PRIVACY COINS

Our definitive guide to privacy coins

COIN RIVET

Independent British blockchain and crypto news

CONTENTS

PRIVACY COINS EXPLAINED

Confidentiality cryptocurrencies, most commonly known as privacy coins, enable users to have complete confidentiality over their transactions and addresses.

When Bitcoin introduced cryptocurrencies to the world, privacy was an underlying attribute due to address confidentiality. Of course we know today that because of metadata, it's possible to easily link IP addresses and usernames to Bitcoin and Ethereum addresses. Plus, because all transactions are broadcasted publicly, users lose some privacy features as well.

Some trade-offs exist when trading cryptocurrencies. There are three main aspects of privacy in the context of cryptocurrencies, corresponding to:

- The identity of the user performing an operation using the cryptocurrency
- The transaction data specific to the operation the user is performing
- The total blockchain state formed by combining the knowledge of all transactions.

An easier way to understand the above points is to ask the following questions:

a) Do I know the identity of the user?
b) Can I see the transaction details sent by other users?
c) Can I see all blockchain transaction data and identify which addresses have which amounts?

By answering each of these questions, you can learn if any given cryptocurrency is confidential and private or not.

Privacy cryptocurrencies

Not long after Bitcoin was developed and released, a number of confidential cryptocurrencies emerged with the sole goal of allowing users to transact freely, with complete privacy and confidentiality.

A brief analysis of each, when facing the above questions, can be seen below:

Addresses	Bitcoin	Monero	Zcash	Dash	Verge	Grin
Public?	YES	NO	NO	YES	YES	NO (USES IP)
Transaction details public?	YES	NO	NO	NO	NO	NO
Blockchain analysis possible?	YES	NO	NO	YES	YES	YES

Privacy technologies

Cryptocurrencies use a number of underlying technologies to ensure that privacy can be achieved. We take a look at some important privacy technologies below.

Second-layer protocols

These protocols include the lightning network, state channels, or Plasma on top of a base layer cryptocurrency. These technologies allow small groups of users to transact amongst themselves off-chain. This means all intermediate state is stored between those users and only periodic summaries of state changes are written to the main blockchain.

As a result, the intermediate states are invisible to outside observers because they never appear on the main blockchain at all. Of course, the second-layer protocol itself can have different levels of privacy for off-chain states among its participants, so this is more of an idea than a privacy technique.

Ring-signature approaches

These approaches take inputs and outputs of different transactions and combine them into a single large transaction to obscure links between addresses of senders and recipients. These include some of the earliest approaches to privacy coins such as Monero.

TOR

Tor approaches that use the Onion routing as a mechanism to hide users' IP addresses, such as Grin and Verge. The software allows users to use the internet anonymously through an encrypted network.

CoinJoins

These are built through a mechanism that enables transactions from multiple senders to be batched into a single transaction. An example using this feature is Verge.

Zero-knowledge based privacy

This privacy comes when users of the protocol supply zero-knowledge proofs (ZKP's), i.e. data which demonstrates knowledge of a piece of information without revealing the information itself. When used correctly, this cryptographic technique can ensure both privacy of transactions/state and soundness of the blockchain.

Mimblewimble

This technology contains:

(a) Elliptic curve cryptography (ECC) which enables Private-Public key encryption – a way to prove you know something without revealing the content of the encrypted information.
(b) Confidential transactions which allow for public verification of the transaction without revealing any significant details such as amounts or addresses.
(c) CoinJoins built through a mechanism that enables transactions from multiple senders to be batched into a single transaction.
(d) Dandelion, an improved gossip protocol network that contains increased privacy working mechanics. It uses hops in between nodes before publicising the transaction to the neighbouring nodes.

In the end, any technology represents a means to an end. Mimblewimble's purpose is to allow value to be transferred and stored in a decentralised manner, privately and without intermediaries.

PRIVACY TECHNOLOGY: MIMBLEWIMBLE EXPLAINED

Mimblewimble is gaining popularity with cryptocurrency enthusiasts. It's becoming a serious side-chain protocol by **improving on Bitcoin's privacy features.**

The initial Mimblewimble whitepaper was drafted by Tom Jedusor in 2016, with clear references to Greg Maxwell's work on confidential transactions and CoinJoin. It also references a paper posted anonymously in 2013 which introduces one-way aggregate signatures – a functionality which obscures inputs and outputs.

The first Mimblewimble implementation, BEAM, was fully released on **January 3 2019** and is now live and can be mined. This means anyone can join to support the network. In order to do so, you will need GPU processor and the ability to set up a node

So where did Mimblewimble start? The first Grin testnet was launched in November 2017 and the project is fully live. The Grin repository is currently maintained by anonymous developers and doesn't have a clear business model just yet, whilst BEAM is a much more hierarchical and organised structure. Both are aiming to achieve the same goal which is to provide a live and functional network for Mimblewimble.

The blueprint of privacy

The purpose Mimblewimble serves is to improve users' privacy. It also allows for close-to-infinite scalability. It does so by combining a number of technologies.

Both Mimblewimble implementations chose to use an ASIC resistant algorithm such as Cuckoo Cycle (in Grin) or Equihash Pow (BEAM) to promote a higher degree of decentralisation, while adopting a secure model.

When a transaction is broadcast, it will hop to a number of other neighbouring nodes before being broadcast to the entire network. It's difficult to find the originator of these hops as each one brings an additional node that would need to be inspected. This is an almost impossible task to accomplish with a set of 3 to 4 hops per transaction.

The Mimblewimble blockchain is bound to the number of users using the network, not to the number of transactions, so you can already imagine the impact on scaling the network. Nodes only need to register block headers for current UTXOs (unspent transactions), not for the entire chain. Plus, this means there are no addresses or transactions.

How does Mimblewimble actually work?

The validation of Mimblewimble transactions relies on two basic properties:

1. Verification of zero sums. The sum of outputs minus inputs always equals zero, proving that the transaction did not create new funds without revealing the actual amounts.

2. Possession of private keys. Like with most other cryptocurrencies, ownership of transaction outputs is guaranteed by the possession of ECC private keys. However, the proof that an entity owns those private keys is not achieved by directly signing the transaction.

Simply put, because there are no amounts as the sum of the inputs and outputs is zero, and because users don't need to sign any transaction with their private keys, there is no need for actual addresses.

What matters, in the end, are unspent transactions (UTXOs).

Mimblewimble's potential

Mimblewimble has the potential to significantly reduce both transaction costs and blockchain size. Where other Blockchains would necessarily have to grow over time, the required Mimblewimble dataset doesn't, which would solve the scaling problem.

From a technological point-of-view, Mimblewimble is a rather intriguing protocol that could offset a new wave of blockchain development. If Grin (and now BEAM) can prove this consensus mechanic properly works without addresses, amounts and signatures, we could finally have a serious contender to Bitcoin.

Its advantages when compared to Bitcoin are:

- Extremely good scalability as the great majority of transaction data can be eliminated over time, without compromising security.
- Increased privacy by mixing and removing transaction data.
- Faster node sync up time, as the nodes would connect with the rest of the network very efficiently.

Let's see what the future holds for both Grin and BEAM; will this novel technology do serious damages to prominent privacy coins like Monero, Zcash or Monaco?

AN OVERVIEW OF BEAM PRIVACY COINS

Many privacy coins currently adopt the Mimblewimble protocol.
Below, we take a look at the Beam privacy coin, currently leading the way with the technology.

Mimblewimble technology aims to reduce the size of blockchains to improve scalability, which is a common issue in many cryptocurrency networks.

Beam and Confidential Transactions

Beam combines elements of the Mimblewimble protocol with additional features to allow 'true' privacy for its users. Like other cryptocurrencies, Beam has its own blockchain that remains decentralised and distributed.

Transactions can be verified, but Mimblewimble's method of verification ensures that no outside observer can obtain any sensitive information about the sender or receiver, or the amount being transacted.

This method is known as 'Confidential Transactions' (CT). CT functions so that only the sender and receiver can know how much money is being transacted.

To enable verification, there is a process known as 'Pedersen commitment.' This process allows others to perform the mathematical calculations on the transactions without the total being revealed.

Beam and Transaction Cut-through

Mimblewimble has a feature known as 'Transaction Cut-through,' which enables the blockchain to be significantly smaller than the Bitcoin blockchain. This feature functions by eliminating old and redundant transactions on the blockchain. It voids spent inputs by aggregating intermediary transactions together, consequently shrinking the blockchain. This was based on a method known as 'CoinJoin,' except it voids the need for private and public keys as well as addresses.

Traditionally, keys and addresses are very important for cryptocurrency, but with Beam's focus on privacy, they are removed to ensure sensitive information leaks are limited. The only elements left are the inputs and outputs.

Beam also enables its users to opt in or out of audits. This is useful for tax and accounting purposes, since you can audit your account and transactions.

Beam isn't decentralised, yet

The Beam privacy coin is being run by a start-up company, but it has the intention of giving operational control over to a dedicated non-profit foundation in the future.

The coin is expected to be governed for around two years. In doing so, it is hoped that the coin can achieve growth before being given to the non-profit foundation.

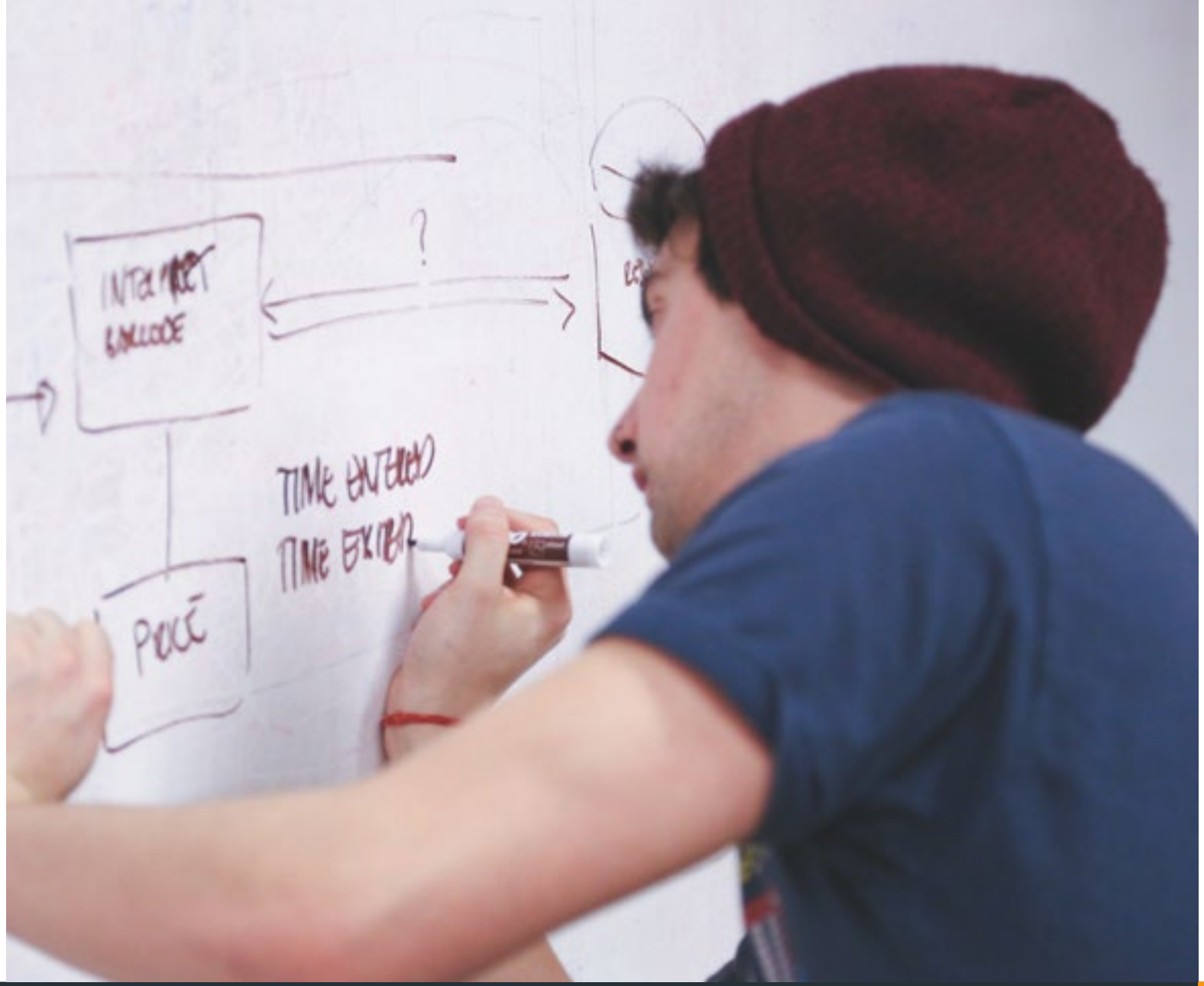
Unusually, no Initial Coin Offering (ICO) was held. In recent memory, many start-up cryptocurrencies have held an ICO to raise funds for their upcoming project. It's believed that everyone has an equal chance to mine/invest in the project.

However, there is a founders' reward which will see the Beam company and foundation receive 20% of all freshly minted tokens for the first five years.

Beam isn't perfect, and it knows it

If you look at the Beam **GitHub**, there is a section that outlines a flaw within the system. Specifically, one malicious node could record all individual transactions. This is because the nodes receive and forward a lot of individual transactions. They are prepared by participants and then broadcast. It is important they are broadcast so the rest of the network can validate them.

However, if an attacker can see the original transaction graph, the obfuscation of all later transactions in that block no longer matters. This is not necessarily an issue that cannot be solved, as Beam have suggested remedies. But, it is important to be mindful that whilst the Beam privacy coin looks promising, it isn't necessarily a perfect system just yet.



WHY THE FIGHT FOR PRIVACY MATTERS

So with all the talks about privacy, we must address a pressing question – why does the fight for privacy matter?

Privacy for many involved in cryptocurrencies and cryptography as a whole is considered a basic human right. Privacy isn't something you earn. Whilst there are obviously people who misuse privacy for terrible acts, the argument goes that we as citizens shouldn't be deprived of the right because of them.

Those who began the work of cryptography, the forebearers of today's cryptocurrencies, did so for privacy.

Why has privacy become the forefront of the battle?

With Bitcoin, there is a lack of privacy due to the public blockchain. When Bitcoin was a small, unknown currency, this wasn't an issue as governments didn't anticipate the rate of growth the cryptocurrency would experience.

The scene is remarkably different now. Thanks to companies such as **Chainalysis**, the Bitcoin blockchain is able to be traced quite extensively.

For many exchanges, regulatory requirements call for the use of Chainalysis so that the stringent KYC and AML measures can be enforced.

Yet for many of the original cypherpunks, this poses an issue.

Ideally, for them, monetary transactions should remain largely anonymous. This is why we are seeing a new rise in efforts to incorporate new privacy features into various cryptocurrencies.

Bitcoin itself is hoping that the increased use of the **Lightning Network** will add another level of privacy as well.

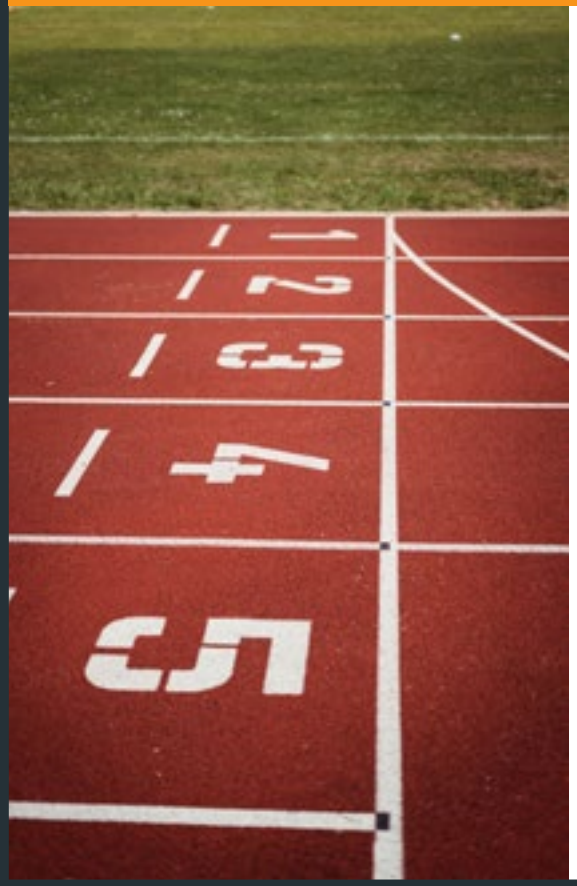
Can governments stop the fight for privacy?

What governments can do to stop such advancements is limited. With all of the code being open source, people are able to share ideas freely, which in turn improves the development of the technology. This is precisely what is happening within the cryptocurrency space right now. Developers are looking at the code of other coins and seeing the benefits that they can add to their own coin.

Whilst the large technology conglomerates continue to find themselves in a bind over privacy leaks and data snooping, the developers within the cryptocurrency and cryptographic community are at the forefront of attempting to protect the rights of the individuals. Not in an effort to commit more crime, but because they believe it is our right as citizens.

TOP FIVE PRIVACY COINS

Privacy is becoming an increasingly important issue throughout the crypto community, with many existing currencies looking to add privacy technologies to their offering. These alternative coins offer a lot of competition to the problems posed by Bitcoin. We take a look at five important privacy coins below.



Monero

Monero, XMR, is a secure, private and untraceable currency system. Monero uses a special kind of cryptography to ensure that all of its transactions remain 100% unlinkable and untraceable.

In essence, the funds you own will not be associated with your public address, like they would with Bitcoin. When you send funds to someone's public address, what happens is that you actually send the funds to a randomly created brand new one-time destination address. This means that the public record does not contain any mention that funds were received to the recipient's public address.

The technology behind Monero's confidentiality features is called ring-signatures. Ring-signatures enable 'transaction mixing' to occur. Transaction mixing means that when funds are sent, the sender randomly chooses several other users' funds to also appear in the transaction as a possible source of the funds being sent. The cryptographical nature of the ring signature means that no one can tell which of the funds were really the source of the transaction – not even the person that gave the funds to the sender in the first place. A system of 'key images' associated with each ring signature ensures that although no one can tell the true source of the funds, it can be easily detected if the sender attempts to anonymously send their funds twice.

In Monero, your public address will never appear in the public record of transactions. Instead, a 'stealth address' is recorded in a way that only you, the recipient, can recognise the incoming funds

Zcash

Zcash is a privacy-protecting, digital currency built on strong science. It helps users transact efficiently and safely with low fees while ensuring digital transactions remain private.

Zcash addresses are either private (**z-addresses**) or transparent (**t-addresses**).

A Z-to-Z transaction appears on the public blockchain, so it is known to have occurred and that the fees were paid. But the addresses, transaction amount and the memo field are all encrypted and not publicly visible. Using encryption on a blockchain is only possible through the use of zero-knowledge proofs. Zcash uses **zk-SNARKs**, a novel form of zero-**knowledge cryptography**.

The strong privacy guarantee of Zcash is derived from the fact that shielded transactions can be fully encrypted on the blockchain, yet still be verified as valid under the network's consensus rules by using **zk-SNARK proofs.**

The acronym zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge". It refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier.

In order to be private yet still allow users to remain compliant with regulatory bodies, an owner of an address may choose to disclose z-address and transaction details with trusted third parties, through the use of view keys and payment disclosure.

Transactions between two transparent addresses (t-addresses) work just like Bitcoin. The sender, receiver and transaction value are publicly visible. The two Zcash address types are interoperable. Funds can be transferred between z-addresses and t-addresses. However, it's important that users understand the privacy implications of shielding or de-shielding information through these transactions.

Dash

Dash is an open source cryptocurrency and is a form of decentralised autonomous organisation (DAO) run by a subset of users, called "masternodes". Masternodes are the responsible to approve and validate transactions. Dash uses a Proof-of-Stake algorithm alongside its masternodes to incentivise the network. The currency permits fast transactions that can be untraceable. 45% of mined coins go to miners, 45% to masternodes, and 10% into a fund that the DAO invests.

Dash is currently being mostly used in countries like Venezuela, where people need to transact quickly with privacy and confidentiality due to hard-imposed government regulations.

The technology behind Dash privacy features is Tumblers, or cryptocurrency mixing, meaning the cryptocurrency itself is not private and if a masternode gets attacked, users' information (addresses, transaction details) could leak.

Verge

Verge is a cryptocurrency built with a fork of Bitcoin but with an emphasis on privacy and confidentiality. The XVG token utilises anonymity-centric networks such as TOR and i2P to make sure the IP addresses of its users are obfuscated and the transactions are completely untraceable. Verge (XVG) started as DogeCoinDark back in 2014, which makes it one of the older anonymous coins, and in 2016 rebranded to Verge.

Much like Dash, Verge wasn't originally built for privacy, meaning its core protocol simply hides transactions through transaction mixing and IP addresses with onion-like routing.

XVG is mainly used due to its cheap transaction fees and quick transaction speed times.

Grin

Grin is a brand new cryptocurrency released in 2019 with the goal of allowing users to transact completely privately and quickly. Grin's aim is to allow for a private-cash based system, hence its blockchain is incredibly scalable. The technology behind Grin is **Mimblewimble.**

Simply put, in Grin there are no transactions or addresses. The blockchain is like a huge UTXO that keeps updating with new transactions, meaning each user keeps its own records, and the ledger just records the latest blockchain state. Grin is the earliest implementation of Mimblewimble and is completely open-source

CONCLUSION

It will be interesting to see the role that privacy coins play in the market over the coming years. They are certainly being perceived as the example to follow, with coins such as Litecoin looking to apply some of the privacy technologies to their own offering.
To see where privacy coins go in the future, we recommend keeping up with the latest news from **Coin Rivet.**

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