ADD ..

https://www.essentialcardano.io/glossary

<https://cardano-ledger.readthedocs.io/en/latest/explanations/glossary.html>

https://github.com/cardano-foundation/docs-cardano-org/blob/main/explore-cardano/glossary

A

**Abstraction** is used to make models that can be used and reused without having to re-write all the program code for each new application on every different type of computer. Abstraction is usually achieved by writing source code in some particular computer language which can be translated into machine code for different types of computers to execute. Abstraction allows program designers to separate a framework from specific instances which implement details.

​​**Absolute vs. Relative Price**: Absolute price is the number of dollars that can be exchanged for a specified quantity of a given good. Relative price is the quantity of some other good that can be exchanged for a specified quantity of a given good. Suppose we have two goods A and B. The absolute price of good A is the number of dollars necessary to purchase a unit of good A. The relative price of good A in terms of B is the amount of good B necessary to purchase a unit of good A.

**ACTUS** (Algorithmic Contract Types Unified Standards) Contract Types are defined based on the underlying contractual algorithm patterns that respectively cover different classes of financial products that each Contract Type pattern is able to express.

**Address**: a data structure used to express different types of information in transaction outputs. To identify between various networks (eg, mainnet or testnet), each address has a network discriminant tag and a proof of ownership (who owns the transaction output). Delegation options and script references are also included in some addresses*.*

The **address of a UTXO** says where the output is ‘going’. The address stipulates the conditions for unlocking the output. This can be a public key hash, or (in the Extended UTXO model) a script hash.

**Agda** is a dependently typed functional programming language. Charles Hoskinson referred to it as 'Super Haskell'

**Atala PRISM** is a decentralized identity solution built on the Cardano blockchain. It creates a new approach to identity management, where users own their identity and have complete control over how their personal data is used and accessed.

An **atomic swap** is an exchange of cryptocurrencies from separate blockchains. The swap is conducted between two entities without a third party's involvement. The idea is to remove centralized intermediaries like regulated exchanges and give token owners total control.

A **51% attack** is a hostile takeover of a Cryptocurrency validated via proof-of-work Algorithms through the acquisition of the majority of the network's hashing power.

B

**Backpressure**: Cardano is designed to automatically deal with heavy traffic. Ouroboros and the network stack function even when saturated. If the network is saturated, Cardano can use the admission control method to regulate and restore normalcy. This is the term ‘backpressure’ mentioned in blogs and documentation, it is basically a strategy for network load management.

**Balance wallet:** your original testnet ada balance, copied from the mainnet through the balance snapshot, is stored in this wallet. This wallet’s stake is not transferable, although it may be moved to and delegated from a Rewards wallet.

The **Bellman–Ford algorithm** computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph. It is slower than Dijkstra’s algorithm for the same problem, but more versatile, as it is capable of handling graphs in which some of the edge weights are negative numbers. The algorithm was first proposed by Alfonso Shimbel (1955), but is instead named after Richard Bellman and Lester Ford Jr., who published it in 1958 and 1956, respectively.

The **Bitcoin halving** is when the reward for Bitcoin mining is halved. Halving takes place every 4 years. The halving policy was written into Bitcoin's mining algorithm to counteract inflation by maintaining scarcity

**Bitcoin Script** is a simple, stack-based programming language that enables the processing of transactions on the Bitcoin blockchain

**BitTorrent** is a communication protocol for peer-to-peer (P2P) file sharing which is used to distribute data and electronic files over the Internet. BitTorrent is one of the most common protocols for transferring large files, such as digital files containing movies or music.

**Bitcoin (BTC)** is a cryptocurrency and a payment system that uses a public distributed ledger called a blockchain. Invented by a single (or potentially a group) under the Satoshi Nakamoto alias. On 31 October 2008, Bitcoin was introduced to a cryptography mailing list and released as open-source software in 2009. There have been various claims and speculation concerning the identity of Nakamoto, none of which has been confirmed. The system is peer-to-peer, so transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in the blockchain, which uses bitcoin as its unit of account.

**Bitcoin Cash** is a cryptocurrency created in mid-2017. A group of developers wanting to increase Bitcoin's block size limit prepared a code change. The change, called a hard fork, took effect in August 2017 and the cryptocurrency split in two. At the time of the fork anyone owning bitcoin was also in possession of the same number of Bitcoin Cash units.

**Block**: a record of recent network transactions. Each block also includes the data necessary for blockchain management, such as an encrypted record of the preceding block. Each finished block is followed by the creation of the next block to continue the chain.

**Block header**: The portion of a block that contains information about the block itself (block metadata), typically including a timestamp, a hash representation of the block data, the hash of the previous block's header, and a cryptographic nonce (if needed).

**Block height** represents the number of blocks that were validated and confirmed in the entire history of a particular blockchain network, from the genesis block (or block zero) until the most recent one. Unlike the genesis block, all other blocks contain a reference, or hash, to the block that came immediately before it, and the block height is the number of each block in that sequence. So the block height of the genesis block is #0, and the block height of the first block is #1.

A **blockchain** is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. A blockchain is ‘an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.’

**Blockstream** is a blockchain technology company led by co-founder Adam Back. Blockstream intends to develop software to ‘break off’ transactions from the bitcoin network and charge a fixed monthly fee to allow people to use alternative ‘sidechains’. Blockstream employs a large number of prominent Bitcoin Core developers.

In general, **bootstrapping** usually refers to a self-starting process that is supposed to proceed without external input. In computer technology the term (usually shortened to booting) usually refers to the process of loading the basic software into the memory of a computer after power-on or general reset, especially the operating system which will then take care of loading other software as needed.

A bull market or **bull run** is a state of a financial market where prices are rising. The term bull market is often used in the context of the stock market. However, it can be used in any financial market including cryptocurrencies.

**Business logic** or domain logic is the part of the program that encodes the real-world business rules that determine how data can be created, stored, and changed. It is contrasted with the remainder of the software that might be concerned with lower-level details.

**Byzantine fault tolerance (BFT)**: A Byzantine fault is a condition of a computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed. The term takes its name from an allegory, the ‘Byzantine Generals Problem’, developed to describe a situation in which, to avoid catastrophic failure of the system, the system’s actors must agree on a concerted strategy, but some of these actors are unreliable.

A **Byzantine fault** is any fault presenting different symptoms to different observers. A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that require consensus among distributed nodes.

**C**

**Canonical**, in computer science, is the standard state or behavior of an attribute. This term is borrowed from mathematics, where it is used to refer to concepts that are unique and/or natural.

**Cardano** is a blockchain platform for changemakers, innovators, and visionaries, with the tools and technologies required to create possibility for the many, as well as the few, and bring about positive global change. Cardano is a proof-of-stake blockchain platform: the first to be founded on peer-reviewed research and developed through evidence-based methods. It combines pioneering technologies to provide unparalleled security and sustainability to decentralized applications, systems, and societies. With a leading team of engineers, Cardano exists to redistribute power from unaccountable structures to the margins – to individuals – and be an enabling force for positive change and progress. 'Cardano is an open platform that seeks to provide economic identity to the billions who lack it by providing decentralized applications to manage identity, value and governance' - Charles Hoskinson <https://twitter.com/IOHK_Charles/status/1290058248347770880?s=20>

**CBOR (Concise Binary Object Representation)** is a binary data serialization format loosely based on JSON. Like JSON it allows the transmission of data objects that contain name–value pairs, but in a more concise manner. This increases processing and transfer speeds at the cost of human-readability.

A **Chain index** is a database of information obtained from Cardano transactions.

**Chainlink** (ticker: LINK) is a decentralized oracle network that brings off-chain data into an on-chain format, bridging the gap between isolated blockchains and real-world data.

**Colored coins** are a class of methods for associating real-world assets with addresses on the Bitcoin network. Examples could be a deed for a house, stocks, bonds or futures.

A **combinator** is a technical term used to indicate the combination of certain processes or things. In the case of Cardano, a **hard fork combinator** combines protocols, thereby enabling the Byron-to-Shelley transition without system interruption or restart. It ensures that Byron and Shelley ledgers appear as one ledger.

In mathematics, semantics, and philosophy of language, the principle of **compositionality** is the principle that the meaning of a complex expression is determined by the meanings of its constituent expressions and the rules used to combine them.

**Concise data definition language** (CDDL) expresses Concise Binary Object Representation (CBOR) data structures. Its main goal is to provide an easy and unambiguous way to express structures for protocol messages and data formats that use CBOR or JSON (JavaScript Object Notation).

**Concurrency,** the property of program, algorithm, or problem decomposition into order-independent or partially ordered units.

A **consensus** **protocol** is a fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies.

**cost per epoch:** The stake pool operator deducts a predetermined charge from the pool payouts every epoch to cover the expenses of maintaining a stake pool. Before the operator collects their profit margin, the cost per epoch is removed from the total ada that is awarded to a pool. Whatever is left is divided evenly among the delegators.

In finance, a **contract for difference (CFD)** is a contract between two parties, typically described as ‘buyer’ and ‘seller’, stipulating that the seller will pay to the buyer the difference between the current value of an asset and its value at contract time (if the difference is negative, then the buyer pays instead to the seller).

A **crowdsale** is a type of crowdfunding that issues tokens that are stored on the user's device. The tokens can function like a share of stock and be bought and sold ("equity tokens"), or they can pay for services when the service is up and running ("user tokens"). **Crowdsales** are a popular use for Ethereum; they let you allocate tokens to network participants in various ways, mostly in exchange for Ether. They come in a variety of shapes and flavors.

**Crypto Twitter** is a term to describe the Twitter subculture and community that surrounds the topics of blockchain and cryptocurrency.

**Crypto tokens** are digital assets that are built on a cryptocurrency blockchain. A blockchain is a digital ledger that stores information in blocks that are linked. This information can be transaction records or full-fledged programs that operate on the blockchain, which are called smart contracts. The ‘coin’ of a cryptocurrency is a token. In effect, it’s the digital code defining each fraction, which can be owned, bought and sold.

A **cryptographic hash** is a math algorithm that maps data of an arbitrary size (often called the ‘message’) to a bit string of a fixed size (the ‘hash value’, ‘hash’, or ‘message digest’). It is a one-way function, that is, a function that is practically impossible to invert. Cryptographic hash functions are a basic tool of modern cryptography.

**Cypherpunk**: A cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Originally communicating through the cypherpunks email list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since the late 1980s.

D

**Daedalus Flight** is a ‘pre-release’ version of the Daedalus wallet.

The **DAO** was a decentralized autonomous organization (DAO) that was launched in 2016 on Ethereum. After raising $150 million USD worth of ether (ETH) through a token sale, The DAO was hacked due to vulnerabilities in its code base.

**DARPA**: The Defense Advanced Research Projects Agency is a research and development agency of the United States Department of Defense responsible for the development of emerging technologies for use by the military

**Dash** is an open source cryptocurrency and is a form of decentralized autonomous organization (DAO) run by a subset of users, called ‘masternodes’. It is an altcoin that was forked from the Bitcoin protocol. The currency permits fast transactions that can be untraceable.

The purpose of **DB Sync** is to follow the Cardano chain and take information from the chain and an internally maintained copy of ledger state. Data is then extracted from the chain and inserted into a PostgreSQL database. SQL queries can then be written directly against the database schema.

A **dead man's switch** is a switch that is designed to be activated or deactivated if the human operator becomes incapacitated, or dies. Typically, funds may be sent to a preset address after a set time has expired.

**Decentralization** is the process by which the activities of an organization, particularly those regarding planning and decision making, are distributed or delegated away from a central, authoritative location or group.

A **decentralized application** (DApp, dApp, or Dapp) is an open-source project that runs on a blockchain network. The distributed nature of these networks provides users with transparency, decentralization, and resistance to attacks.

**Decentralized identifiers (DIDs)** are a type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (such as a person, organization, thing, data model or abstract entity) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.

**Decentralized Exchanges (DEX)** are peer-to-peer (p2p) online services that allow direct cryptocurrency transactions between interested parties. ErgoDEX and WingRiders are just two of many on Cardano.

**Delegation**: By delegating the stake related to their ada holdings to a stake pool, ada owners participate in the network and collect rewards each epoch (five days). Delegators are rewarded in proportion to the amount of stake delegated.

**DID document**: a set of data describing the DID subject, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID. A DID document might have one or more different representations.

**Digital footprint** or digital shadow refers to one’s unique set of traceable digital activities, actions, contributions and communications manifested on the Internet or on digital devices. On the World Wide Web, the internet footprint; also known as cyber shadow, electronic footprint, or digital shadow, is the information left behind as a result of a user’s web-browsing and stored as cookies.

A **directed acyclic graph** is a directed graph with no directed cycles. That is, it consists of vertices and edges, with each edge directed from one vertex to another, such that following those directions will never form a closed loop.

**Distributed ledger technology (DLT)** is a protocol or database that is consensually shared and synchronized across many sites, institutions, or geographies, accessible by many people, and enables the secure functioning of a decentralized digital database.

**Docker** is a software tool that makes it easier to deploy applications by using ‘containers’, each of which holds all the parts, such as libraries, that the application needs to run.

**Dogecoin** is a cryptocurrency featuring a likeness of the Shiba Inu dog from the ‘Doge’ internet meme as its logo. Introduced as a ‘joke currency’ in 2013, Dogecoin quickly developed its own online community and reached a capitalization of US$1bn in 2018.

A **domain-specific language (DSL)** is a computer language specialized to a particular application domain. This is in contrast to a general-purpose language (GPL), which is broadly applicable across domains.

**Double-spending** is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified. As with counterfeit money, such double-spending leads to inflation by creating a new amount of copied currency that did not previously exist. This devalues the currency relative to other monetary units or goods and diminishes user trust as well as the circulation and retention of the currency. Fundamental cryptographic techniques to prevent double-spending, while preserving anonymity in a transaction, are blind signatures and, particularly in offline systems, secret splitting.

**E**

**EDI**, The Edinburgh Decentralisation Index will collect stratified metrics describing the decentralisation of blockchain systems. The EDI will take numerous metrics from different disciplines – such as economics, information theory and network science – and measure them across different dimensions of blockchain systems, assigning weights to them. These will then be merged into a single index that will represent the overall decentralisation of a system. More details: https://www.ed.ac.uk/informatics/blockchain/edi ed.ac.uk/informatics/blockchain/edi

In public-key cryptography, **Edwards-curve Digital Signature Algorithm (EdDSA**) is a digital signature scheme using a variant of Schnorr signature based on Twisted Edwards curves. It is designed to be faster than existing digital signature schemes without sacrificing security.

In math and computer science, the **\*\*Entscheidungsproblem\*\*** (pronounced German for ‘decision problem’) is a challenge posed by David Hilbert and Wilhelm Ackermann in 1928. The problem asks for an algorithm that takes as input a statement of a first-order logic and answers ‘Yes’ or ‘No’ according to whether the statement is universally valid, i.e., valid in every structure satisfying the axioms. By the completeness theorem of first-order logic, a statement is universally valid if and only if it can be deduced from the axioms, so the Entscheidungsproblem can also be viewed as asking for an algorithm to decide whether a given statement is provable from the axioms using the rules of logic**.**

**Epoch:** a set group of slots that constitute a period of time (currently 5 days).

**Ethereum ERC20 Contract** is a standard for building tokens on the Ethereum Blockchain. Before ERC20 tokens, Cryptocurrency exchanges had to build custom bridges between platforms to support the exchange of any token. For this reason, six rules were created by an Ethereum developer named Fabian Vogelsteller and placed under the name ERC20, which means ‘ethereum request for comment.’

**ERC721** is a free, open standard that describes how to build non-fungible or unique tokens on the Ethereum Blockchain.

**Ergo (**ergoplatform.org) is a proof-of-work smart-contract platform that enables new models of financial interaction, underpinned by a safe and rich scripting language built with flexible and powerful zero-knowledge proofs (Σ-protocols).

**Ethereum** is a decentralized, open source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform. Ethereum was conceived in 2013 by programmer Vitalik Buterin. Additional founders of Ethereum included Gavin Wood, Charles Hoskinson, Anthony Di Iorio and Joseph Lubin.

**Ethereum 2.0** is a new version of the Ethereum blockchain that will switch to a proof of stake consensus mechanism, moving from the original, existing proof of work mechanism.

**F**

**Fiat money** has been defined variously as:

* Any money declared by a government to be legal tender
* State-issued money which is neither convertible by law to any other thing, nor fixed in value in terms of any objective standard
* Intrinsically valueless money used as money because of government decree
* An intrinsically useless object that serves as a medium of exchange, also known as fiduciary money.

A **finite-state machine** (FSM) or simply a **state machine**, is a mathematical model of computation. It is an abstract machine that can be in exactly one of a finite number of states at any given time. The FSM can change from one state to another in response to some external inputs and/or a condition is satisfied; the change from one state to another is called a transition. An FSM is defined by a list of its states, its initial state, and the conditions for each transition.

**First-principles thinking** is one of the best ways to reverse-engineer complicated problems and unleash creative possibilities. Sometimes called ‘reasoning from first principles,’ the idea is to break down complicated problems into basic elements and then reassemble them from the ground up.

**Formal verification** is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics. Formal verification can be helpful in proving the correctness of systems such as: cryptographic protocols, combinational circuits, digital circuits with internal Memory, and software expressed as source code.

In computer science, **formal methods** are a particular kind of mathematically based techniques for the specification, development and verification of software and hardware systems. The use of formal methods for software and hardware design is motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analysis can contribute to the reliability and robustness of a design.

A **Founders' Agreement** is a contract that a company's founders enter into that governs their business relationships. The Agreement lays out the rights, responsibilities, liabilities, and obligations of each founder.

**Functional programming** is a rigorous style of building the structure and elements of computer programs that treats computation as the evaluation of mathematical functions and avoids changing the properties of the data being processed. It is a ‘declarative’ paradigm in that programming is done with expressions or declarations instead of statements. In functional code, the output value of a function depends only on its arguments, so calling a function with the same value for an argument always produces the same result. This is in contrast to imperative programming where, in addition to a function’s arguments, the global state of a program can affect a function’s resulting value. Eliminating side-effects, that is, changes in state that do not depend on the function inputs, can make understanding a program easier, which was one of the motivations for the development of functional programming.

In economics, **fungibility** is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part.

**G**

**Game theory** is the study of mathematical models of strategic interaction in between rational decision-makers. It has applications in all fields of social science, as well as in logic and computer science. Originally, it addressed zero-sum games, in which each participant’s gains or losses are exactly balanced by those of the other participants. Today, game theory applies to a wide range of behavioral relations and is now an umbrella term for the science of logical decision making in humans, animals, and computers.

**Gas (Ethereum)** refers to the fee, or pricing value, required to successfully conduct a transaction or execute a smart contract on the Ethereum blockchain platform. Priced in small fractions of the cryptocurrency ether, commonly referred to as gwei or sometimes nanoeth, the gas is used to allocate resources of the Ethereum Virtual Machine (EVM) so that decentralized applications such as smart contracts can self-execute is a secured fashion. The maximum amount of gas that you’re willing to spend on a particular transaction is known as the gas limit.

**Genesis block**: A **genesis block** is the first block of a block chain. The genesis block is almost always hardcoded into the software of the applications that utilize its block chain. It is a special case in that it does not reference a previous block.

**GitHub Gist** allows developers to instantly share code, notes, and snippets. Every gist is a Git repository, which means that it can be forked and cloned.

A **gossip protocol** is a procedure or process of computer peer-to-peer communication that is based on the way epidemics spread. Some distributed systems use peer-to-peer gossip to ensure that data is routed to all members of an ad-hoc network. Some ad-hoc networks have no central registry and the only way to spread common data is to rely on each member to pass it along to their neighbors.

Blockchain **governance** brings together norms and culture, laws and code, and the people and the institutions that are needed to run a system and ensure its stability in the long term. Governance, including voting and a treasury for long-term funding, is the focus of the Voltaire stage of the Cardano roadmap.

**H**

In computability theory, the **halting problem** is the problem of determining, from a description of an arbitrary computer program and an input, whether the program will finish running, or continue to run forever.

**Hard fork**: a total overhaul of the network’s protocol, resulting in a shift in operational flow from one model to another. Cardano has a unique mechanism, called the hard fork combinator, for executing hard forks with minimal disruption.

**Haskell** is a general-purpose, statically typed, purely functional programming language with type inference and lazy evaluation. Designed for teaching, research and industrial applications, Haskell has pioneered a number of programming language features.

**HODL** is slang in the cryptocurrency community for holding the cryptocurrency rather than selling it. HODL can also mean ‘Hold On for Dear Life’ and refers to not selling, even during strong market volatility and poor market performance.

**Howey Test**: Securities and Exchange Commission (SEC) v. W. J. Howey Co. (1946). The case resulted in a test, known as the **Howey test**, to determine whether an instrument qualifies as an ‘investment contract’ for the purposes of the Securities Act: ‘a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party. The Howey Test has remained a notable determiner of regulatory oversight for many decades. In the past few years, it has been called into question, most frequently in conjunction with discussions about Cryptocurrencies and Blockchain technology’.

In economics, **hyperinflation** quickly erodes the real value of a local currency as the prices of all goods rise. This causes people to minimize their holdings in that currency as they switch to more stable foreign currencies (hard currency).

I

In DeFi, **impermanent loss** refers to the loss in value when investing liquidity in a liquidity pool compared to just holding tokens. The event occurs when the price of a user's tokens changes compared to when they deposited them in a liquidity pool. The larger the change is, the bigger the loss.

**Incentive**: a method of encouraging members to participate in the network by providing them with a return proportionate to their efforts.  By promoting persistent, active, and robust engagement, incentives strive to maintain equality and fairness in a dispersed network of participants. The incentives necessary in Cardano’s incentives model are calculated using game theory.

**Initial coin offering (ICO)** is a means of crowdfunding via use of cryptocurrency, which can be a source of capital for start-up companies and open-source software projects. In an ICO, a percentage of the newly issued cryptocurrency is sold to investors in exchange for legal tender or other cryptocurrencies such as bitcoin or ether.

The **Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

**Isomorphism:** corresponding or similar in form and relations.

J

**Jörmungandr** was a node implementation, written in rust, with the initial aim to support the Ouroboros type of consensus protocol. It was repurposed to support Project Catalyst. Jörmungandr refers to the Midgard Serpent in Norse mythology. It is a hint to Ouroboros, the Ancient Egyptian serpent, who eat its own tail, as well as the IOHK paper on proof of stake.

**JSON - JavaScript Object Notation -**  is an open-standard file format that uses human-readable text to transmit data objects consisting of attribute value pairs and array data types (or any other serializable value).

K

**Key pair**: Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security. Within the blockchain, these keys are used to process and authorize transactions*.*

**Kovan** is a Proof of Authority (PoA) publicly accessible blockchain for Ethereum; created and maintained by a consortium of Ethereum developers.

L

**Lambda calculus** (λ-calculus) is a formal system in math logic for expressing computation based on function abstraction and application using variable binding and substitution. It is a universal model of computation that can be used to simulate any Turing machine. It was introduced by the mathematician Alonzo Church in the 1930s as part of his research into the foundations of mathematics.

In the decentralized ecosystem, a **Layer 1** refers to the blockchain protocol itself. **Layer 2** refers to a technology that operates on top of a blockchain to improve its scalability and efficiency. For example, Bitcoin is a Layer 1 network, and the Lightning Network is a Layer 2 to improve transaction speeds. Hydra is a layer 2 protocol built on top of Cardano, layer 1.

**Ledger**: a distributed ledger (also called a shared ledger or referred to as distributed ledger technology) is a consensus of replicated, shared, and synchronized digital data geographically spread across sites, countries, or institutions. There is no central administrator or centralized data storage.

A **light client**, or thin client is a lightweight computer that has been optimized for establishing a remote connection with a server-based computing environment. The server does most of the work, which can include launching software programs, performing calculations, and storing data. This contrasts with a fat client or a conventional personal computer; the former is also intended for working in a client–server model but has significant local processing power, while the latter aims to perform its function mostly locally.

The **Lightning Network** is a Layer 2 payment protocol that operates on top of a blockchain. It theoretically enables fast transactions between participating nodes and has been touted as a solution to the bitcoin scalability problem.

**Liquid democracy** is a form of delegative democracy where an electorate engages in collective decision-making through direct participation and dynamic representation. This democratic system leverages parts of both direct and representative democracy.

The **longest chain** is what individual nodes accept as the valid version of the blockchain. The rule that nodes adopt the longest chain of blocks allows every node on the network to agree on what the blockchain looks like, and therefore agree on the same transaction history. The Longest Chain Rule ensures that the network will recognise the ‘chain with most work’ as the main chain. The chain with the most work is typically (not always) the longest of the forks.

**M**

**Mainnet**: The blockchain that has been deployed and is now in use. Assets stored on the mainnet have value, but assets held on the testnet do not.

A **market maker or liquidity provider** quotes both a buy and a sell price in a financial instrument or commodity held in inventory, hoping to make a profit on the bid-offer spread, or turn. The U.S. Securities and Exchange Commission defines a ‘market maker’ as a firm that stands ready to buy and sell stock on a regular and continuous basis at a publicly quoted price.

**Marlowe** is a programming language created specifically for the creation of financial smart contracts. It is restricted to financial applications and is intended for finance professionals rather than programmers.

**Marlowe Playground:** A browser-based tool for writing and testing Marlowe smart contracts. Its purpose is to encourage developers who have no Haskell or Javascript experience to build financial products on Cardano.

A **maximalist** is a person who holds extreme views and is not prepared to compromise.

Omni (formerly **Mastercoin**) is a digital currency and communications protocol built on the bitcoin blockchain. It is one of several efforts to enable complex financial functions in a cryptocurrency.

The **mempool (memory pool)** is a smaller database of unconfirmed or pending transactions which every node keeps. When a transaction is confirmed by being included in a block, it is removed from the mempool. You can think of a mempool as being like a ‘waiting room’ where a transaction sits before it is added to a block.

A hash tree or **Merkle tree** is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

A **mesh network** is a local area network (LAN) where the nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible. The nodes cooperate with one another to efficiently route data to and from clients.

**Metadata**: a collection of extra data expressing transaction circumstances or owner information. Metadata is used in smart contracts to indicate the circumstances under which a transaction should take place.

The **minimum attack vector** (MAV) is the minimum number of participants required to hijack control in order to attack, or manipulate, the network.

Broadly speaking, **modularity** is the degree to which a system’s components may be separated and recombined, often with the benefit of flexibility and variety in use. The concept of modularity is used primarily to reduce complexity by breaking a system into varying degrees of interdependence and independence across and ‘hide the complexity of each part behind an abstraction and interface.’

**MPC (multi-party computation)** enables multiple parties – each holding their own private data – to evaluate a computation without ever revealing any of the private data held by each party.

**Mt Gox** was a bitcoin exchange based in Tokyo. Launched in 2010, three years later it was handling 70% of all bitcoin transactions worldwide. In February 2014 Mt Gox suspended trading, closed its website and exchange service, and filed for bankruptcy protection from creditors. In April 2014, the company began liquidation proceedings.

A **multi-asset (MA)** ledger can do the accounting for or interact with more than one type of asset. Cardano uses native tokens to provide this feature.

In telecoms and computer networks, **multiplexing** (aka muxing) is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share an expensive resource. For example, in telecoms, several telephone calls may be carried using one wire. Multiplexing originated in the 1870s and is now widely applied in communications.

**Multisignature** (multi-signature) is a digital signature scheme which allows a group of users to sign a single document. Usually, a multisignature algorithm produces a joint signature that is more compact than a collection of distinct signatures from all users. Multisignature can be considered as generalization of both group and ring signatures providing additional security for cryptocurrency transactions.

**N**

**Nash equilibrium** is used in game theory for modeling and defining the solution in a game where players do not cooperate together.

**Network Time Protocol (NTP)** is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.

In telecom networks, a **node** is either a redistribution point or a communication endpoint. The definition of a node depends on the network and protocol layer referred to. A physical network node is an active electronic device that is attached to a network, and is capable of creating, receiving, or transmitting information over a communications channel.

**Non-fungible token (NFT).** Such a token proves ownership of a digital item in the same way that people own crypto coins. However, unlike crypto coins, which are identical and worth the same, an NFT is unique. A craze started with the Christie’s auction of *Everydays: the First 5,000 Days*, a collage of 5,000 digital pieces on March 11, 2021. Mike Winkelmann, known as Beeple, created the digital art and made an NFT of it. Bidding started at $100. It sold for $69.3m. Ten days later, Twitter co-founder Jack Dorsey sold an NFT of the first tweet for 1,630.5 ether ($2.9m) and donated the proceeds to charity. NFT became the Collins Dictionary’s word of the year for 2021. However, when the buyer of Dorsey’s NFT tried to sell it a year later, the highest bid was just $6,800. Ultimately, the value of an NFT is determined solely by what someone is willing to pay for it.

An **NFT drop** is the release of a non-fungible token project. A drop refers to the exact date, time, and generally the minting price of the NFT. Many NFT drops have purchase limits that apply to the number of NFTs you are able to mint in one transaction.

**Nix** is a cross-platform package manager that utilizes a purely functional deployment model. Software is installed into unique directories generated through cryptographic hashes. It is also the name of the tool’s programming language, specifically for software configuration and deployment.

A **nonce** is an arbitrary number that can be used just once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

**Non-Interactive Proofs of Proof-of-Work (NIPoPoWs)** are short stand-alone strings that a computer program can inspect to verify that an event happened on a proof-of-work-based blockchain without connecting to the blockchain network and without downloading all block headers. For example, these proofs can illustrate that a cryptocurrency payment was made.

**O**

**Off-chain code**: The part of a contract application’s code which runs off the chain, usually as a contract application. **On-chain code**: The part of a contract application’s code which runs on the chain (i.e. as scripts).

**Oligarchy**, meaning ‘few’, and ‘to rule or to command’, is a form of power structure in which power rests with a small number of people.

**OG** (crypto Original Gangster) is slang for a founder of any early crypto blockchain such as Vitalik Buterin, who invented Ethereum. A crypto OG can also refer to an early investor in Bitcoin or Ethereum.

**Open-source** software (OSS) is software in which source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose.

**P**

The term **Parallelism** refers to techniques to make programs faster by performing several computations at the same time.

**Parametric insurance** is a type of insurance that does not indemnify the pure loss, but ex-ante (Latin for ‘before the event”) agrees to make a payment upon the occurrence of a triggering event. The triggering event is often a catastrophic natural event which may ordinarily precipitate a loss or a series of losses. But parametric insurance principles are also applied to Agricultural crop insurance and other normal risks not of the nature of disaster, if the outcome of the risk is correlated to a parameter or an index of parameters.

**Pegging** means attaching or tying a currency's exchange rate to another currency

**Peer review** is the evaluation of work by one or more people with similar competences as the producers of the work (peers). It functions as a form of self-regulation by qualified members of a profession within the relevant field. Peer review methods are used to maintain quality standards, improve performance, and provide credibility. In academia, scholarly peer review is used to determine an academic paper's suitability for publication.

**Peer-to-peer (P2P):** distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. In Cardano this involves sending transactions (or files) directly between nodes in a decentralized system without relying on a centralized authority.

**Permissioned v permissionless**. At the simplest level, the distinction lies in whether the design of the network is open for anyone to participate – permissionless – or limited only to designated participants, or permissioned.

**Pledging**: when a stake pool operator assigns their own ada stake to support their stake pool. This provides protection against Sybil attacks by preventing pool owners from creating a large number of pools without themselves owning a lot of stake.

**Plutus:** a Turing-complete programming framework for constructing functional smart contracts. Plutus is a Haskell-based programming language.

**Plutus Core** is the programming language in which scripts on the Cardano blockchain are written. Plutus Core is a small functional programming language — a formal specification is available. Plutus Core is not read or written by humans; it is a compilation target for other languages.

**Plutus Tx**: The libraries and compiler for compiling Haskell into Plutus Core to form the on-chain part of a contract application.

**Polkadot** is a blockchain network being built to enable Web3, a decentralized and fair internet where users control their personal data and markets prosper from network efficiency and security. Polkadot is the flagship project of the Web3 Foundation.

**Polymorphic**: occurring in several different forms. In computing (feature of a programming language) allowing routines to use variables of different types at different times.

**Polymorphism** is the provision of a single interface to entities of different types.

The **Portable Operating System Interface (POSIX)**  is a family of standards specified by the IEEE Computer Society for maintaining compatibility between operating systems. POSIX defines the application programming interface (API), along with command line shells and utility interfaces, for software compatibility with variants of Unix and other operating systems.

**PostgreSQL**, also known as Postgres, is a free and open-source relational database management system emphasizing extensibility and SQL compliance.

**Price discovery** is the process of determining the price of an asset in the marketplace through the interactions of buyers and sellers.

**Profit margin**: The stake pool operator takes a portion of total ada rewards before dividing the remainder of the rewards with all of the pool’s delegators. If the operator’s profit margin is low, they’re taking less risks, which means delegators should anticipate reaping more of the rewards for their delegated stake. A private pool is one with a profit margin of 100%, indicating that the operator receives all of the rewards and the delegators get none.

**Programmability** is the capability within hardware and software to change; to accept a new set of instructions that alter its behavior. Programmability generally refers to program logic (business rules), but it also refers to designing the user interface, which includes the choices of menus, buttons and dialogs.

**Proof of stake (PoS)** is a type of algorithm by which a cryptocurrency blockchain network aims to achieve consensus. In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and funds committed (ie, the **stake**). In contrast, the algorithm of **proof-of-work**-based (PoW) cryptocurrencies such as bitcoin uses mining; that is, the solving of computationally intensive puzzles to validate transactions and create blocks.

**Project Catalyst** is a series of experiments that seek to encourage the highest levels of community innovation. Catalyst is bringing on-chain governance to Cardano by allowing the community to determine priorities for growth.

**Proxy signature** is a special type of digital signature which allows one user (original signer) to delegate his/her signing right to another signer (proxy signer). The latter can then issue signatures on behalf of the former.

**Public-key cryptography**, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

**Pull requests** are a feature specific to GitHub. They provide a simple, web-based way to submit your work (often called “patches”) to a project. It's called a pull request because you're asking the project to pull changes from your fork.

A **pure function** is a function that has the following properties: first, its return value is the same for the same arguments (no variation with local static variables, non-local variables, mutable reference arguments or input streams from input-output devices); second, its evaluation has no side effects (no mutation of local static variables, non-local variables, mutable reference arguments or inputs and outputs).

R

**RAM (random-access memory)** is a form of computer memory that can be read and changed in any order, typically used to store working data and machine code. A random-access memory device allows data items to be read or written in almost the same amount of time irrespective of the physical location of data inside the memory.

**Raspberry Pi**: computer on a credit-card-sized board. Idea developed by Eben Upton and others from Cambridge University’s Computer Lab and launched by their Raspberry Pi Foundation. Taking inspiration from the 1980s BBC Computer Literacy Project, the single-board computer running Linux with open-source software was launched in 2012 costing £22 to encourage computing in schools and the developing world.

**Recursion** occurs when something is defined in terms of itself or of its type. Recursion is used in a variety of disciplines ranging from linguistics to logic. The most common application of recursion is in mathematics and computer science, where a function being defined is applied within its own definition. While this apparently defines an infinite number of instances (function values), it is often done in such a way that no infinite loop can occur.

**Redeemer**: The argument to the validator script which is provided by the transaction which spends a script output.

**Regression testing** is re-running tests to ensure that previously developed and tested software is performing as expected after a change.

**Resident set size (RSS)** is the portion of memory occupied by a process that is held in main memory (RAM).

**Reward**:an amount contained in each new block that is paid out to the stakeholder by the network.

Coined by Vitalik Buterin, who led the creation of Ethereum, the **‘blockchain trilemma**’ sets out the challenges developers face in creating a blockchain that is scalable, decentralized and secure, without compromising on any facet. Blockchains are forced to make trade-offs between these three aspects:

* decentralization: creating a blockchain system that does not rely on a central point of control.
* scalability: the ability of a blockchain to handle a growing number of transactions.

security: the ability of a blockchain to operate as expected, and defend itself from attacks, bugs, and other unforeseen issues.

**Rewards Wallet:** a wallet that contains ada and may be used to delegate stakes. A stake may only be delegated to a single stake pool from a single Rewards wallet. You’ll need to construct numerous Rewards wallets and divide ada across them if you want to delegate to more than one stake pool. Split pool delegation has been promised by IOG for some time but has been postponed, to allow focusing resources on other roadmap priorities.

The **Ring of Gyges** is a mythical, magical artifact mentioned by the philosopher Plato in his *Republic*. It grants its owner the power to become invisible at will. Through the story of the ring, *Republic* considers whether an intelligent person would be just, if they did not have to fear reputational damage if they committed injustices.

**RootStock** is a smart-contract peer-to-peer platform built on top of the Bitcoin blockchain. Its goal is to add value and functionality to the core Bitcoin network by the implementation of smart contracts as a sidechain.

**Rust** is a lightweight, portable programming language from Mozilla that compiles to the web, iOS and Android. Rust is a multi-paradigm, general-purpose language designed for performance and safety, especially safe concurrency.

**S**

**Saturation**: a stake pool is saturated when it has more stake delegated to it than is optimal for the network. The saturation level is expressed as a percentage. When a stake pool achieves 100% saturation, the rewards start to shrink. The saturation mechanism was created to avoid centralization by encouraging ada owners to delegate to several stake pools, and operators to build more pools to keep receiving maximum rewards. Saturation aims to safeguard both the interests of ada holders delegating their stake and the interests of stake pool operators (SPOs).

The Boolean satisfiability problem (abbreviated **SATISFIABILITY** or **SAT**) is the problem of determining if there exists an interpretation that satisfies a given Boolean formula. It asks whether the variables of a given Boolean formula can be consistently replaced by the values TRUE or FALSE in such a way that the formula evaluates to TRUE. If this is the case, the formula is called satisfiable. On the other hand, if no such assignment exists, the function expressed by the formula is FALSE for all possible variable assignments and the formula is unsatisfiable.

**Satisfiability modulo theories (SMT)** is the problem of determining whether a mathematical formula is satisfiable. It generalizes the Boolean satisfiability problem (SAT) to more complex formulas involving real numbers, integers, and/or various data structures such as lists, arrays, bit vectors, and strings. The name is derived from the fact that these expressions are interpreted within (‘modulo’) a certain formal theory in first-order logic with equality (often disallowing quantifiers). **SMT solvers** are tools which aim to solve the SMT problem for a practical subset of inputs.

A **script** is a generic term for an executable program used in the ledger. In the Cardano blockchain, these are written in Plutus Core.

A **script output**: A UTXO locked by a script.

The **semantic gap** characterizes the difference between two descriptions of an object by different linguistic representations, for instance languages or symbols. According to Hein, the semantic gap can be defined as "the difference in meaning between constructs formed within different representation systems". In computer science, the concept is relevant whenever ordinary human activities, observations, and tasks are transferred into a computational representation.

**Separation of concerns** is a design principle for separating a computer program into distinct sections, so that each section addresses a separate concern. A concern is a set of information that affects the code of a computer program.

A **server** is a computer program or device that provides a service to another computer program and its user, also known as the client.

A **Sidechain** is a blockchain that runs in parallel to the main blockchain. Tokens can be transferred and synchronized between the main chain and the sidechain.

**Slashing** is a mechanism used by some PoS protocols (but not Cardano) to discourage harmful behavior and make validators more responsible. They help keep the network secure because, without slashing penalties, a validator can use the same node to validate blocks on more than one chain or do so on the wrong chain.

**Slot**: Within an epoch, a set duration of time. Time is separated into numbered slots for each epoch. Active slots are those that are occupied by blocks.

**Slot leader**: an elected node that has been chosen to construct a block in the current slot. An arbitrary election takes place based on the proportionate stake.

A **smart contract** is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts were first proposed by Nick Szabo in 1996. Proponents of smart contracts claim that many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim with smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting.

**SNARK** stands for ‘Succinct Non-Interactive Argument of Knowledge.’ A (zero knowledge) zk-SNARK is a cryptographic proof that allows one party to prove it possesses certain information without revealing that information. This proof is made possible using a secret key created before the transaction takes place.

**Solidity** is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum.

**Sound money** is money that is not liable to sudden appreciation or depreciation in value.

**Stablecoins** are cryptocurrencies designed to minimize the volatility of its price, relative to some ‘stable’ asset or a basket of assets. A stablecoin can be pegged to another cryptocurrency, fiat money, or to exchange-traded commodities. Stablecoins redeemable in currency, commodities, or fiat money are said to be backed, whereas those tied to an algorithm are referred to as seigniorage-style (not backed).

**Stake pool**:a stable, block-producing server node that aggregates the stakes of several stakeholders (in Cardano’s case, ada holders) into a single entity, or pool.

**Staking** involves holding funds in a cryptocurrency wallet to support the security and operations of a blockchain network, and in return receive staking rewards. In other words, staking is the process of actively participating in transaction validation (similar to mining) on a proof-of-stake (PoS) blockchain.

**State channels** refer to the process in which users transact with one another directly outside of the blockchain, or 'off-chain,' and greatly minimize their use of 'on-chain' operations.

**Stateful** services keep track of sessions or transactions and react differently to the same inputs based on that history. **Stateless** services rely on clients to maintain sessions and center around operations that manipulate resources, rather than the state.

**Segregated Witness,** or SegWit, is the name used for an implemented soft fork change in the transaction format of bitcoin.

A **semaphore** is a variable, or abstract data type, used to control access to a common resource by multiple threads and avoid critical section problems in a concurrent system such as a multitasking operating system. Semaphores are a type of synchronization primitives. A trivial semaphore is a plain variable that is changed depending on programmer-defined conditions.

In the context of data storage, **serialization** is the process of translating data structures or object state into a format that can be stored (for example, in a file or memory buffer) or transmitted (for example, across a network) and reconstructed later (possibly on a different computer). When the resulting series of bits is reread according to the serialization format, it can be used to create a semantically identical clone of the original object.

**Sharding** splits a blockchain company’s entire network into smaller partitions, known as ‘shards.’ Each shard consists of its own data, making it distinctive and independent when compared to other shards.

**Slippage** refers to the difference between the expected price of a trade and the price at which the trade is executed. Slippage can occur at any time but is most prevalent during periods of higher volatility when market orders are used.

**Spot trading** is a continuous process of buying and selling tokens and coins at a spot price for immediate settlement. The trader usually intends to gain profits from market fluctuations.

In telecommunication and radio communication, **spread-spectrum techniques** are methods by which a signal generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

**Stack Overflow** is a question-and-answer site for professional and enthusiast programmers. It is a privately held website, the flagship site of the Stack Exchange Network, created in 2008 by Jeff Atwood and Joel Spolsky.

**Static analysis**, static projection, or static scoring is a simplified analysis wherein the effect of an immediate change to a system is calculated without regard to the longer-term response of the system to that change. **Static analysis is** a simplified analysis wherein the effect of an immediate change to a system is calculated without regard to the longer-term response of the system to that change. If the short-term effect is then extrapolated to the long term, such extrapolation is inappropriate.

A **stiftung** is a foundation which exists to give effect to the stated, non-commercial wishes of its founder, as set out in a foundation deed and the articles of association (statutes).

In a **Sybil attack**, the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence. It is named after the subject of the book *Sybil*, a case study of a woman diagnosed with dissociative identity disorder.

In a **synchronous system**, operations are coordinated by one, or more, centralized clock signals. An asynchronous digital system, in contrast, has no global clock. Asynchronous systems do not depend on strict arrival times of signals or messages for reliable operation. Coordination is achieved via events such as: packet arrival, changes (transitions) of signals, handshake protocols, and other methods.

**T**

**Terra (LUNA)** is a Decentralized system focused on enhancing the DeFi space through programmable payments to drive adoption. The Protocol has a native Token, LUNA, and is backed by a host of fiat-pegged Stablecoin. By employing Stablecoin, Terra presents a payment infrastructure void of the shortcomings of traditional payment methods such as Credit card and old Blockchain-based payment systems.

A **testnet** is an alternative blockchain used by software developers to check that their code runs properly before they make possibly costly deployments to a **mainnet**. The testnet uses identical technology and software as the ‘mainnet’ blockchain, in other words a parallel network, except the testnet doesn’t make ‘actual’ transactions with ‘value’ and is intended for testing purposes. Testnet coins are distinct from actual coins on a mainnet, as testnet coins do not have any monetary value.

**Tether** (ticker USDT) is a cryptocurrency that is hosted on the Ethereum and Bitcoin blockchains, among others. Its tokens are issued by the Hong Kong company Tether Limited, which in turn is controlled by the owners of Bitfinex. Tether is called a stablecoin because it was originally designed to always be worth US$1.00, maintaining $1.00 in reserves for each tether issued.

**Tezos** (ticker: XTZ) is a decentralized blockchain founded by Arthur Breitman and Kathleen Breitman. The Breitmans also founded Dynamic Ledger Solutions (DLS), a company primarily focused on developing Tezos technology and owns the Tezos Intellectual property. The currency was launched in an initial coin offering (ICO) on July 1, 2017.

**TLA⁺** is a formal specification language developed by Leslie Lamport. It is used for designing, modeling, documentation, and verification of programs, especially concurrent systems and distributed systems

**Token:** A cryptographic token that reflects the value as defined by the community, market state, or self-governed entity. A fungible or non-fungible token may be used as a payment unit, a reward, a trade asset, or a data holder.

A **toolchain** is a set of programming tools that is used to perform a complex software development task or to create a software product, which is typically another computer program or a set of related programs.

The **tragedy of the commons** is a situation in a shared-resource system where individual users, acting independently according to their own self-interest, behave contrary to the common good of all users, by depleting or spoiling that resource through their collective action.

**Transaction output:** Outputs produced by transactions. They are consumed when they are spent by another transaction. Typically, some kind of evidence is required to be able to spend a UTXO, such as a signature from a public key, or (in the Extended UTXO Model) satisfying a script.

The **Transmission Control Protocol (TCP)** is one of the main protocols of the **Internet Protocol (IP)** suite. Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World-Wide Web, email, and file transfer rely on TCP.

A system is said to be **Turing complete** if it can be used to simulate any Turing machine. This means that this system is able to recognize or decide other data-manipulation rule sets. Turing completeness is used as a way to express the power of such a data-manipulation rule set. Virtually all programming languages today are Turing complete. The concept is named after English mathematician and computer scientist Alan Turing.

A **Turing machine** is a mathematical model of computation that defines an abstract machine, which manipulates symbols on a strip of tape according to a table of rules. Despite the model’s simplicity, given any computer algorithm, a Turing machine capable of simulating that algorithm’s logic can be constructed.

**Transport Layer Security (TLS)** and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a computer network.

The **Travel Rule** requires parties to obtain and exchange beneficiary and originator information with virtual assets transfers over a certain threshold.

**Tricameralism** is the practice of having three legislative or parliamentary chambers. It is contrasted with unicameralism and bicameralism, each of which is far more common

The **(TVL) Total Value Locked** into a smart contract or set of smart contracts that may be deployed or stored at one or more exchanges or markets. This is used as a measurement of investor deposits. It is the dollar value of all the coins or tokens locked into a platform, protocol, lending program, yield farming program, or insurance liquidity pool.

**U**

**ulimit** is a built-in Linux shell command that allows viewing or limiting system resource amounts that individual users consume. Limiting resource usage is valuable in environments with multiple users and system performance issues.

**Uniswap** is a Decentralized Exchange (DEX) built on Ethereum that utilizes an automated market-making system instead of a traditional order-book. It was inspired by a Reddit post from Vitalik Buterin and was founded by Hayden Adams in 2017.

The framework of **universal composability** is a general-purpose model for the analysis of cryptographic protocols. It guarantees very strong security properties. Protocols remain secure even if arbitrarily composed with other instances of the same or other protocols. Security is defined in the sense of protocol emulation. Intuitively, a protocol is said to emulate another one, if no environment (observer) can distinguish the executions. Literally, the protocol may simulate the other protocol (without having access to the code). The notion of security is derived by implication.

An **unspent transaction output (UTXO)** is the technical term for the amount of digital currency that remains after a cryptocurrency transaction. The **Unspent Transaction Output (UTXO)** model is commonly used in the field of Distributed Ledger Technology (DLT) to transfer value between participants. A UTXO is the technical term for the amount of digital currency that remains after a cryptocurrency transaction. You can think of it as the change you receive after buying an item.

**Utility token:** a digital token that represents a certain project or environment and has specific capabilities. These tokens may be used as payment units, prizes, or as a means of gaining entry to a particular network.

**UTXO congestion**: The effect of multiple transactions attempting to spend the same transaction output.

The **UTXO set** is the comprehensive set of all UTXOs existing at a given point in time. The sum of the amounts of each UTXO in this set is the total supply of existing currency at that point of time. Anyone can verify the total supply at any time in a trustless manner.

**V**

A **validator script** is the script attached to a script output in the Extended UTXO model. Must be run and return positively in order for the output to be spent. It determines the address of the output.

**Validation context**: A data structure containing a summary of the transaction being validated, and the current input whose validator is being run.

In cryptography, a **verifiable-random function (VRF)** is a pseudo-random function that provides publicly verifiable proofs of its outputs’ correctness.

**W**

**Wanchain**, the Wide Area Network chain, is an interoperability solution with a mission to drive blockchain adoption through crosschain interoperability by building fully decentralized bridges that connect siloed blockchain networks

A cryptocurrency **wallet** stores the public and private keys which can be used to receive or spend a cryptocurrency. A wallet can contain many public keys but only one private key, which must be kept safe from loss or theft. Once a private key is lost that ends the life of that wallet. The cryptocurrency itself is not in the wallet. The cryptocurrency is decentrally stored and maintained in a publicly available ledger called the blockchain. Every piece of cryptocurrency has a private key. With the private key, it is possible to digitally sign a transaction and write it in the public ledger, in effect spending the associated cryptocurrency.

**Web 2.0** allows anyone to create content but centralises authorities and gatekeepers, such as major search engines and social

**Web3** (also known as Web 3.0) is an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics

**WebSocket** is a communications protocol, providing full-duplex communication channels over a single TCP connection.The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.

***Why Cardano?*** The original essay from 2017 outlining the background, philosophy and inspiration behind the Cardano blockchain. By Charles Hoskinson. See: why.cardano.org/

**Y**

**Yield farming** is a DeFi term for leveraging DeFi protocols and products to generate high returns that sometimes reach over 100% in annualized yields 'when factoring in interest, token rewards, ‘cashback’ bonuses, and other incentives.' Yield farming is a way for cryptocurrency enthusiasts to maximize their returns. It typically involves users lending or locking up their funds using smart contracts. In return, users earn fees in the form of crypto.

johns