



Blockchain Assets

CRYPTOASSET MANAGERS

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	W
/	π	o	γ	ç	45	o	ω	τ	g	g	~	3	25	n	ε	s	#	α	-	13	~	≡	e
//	k	o	o	n	r	x	c	⊥	þ	∞	≈	ε	ε	π	€	f	+	λ	=	þ	Δ	o	5
x	e	g	Δ	o	g	φ	d	⊥	ψ	∞	+	ω	o	4p	ts	ff	π	γ	π	γ	x	H	Ly
x	F	o	Δ	u	h	ε	+	⊥	5	ω	o	m	q	z	ε	ss	+	o	u	q	K	H	λ

This is a cypher (coded way of writing) used by Mary, Queen of Scots. It was used as evidence of her involvement in the Babington Plot of 1586, which was a plan to assassinate Queen Elizabeth I of England and put Mary Queen of Scots on the throne in her place. - The National Archives Kew, Richmond TW9 4DU

Dear Investors,

In this newsletter I cover the topic of quantum computing and AI enabled cybersecurity challenges for digital systems in general and cryptoassets in particular.

Cybersecurity is an arms race between those who build systems to protect information and assets and those who try to defeat them. For centuries that contest was between cryptographers and cryptanalysts. Today AI and quantum computing are new weapons being introduced to the contest.

The focus of this newsletter is on what action is being taken today to secure the traditional and decentralised systems from AI and quantum assisted attacks, now and in the future.

But first the cryptomarkets and other news...

Our Fund ended the quarter up 51.68% with a unit price of AUD 4.2071. The value has fallen slightly since then, due in part to concerns about AI-assisted mathematical discoveries ([see here](#)) that have emerged over the last two weeks. These concerns, together with the longer-term threat of quantum computing, are the subject of this newsletter.

While understanding quantum and AI associated risks is important. We hold no concerns regarding the safety of our assets. Our main custodian, Anchorage Digital Bank N.A. have advised they have already implemented post-quantum cryptography within their security infrastructure and designed their custody systems so that new cryptographic standards can be adopted without rebuilding the underlying architecture.

US Whitehouse Crypto, Technology and Finance Meeting

On 19 August 2026 President Trump hosted at the Whitehouse 15 leaders in crypto, technology and finance. The 40 minute press conference can be viewed [here](#).

This was a significant meeting. It brought together traditional market institutions such as the New York Stock Exchange, represented by Jeff Sprecher, Chairman and CEO of its parent company Intercontinental Exchange (ICE); Nasdaq, led by Adena Friedman; and Robinhood, led by Vlad Tenev. It also included the heads of major regulators, including the SEC and CFTC, crypto-native businesses such as Coinbase and Kraken, and blockchain infrastructure developers such as Chainlink.

The integration of crypto technology, including stable coins, tokenisation, bitcoin and everything else, into the traditional financial system is exactly what we have expected to happen. A few years ago this seemed a long way off. Today, we can see that integration is starting to happen in a profound and irreversible way.

Thus far, demand for our assets has primarily come from a combination of short-term speculative demand and long-term strategic holding. We have not yet experienced significant utility demand (demand from people and businesses because they actually need these assets to use blockchain networks to conduct economic activity, settle transactions, access applications or pay network fees).

As strategic long-term holders, our thesis has always been that utility demand is ultimately what will justify the value of these assets. When that demand begins to emerge at scale, we expect it to reinforce both speculative and strategic demand, creating a positive flywheel: increasing utility drives greater adoption and demand, which attracts capital and development, which in turn creates further utility and adoption.

We would not continue to hold our assets unless we believed that utility-driven demand would eventually materialise. Meetings like the one at the Whitehouse are encouraging. The conversations are moving from whether blockchain infrastructure will be adopted to how it will be implemented.

Utility demand will not come only from the integration of traditional finance with blockchain infrastructure. We also expect demand to emerge from the agentic, AI-driven economy I wrote about in last quarter's newsletter. Autonomous agents will need infrastructure through which they can transact, make payments, enter economic relationships and exchange value without relying on human intervention. Public blockchain networks are uniquely suited to provide that infrastructure.

Developments in the US Bond Markets

Some of the increased institutional demand for Bitcoin has been attributed to growing concerns about the US fiscal position and developments in the US Bond market.

By way of background the US Treasury Department and the US Federal Reserve have traditionally had separate but related responsibilities. The Treasury manages the Government's finances,

including its borrowing and debt issuance, and is considered to be on the fiscal side of economic management. The Fed on the other hand manages the monetary side of the economy, this deals principally with interest rates, inflation management and monetary conditions.

One important reason for the distinction is that the Treasury, because it is part of the Executive Government and implements Government fiscal policy, has a natural connection to the political position of the incumbent government whereas the Fed has operational independence in conducting monetary policy.

There is often tension between the two. For example, in times of inflation an expanding Federal budget can offset the efforts of the Fed to dampen inflation by increasing rates. Economic commentators note in such cases that fiscal and monetary policies are pulling in opposite directions.

We have a similar issue in Australia at the moment, but the issue in the US is more extreme and this is what is impacting the US Bond markets and strengthening the investment case for Bitcoin.

The two specific items I want to focus on are the 'US Treasury support for the Japanese Yen' and the US Treasury Buyback of long dated bonds.

Support for Japanese Yen

Typically foreign exchange rates are set by free open markets supply and demand principles. Every now and then a Government will 'intervene' in the market to act as a buyer of its own currency in the hope that the currency will hold to a certain level relative to the USD. We have seen Japan's Ministry of Finance (MoF) intervene in the market to keep the Japanese Yen (JPY) from falling too low relative to the USD. This type of intervention is not ideal but it happens and is now generally accepted as part of the market dynamic.

On 31 July 2026, there was a significant development. The US Treasury joined the MoF in a coordinated intervention to support the JPY. There are a number of reasons why it is in the interests of the US to prevent a disorderly decline of JPY, which I will not go into here.

The important point is that the US Government was prepared to intervene directly in the foreign exchange market to support the value of another major country's currency. This is unusual, although not unprecedented. What makes the current intervention particularly interesting is the close relationship between Japan and the US Treasury market, given that Japan is the world's largest foreign holder of US Government debt.

US Treasury Buyback

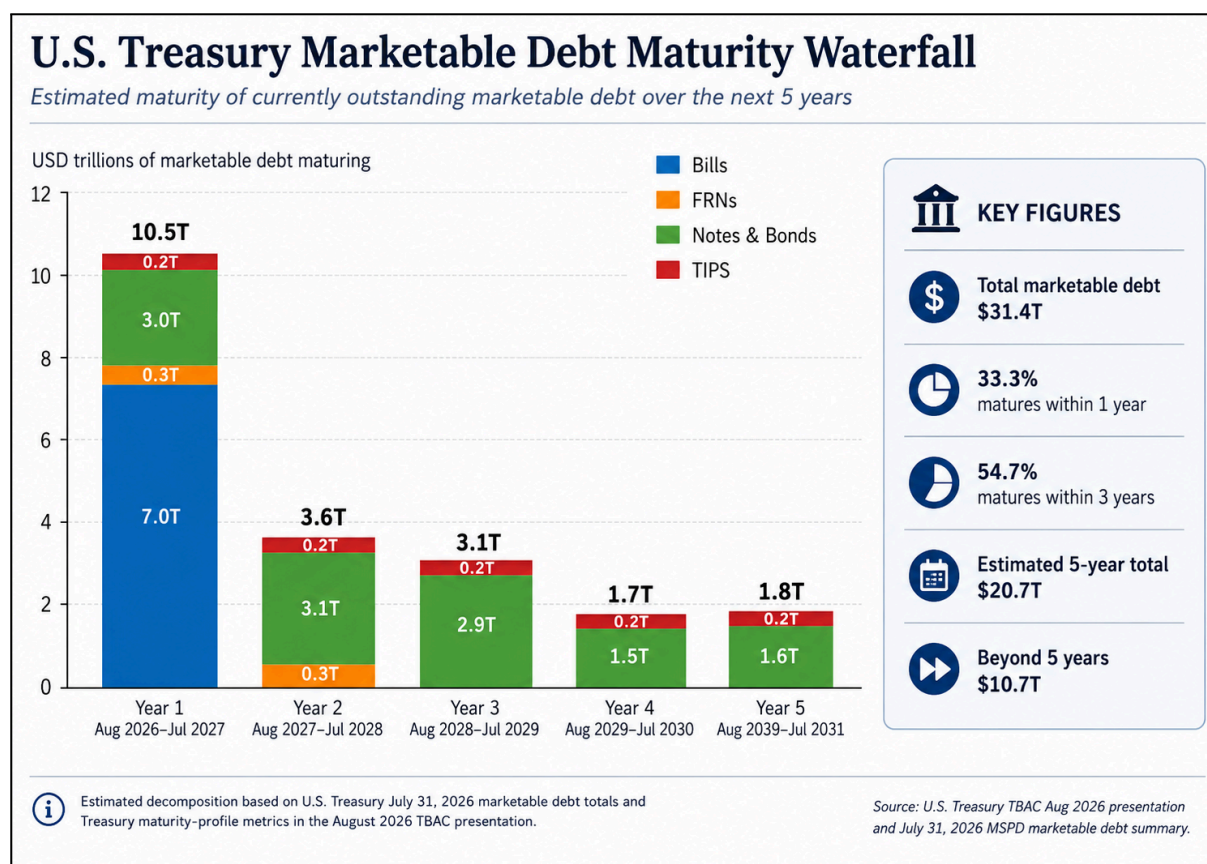
On 18 August 2026 US gross national debt passed USD 40 trillion for the first time, equivalent to approximately 123% of annual GDP. The interest bill on this debt is becoming one of the largest items in the US Federal budget, with net interest expenditure now running at more than USD 1 trillion a year. So even if the Government wants to reduce expenditure, its ability to do so is

increasingly constrained by the cost of servicing its accumulated debt.

At the same time, purchasers of long-dated US Treasury bonds are demanding higher yields to compensate for inflation, fiscal and duration risk. Higher yields progressively increase the Government's interest expenditure as existing debt matures and has to be refinanced.

The following day (on 19 August) the US Treasury announced that it would at least double its buybacks of long-dated Treasury securities, increasing individual operations from USD 2 billion to at least USD 4 billion. These buybacks are not quantitative easing, and are mechanically quite different from QE as practised by the Fed. Treasury says their purpose is to improve liquidity in the long-dated Treasury market, although critics argue that they also risk influencing long-term bond prices and yields.

Over the next few years a very large proportion of US Government debt has to mature and be refinanced. This refinancing wall comes at the same time as the Government must continue issuing additional debt to finance large fiscal deficits. The combination increases the amount of Treasury debt that investors must absorb and can put upward pressure on interest rates.



Impact of Interventions

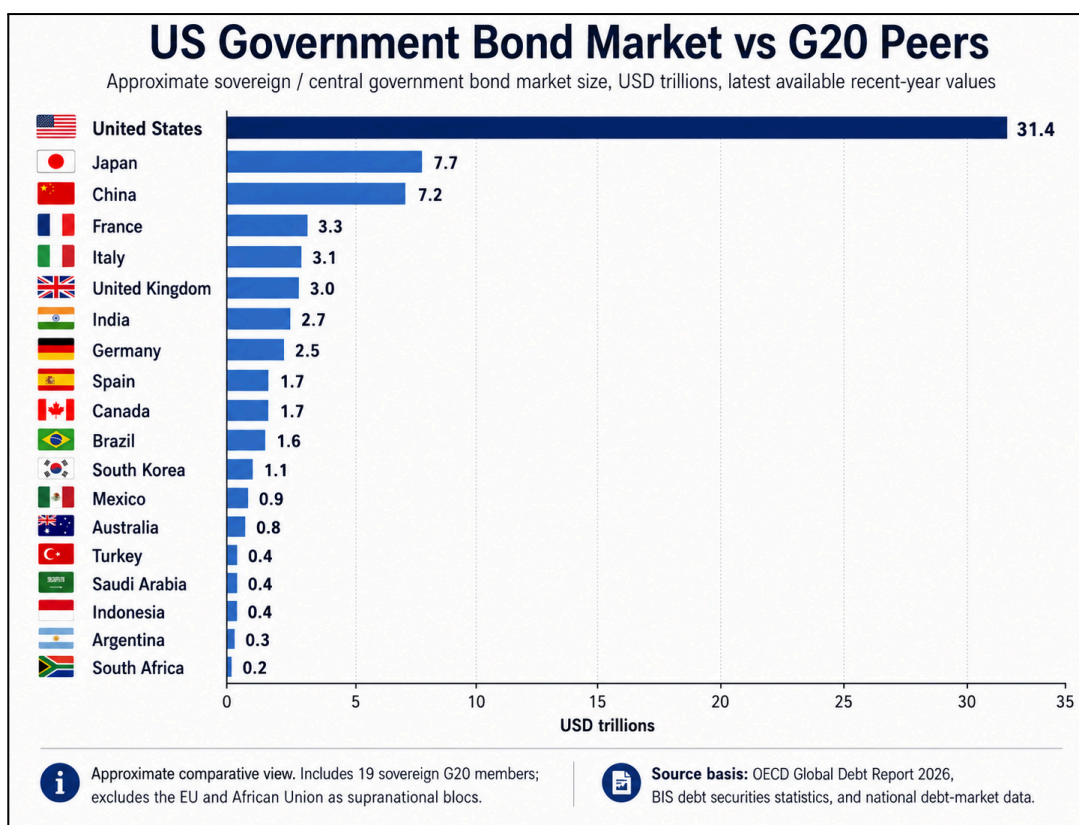
The interventions at this time are attempting to slow the fall of the JPY/USD exchange rate and ease some of the pressure in long-term US debt markets.

Even if these objectives are achieved, it is a short term fix. Nothing is being done to address the underlying structural defect of the US fiscal position. Well respected macro economic analyst [Lyn Alden](#) has used the saying '...nothing stops this train...' to make the point that structurally large fiscal deficits are extremely difficult to reverse. She has likened the current US situation to watching a slow moving train wreck.

In a Wall Street Journal opinion piece on 24 August [Stanley Druckenmiller](#) set out his, albeit AI assisted, view of the Treasury intervention, simply saying 'Let the Bond Market Speak'. In his opinion, the intervention by the Treasury is misguided. In his view fiscal problems cannot ultimately be solved with liquidity operations. His argument is that if Washington wants sustainably lower long-term rates, it ultimately has to address the structural deficit rather than attempt to suppress the signal coming from the bond market.

Other Sovereign Bond Markets

The issues facing the US bond market are present in bond markets across the G20. Japanese Government Bonds (JGBs) in particular are experiencing upward pressure on interest rates. However, the US market is by far the largest and what happens in the US market will impact not only all bond markets but all markets in general.



The Bitcoin Lifeboat - The Monetary Debasement Trade

For the foreseeable future, many macro investors are of the view that we are living in a world of fiat currency debasement. Monetary debasement is corrosive to traditional portfolios. As interest rates rise, investors will naturally be attracted by the higher yields available on Government bonds and may reduce their allocation to equities in favour of what has traditionally been considered the safer asset.

The problem is that this may prove to be something of a trap. Higher interest rates and the reallocation of capital into bonds can put downward pressure on equity valuations. But if inflation and fiscal deficits remain structurally high, bond investors are not necessarily safe either. Rising yields reduce the market value of existing long-dated bonds, while monetary debasement progressively reduces the real purchasing power of the dollars ultimately repaid. Moving from equities into long-term bonds in the hope of escaping monetary debasement can therefore be a little like running into a burning building hoping that, by doing so, the fire will go out.

This creates an unusual problem for the traditional portfolio. Equities can suffer from higher discount rates and the reallocation of capital towards bonds, while bonds can suffer from rising

yields and the erosion of their real value. There may be periods when there is simply nowhere particularly attractive to hide within the traditional financial system.

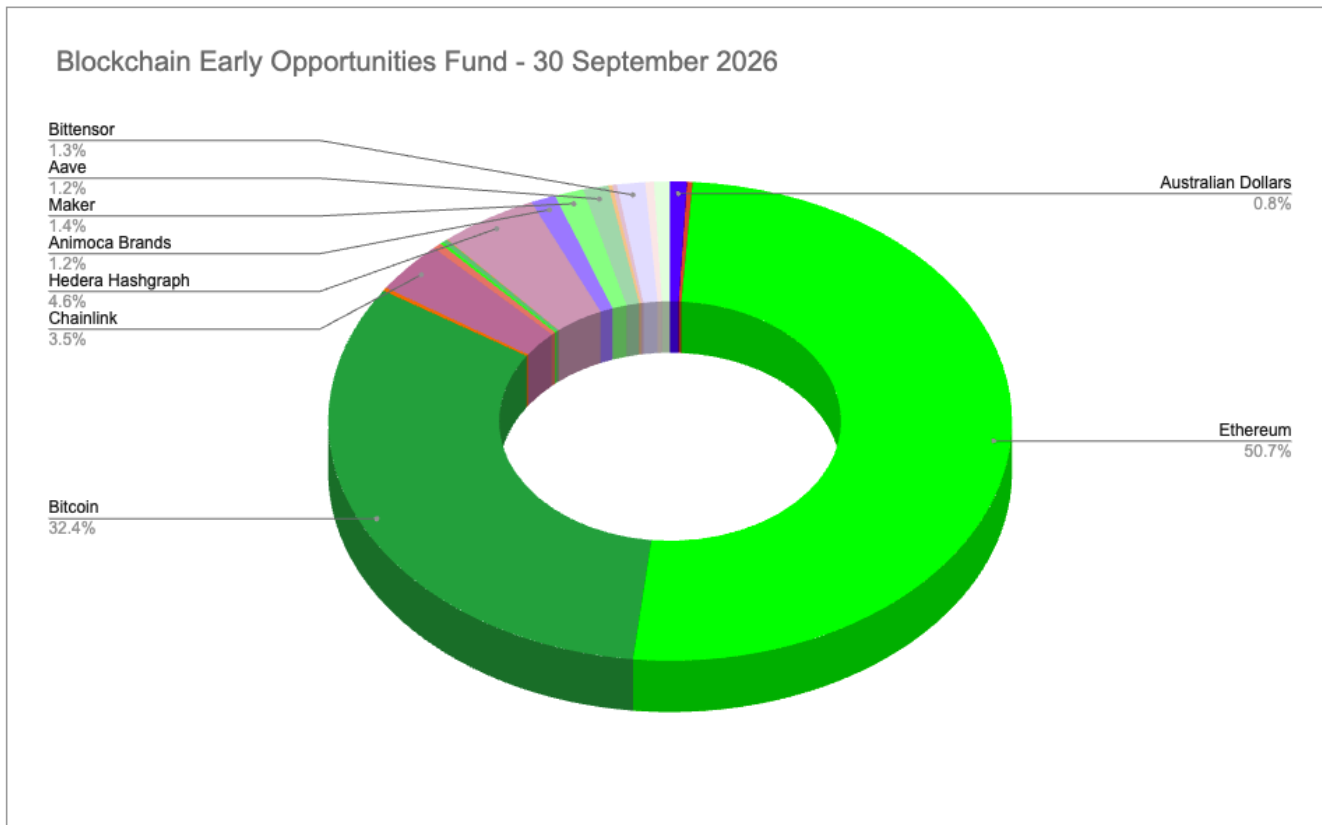
Physical gold has traditionally provided one escape route because its value is not a promise by a Government to repay a fixed number of currency units. Its supply is limited and its price is determined by supply and demand. Much of what gold investors talk about is therefore relevant also to Bitcoin. We are of the view that Bitcoin ('Digital Gold') is better at being gold than gold itself.

Our thesis has always been that the debasement of fiat currencies, particularly the USD, will drive adoption of Bitcoin as a store-of-value monetary asset. Bitcoin sits outside both sides of the traditional equity/bond trade: it is neither a claim on corporate earnings nor a promise by a Government to repay fiat currency in the future. In a world in which investors increasingly question the long-term purchasing power of that currency, Bitcoin offers something different.

That is the Bitcoin lifeboat. Our Bitcoin thesis may now be beginning to play out.

[End of Page]

30 September 2026	Unit Price	Return for the Quarter	\$100,000 invested on 1 July 2017 now worth	Annualised Return
	\$4.2071	51.68%	\$420,710	17.71%



[End of Page]

The Cryptography of Cryptoassets

On 8 February 1587, Mary Queen of Scots was beheaded after being found guilty of treason.

The decisive evidence against her came from secret letters that had been intercepted and deciphered by the cryptanalysts working for Sir Francis Walsingham, Elizabeth I's spymaster.

This was not the first or the last time that being able to crack a code has changed the course of history.

Secret writing, in Roman times and earlier, involved systems for rearranging or substituting letters and symbols so that a message could be read only by someone who knew the method or possessed the secret key. People who specialise in creating the different types of secret writing are called Cryptographers.

On the other side we have Cryptanalysts. These are people who specialise in breaking coded messages.

Over the course of history there is a constant battle between the creators and the breakers of code. There have been many periods in history where codes have been unbreakable for very long periods of time. There have also been periods of time where cryptanalysts have had the upper hand. It ebbs and flows.

For most of history cryptography was done with pen and paper and the minds of polymaths, linguists, classical scholars, mathematicians and puzzle addicts. As technology like the telegraph began to develop in the mid 1800s the demand for stronger cryptography increased. Of course

the world wars accelerated technology development and cryptography. The story of the Bletchley Park crew and Alan Turing cracking the Enigma Machine is a well known example.

In June 1976, two cryptographers (Whitfield Diffie and Martin Hellman) publicly unveiled the concept of public-key cryptography at the National Computer Conference in New York. This new form of cryptography was another paradigm shift in the history of cryptography and it remains one of the foundations of modern secure communications.

One important branch of public-key cryptography is Elliptic Curve Cryptography (ECC). It is this form of cryptography that is used by Bitcoin, Ethereum and many other blockchains to create the public and private keys that allow users to control their cryptoassets.

In addition to securing wallets, different types of cryptography are used for different functions of blockchains.

For example, Bitcoin uses cryptographic hash functions (SHA-256 and RIPEMD-160) to create digital fingerprints of data, secure mining, construct addresses and link blocks together. A cryptographic technique called Merkle Trees is used to verify transactions efficiently.

When the Bitcoin whitepaper was released in 2008, it brought together decades of cryptographic research and earlier experiments in digital money to create something that had never previously succeeded: a functioning decentralised monetary network that did not require a trusted central authority.

At the foundation of the security of Bitcoin, Ethereum and almost every other cryptoasset are cryptographic techniques that have been developed, tested and scrutinised over decades.

Today, the contest between cryptographers and cryptanalysts is entering another potentially important period. Two rapidly developing technologies, quantum computing and artificial intelligence, may significantly change the balance between them.

Quantum Computing

Quantum theory is a branch of physics that emerged in the early twentieth century. It's a theory that subatomic particles (such as electrons and photons) behave in different ways than what we expect to be the case from observing the larger objects we can see with the naked eye.

Quantum computers are trying to build a computer using the rules that emerge from the quantum behaviour of things. This way quantum computers may harness the rules that nature already uses.

Today's most advanced quantum computers are still experimental machines, but we have moved beyond simply proving that quantum computation is possible. Quantum processors can now perform certain specialised calculations beyond the practical capabilities of classical computers. What we do not yet have is a large-scale, fault-tolerant quantum computer capable of reliably solving broad classes of commercially or cryptographically useful problems.

There are several measures of progress. One is Random Circuit Sampling (RCS), a benchmark

used to test whether a quantum processor can perform a computation beyond the practical reach of classical supercomputers. Another, arguably more important milestone, is quantum error correction: whether thousands or eventually millions of imperfect physical qubits can be combined into reliable 'logical qubits'. Google has demonstrated important progress on both fronts. The remaining problems are principally ones of quality, error correction and enormous scale.

One milestone which increasingly has the attention of Governments is the so-called Q-Day. This day is defined as the day where a quantum computer can derive a private key from a public key quickly enough to make today's public key cryptography insecure in practice.

The Australian Signals Directorate (ASD) refers to the development of a cryptographically relevant quantum computer (CRQC).

Nobody knows when Q-Day will arrive. Estimates vary widely, but some credible assessments envisage a timeframe of 10–30 years. The time for planning is now. Governments and companies are already migrating to post-quantum cryptography.

The reason is something called 'Harvest now, decrypt later'. An attacker can record encrypted communications today and crack them later if, in 15 years, they possess a sufficiently capable quantum computer.

The Australian Government treats quantum as a whole-of-economy issue. In September 2025 the ASD re-released an updated document titled [Planning for post-quantum cryptography](#).

Bitcoin and Ethereum Q-Day Planning

While centralised systems are migrating towards post-quantum cryptography through industry bodies, standards organisations and government coordination, decentralised systems such as Bitcoin and Ethereum are confronting the same problem through open-source research, developer communities and their respective protocol upgrade processes.

Ethereum now has a dedicated Post-Quantum Security research team within the Ethereum Foundation, while Bitcoin developers are actively considering a number of post-quantum proposals through the Bitcoin Improvement Proposal process.

What are the risks?

The risks faced by traditional systems are somewhat different from those faced by cryptoassets.

Quantum computers do not threaten all aspects of blockchain cryptography equally.

Bitcoin's Proof-of-Work mechanism uses SHA-256. Quantum computing could theoretically make searching SHA-256 faster through Grover's algorithm, but this is not regarded as Bitcoin's primary quantum vulnerability. The more significant risk is to the elliptic-curve cryptography used to prove ownership of bitcoin.

A sufficiently capable quantum computer running Shor's algorithm could derive a Bitcoin private key from an exposed public key. This

would affect both Bitcoin's ECDSA and Schnorr signature systems.

Some of Bitcoin's earliest outputs are particularly vulnerable because their public keys have been visible on the blockchain since they were created. However, the issue is not confined to early Bitcoin. Other types of Bitcoin outputs can also expose public keys, including modern Taproot outputs and addresses whose public keys have previously been revealed through spending or address reuse.

Ethereum faces a similar but broader cryptographic migration.

Ethereum's Proof-of-Stake economics are not themselves inherently broken by quantum computing. However, the present consensus mechanism relies on BLS signatures used by validators to sign and aggregate their votes. BLS signatures rely on elliptic-curve cryptography and would therefore be vulnerable to a sufficiently powerful quantum computer.

Ethereum must consequently replace this cryptography before a relevant CRQC emerges. Its current post-quantum roadmap identifies not only validator BLS signatures, but also Ethereum account signatures, KZG commitments and some zero-knowledge proof systems as areas requiring quantum-resistant upgrades.

Preparing for Q-Day

Ethereum

Post-quantum preparation has been part of Ethereum's development roadmap for some

time and in 2026 this work accelerated substantially.

In March 2026, researchers from Google Quantum AI, the Ethereum Foundation, Stanford and Berkeley published a comprehensive whitepaper titled [Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations](#). The paper provides updated estimates of the quantum computing resources that would be required to break the elliptic-curve cryptography used by Ethereum, Bitcoin and other cryptoassets.

In January 2026 the Ethereum Foundation also established a dedicated Post-Quantum Security team and has now published a [post-quantum roadmap](#).

The objective is not simply to wait until Q-Day and then replace one piece of cryptography with another.

Ethereum is being designed so that its underlying cryptography can be changed progressively as technology evolves. This is sometimes referred to as *cryptographic agility*.

There are several parts of Ethereum that will eventually need to change.

The cryptography used by Ethereum wallets will need to become quantum resistant. The cryptography used by validators to operate Ethereum's Proof-of-Stake system will also need to change. Some of the cryptography used by Ethereum's Layer 2 networks and other scaling technology will need to be upgraded as well.

Importantly, work on all of these areas is already underway.

Ethereum is developing new forms of quantum-resistant signatures, together with technology that will allow them to be used efficiently across the network. More than ten Ethereum client teams have been participating in post-quantum testing and there are already public implementations of some of the proposed technology.

The Ethereum Foundation has also established a USD 1 million research prize aimed at strengthening some of the cryptography that may form part of Ethereum's future post-quantum system.

Ethereum's published roadmap envisages the transition occurring progressively. Quantum-resistant technology would be introduced into the network and then wallets, validators and applications would be able to migrate over time.

The Ethereum Foundation currently targets approximately 2029 for much of the core post-quantum infrastructure, although these are planning targets rather than guaranteed dates.

One important development is Ethereum's increasing emphasis on hash-based cryptography. The emerging Lean Ethereum roadmap favours post-quantum digital signatures constructed from cryptographic hash functions rather than mathematical structures such as elliptic curves or lattices. The reason for this preference has become particularly relevant following recent advances in AI-assisted mathematics, discussed below.

The important point is that Ethereum does not need to wait for Q-Day and then suddenly replace its cryptography. The objective is to introduce quantum-resistant alternatives well

beforehand and allow the network and its users to migrate progressively.

Bitcoin

Bitcoin is also actively preparing for the possibility of Q-Day, although the process is quite different from Ethereum.

Bitcoin has no foundation or central development organisation capable of publishing an official Bitcoin roadmap.

Changes to the Bitcoin protocol emerge through research, Bitcoin Improvement Proposals (BIPs), software development and ultimately broad adoption by the Bitcoin network.

Adam Back, the cryptographer who invented Hashcash and is cited in the Bitcoin Whitepaper, has been one of the prominent voices arguing that Bitcoin should begin preparing well before Q-Day. His company Blockstream has developed a substantial body of research into post-quantum Bitcoin security.

The principal quantum vulnerability in Bitcoin is the cryptography used to prove ownership of bitcoin.

A sufficiently powerful quantum computer could potentially derive a private key from an exposed public key and then use that private key to spend the bitcoin.

Bitcoin held in some types of addresses where the public key has not yet been revealed has an additional layer of protection. However, these coins would still ultimately need to migrate to quantum-resistant addresses before Q-Day.

Bitcoin's SHA-256 hashing, which underpins Proof-of-Work, is much less affected by quantum computing. The principal challenge is therefore not to redesign Bitcoin, but to replace or provide an alternative to its quantum-vulnerable digital signatures.

Several parts of a possible migration pathway are already emerging.

BIP 360, known as Pay-to-Merkle-Root, is a draft Bitcoin Improvement Proposal designed with quantum resistance in mind.

Blockstream Research is developing a hash-based post-quantum signature system known as SHRINCS.

Another proposal, BIP 361, *Post Quantum Migration and Legacy Signature Sunset*, considers how Bitcoin could progressively migrate away from its existing digital signatures once an accepted post-quantum alternative becomes available.

Post-quantum signed transactions have also already been demonstrated using Liquid, a production Bitcoin sidechain.

The important point for investors is that Bitcoin's quantum vulnerability is well understood. Replacement technologies are being developed, proposed changes to the Bitcoin protocol already exist and practical testing has begun.

All of this is happening well before any cryptographically relevant quantum computer is known to exist.

Artificial Intelligence and Cryptography

Until recently, the potential threat from artificial intelligence to Bitcoin and Ethereum was principally associated with AI-assisted cyberattacks.

However, developments in early October 2026 have raised a second and potentially more profound concern.

Artificial intelligence may not only make cybercriminals more effective. It may also accelerate mathematical discovery to the point where previously unknown weaknesses in cryptography are discovered.

The distinction is important.

AI-Assisted Cyber Attacks

AI-enhanced cyberattacks are not, in themselves, a known practical threat to the underlying cryptography securing the Bitcoin and Ethereum blockchains.

There is no known practical AI attack that can simply calculate a Bitcoin or Ethereum private key from its public key, defeat the cryptographic hash functions used by these networks or break the elliptic-curve cryptography on which much of their security relies.

The present cyber risk from AI is primarily further up the technology stack. AI can make attackers much better and faster at finding weaknesses in software, wallets, applications, interfaces and human behaviour. It can automate attacks, discover software vulnerabilities more quickly and produce much

more sophisticated phishing and social-engineering attacks.

This type of risk is not specific to cryptoassets.

Banks, governments, technology companies and blockchain systems all use complex software built around underlying cryptographic systems. In each case the cryptography may be sound while the software, device or person using it remains vulnerable.

The Australian Signals Directorate makes much the same point. AI is increasing the speed, scale and sophistication with which cyber vulnerabilities can be discovered and exploited.

However, recent developments suggest that the threat from AI may extend beyond the software systems surrounding cryptography.

AI-Assisted Mathematical Discovery

On 6 October 2026, OpenAI announced the publication of a large collection of mathematical research generated by one of its advanced AI models.

The release included more than 700 mathematical manuscripts, grouped into hundreds of families of results, covering a wide range of mathematical disciplines.

[OpenAI – Sharing AI Progress in Mathematics](#)

The significance of this development is not that AI has broken cryptography. It has not.

Rather, it is evidence that AI is becoming capable of contributing to original mathematical research at considerable scale. The results still require examination and

verification by mathematicians, but the implications could be substantial.

This brings us back to the historical contest between cryptographers and cryptanalysts.

Much of modern public-key cryptography relies on mathematical problems that are believed to be extraordinarily difficult to solve.

Bitcoin and Ethereum, for example, use elliptic-curve cryptography. The public key is mathematically derived from a private key. Reversing that calculation, to recover the private key from the public key, is believed to be computationally infeasible using today's conventional computers.

But this security rests on our present understanding of mathematics.

It is possible that more efficient methods of solving these mathematical problems exist but have simply not yet been discovered.

History provides examples. The development of increasingly sophisticated algorithms for factoring large numbers substantially reduced the computational difficulty of attacking RSA cryptography compared with earlier approaches.

What if AI could discover similar mathematical breakthroughs in a fraction of the time that human mathematicians would require?

That is the question now being raised by two of Ethereum's leading researchers, Justin Drake and Vitalik Buterin.

Justin Drake and Vitalik Buterin – Preparing for an AI Breakthrough

Following OpenAI's announcement, Ethereum researcher Justin Drake called upon the blockchain industry to begin preparing for what he describes as *bunker mode*.

Drake argues that AI-assisted mathematical discovery could potentially produce an algorithm capable of recovering private keys from exposed public keys using conventional computing hardware.

In his assessment, it is reasonable to prepare for the possibility that elliptic-curve cryptography could be broken before Q-Day. He has even raised the possibility that such a breakthrough might occur within months rather than years.

This is a particularly aggressive assessment and remains speculative. There is currently no publicly demonstrated practical algorithm capable of doing this.

Nevertheless, Drake recommends that cryptoasset holders, particularly large institutional holders, consider moving assets to fresh addresses whose public keys have not yet been exposed.

This is a precautionary measure rather than a complete solution.

In Bitcoin, some address types conceal the underlying public key behind a cryptographic hash until the assets are spent. In Ethereum, ordinary externally owned accounts similarly conceal the public key until a transaction is signed.

Other Bitcoin address types, including Taproot, expose public-key information from the outset.

An address whose public key remains concealed would be less exposed to an attack that depends on recovering a private key from a known public key. However, moving assets to fresh addresses would not protect against every possible future cryptographic attack.

Vitalik Buterin broadly acknowledges the concern but takes a more measured position on the immediate response.

He does not recommend that investors rush to move their funds. In particular, he warns that poorly executed migrations may themselves result in the loss of cryptoassets.

Buterin's more fundamental concern is that AI could discover unexpected weaknesses not only in elliptic-curve cryptography, but also in some of the mathematical techniques currently being adopted as protection against quantum computing.

One important example is *lattice-based cryptography*.

Lattice-based systems are among the principal technologies being developed to resist quantum attacks. They underpin standards such as ML-DSA, a post-quantum digital signature scheme.

Buterin argues that the same AI-assisted mathematical discovery that might undermine elliptic-curve cryptography could also reveal previously unknown weaknesses in lattice-based systems.

A cryptographic system believed to be secure against quantum computing might therefore turn out to be vulnerable to a new mathematical discovery made by AI.

This is an important distinction.

Quantum computing threatens certain mathematical problems because quantum algorithms, such as Shor's algorithm ([see here](#)), are already known to solve them efficiently in principle.

The potential threat from AI is different. AI might discover new algorithms that humans do not currently know exist. Those algorithms might then be executed on conventional computers.

Both Drake and Buterin therefore favour greater reliance on *hash-based cryptography* wherever it is technically possible.

Cryptographic hash functions are designed to avoid the exploitable mathematical structure found in elliptic curves and lattices. Hash-based digital signatures, including systems based on Winternitz signatures and SPHINCS+, are consequently attractive candidates for future blockchain security.

This is not a guarantee that hash functions can never be broken. Nor can hash functions alone replace every application of public-key cryptography, particularly public-key encryption.

But the view emerging from Ethereum's research community is that hash-based cryptography may provide a more conservative foundation for long-term security against both quantum computing and AI-assisted mathematical discovery.

This thinking is already reflected in Ethereum's Lean roadmap.

An important qualification is necessary.

There is currently no known practical AI-assisted attack capable of deriving Bitcoin

or Ethereum private keys from their public keys. Nor is there evidence that AI has discovered a classical equivalent of Shor's algorithm.

The immediate risk remains hypothetical.

What has changed is the possibility that the timeframe for discovering fundamental mathematical weaknesses could shorten dramatically.

The contest between cryptographers and cryptanalysts may be entering a period in which both sides are assisted by increasingly powerful artificial intelligence.

Conclusion

Quantum computing and recent advances in AI-assisted mathematical discovery present new challenges to the cryptography underpinning Bitcoin, Ethereum and much of the digital economy.

The Bitcoin and Ethereum communities include some of the world's leading cryptographers and computer scientists, who are already developing and testing new cryptographic systems to address these emerging risks. Importantly, the same advances in AI that may accelerate the discovery of cryptographic weaknesses can also assist in developing stronger cryptographic systems.

The history of cryptography is one of continuous innovation, with cryptographers responding to new challenges by developing

stronger systems. There is every reason to expect that process to continue.

Risks Specific to Our Custodial Arrangements

We are also reassured by the preparations of our principal custodian, Anchorage Digital Bank, N.A. Anchorage has confirmed that its Bitcoin custody arrangements already incorporate precautions to minimise public-key exposure. It has implemented post-quantum cryptography within its security infrastructure and designed its custody systems to accommodate new cryptographic standards without rebuilding the underlying architecture. Anchorage continues to work closely with blockchain developers on future migration strategies and has advised that no immediate action is required.

As always, please do not hesitate to contact me on 04 5090 0151 or at ian@bca.fund if you have any questions.

Best Regards



Ian Love
Founder and CEO
Blockchain Assets Pty Ltd

The content of this newsletter has primarily been prepared by a human, Ian Love. Artificial intelligence may have been utilised for some fact-checking and for providing explanations of some specific words and concepts.

To the extent that any of the information which we have supplied to you may be deemed to be "general advice" within the meaning of the Corporations Act, we draw your attention to:- (a) in preparing, supplying or conveying any general advice, we did not take into account your investment objectives, financial situation or specific needs; and (b) a person should consider whether or not a financial product is appropriate for them with or without the assistance of an authorised representative, having regard to their investment objectives, financial situation or specific needs and any relevant Information Memorandum. Any financial products offered by Blockchain Assets Pty Ltd are only available to wholesale clients.