log structured as hash-linked blocks of transactions. Peers receive blocks of transactions from the ordering service, mark the block's transactions as valid or invalid based on endorsement policies and concurrency violations, and append the block to the hash chain on the peer's file system.</p>
Chaincode	<p>Chaincode is a computer program that either provides functionalities for Enterprise transactions or state. It is useful to distinguish chaincode specific for an enterprise and chaincode that provides domain agnostic functions.</p> <p>Fabric: The current trend in Fabric is to use the term chaincode to cover both enterprise specific and domain agnostic chaincode. Enterprise specific chaincode is what most people call smart contracts.</p> <p>Chaincode - Smart contracts in Hyperledger Fabric. They encapsulate both the asset definitions and the business logic (or transactions) for modifying those assets.</p>
Cryptography	<p>Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.</p> <p><i>Adapted from: Wikipedia</i></p> <p>Cryptography - The study of the techniques used to allow secure communication between different parties, and to ensure the authenticity and immutability of the data being communicated.</p>
Hash	<p>A hash of a (variable length) piece of data results in a unique fixed length data field. The hash is a one-way function that assigns to the variable length field a unique fixed length data field. It is not possible to reconstruct from the hash of the original variable length data field, therefore, a making a hash a one-way function.</p>
Key Pairs	<p>Public key</p> <p>Public Key is the Public Key Infrastructure (PKI) component that a person or organization shares with third-parties. Such a third party uses the Public Key to encrypt messages that are sent back to the owner of the public key. The owner of the Public Key then uses the associated Private Key to decrypt the message.</p> <p>Private key</p> <p>Private Key is the Public Key Infrastructure (PKI) component that a person or organization should keep confidential. The Private Key is used to decrypt messages sent by third parties that were encrypted using the Public Key.</p>
Digital Certificate	<p>A document that contains attributes related to the bearer of the certificate, that is secured by cryptography. Digital Certificates are issued by a Certificate Authority (CA), and is used by the bearer to prove their identity provided that the other party trusts the CA.</p>
Permissioned	<p>The term permissioned blockchain technology is sometimes used as a synonym for blockchain for enterprise or blockchain for business. Permissioned blockchains require permission to read the information on the blockchain, limit the parties who can transact on the blockchain and set who can write new blocks into the chain.</p>
Consensus	<p>A consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes. Solving that issue – known as the consensus problem – is important in distributed computing and multi-agent systems.</p> <p><i>Consensus, as an algorithm</i></p> <div> <p><i>An algorithm to achieve agreement on a block among peers in the network. By having it in the system, reliability is increased.</i></p> </div> <p><i>Consensus, as a component</i></p> <div> </div>

	<p>Preserves consistent state among the peers within a peer network. Iroha uses own consensus algorithm called Yet Another Consensus (aka YAC). Distinctive features of this algorithm are its scalability, performance, and Byzantine fault tolerance. If there are missing blocks, they will be downloaded from another peer via Synchronizer. Committed blocks are stored in Ametsuchi block storage.</p>
Transaction	A transaction consists of facts (populated fields) about a state transition in the Universe of Discourse (the scope of the business communication). This could be in regard to anything, not just monetary assets.
World State	<p>The World State consists of facts (populated fields) about the current state of the Universe of Discourse as agreed by the blockchain network community. This could regard anything, not just monetary assets. The World State State changes after each block that is added to the Blockchain; see exception for Fabric.</p> <p><i>Fabric:</i> In case there is a block with only invalid transactions, there is no new state in Fabric after adding such a block to the blockchain.</p>
Channel	<p>A channel is a virtual blockchain with its own private ledger only visible to the organizations that make up the channel.</p> <p>Fabric: A Fabric blockchain network will have at least two channels (exactly 1 system channel and at least 1 application channel). The visibility of an application channel's ledger is limited to the organizations that make up the channel.</p> <p>An organization can be involved in any number of application channels and any application channel can have any number of organizations. Each network has at least one application channel with its own blockchain and every application channel has its own private blockchain.</p>
Immutability	Immutability of a block means that once the contents of the block is committed to the blockchain, it is free from tampering.
Trust	<p>"A blockchain is a distributed database with no central authority and no [single] point of trust. When you want to share a database, but you don't have a lot of trust in the other people who might use it, a blockchain can be very helpful. In this context, "trust" could mean many things. Trust could mean trusting others to perform actions on the database properly. Trust could mean not trying to pry into each other's private information. Or trust could mean not degrading someone else's performance to gain a competitive advantage. Discussing trust brings up the two main kinds of blockchain. Most cryptocurrencies use permissionless blockchains where anyone can join and have full rights to use it. For example, anyone can buy Bitcoin or Ether because those use wide-open, permissionless blockchains. On the other hand, business blockchains tend to be permissioned. This means a person needs to meet certain requirements to perform certain actions on the blockchain. Some permissioned blockchains restrict access to pre-verified users who have already proven they are who they say they are. Others allow anyone to join, but only let trusted identities verify transactions on the blockchain. Remember our example of the database shared between head office and the field reps of a company. If a blockchain was used to manage that database, it would definitely be permissioned: Everyone accessing the blockchain would have to be an employee of the company or perhaps a trusted trading partner."</p> <p><i>Source: An Introduction to Hyperledger, The Hyperledger White Paper WG, v1.1</i></p>
Governance	<p>Governance is the way the rules, norms and actions are structured, sustained, regulated and held accountable. 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. For instance, a government may operate as a democracy where citizens vote on who should govern and the public good is the goal, while a non-profit organization may be governed by a small board of directors and pursue more specific aims.</p> <p>In addition, a variety of external actors without decision-making power can influence the process of governing. These include lobbies, think tanks, political parties, non-government organizations and the media.</p> <p><i>Source: Wikipedia.</i></p>
Node	<p>A node is a HLF blockchain network is a piece of software.</p> <p>Fabric: In Hyperledger Fabric it is either a <i>peer</i>, which is either an endorsing peer or a committing peer, or element of the ordering service. For Hyperledger Fabric the following integrity rules hold: The endorsing peers are a subset of the committing peers. Every peer is a committing peer. No element of the set of peers is an orderer.</p>
Peer	<p>A peer is a participant in blockchain; in general, a peer can endorse a transaction, commit a transaction or order transactions in a block.</p> <p>Fabric: The nodes inside a Fabric network consists of peers and orderers. The set of peers and the set of orderers have no element in common. All peers have the role of maintaining the ledger of the channel, consisting of the blockchain and the World State; some peers use smart contracts to simulate the transaction and to decide on the endorsement of a submitted transaction.</p>
Chaincode	<p>Chaincode is a computer program that either provides functionalities for Enterprise transactions or state. It is useful to distinguish chaincode specific for an enterprise and chaincode that provides domain agnostic functions.</p> <p>Fabric: The current trend in Fabric is to use the term chaincode to cover both enterprise specific and domain agnostic chaincode. Enterprise specific chaincode is what most people call smart contracts.</p>
Ledger	<p>The ledger consists of two components, the immutable chain containing the transactions (transitions) and the state.</p> <p>According to the Fabric documentation (v1.2) the ledger consists of the blockchain and the World State.</p>
	<h2>blocked URL</h2> <p>LinuxFoundationX: LFS171x Blockchain for Business - An Introduction to Hyperledger Technologies</p>
	<h2>Glossary</h2> <p>On this page, we will have a list of the key concepts that are used in this course, and their definitions, that will help you when going through the course content. These definitions will be quickly accessible from anywhere within the course, just click on the Glossary tab.</p> <p>Block - A set of transactions that are bundled together and added to the chain at the same time.</p> <p>Byzantine Fault Tolerance Algorithm - A consensus algorithm designed to defend against failures in the system caused by forged or malicious messages. In order to be fault tolerant of a Byzantine fault, the number of nodes that must reach consensus is 2f+1 in a system containing 3f+1, where f is the number of faults in the system.</p> <p>Chaincode - Smart contracts in Hyperledger Fabric. They encapsulate both the asset definitions and the business logic (or transactions) for modifying those assets.</p> <p>Consensus Algorithm - Refers to a system of ensuring that parties agree to a certain state of the system as the true state.</p> <p>Cryptocurrency - is a digital asset that is used as a medium of exchange. A cryptocurrency is exchanged by using digital signatures to transfer ownership from one cryptographic key pair to another key pair. Since this digital asset has characteristics of money (like store of value and medium of exchange), it is generally referred to as currency. <i>Note:</i> It should not be confused with digital currency or virtual currency.</p> <p>Cryptoeconomics - A field of study that explores the intersection of cryptography and economic incentives. While cryptography is used for ensuring network security at various levels and functions, the built-in economic incentives provided to the participating nodes in the network ensure that, at any given point, the majority of players in the network operate in a desirable way.</p> <p>Cryptography - The study of the techniques used to allow secure communication between different parties, and to ensure the authenticity and immutability of the data being communicated.</p> <p>Distributed Ledger - A type of data structure which resides across multiple computer devices, generally spread across locations and regions.</p> <p>Hash Function - It is used to map data of any size to a fixed length. The output of a hash function is referred to as a hash, hash value, or digest. One important characteristic of a hash function is that, when given a specific input, the hash function will always produce the exact same output.</p> <p>Key/Value Pair - It consists of two parts, one designated as a 'key', and another as a 'value'. The 'key' is an identifier that allows you to look up the 'value'. The 'value' is the data that is stored for a given 'key'.</p> <p>Mining - The process of solving computational challenging puzzles in order to create new blocks in the Bitcoin blockchain.</p> <p>Node - Computer device attached to a blockchain network. Types of nodes include: mining nodes, validator nodes, committer nodes, and endorser nodes. Nodes are sometimes also called 'peers' because they make up the devices within a peer-to-peer network.</p> <p>Peer-to-Peer Network - A network which consists of computer systems directly connected to each other via the Internet without a central server.</p> <p>Private/Public Keys - Private keys are used to derive a public key. While private keys remain confidential, public keys are available to everyone in the network (similar to an email address). Anything encrypted with a public key can only be decrypted using its corresponding private key, and vice versa.</p>

Proof of Elapsed Time (PoET) - Consensus algorithm used by Hyperledger Sawtooth that utilizes a lottery function in which the node with the shortest wait time creates the next block.

Proof of Stake (PoS) - Consensus algorithm where nodes are randomly selected to validate blocks, and the probability of this random selection depends on the amount of stake held.

Proof of Work (PoW) - Consensus algorithm first utilized by Bitcoin that involves solving a computational challenging puzzle in order to create a new block.

Smart Contract - Computer program that executes predefined actions when certain conditions within the system are met. Smart contracts were first proposed by Nick Szabo in 1996 (http://www.fon.hum.uva.nl/rob/Courses/InformationinSpeech/CDROM/Lecture/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html).

State - Contains up-to-date data that represents the latest values for all keys included in the network's ledger. The state of a network encompasses all past transactions in the network, from the genesis block to the present time.

Transaction - A record of an event, cryptographically secured with a digital signature, that is verified, ordered, and bundled with other such records into blocks.

Transaction Families - Smart contracts in Hyperledger Sawtooth. They define the operations that can be applied to transactions. Transaction families consist of both transaction processors (the server-side logic) and clients (for use from web or mobile applications).

Turing-Complete - Named after Alan Turing, an English mathematician and computer scientist, it refers to a computer that can solve any problem that a Turing Machine can. A Turing Machine is a machine that can simulate any computer algorithm, no matter how complicated. Bitcoin scripting language is not Turing-Complete, as there are no looping and branching types of computing sequences. Ethereum's Solidity language is considered Turing-Complete, as it does have looping and branching.

Glossary FABRIC

Terminology is important, so that all Hyperledger Fabric users and developers agree on what we mean by each specific term. What is a smart contract for example. The documentation will reference the glossary as needed, but feel free to read the entire thing in one sitting if you like; it's pretty enlightening!

Anchor Peer

Used by gossip to make sure peers in different organizations know about each other.

When a configuration block that contains an update to the anchor peers is committed, peers reach out to the anchor peers and learn from them about all of the peers known to the anchor peer (s). Once at least one peer from each organization has contacted an anchor peer, the anchor peer learns about every peer in the channel. Since gossip communication is constant, and because peers always ask to be told about the existence of any peer they don't know about, a common view of membership can be established for a channel.

For example, let's assume we have three organizations — A, B, C — in the channel and a single anchor peer — peer0.orgC — defined for organization C. When peer1.orgA (from organization A) contacts peer0.orgC, it will tell peer0.orgC about peer0.orgA. And when at a later time peer1.orgB contacts peer0.orgC, the latter would tell the former about peer0.orgA. From that point forward, organizations A and B would start exchanging membership information directly without any assistance from peer0.orgC.

As communication across organizations depends on gossip in order to work, there must be at least one anchor peer defined in the channel configuration. It is strongly recommended that every organization provides its own set of anchor peers for high availability and redundancy.

ACL

An ACL, or Access Control List, associates access to specific peer resources (such as system chaincode APIs or event services) to a [Policy](#) (which specifies how many and what types of organizations or roles are required). The ACL is part of a channel's configuration. It is therefore persisted in the channel's configuration blocks, and can be updated using the standard configuration update mechanism.

An ACL is formatted as a list of key-value pairs, where the key identifies the resource whose access we wish to control, and the value identifies the channel policy (group) that is allowed to access it. For example `lscc/GetDeploymentSpec: /Channel/Application/Readers` defines that the access to the life cycle chaincode `GetDeploymentSpec` API (the resource) is accessible by identities which satisfy the `/Channel/Application/Readers` policy.

A set of default ACLs is provided in the `configtx.yaml` file which is used by `configtxgen` to build channel configurations. The defaults can be set in the top level "Application" section of `configtx.yaml` or overridden on a per profile basis in the "Profiles" section.

Block

[blocked URL](#)

Block B1 is linked to block B0. Block B2 is linked to block B1.

A block contains an ordered set of transactions. It is cryptographically linked to the preceding block, and in turn it is linked to be subsequent blocks. The first block in such a chain of blocks is called the genesis block. Blocks are created by the ordering system, and validated by peers.

Chain

[blocked URL](#)

Blockchain B contains blocks 0, 1, 2.

The ledger's chain is a transaction log structured as hash-linked blocks of transactions. Peers receive blocks of transactions from the ordering service, mark the block's transactions as valid or invalid based on endorsement policies and concurrency violations, and append the block to the hash chain on the peer's file system.

Chaincode

See [Smart-Contract](#).

Channel

[blocked URL](#)

Channel C connects application A1, peer P2 and ordering service O1.

A channel is a private blockchain overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it. Channels are defined by a [Configuration-Block](#).

Commit

Each [Peer](#) on a channel validates ordered blocks of transactions and then commits (writes/appends) the blocks to its replica of the channel [Ledger](#). Peers also mark each transaction in each block as valid or invalid.

Concurrency Control Version Check

Concurrency Control Version Check is a method of keeping state in sync across peers on a channel. Peers execute transactions in parallel, and before commitment to the ledger, peers check that the data read at execution time has not changed. If the data read for the transaction has changed between execution time and commitment time, then a Concurrency Control Version Check violation has occurred, and the transaction is marked as invalid on the ledger and values are not updated in the state database.

Configuration Block

Contains the configuration data defining members and policies for a system chain (ordering service) or channel. Any configuration modifications to a channel or overall network (e.g. a member leaving or joining) will result in a new configuration block being appended to the appropriate chain. This block will contain the contents of the genesis block, plus the delta.

Consensus

A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.

Consenter set

In a Raft ordering service, these are the ordering nodes actively participating in the consensus mechanism on a channel. If other ordering nodes exist on the system channel, but are not a part of a channel, they are not part of that channel's consenter set.

Consortium

A consortium is a collection of non-orderer organizations on the blockchain network. These are the organizations that form and join channels and that own peers. While a blockchain network can have multiple consortia, most blockchain networks have a single consortium. At channel creation time, all organizations added to the channel must be part of a consortium. However, an organization that is not defined in a consortium may be added to an existing channel.

Chaincode definition

A chaincode definition is used by organizations to agree on the parameters of a chaincode before it can be used on a channel. Each channel member that wants to use the chaincode to endorse transactions or query the ledger needs to approve a chaincode definition for their organization. Once enough channel members have approved a chaincode definition to meet the Lifecycle Endorsement policy (which is set to a majority of organizations in the channel by default), the chaincode definition can be committed to the channel. After the definition is committed, the first invoke of the chaincode (or, if requested, the execution of the Init function) will start the chaincode on the channel.

Current State

See [World-State](#).

Dynamic Membership

Hyperledger Fabric supports the addition/removal of members, peers, and ordering service nodes, without compromising the operability of the overall network. Dynamic membership is critical when business relationships adjust and entities need to be added/removed for various reasons.

Endorsement

Refers to the process where specific peer nodes execute a chaincode transaction and return a proposal response to the client application. The proposal response includes the chaincode execution response message, results (read set and write set), and events, as well as a signature to serve as proof of the peer's chaincode execution. Chaincode applications have corresponding endorsement policies, in which the endorsing peers are specified.

Endorsement policy

Defines the peer nodes on a channel that must execute transactions attached to a specific chaincode application, and the required combination of responses (endorsements). A policy could require that a transaction be endorsed by a minimum number of endorsing peers, a minimum percentage of endorsing peers, or by all endorsing peers that are assigned to a specific chaincode application. Policies can be curated based on the application and the desired level of resilience against misbehavior (deliberate or not) by the endorsing peers. A transaction that is submitted must satisfy the endorsement policy before being marked as valid by committing peers.

FabToken

FabToken is an Unspent Transaction Output (UTXO) based token management system that allows users to issue, transfer, and redeem tokens on channels. FabToken uses the membership services of Fabric to authenticate the identity of token owners and manage their public and private keys.

FabToken

FabToken is an Unspent Transaction Output (UTXO) based token management system that allows users to issue, transfer, and redeem tokens on channels. FabToken uses the membership services of Fabric to authenticate the identity of token owners and manage their public and private keys.

Follower

In a leader based consensus protocol, such as Raft, these are the nodes which replicate log entries produced by the leader. In Raft, the followers also receive "heartbeat" messages from the leader. In the event that the leader stops sending those message for a configurable amount of time, the followers will initiate a leader election and one of them will be elected leader.

Genesis Block

The configuration block that initializes the ordering service, or serves as the first block on a chain.

Gossip Protocol

The gossip data dissemination protocol performs three functions: 1) manages peer discovery and channel membership; 2) disseminates ledger data across all peers on the channel; 3) syncs ledger state across all peers on the channel. Refer to the [Gossip](#) topic for more details.

Hyperledger Fabric CA

Hyperledger Fabric CA is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users. The CA issues one root certificate (rootCert) to each member and one enrollment certificate (ECert) to each authorized user.

Init

A method to initialize a chaincode application. All chaincodes need to have an Init function. By default, this function is never executed. However you can use the chaincode definition to request the execution of the Init function in order to initialize the chaincode.

Install

The process of placing a chaincode on a peer's file system.

Instantiate

The process of starting and initializing a chaincode application on a specific channel. After instantiation, peers that have the chaincode installed can accept chaincode invocations. This method was used in the previous version of the chaincode lifecycle. For the current procedure used to start a chaincode on a channel with the new Fabric chaincode lifecycle introduced as part of the Fabric v2.0 Alpha, see [Chaincode-definition](#).

Invoke

Used to call chaincode functions. A client application invokes chaincode by sending a transaction proposal to a peer. The peer will execute the chaincode and return an endorsed proposal response to the client application. The client application will gather enough proposal responses to satisfy an endorsement policy, and will then submit the transaction results for ordering, validation, and commit. The client application may choose not to submit the transaction results. For example if the invoke only queried the ledger, the client application typically would not submit the read-only transaction, unless there is desire to log the read on the ledger for audit purpose. The invoke includes a channel identifier, the chaincode function to invoke, and an array of arguments.

Leader

In a leader based consensus protocol, like Raft, the leader is responsible for ingesting new log entries, replicating them to follower ordering nodes, and managing when an entry is considered committed. This is not a special type of orderer. It is only a role that an orderer may have at certain times, and then not others, as circumstances determine.

Leading Peer

Each [Organization](#) can own multiple peers on each channel that they subscribe to. One or more of these peers should serve as the leading peer for the channel, in order to communicate with the network ordering service on behalf of the organization. The ordering service delivers blocks to the leading peer(s) on a channel, who then distribute them to other peers within the same organization.

Ledger

[blocked URL](#)

A Ledger, 'L'

A ledger consists of two distinct, though related, parts – a “blockchain” and the “state database”, also known as “world state”. Unlike other ledgers, blockchains are immutable – that is, once a block has been added to the chain, it cannot be changed. In contrast, the “world state” is a database containing the current value of the set of key-value pairs that have been added, modified or deleted by the set of validated and committed transactions in the blockchain.

It's helpful to think of there being one logical ledger for each channel in the network. In reality, each peer in a channel maintains its own copy of the ledger – which is kept consistent with every other peer's copy through a process called consensus. The term Distributed Ledger Technology (DLT) is often associated with this kind of ledger – one that is logically singular, but has many identical copies distributed across a set of network nodes (peers and the ordering service).

Log entry

The primary unit of work in a Raft ordering service, log entries are distributed from the leader orderer to the followers. The full sequence of such entries known as the “log”. The log is considered to be consistent if all members agree on the entries and their order.

Member

See [Organization](#).

Membership Service Provider

[blocked URL](#)

An MSP, 'ORG.MSP'

The Membership Service Provider (MSP) refers to an abstract component of the system that provides credentials to clients, and peers for them to participate in a Hyperledger Fabric network. Clients use these credentials to authenticate their transactions, and peers use these credentials to authenticate transaction processing results (endorsements). While strongly connected to the transaction processing components of the systems, this interface aims to have membership services components defined, in such a way that alternate implementations of this can be smoothly plugged in without modifying the core of transaction processing components of the system.

Membership Services

Membership Services authenticates, authorizes, and manages identities on a permissioned blockchain network. The membership services code that runs in peers and orders both authenticates and authorizes blockchain operations. It is a PKI-based implementation of the Membership Services Provider (MSP) abstraction.

Ordering Service

Also known as *orderer*. A defined collective of nodes that orders transactions into a block. The ordering service exists independent of the peer processes and orders transactions on a first-come-first-serve basis for all channel's on the network. The ordering service is designed to support pluggable implementations beyond the out-of-the-box SOLO and Kafka varieties. The ordering service is a common binding for the overall network; it contains the cryptographic identity material tied to each [Member](#).

Organization

[blocked URL](#)

An organization, 'ORG'

Also known as “members”, organizations are invited to join the blockchain network by a blockchain service provider. An organization is joined to a network by adding its Membership Service Provider ([MSP](#)) to the network. The MSP defines how other members of the network may verify that signatures (such as those over transactions) were generated by a valid identity, issued by that organization. The particular access rights of identities within an MSP are governed by policies which are also agreed upon when the organization is joined to the network. An organization can be as large as a multi-national corporation or as small as an individual. The transaction endpoint of an organization is a [Peer](#). A collection of organizations form a [Consortium](#). While all of the organizations on a network are members, not every organization will be part of a consortium.

Peer

[blocked URL](#)

A peer, 'P'

A network entity that maintains a ledger and runs chaincode containers in order to perform read/write operations to the ledger. Peers are owned and maintained by members.

Policy

Policies are expressions composed of properties of digital identities, for example: `Org1.Peer OR Org2.Peer`. They are used to restrict access to resources on a blockchain network. For instance, they dictate who can read from or write to a channel, or who can use a specific chaincode API via an [ACL](#). Policies may be defined in `configtx.yaml` prior to bootstrapping an ordering service or creating a channel, or they can be specified when instantiating chaincode on a channel. A default set of policies ship in the sample `configtx.yaml` which will be appropriate for most networks.

Private Data

Confidential data that is stored in a private database on each authorized peer, logically separate from the channel ledger data. Access to this data is restricted to one or more organizations on a channel via a private data collection definition. Unauthorized organizations will have a hash of the private data on the channel ledger as evidence of the transaction data. Also, for further privacy, hashes of the private data go through the [Ordering-Service](#), not the private data itself, so this keeps private data confidential from Orderer.

Private Data Collection (Collection)

Used to manage confidential data that two or more organizations on a channel want to keep private from other organizations on that channel. The collection definition describes a subset of organizations on a channel entitled to store a set of private data, which by extension implies that only these organizations can transact with the private data.

Proposal

A request for endorsement that is aimed at specific peers on a channel. Each proposal is either an Init or an invoke (read/write) request.

Prover peer

A trusted peer used by the FabToken client to assemble a token transaction and list the unspent tokens owned by a given authorized party.

Prover peer

A trusted peer used by the FabToken client to assemble a token transaction.

Query

A query is a chaincode invocation which reads the ledger current state but does not write to the ledger. The chaincode function may query certain keys on the ledger, or may query for a set of keys on the ledger. Since queries do not change ledger state, the client application will typically not submit these read-only transactions for ordering, validation, and commit. Although not typical, the client application can choose to submit the read-only transaction for ordering, validation, and commit, for example if the client wants auditable proof on the ledger chain that it had knowledge of specific ledger state at a certain point in time.

Quorum

This describes the minimum number of members of the cluster that need to affirm a proposal so that transactions can be ordered. For every consenter set, this is a majority of nodes. In a cluster with five nodes, three must be available for there to be a quorum. If a quorum of nodes is unavailable for any reason, the cluster becomes unavailable for both read and write operations and no new logs can be committed.

Raft

New for v1.4.1, Raft is a crash fault tolerant (CFT) ordering service implementation based on the [etcd library](#) of the *Raft protocol* [<https://raft.github.io/raft.pdf>](https://raft.github.io/raft.pdf)_. Raft follows a “leader and follower” model, where a leader node is elected (per channel) and its decisions are replicated by the followers. Raft ordering services should be easier to set up and manage than Kafka-based ordering services, and their design allows organizations to contribute nodes to a distributed ordering service.

Software Development Kit (SDK)

The Hyperledger Fabric client SDK provides a structured environment of libraries for developers to write and test chaincode applications. The SDK is fully configurable and extensible through a standard interface. Components, including cryptographic algorithms for signatures, logging frameworks and state stores, are easily swapped in and out of the SDK. The SDK provides APIs for transaction processing, membership services, node traversal and event handling.

Currently, the two officially supported SDKs are for Node.js and Java, while three more – Python, Go and REST – are not yet official but can still be downloaded and tested.

Smart Contract

A smart contract is code – invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the [World State](#). In Hyperledger Fabric, smart contracts are referred to as chaincode. Smart contract chaincode is installed onto peer nodes and then defined and used on one or more channels.

State Database

Current state data is stored in a state database for efficient reads and queries from chaincode. Supported databases include levelDB and couchDB.

System Chain

Contains a configuration block defining the network at a system level. The system chain lives within the ordering service, and similar to a channel, has an initial configuration containing information such as: MSP information, policies, and configuration details. Any change to the overall network (e.g. a new org joining or a new ordering node being added) will result in a new configuration block being added to the system chain.

The system chain can be thought of as the common binding for a channel or group of channels. For instance, a collection of financial institutions may form a consortium (represented through the system chain), and then proceed to create channels relative to their aligned and varying business agendas.

Transaction

blocked URL

A transaction, 'T'

Transactions are created when a chaincode or FabToken client is used to read or write to data from the ledger. If you are invoking a chaincode, application clients gather the responses from endorsing peers and then package the results and endorsements into a transaction that is submitted for ordering, validation, and commit. If using FabToken to create a token transaction, the FabToken client uses a prover peer to create a transaction that is submitted to the ordering service and then validated by committing peers.

World State

blocked URL

The World State, 'W'

Also known as the “current state”, the world state is a component of the HyperLedger Fabric [Ledger](#). The world state represents the latest values for all keys included in the chain transaction log. Chaincode executes transaction proposals against world state data because the world state provides direct access to the latest value of these keys rather than having to calculate them by traversing the entire transaction log. The world state will change every time the value of a key changes (for example, when the ownership of a car – the “key” – is transferred from one owner to another – the “value”) or when a new key is added (a car is created). As a result, the world state is critical to a transaction flow, since the current state of a key-value pair must be known before it can be changed. Peers commit the latest values to the ledger world state for each valid transaction included in a processed block.