INTRODUCTION TO CONSENSUS MECHANISMS

Jianing Wu — Senior Analyst, Research
08/23/2021

A decentralized system implies that no single participant has control over the system's rules, inputs and outputs. Security therefore becomes the biggest challenge to any decentralized system. This is especially true when participants don't trust each other and the system provides a record of transactions that ascribe value (like on a public blockchain).

Without third-party verification, how can participants validate transactions and prevent malicious actors from inserting fake and fraudulent information?

Satoshi Nakamoto provided a solution to this question by combining various ideas to create a distributed, immutable and cryptographic ledger of transactions. At its core is the proof-of-work consensus mechanism—a way to verify transactions by proving to others that considerable computing efforts were spent for the information to be appended to the ledger.

What's a Consensus Mechanism?

A consensus mechanism is an algorithm to approve transactions or records onto a decentralized ledger such that fake or fraudulent records are rejected.

The algorithm is run when new blocks are being appended to the existing chain of blocks, which is how the blockchain gets updated as an append-only ledger.

The idea is that by imposing a requirement of certain effort spent (or risk taken), malicious actors would refrain from tampering with the ledger, as they deem the effort (or loss) to be unprofitable. The very first purpose of proof of work's invention was to filter email spam.

Hashcash, a proof-of-work system proposed by Adam Back in 1997, requires email senders to create and attach stamps on email headers to prove to receivers that they spent CPU power to generate emails. These stamps are one-way encryption algorithms that are easy to verify by the receiver but hard (in computing terms) to generate by the sender. In this model, spammers would be reluctant to send out large quantities of email, as it becomes unprofitable to use a large amount of CPU power to create stamps. However, the price of sending a single email is still affordable by regular users.

Since consensus mechanisms in the blockchain world are generally referred to as activities of "mining" and "staking," they are frequently regarded as methods to issue new coins. However, their primary purpose is to secure the decentralized network, whereas rewards in the form of coins are an added economic incentive for workers to maintain the network.

Comparison of Major Consensus Mechanisms					
	Invented Year	Nouns	Pros	Cons	Blockchain
Proof-of-Work (PoW)	1993	mining | miners	• secure • simple • relatively long history	• energy intensive • susceptible to be centralized	Bitcoin, Litecoin, Ethereum (up to Serenity)
Proof-of-Stake (PoS)	2012	minting | validators	• energy efficient • less centralized • better designed for attack recovery	• shorter track record • nothing-at-stake problem • long-range attacks	Ethereum (planned to be implemented in Serenity), Cardano
Delegated Proof-of-Stake (DPoS)	2014	minting | witnesses, delegates	• same as PoS • but more democratic • faster	• susceptible to be centralized	Bitshares, Steemit, Ark, Lisk

Various Consensus Mechanisms (detailed explanations can be found *here*)

Major consensus mechanisms include proof-of-work (PoW), proof-of-stake (PoS) and delegated proof-of-stake (DPoS).

PoW is the oldest consensus mechanism. It accounts for more than 75% of the market cap of blockchain protocols. It is used by Bitcoin, Ethereum (up to Serenity), Litecoin, and others.

In PoW, miners append new blocks with transaction information to existing blocks (called **mining**) by finding a random number (called **nonce**) that can be run through a universal encrypting function to the network (called **hash**) and can satisfy a difficulty requirement. This consists of the process of "solving" the mathematical task, which demands considerable energy and effort.

PoS, on the other hand, doesn't require participants to use computing power to hash blocks and solve a mathematical requirement, but it requires them to stake ether. Participants are randomly selected to become block validators based on their wealth, and validators need to stake an amount of cryptocurrency that covers the transaction fee and their potential reward until the block is successfully appended. If inconsistent, absent and abnormal behaviors are detected, dishonest participants could lose their stakes and be banned from the network.

DPoS is a variation of PoS. It changes the selection process in PoS from randomized algorithms to a more democratic approach, allowing stakers to vote for their representatives, who would carry out the validation act.

Besides PoW, PoS and DPoS, there are many proof-of-X mechanisms that try to establish a decentralized and secure network. They include proof-of-capacity, proof-of-elapsed-time time and proof-of-importance, etc.

Another major family of consensus mechanisms is Byzantine Fault Tolerance. It has several variations, such as practical Byzantine Fault Tolerance (pBFT), which is currently used by Hyperledger Fabric. pBFT's improved version is used by the People's Bank of China (PBoC) to develop its Central Bank Digital Currency (CBDC). Another variation is called delegated Byzantine Fault Tolerance (dBFT), which is used by Neo. The Stellar network's model of consensus leverages a federated Byzantine agreement (FBA) model, and it seeks to establish upon these models to build an open network for storing and moving money.

Conclusion

The consensus mechanism is a key component to a decentralized network. It not only secures the system but also affects its efficiency and scalability.

Since Bitcoin's birth, there have been many other consensus mechanisms created. Each of them has its own characteristics that determine the associated network's attributes. To learn more about them and how they differ, you can read more *here*.

Important Risks Related to this Article

There are risks associated with investing, including the possible loss of principal. Crypto assets, such as bitcoin and ether, are complex, generally exhibit extreme price volatility and unpredictability, and should be viewed as highly speculative assets. Crypto assets are frequently referred to as crypto "currencies," but they typically operate without central authority or banks, are not backed by any government or issuing entity (i.e., no right of recourse), have no government or insurance protections, are not legal tender and have limited or no usability as compared to fiat currencies. Federal, state or foreign governments may restrict the use, transfer, exchange and value of crypto assets, and regulation in the U.S. and worldwide is still developing.

Crypto asset exchanges and/or settlement facilities may stop operating, permanently shut down or experience issues due to security breaches, fraud, insolvency, market manipulation, market surveillance, KYC/AML (know your customer / Anti-Money Laundering) procedures, non-compliance with applicable rules and regulations, technical glitches, hackers, malware or other reasons, which could negatively impact the price of any cryptocurrency traded on such exchanges or reliant on a settlement facility or otherwise may prevent access or use of the crypto asset.

Crypto assets can experience unique events, such as forks or airdrops, which can impact the value and functionality of the crypto asset. Crypto asset transactions are generally irreversible, which means that a crypto asset may be unrecoverable in instances where: (i) it is sent to an incorrect address, (ii) the incorrect amount is sent, or (iii) transactions are made fraudulently from an account. A crypto asset may decline in popularity, acceptance or use, thereby impairing its price, and the price of a crypto asset may also be impacted by the transactions of a small number of holders of such crypto asset. Crypto assets may be difficult to value and valuations, even for the same crypto asset, may differ significantly by pricing source or otherwise be suspect due to market fragmentation, illiquidity, volatility and the potential for manipulation. Crypto assets generally rely on blockchain technology and blockchain technology is a relatively new and untested technology which operates as a distributed ledger.

Blockchain systems could be subject to internet connectivity disruptions, consensus failures or cybersecurity attacks, and the date or time that you initiate a transaction may be different then when it is recorded on the blockchain. Access to a given blockchain requires an individualized key, which, if compromised, could result in loss due to theft, destruction or inaccessibility. In addition, different crypto assets exhibit different characteristics, use cases and risk profiles.

Information provided by WisdomTree regarding digital assets, crypto assets or blockchain networks should not be considered or relied upon as investment or other advice, as a recommendation from WisdomTree, including regarding the use or suitability of any particular digital asset, crypto asset, blockchain network or any particular strategy. WisdomTree is not acting and has not agreed to act in an investment advisory, fiduciary or quasi-fiduciary capacity to any advisor, end client or investor, and has no responsibility in connection therewith, with respect to any digital assets, crypto assets or blockchain networks.

For standardized performance and the most recent month-end performance click here NOTE, this material is intended for electronic use only. Individuals who intend to print and physically deliver to an investor must print the monthly performance report to accompany this blog.

View the online version of this article here.

IMPORTANT INFORMATION

U.S. investors only: Click here to obtain a WisdomTree ETF prospectus which contains investment objectives, risks, charges, expenses, and other information; read and consider carefully before investing.

There are risks involved with investing, including possible loss of principal. Foreign investing involves currency, political and economic risk. Funds focusing on a single country, sector and/or funds that emphasize investments in smaller companies may experience greater price volatility. Investments in emerging markets, currency, fixed income and alternative investments include additional risks. Please see prospectus for discussion of risks.

Past performance is not indicative of future results. This material contains the opinions of the author, which are subject to change, and should not to be considered or interpreted as a recommendation to participate in any particular trading strategy, or deemed to be an offer or sale of any investment product and it should not be relied on as such. There is no guarantee that any strategies discussed will work under all market conditions. This material represents an assessment of the market environment at a specific time and is not intended to be a forecast of future events or a guarantee of future results. This material should not be relied upon as research or investment advice regarding any security in particular. The user of this information assumes the entire risk of any use made of the information provided herein. Neither WisdomTree nor its affiliates, nor Foreside Fund Services, LLC, or its affiliates provide tax or legal advice. Investors seeking tax or legal advice should consult their tax or legal advisor. Unless expressly stated otherwise the opinions, interpretations or findings expressed herein do not necessarily represent the views of WisdomTree or any of its affiliates.

The MSCI information may only be used for your internal use, may not be reproduced or re-disseminated in any form and may not be used as a basis for or component of any financial instruments or products or indexes. None of the MSCI information is intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such. Historical data and analysis should not be taken as an indication or guarantee of any future performance analysis, forecast or prediction. The MSCI information is provided on an "as is" basis and the user of this information assumes the entire risk of any use made of this information. MSCI, each of its affiliates and each entity involved in compiling, computing or creating any MSCI information (collectively, the "MSCI Parties") expressly disclaims all warranties. With respect to this information, in no event shall any MSCI Party have any liability for any direct, indirect, special, incidental, punitive, consequential (including loss profits) or any other damages (www.msci.com)

Jonathan Steinberg, Jeremy Schwartz, Rick Harper, Christopher Gannatti, Bradley Krom, Tripp Zimmerman, Michael Barrer, Anita Rausch, Kevin Flanagan, Brendan Loftus, Joseph Tenaglia, Jeff Weniger, Matt Wagner, Alejandro Saltiel, Ryan Krystopowicz, Jianing Wu, and Brian Manby are registered representatives of Foreside Fund Services, LLC.

WisdomTree Funds are distributed by Foreside Fund Services, LLC, in the U.S. only.

You cannot invest directly in an index.

DEFINITIONS

Blockchain : a distributed ledger system in which a record of transactions made in cryptocurrencies are maintained across computers linked in a peer-to-peer network

Proof of Work (PoW) : A system that requires a not-insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks.

Proof of Stake (PoS) : The Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins they hold

Delegated Proof of Stake : A consensus algorithm developed to secure a blockchain by ensuring representation of transactions within it. DPoS is designed as an implementation of technology-based democracy, using voting and election process to protect blockchain from centralization and malicious usage.

Bitcoin (the currency) : A digital currency (also called a cryptocurrency) created in 2009, which is operated by a decentralized authority as opposed to a traditional central bank or monetary authority.

Proof of Capacity (PoC) : Proof of capacity (PoC) is a consensus mechanism algorithm used in blockchains that allows for mining devices in the network to use their available hard drive space to decide mining rights and validate transactions.

Proof of Elapsed Time (PoET) : Proof of elapsed time (PoET) is a blockchain network consensus mechanism algorithm that prevents high resource utilization and high energy consumption and keeps the process more efficient by following a fair lottery system.

Proof of Importance (PoI) : Proof of importance (PoI) is a cryptocurrency term defined as a blockchain consensus technique – essentially, proof of importance works to prove the utility of nodes in a cryptocurrency system, so that they can create blocks.