AUSTRALIAN BITCOIN INDUSTRY BODY

# Laws Amendment Feedback

Treasury Laws Amendment (2022 Measures No. 4) Bill 2022

**December 2022**

[redacted]

# Introduction

## Bitcoin

Bitcoin is a revolutionary invention on par with the printing press, the railroad, heavier than air flight and the internet. Satoshi Nakamoto, Bitcoin's pseudonymous founder, has managed to create something that is both scarce and digital. This gives Bitcoin superior monetary properties to gold, as Bitcoin's supply is fixed, known and fully verifiable, with the instant global reach of the internet. The combination of these two properties make Bitcoin the best form of money humanity has ever seen, superseding gold which for 5,000 years has served this role.

As with any revolutionary technology, the implications of this technology are not fully appreciated by society, even *after* its invention. It is of note that the scientific community denied that heavier than air flight was possible even years the Wright brothers successfully flew the Wright Flyer. Similarly, even 12 years after its invention, Bitcoin is often criticised today in the media. Bitcoin will change society for the better in ways that are not possible to completely understand now, but history provides a useful guide as to the most likely path forward.

Until a century or so ago, human societies converged on a bi-metallic monetary standard based on gold and silver coins, gold being more valuable given its relative scarcity, while silver was more practical for everyday transactions. Technology negated the need for silver in the monetary system, with the combination of banking and communication technologies enabling a purely gold based system. Critically, the countries that were slowest to adopt the gold standard, and continued to use silver, were significantly worse off as result. The reduced demand for silver lowered the cost of acquiring it. The earlier adopters of the gold standard were then able to cheaply buy the assets and resources of those remaining on a silver standard, such as China and India. Please refer to *The Bitcoin Standard* for a more detailed explanation.

A key aspect of Bitcoin is that it is decentralised. This property makes it impossible for any person, body or sovereign nation to change key aspects of Bitcoin such as it's monetary supply. Therefore, two parties who do not trust each other can transact over the Bitcoin network without an intermediary, such as a bank. It is also not possible to censor transactions or stop the use of Bitcoin. Bitcoin can even be downloaded via satellite, and transactions can be sent via SMS. So while some countries will ban the use of Bitcoin in their jurisdiction, they cannot stop it from being adopted in other countries. They will be poorer for it as they will be later adopters of Bitcoin, when the cost to acquire it will be orders of magnitude higher than it is today.

### Altcoins

Being decentralised, Bitcoin does not have a CEO, public relations department, legal representation or marketing budget. As well, because Bitcoin is freely available, open-source software, anyone can download it, modify it and create their own cryptocurrency. While Bitcoin is open-source, and anyone can review its code, not everyone has the skills to do so. Understanding its technical design, which is not intuitive, takes some time and technical skill. Further, the earliest adopters of Bitcoin, generally software experts, have profited enormously from it's initial valuation of zero to its current worth in the tens of thousands of dollars.

The combination of these factors has lead to a host of supposed competitors to Bitcoin, known as altcoins, entering the industry. These altcoins have significant marketing budgets, dubious ethical standards, and have taken advantage of the fact that the majority of people do not understand how blockchains operate. In order to differentiate themselves from Bitcoin, they have sacrificed decentralisation for some other aspect, such as speed or complexity. All of them eventually discover that it is not possible to scale to a global monetary system while remaining decentralised. While some have developed interesting technology, this technology can also be copied and operate as a side-chain of Bitcoin, or run more efficiently from a cloud based server, as software generally is today. Refer to Appendix A for a more detailed explanation.

Altcoins are essentially pyramid schemes. They use their marketing budgets to convince unsuspecting investors that their token will be the next Bitcoin. Investors, overcome with greed, and imagining never having to work again, buy the token. As with every pyramid scheme, the early investors do actually make money. This fact, aided by the leverage available at many exchanges, convinces even more investors to part with their money. Eventually, it is not possible to sustain the momentum, and because no value is being created, the price of the token collapses. The investors lose everything while the founders become rich. Because of these perverse incentives, another coin then pops up with the same story and the situation is repeated. There are literally thousands of examples of this, including a token called PonziCoin (ticker: PONZI) which has a picture of a pyramid as its logo. If enough people believe in a delusion it can appear to be true for considerably longer than a rational person would expect. The cryptocurrency Ethereum, which has the appearance of being a legitimate technology, with even the CME Group offering Ethereum futures, allows its users to deposit Ether tokens into its staking smart contract but not withdraw them. Anyone familiar with pyramid schemes would recognise this as a major red flag. Further, the recent failure of the exchange FTX and its token FTT provides another prominent example of this point.

## Australian Bitcoin Industry Body (ABIB)

ABIB is a member based not-for profit organisation that represents the Bitcoin industry and proponents in Australia. Its members included Bitcoin-only exchanges and wallets, and its sponsors include developers, podcasters, educators and miners.

ABIB aims to progress several objectives:

- To provide a source of accurate information regarding Bitcoin for Australian regulators and media, filling the absence that has resulted from Bitcoin being a decentralised protocol.
- To encourage the adoption of Bitcoin within Australia, to ensure that Australia and Australians benefit from this revolutionary technology.
- To educate its the community on the latest developments in Bitcoin.
- To present a unified voice representing the Australian Bitcoin community.

# Treasury Laws Amendment (2022 Measures No. 4) Bill 2022

The Australian Bitcoin Industry Body (ABIB) appreciates the invitation to make a submission to the Inquiry into Treasury Laws Amendment (2022 Measures No. 4) Bill 2022 [Provisions].

Upon review of the amendments, we have no concerns regarding the way in which the consultation documents have been translated into legal amendments.

We remain aligned with the view that bitcoin and other cryptocurrencies are not foreign currencies, per our submission to the consultation process: *Clarifying crypto not taxed as foreign currency.*

However, we wish to continue to make the point that bitcoin is different to all other cryptocurrencies. It is for this reason that ABIB was formed, as a separate entity to represent the views of the bitcoin-only industry. The arguments for this position have been made in the Introduction and Appendix. ABIB is available for further discussion around this point.

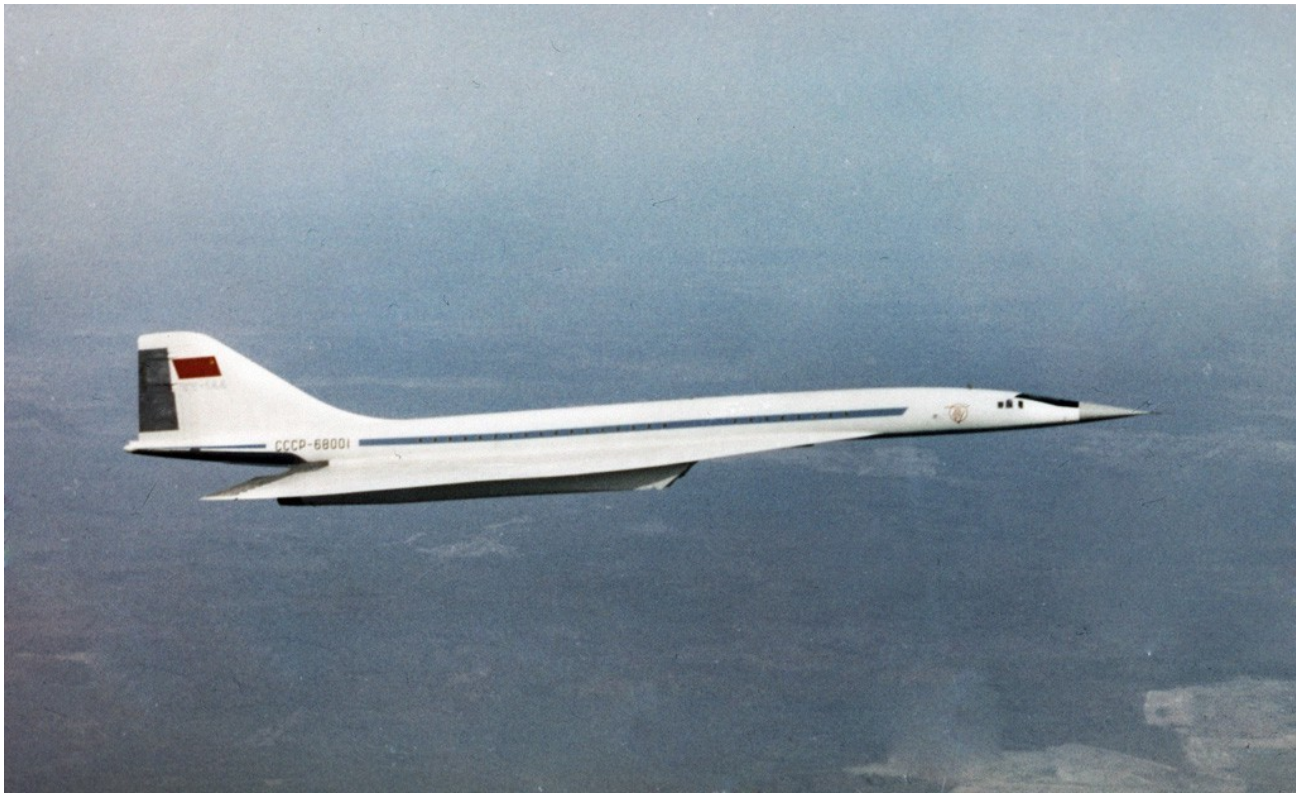
**Australian Bitcoin Industry Body (ABIB)**
ABN: 85 652 894 696 / ACN: 652 894 696
info@bitcoinindustrybody.org.au
www.bitcoinindustrybody.org.au

**Appendix A**

# Why Bitcoin will Outlast Altcoins

By Jeremy Majid - 15 September 2021

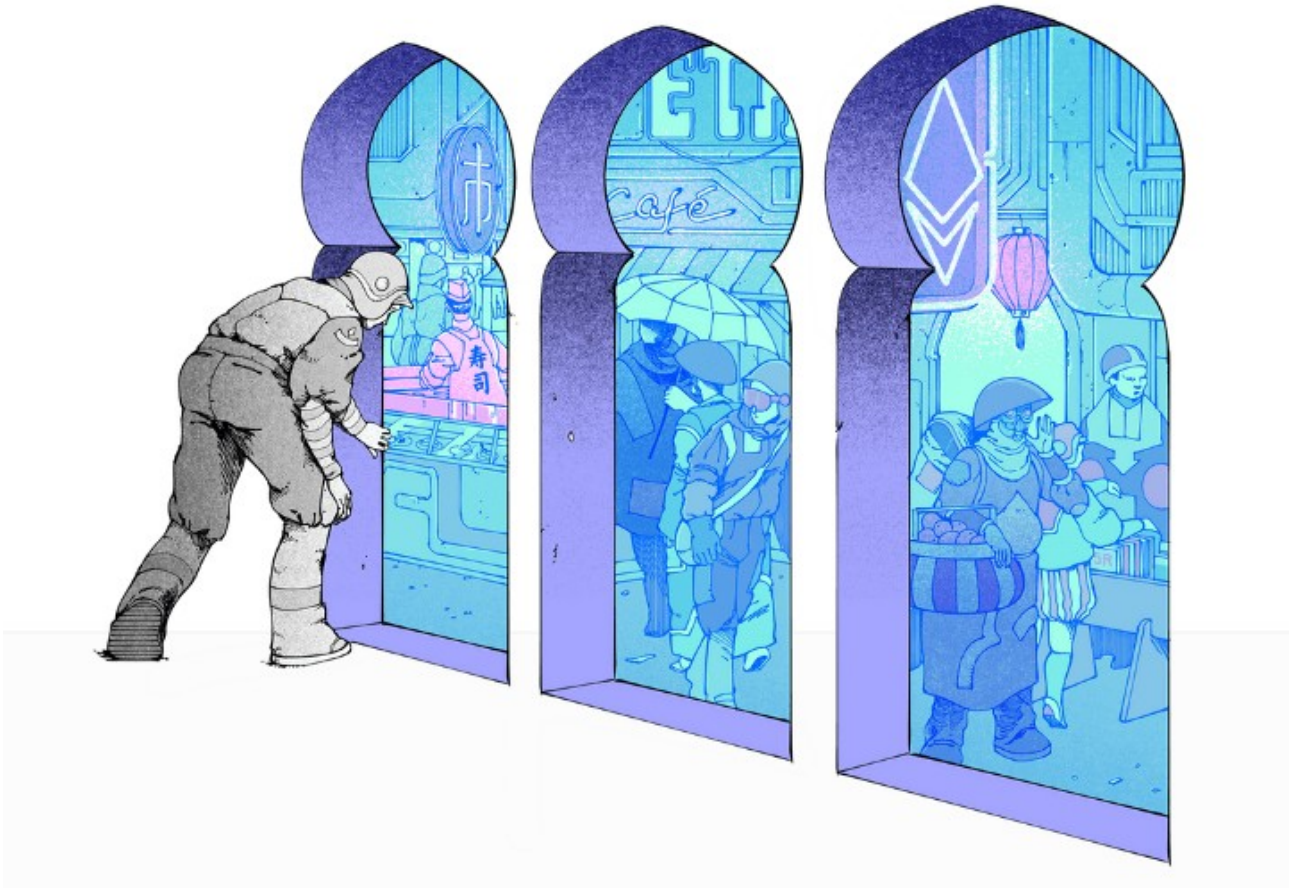
In 1969, within months of each other, two competing projects launched the supersonic era, or so people thought. This was when the Concorde and the Tupolev TU-144 (pictured below) made their maiden flights. Both planes were capable of flying passengers at twice the speed of sound, over 2,000km/h. To give some context to just how major an advance these projects were compared to the commercial airliners at the time, the Boeing 747 had its first flight *after* the Tupolev, in fact only six weeks later.




These two supersonic airliners drove a captivating narrative. They represented the height of human innovation, our mastery over physics. Unfortunately, the supersonic era never eventuated, due to some inconveniences related to the laws of physics, but that didn't stop US$3 billion dollars (1970's dollars, that could buy an ounce of gold for $160) being invested in the Concorde program. An expert in fluid mechanics would have understood at the time why these projects would fail, but likely not be able to explain it in simple terms. In short, flying at supersonic speeds uses a *lot* of fuel. A Concorde used over 14L of fuel per passenger per 100km, not helped by its tiny capacity of 100 seats (for comparison, the 1988 Boeing 747–400 used 3.35L per passenger per 100km and is considered inefficient today). This made supersonic jets incredibly expensive to operate. They also

create a sonic boom (a loud noise that can shatter windows on the ground) meaning these planes could only fly over the ocean. As such, they were only ever a niche offering for the elite. Only 20 Concorde planes and 16 Tupolev TU-144s were ever built. In comparison, over 1,500 747s have been built, and it remains in production, with the last models to be manufactured in 2022.


Something akin to the supersonic narrative has taken hold in the altcoin space. It started with Ethereum, which launched in 2015, and has since inspired new projects leading to the situation today where there are thousands of cryptocurrency tokens. Many have been so captivated by these altcoins, their stories expertly spread with slick marketing, that they have invested significant sums of money. The extreme volatility in the prices of these tokens has attracted hordes of speculators. Some tokens have not even attempted to develop any new technology, simply issuing tokens without a blockchain, and are capitalising on the enthusiasm while they can. While altcoin projects present seemingly cutting-edge solutions, they all contain a technical flaw that can be seen if you look closely enough.




Ethereum Marketing (above) vs Bitcoin marketing (below

Before assessing altcoins, it's important to first understand how Bitcoin works. Bitcoin aims to take layered, hard money, which existed at one point in society, and decentralise it so that no government or central party can debase it. Historically, the layered hard money solution consisted of a secure vault (base layer), that could safely store gold (hard money). From this layer, paper gold-certificates were issued which were redeemable for gold and were used for daily transactions. This system kept the base layer extremely secure, although it was inconvenient to transact with. It ultimately failed as the centralised parties that managed the vaults, realising that citizens couldn't see inside the vault to count the gold, couldn't resist creating extra gold-certificates. This ultimately led to the fiat currencies we have today.


1928 10 Dollar gold certificate. Over decades this became 10 Dollars of fiat currency.

Bitcoin has created a decentralised, digital version of the gold vault that anyone can audit. To facilitate decentralisation, it is critically important that the blockchain (the base layer) is kept to the bare minimum of transaction information, ensuring that the entire blockchain can be stored on affordable hardware. Over the last 12 years, developers have been innovating to fit more transactions into the limited space in each Bitcoin block. It is possible to run your own instance of the Bitcoin blockchain at home, known as a Bitcoin full node. With an old laptop, a 1 TB external hard-drive (around $50 currently) and an unmetered internet connection, a user can run their own Bitcoin full node. With this setup, users can audit the money supply of the Bitcoin protocol at any time and account for every bitcoin in existence.

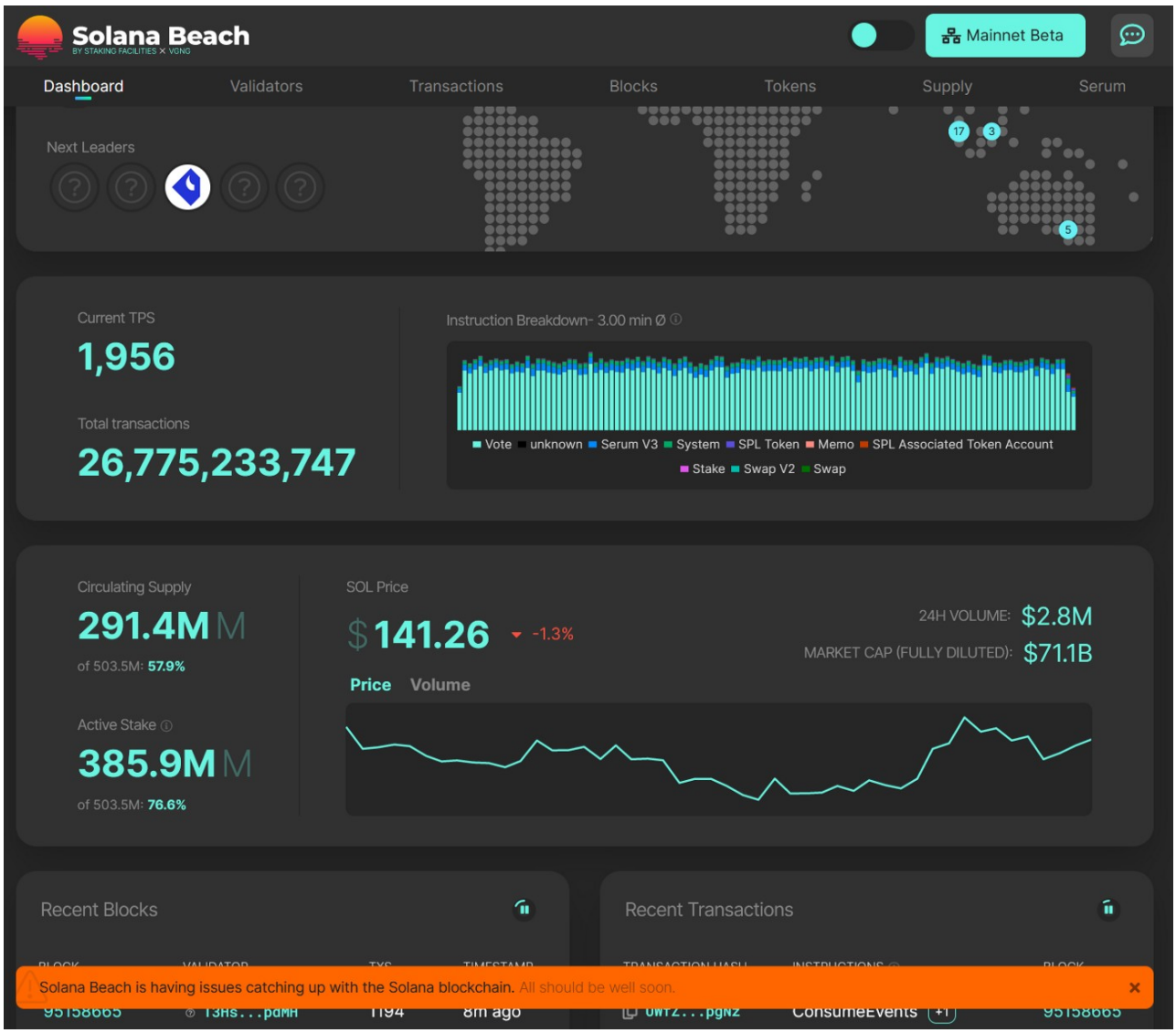
Like a gold vault, the Bitcoin base layer took time to build and is slow to transact with (relative to credit cards), but it is really secure. It's also incredibly resilient, as the focus on making full nodes accessible has allowed it to become highly decentralised (there are over 50,000 nodes running currently). With no party in control, it is impossible to change key elements of the Bitcoin protocol without overwhelming consensus, which is what protects its property as hard money. But the base layer is not, and will never be, a good solution for daily transactions. Instead, a new layer has been

developed on top of the Bitcoin blockchain called Lightning. Lightning is a convenient way of spending bitcoin without compromising the security of the base layer. Transactions on Lightning travel at the speed of light, so they are effectively instant. They are also effectively free (less than 1 cent currently).

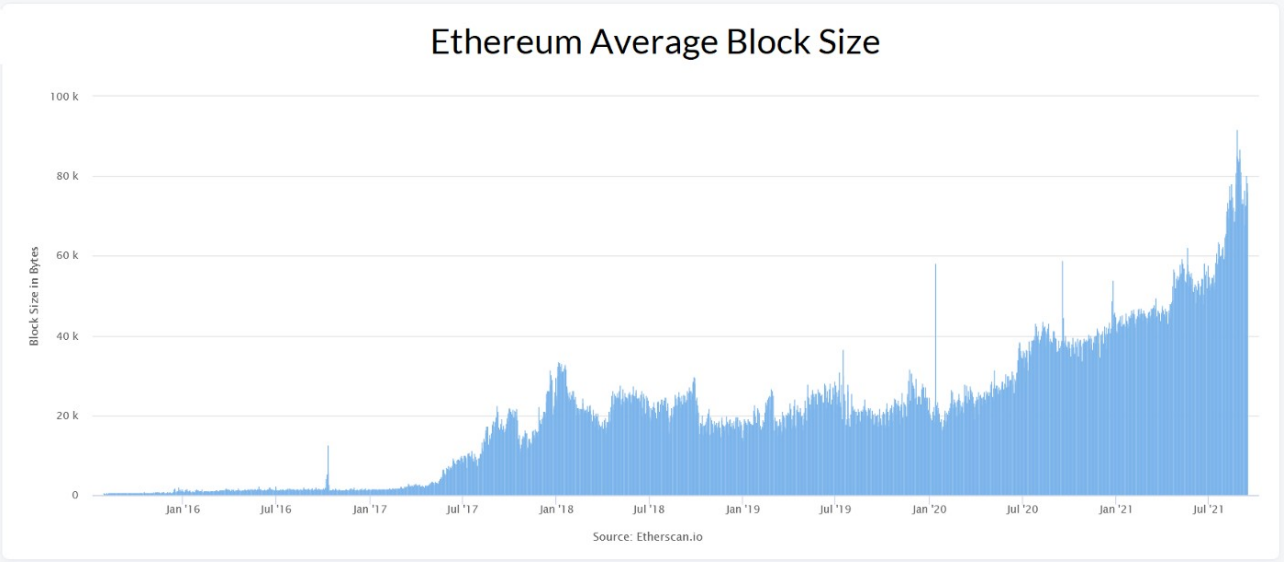
Projects like Ethereum, Cardano, Solana and others claim to offer superior blockchains to Bitcoin. However, they have achieved this by putting significantly more (or all) of their functionality on the base layer blockchain. This has allowed these projects to grow quickly, because they do more things than Bitcoin can currently, like code-based loans ('smart contracts') and issue tokens that represent digital items such as art (NFTs). To do this, they have sacrificed security and decentralisation. Rather than focusing on first building a secure vault, they have bypassed this step and moved straight to the consumer facing technology. It's akin to a bank allowing a grocery store and café inside their gold vault in order to make transactions more convenient. This mentality has unfortunately had predictable consequences, with many hackers helping themselves to some of the tokens. This happens surprisingly frequently, there have already been 20 occasions where more than $10 million has been lost from an altcoin platform.

Ensuring that running a full node is accessible to the average user is critical to maintaining decentralisation. Therefore, analysing how easy it is to run a node gives strong clues as to a protocol's future direction. Bitcoin has been designed so that a node can be run on your computer while you do other work, or on an old laptop that is currently sitting idle. One of the key factors is the RAM (or short-term memory) requirement, which for Bitcoin is 2GB. The recommended RAM requirement on Ethereum is 16GB, as well as a higher specification computer chip and hard-drive. Essentially, running an Ethereum node would require having a dedicated modern computer. A laptop that meets these requirements today would cost over $1,000; not an option for most people.

Then there is all the data being generated. Bitcoin generates up to 1.5MB in each block, which takes on average 10 minutes to generate. Ethereum blocks arrive every 13 seconds, containing an average of 80KB each. Over a comparative 10-minute period, Ethereum would be generating 3.7MB of data. While this figure by itself is not alarming, it is put into context by the scaling plan for Ethereum, which uses a concept called sharding, which increases throughput by creating 63 new blockchains (keeping the current on as the 64th). With sharding, Ethereum would be generating 236MB of data every 10 minutes. As this would very quickly become unmanageable, nodes will only validate one of the 64 chains, or said another way, nodes won't validate 98.5% of transactions. Not to be outdone, Ethereum competitor Solana produces blocks at a rate of 2 per second. This is too fast for the Solana blockchain explorer Solana Beach which was having difficulty keeping up. The fragility of this design became apparent recently when Solana stopped producing blocks for several hours and had to be restarted, erasing transactions in the process.




Anyone investing money into a protocol should make the effort to understand these technical details, they are akin to understanding fuel consumption and shock-waves in airplanes; knowing these details allows you to see early on that a Boeing 747 is going to be much more successful than a Concorde. Looking only at nodes, the logical conclusion as you project out to the future is that Ethereum, and every protocol that has prioritised faster or more complicated blockchains, will require dedicated and expensive hardware and internet bandwidth out of the reach of the average person. In other words, they will become centralised. These centralised protocols will require you to trust someone else to tell you key information such as the state of the token supply, which defeats the purpose of having a blockchain. Anyone familiar with monetary history will know that trusting centralised entities to manage the supply of money has never worked out well.




So, does this mean that all of the innovation currently happening in the altcoin space is being wasted? It does seem that there are some genuine use cases being addressed. For example, decentralised sharing of hard-drive, CPU and GPU capacity could see real world use. As well, while NFTs seem to be in an epic bubble, the ability for digital creatives to distribute their work and receive fair compensation solves a genuine problem. Finally, Arweave's idea of permanent storage could be revolutionary in countries that tightly control the flow of information.

A side-chain or second layer of Bitcoin can already do many of the things being promised by altcoins, such as fast and private transactions, enabling apps to build on it, the transfer of stable coins and issuance and exchange of security tokens. Additionally, a Bitcoin software improvement is currently being worked on that could make it possible for Bitcoin to be both the currency and payment rails for any altcoin project. In the future, it might be possible to take the open-source code from an altcoin project and run it as a side-chain of Bitcoin, using bitcoin as the means of payment. The Lightning layer is just the first glimpse at how the Bitcoin base layer may one day support an entire ecosystem of layers and side-chains that offer a myriad of services in exchange for bitcoin.