CONSENSUS PROTOCOLS

Our definitive guide to consensus protocols

COIN RIVET

Independent British blockchain and crypto news

CONTENTS

WHAT CONSENSUS IS IN CRYPTOCURRENCY

Blockchains are an incentivised distributed ledger using a plurality of technologies ranging from decentralised communications protocols, storage protocols and consensus mechanisms. In this guide, we explain how different Blockchain consensus algorithms work, their benefits and risks, and some examples of prominent cryptocurrencies using each alternative consensus mechanic.

Consensus happens when a network of nodes ensures the block in a blockchain is accurate – and the only version of the truth. This helps to support the decentralised natures of many cryptocurrencies and prevents individuals from hacking the system or making any alterations.

The terminology used throughout this guide is most frequently used when discussing the successful mining of cryptocurrency.

Blockchain consensus algorithms are paramount to verifying the authenticity of distributed blockchain platforms and are the process of building agreement among a network of mutually distrusting participants.

What's needed for consensus to work?

In order for a blockchain to properly work, nodes need to reach consensus on the state of transactions and blocks. Mostly, transactions are either accepted, rejected, or left pending. Consensus algorithms allow nodes (and mining hardware/software) to agree on:

1. Transaction data such as amounts and addresses
2. Block state, meaning if a certain block is valid or invalid

In essence, consensus refers to the set of rules that govern the consensus mechanism and ensure its trustless nature. A consensus protocol has three key properties on which its applicability and efficacy can be determined.

- Safety: a consensus protocol is determined to be safe if all nodes produce the same output and the outputs produced by the nodes are valid according to the rules of the protocol. This is also referred to as consistency of the shared state.
- Liveness: a consensus protocol guarantees liveness if all non-faulty nodes participating in consensus eventually produce a value.

- Fault tolerance: a consensus protocol provides fault tolerance if it can recover from failure of a node participating in consensus.

Before we dive-deep into each alternative consensus algorithm, it's important to understand that each is linked to a governance model. The two most common are:

- Decentralised governance models where the community participates in the decision-making process. This is achieved by either committing code to the software in order to improve the consensus mechanics, or simply by transacting in the network. Some of the oldest cryptocurrencies that fall under this category are Bitcoin, Litecoin and Dogecoin.
- Centralised governance models which are usually represented by federated consensus. A party composed of trusted institutions, ranging from for-profit companies and non-profit organisations to financial institutions, have the power to control the network, transactions and overall consensus mechanics. There are a variety of top-10 projects that fall under this category including Stellar Lumens, Ripple and Bitcoin Cash.

DIFFERENT CONSENSUS ALGORITHMS EXPLAINED

There are three main consensus mechanisms.

1. **Proof-of-Work (PoW)** based on cryptographic calculations that require miners to spend energy to solve computational problems in order to find a hash. The longer the hash, the more secure it is.
2. **Proof-of-Stake (PoS)** based on each participant stake. The PoS requires participants to stake some of their tokens in order to become network validators. PoS is seen to have two main issues. The first is the nothing at stake problem, where participants can't lose their stake even if they voted for all blocks and did not follow the protocol rules. The second is the fact the network is prone to more centralisation as there is no mining. Both problems get addressed in alternative PoS versions discussed below.
3. **Delegated Byzantine Fault Tolerance (DBFT)** based on a federated consensus, meaning the network reaches consensus through the agreement from a number of central authority nodes.

   Although this consensus algorithm allows scalable solutions to be built on top, it decreases security and user privacy as the network is not truly decentralised and has central points of failure.

Each consensus mechanic has a different purpose, usually connected to either enabling security + privacy, scalability + security or privacy + scalability.

Below, we explain each blockchain consensus algorithm, as well as what it promotes.

	POW	POS	DBFT
Security	Yes	No	Yes
Scalability	No	Yes	Yes
Privacy	Yes	Yes	No

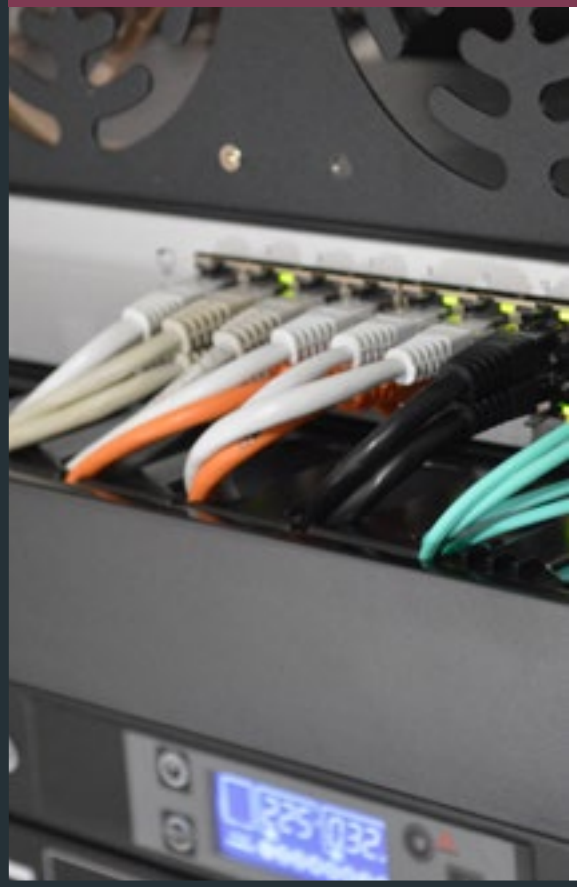
Examples and variants

There are already pluralities of cryptocurrencies with different consensus protocols implemented and fully functional. Below, we list the most used according to each user-base and marketcap.

	POW		PoS			DBFT	
	PoA	DPoW	PoB	PoeT/PoA/PoI	DPos	PBFT	FBA
Security	Yes	Yes	Yes	No	No	No	Yes
Scalability	No	Yes	Yes	Yes	Yes	Yes	Yes
Privacy	Yes	No	Yes	Yes	No	No	No
Project	Decred	Komodo	Slimcoin	POET/POA/NEM	EOS/Steemit	HyperLedger	Stellar/ Ripple

PROOF-OF-WORK EXPLAINED

Proof-of-Work is a consensus protocol used by Bitcoin and many other cryptocurrencies to validate the transactions that occur in their networks. This protocol is used by **miners** to confirm transactions and add new blocks to the chain.



While we'll be reading about the proof-of-work breakthrough for years to come, the truth is that the technologies that **Satoshi** combined to create a blockchain-based currency already existed.

A **blockchain** is a decentralised, trusted ledger of transactions which occur within a network, and are validated by a network of separately-owned computers using a cryptographic protocol to assess the accuracy of the data contained on the ledger. The real innovation behind Bitcoin lies in the integration of three separate technologies: a decentralised ledger, cryptographic keys, and the protocol known as PoW. .

How does Proof-of-Work actually work?

If you receive one Bitcoin, that transaction is registered on a block with other transactions. It's communicated to the decentralised network where different machines or miners employ their computing power to validate it (along with the rest of the block).

The network nodes validate the information by competing among themselves to find the solution to increasingly more complex mathematical riddles. They present solutions on a trial-and-error basis until one finds the correct number and communicates it to the remaining machines. When a majority of nodes agree that one miner has solved the problem, a consensus is achieved.

For this work, the miner receives a reward in the form of transaction fees and the block of transactions is added to the decentralised, shared ledger where it becomes an immutable part of the blockchain. When these different nodes compete until they reach a solution on which the whole network agrees, they use up a lot of computational power, energy, and time. As the problems increase in complexity, so do these costs, which provides a further incentive not to cheat the system. Why would you go through all the effort and cost of investing in powerful computers to then miss out on the rewards?

The PoW protocol that allows for this validation is brilliant in its inception because it relies on human self-interest to guarantee the integrity of the blockchain. PoW exists so that transactions can't be falsified.

Variations of Proof-of-Work

The PoW group has two main variations, **Proof-Of-Authority and Delegated PoW.** Each has its own merits and drawbacks. While the first cannot properly allow for a huge network to scale as mining is still a requirement, the second promotes scalability by taking away some decentralisation features.

In both, there is a cost associated to electricity, however in the latter that cost may be linked to an underlying protocol. For example Komodo uses Bitcoin's blockchain to guarantee its networks security by connecting its blocks to Bitcoin's blockchain's hash.

Why does Proof-of-Work consensus matter?

PoW is essential because it allows for trust in a trustless environment. The capability to generate blocks of transactions is a display of computational power that blockchains need to validate the information they contain.

When miners agree to compete for the reward for getting the next block right, they implicitly also agree to abide by the rules of that community of nodes, instead of manipulating the blockchain for their own nefarious purposes.

By increasing the difficulty of verifying each block, Proof-of-Work ensures excessive mining doesn't take place. This preserves the supply of that cryptocurrency while incentivising miners to keep the network running.

Since it uses limited resources like time, computational strength, and energy, proof of work isn't infinitely scalable, which raises some issues. As an example, it's estimated that the electricity used in validating one Bitcoin transaction could power the average Dutch household for two weeks.

An alternative to tackle the resource inefficiencies inherent to this protocol is the Proof-of-Stake (PoS) consensus mechanism. In PoS, the network values seniority and investment in the cryptocurrency over computational power. Since every time a new block is created the miner has to trade in old units of that crypto for new ones, that miner will be in a weaker position to create the next block.

This ensures a continual turnover in who gets to mine each block while also incentivising the trustworthiness of that crypto by making the largest holders an integral part of the process.

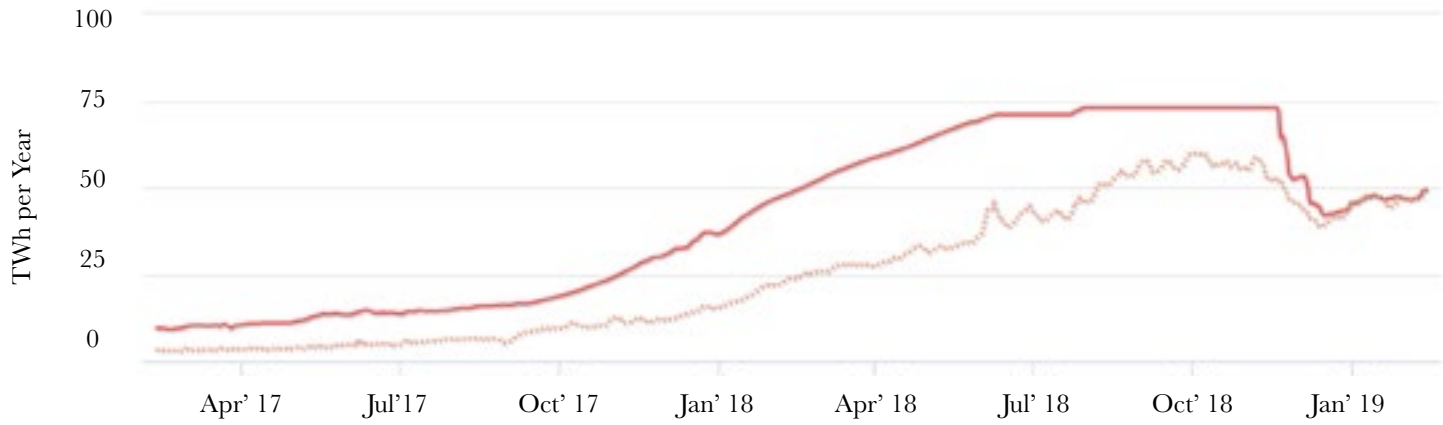
ARGUMENTS AGAINST PROOF-OF-WORK

One of the most debated topics in the cryptocurrency sphere is whether **Bitcoin's Proof-of-Work (PoW) consensus is wasteful**, and if so, why doesn't the community simply change to a more environmentally friendly PoW consensus?

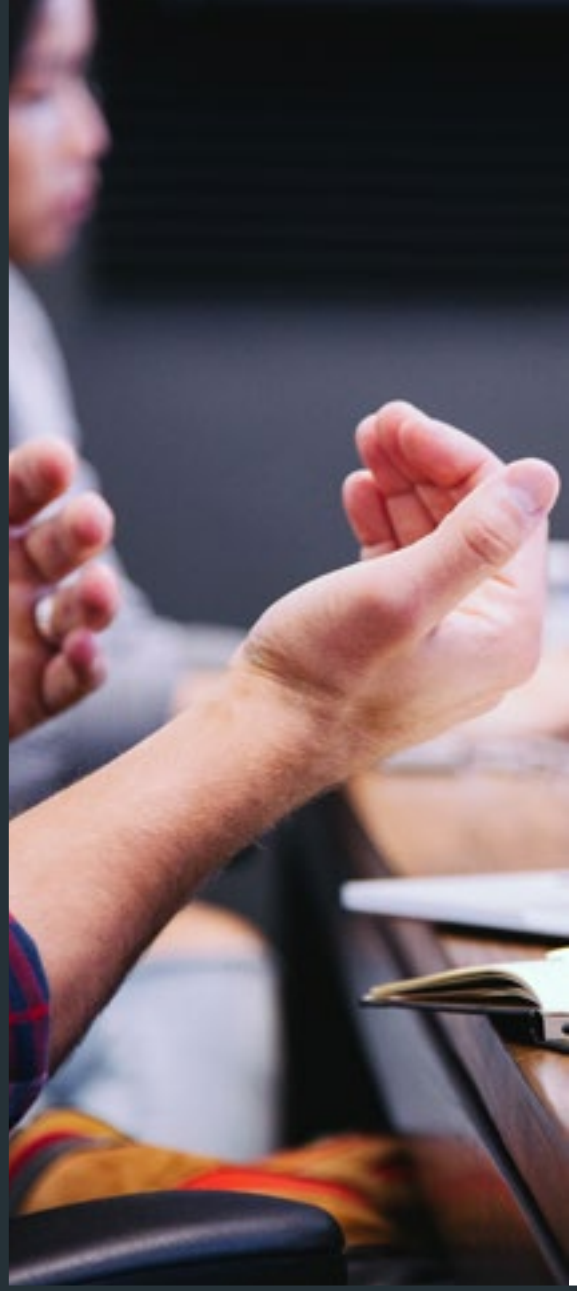
Usually, when the topic is debated, there are two major positions:

1. Bitcoin's PoW is **wasting tons of usable energy.**
2. Bitcoin's PoW mostly uses cheap, environmentally friendly energy.

Bitcoin Energy Consumption Index Chart



Source: digiconomist.net/bitcoin-energy-consumption From Feb 2, 2017 to Feb 20, 2019



Both arguments do have a point. However, it seems the key reason why Bitcoin needs so much energy going into its hash rate is somehow forgotten.

Bitcoin's hash rate

What keeps Bitcoin's blockchain secure is the total amount of hash rate.

Even when miners do not earn a block reward, they're still keeping the network secure as they're contributing to increasing Bitcoin's hash rate.

As you can imagine, this is the first reason favouring the argument that Bitcoin does need incredible amounts of energy going into its hash rate, as it's the process that secures the network against unwanted players.

51% attacks

In order to perform a 51% attack on Bitcoin, a miner would need to control more than half of the total Bitcoin hash rate, which in essence is almost impossible.

We could potentially see a state-wide attempt to control Bitcoin, but to organise this without any miner/Bitcoin enthusiast/developer noticing would be highly unlikely.

Moreover, there are easier and better ways to perform a considerable and more devastating network attack.

For example, if you have alternative consensus mechanics that aren't energy dependent, like Proof-of-Stake (PoS), it's highly likely your network will end up being controlled by a small group of people at some point in time. This is due to the fact there is no energy requirement, and so whoever controls the money supply, controls the network.

Decentralised governance

The key reason why Bitcoin is safer to use as a store of value and medium of exchange when compared to any other cryptocurrency is its decentralised governance, both at a technical level and at a social level.

For any cryptocurrency to be properly decentralised, it should have at least one of the following properties, as highlighted by one of the most prominent Bitcoin developers and educators, Jimmy Song:

1. A creator that's still involved.
2. A development team that forces upgrades on all the users (hard forks).
3. A foundation/organisation which directs what the coin will do.

The core idea of Jimmy's argument is that there should not be any entity with enough power to impose network changes on their own, be it through hash rate control, GitHub repository control, supply control, or any other control mechanism.

To properly achieve decentralisation, PoW is by far the safest and most effective consensus mechanism. Whether or not you think Bitcoin promotes a wasteful mechanism, one cannot deny that spending energy securing Bitcoin's global network of money does not seem like a waste at all.

DELEGATED PROOF-OF-STAKE (POS) CONSENSUS EXPLAINED

Proof-of-Stake offers a great alternative, addressing some of the aforementioned limitations. Lets take a look below.

Proof-of-Work vs Proof-of-Stake

Proof-of-Work (PoW) and Proof of Stake (PoS) are the most common consensus algorithms in the world of cryptocurrencies. They are both used to help network nodes agree on a single accounting system.

Bitcoin and most other major cryptocurrencies use the Proof-of-Work algorithm. However, this is an expensive and energy consuming system that requires miners to handle intricate puzzles to verify the integrity of a transaction and add it to a block.

The miner who solves the puzzle first receives a block reward, which is a part of the transacted currency. The **Bitcoin block mining reward** halves every 210,000 blocks. This means that the current block reward of 12.5 Bitcoins will decrease to 6.25 coins in the near future.

The Proof-of-Stake consensus algorithm, however, sees miners become forgers. They don't need to put in the same amount of work to create blocks. Instead, they build blocks based on their stake in the currency and the time they've been in the network.

This algorithm reduces energy consumption significantly. That's why networks like **Ethereum** are developing new protocols to move from a PoW system to a PoS one.

What is Delegated Proof-of-Stake (DPoS)?

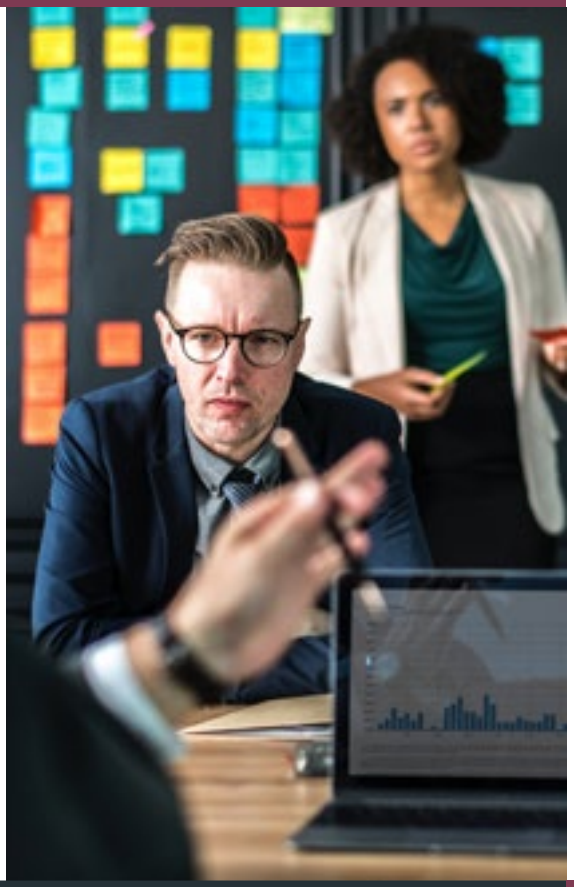
Delegated Proof-of-Stake (DPoS) is the democratic version of the Proof-of-Stake consensus algorithm since it includes a voting process. Token holders vote in real time for witnesses and delegates. They then become responsible for validating transactions and keeping their nodes continuously running to maintain the blockchain.

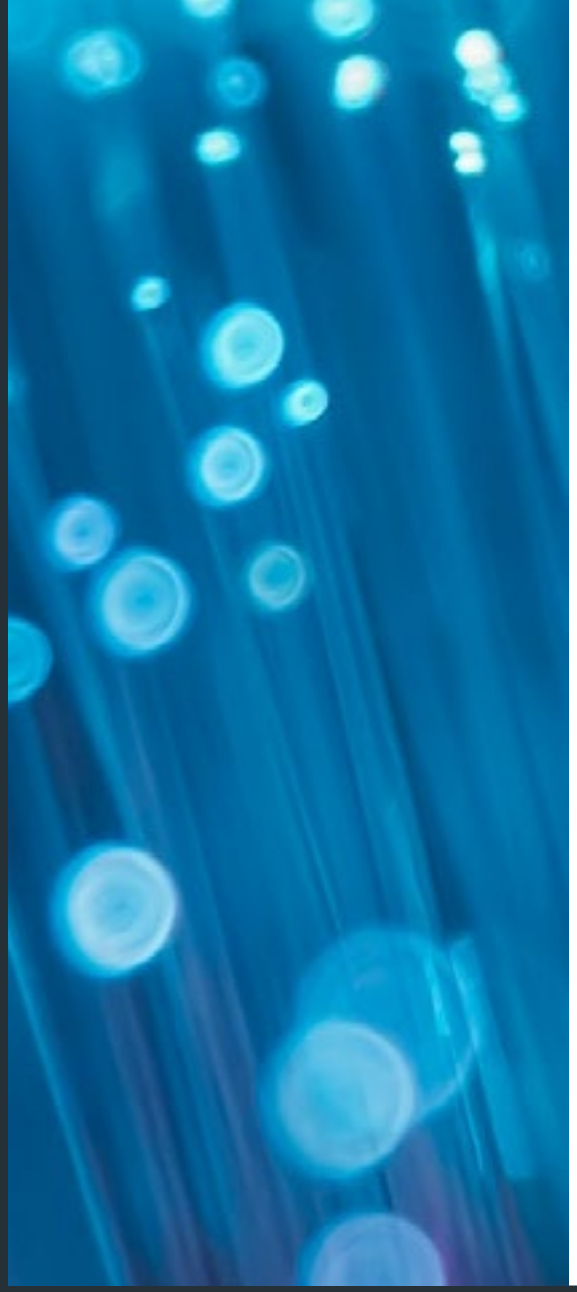
Witnesses are paid for their role in generating and adding blocks to the blockchain. And, as in any democracy, they need a solid reputation to maintain their popularity across token holders. Delegates, on the other hand, are responsible for maintaining the blockchain.

As the voting process is continuous, any witness or delegate that has lost credibility can be voted off. That's because all witnesses and delegates are chosen with the network's best interest in mind.

How does the Delegated Proof-of-Stake consensus work?

Delegated Proof of Stake, as a new method of securing a network, was created by Dan Larimer, who also founded **Bitshares** in 2014. According to its creator, DPoS can handle a higher transaction volume and provide faster





confirmation times than PoW and PoS systems while being more energy efficient.

This is possible thanks to the smaller number of trusted witnesses required to verify each block in the chain. A lower number of users means each block can include more transactions, which automatically leads to an increased transaction speed. This is important as blockchains look to scale to onboard more users.

There are several safeguards in place to guarantee the integrity of the network. These include:

- Witnesses share the power equally. None of them can use their resources to gain more power inside the system.
- When a witness signs a block, it must have verification that another trusted node signed the block before it.
- Witnesses that miss their turn can lose their votes and positions in the network. This leaves a free place for another user to be elected.

This system gives all token holders the chance to become delegates, regardless of their resources. Networks also build a reputation score to help voters make educated decisions when choosing their delegates.

In DPoS, a token holder's reputation is the most important asset because delegates get rewards based on their status. It takes a long time to build up trust, and any misstep can have disastrous effects on someone's credibility.

DPoS pros and cons

Like any new technology, this consensus algorithm comes with a series of advantages and disadvantages.

DPoS pros:

- The network processes more transactions in a given period.
- DPoS blockchains are more scalable than networks with PoW or PoS since they don't require high computational power.
- The digital democracy gives more token holders the chance to decide the block producers, compared to PoW where miners with more capital produce more blocks.
- The system is energy efficient, which means it's also environmentally friendly.

DPoS cons:

- Decentralisation is often hard to maintain, as the decision lays in the hands of a limited number of holders, leaving room for **conspiracy and censorship.**
- Low participation in the voting process can generate centralisation, by placing the power in the hands of a limited number of token holders (like any democracy).

Besides BitShares, other cryptocurrencies that use the Delegated PoS consensus or similar systems derived from it are Lisk, Nano, EOS, Steem, Ark, Golos, PeerPlays, Cardano, and Tezos. Each one of these networks implements the system differently.

The energy perspective

PoW is still the most popular and trusted consensus algorithm, but its sustainability is often thrust into the spotlight due to its dependence on a high amount of power. While PoS and DPoS are currently not without their issues, they look to be good systems for cryptocurrency sustainability in the future.

CONCLUSION

No matter where you stand in terms of environmental opinions, cost considerations, or preference for different algorithms, there's no denying the importance of consensus when it comes to adding transactions to a blockchain.

As the cryptocommunity looks to keep transactions immutable, secure, and inexpensive, these algorithms may continue to change.

By **keeping up-to-date with the latest news**, you'll be the first to know about any new technologies, the benefits of different algorithms, and how you can mine for your cryptocurrency more efficiently.

Bringing you news, analysis, opinion and insight from the fast-moving blockchain world. Our team of journalists and contributors cover the likes of cryptocurrencies, wallets, exchanges and ICOs across a wide range of sectors including retail, fintech, banking and gaming. We go beyond the press releases and marketing hype to tackle all the industry topics that matter.

Featured in

FOX NEWS EXPRESS COINGEEK

coinrivet.com