Bitnet: A Peer-to-Peer Programmable Money Network

Masayoshi Kobayashi
masayoshikob@gmail.com
www.bitnet.money

Abstract. Peer-to-peer networks based on blockchain technology made possible for value to be transferred from one individual to another without the need for an intermediary financial institution, enabling self-custody and full control of funds by the individual participants of such networks. The evolution of the technology started with the launch of Bitcoin in 2009 with a further breakthrough being achieved by Ethereum in 2015 with the introduction of smart contracts, making money highly programmable, enabling the tokenisation of value through fungible and non-fungible assets, and more. Bitcoin's original intent was to serve as a decentralised medium of exchange, but for reasons we will elaborate further in this paper, it has failed in its core mission, and instead converged into what could be compared to a digital version of gold, or a decentralised digital store of value. Ethereum on the other hand, enables the implementation of more adequate payment technology but fails in being sufficiently decentralised, with more than half of its current supply in circulation (around 70M out of 120M, at the time of writing) being pre-mined, creating an uneven and unfair distribution of the circulating supply of ETH, which is added to the fact it has now migrated from what is seen as an efficient and truly decentralised consensus mechanism, PoW, to an unproven and somewhat fragile PoS consensus mechanism, further favouring big holders at the expense of newcomers. It also has an appointed CEO and a very centralised and concentrated core development team, that hold the *de facto* power to decide on the implementation of improvement proposals that could drive price, adoption, and the distribution of ETH, making such currency resemblant of a security more than what should be a properly decentralised means of exchange. Bitnet aims to solve these issues by conceiving a PoW implementation of Ethereum to run in parallel with Bitcoin and serve as a truly decentralised vehicle for programmable money, with a built-in monetary policy that favours its usage as a means of exchange rather than a store of value, with a predictable and hardcoded supply creation mechanism that allows for a healthy supply growth over time to foster economic expansion, true decentralisation, and fairness.

1. Introduction

The conception of what is now known as blockchain technology by Satoshi Nakamoto in 2009 with the creation of Bitcoin has been a pillar for the development of decentralised technologies that facilitate payments across the globe and empower individuals to take control of their own finances with self-custody. It marked a generational shift in how we understand and use money. This trend has been further exacerbated by the launch of Ethereum in 2015 and the introduction of smart contracts, that in essence made money programmable and enabled it to attend different niches of society with different financial

needs, whilst also facilitating a new era of digital commerce with proof of ownership of non-fungible tokens, both entirely digital and in representation of physical real-world non-fungible assets.

However, both Bitcoin and Ethereum have built-in design or conception flaws that either make them unsuitable to be used as originally intended, in the case of Bitcoin, or fragile and susceptible to failure due to centralisation, in the case of Ethereum.

Bitnet aims to solve these issues by conceiving a Proof-of-Work implementation of Ethereum to run in parallel with Bitcoin and serve society as a truly decentralised vehicle for programmable money, with a built-in monetary policy that favours its usage as a means of exchange rather than a store of value, with a predictable and hardcoded supply creation mechanism that allows for a healthy supply growth over time to foster economic expansion, true decentralisation, and fairness to new users.

2. The Bitcoin Problem

Bitcoin was created to function as a peer-to-peer electronic cash system, but despite its inherent qualities, it fails to do so by design, with its deflationary monetary policy, limited supply, and the lack of programmability. These constraints diminish its use cases whilst impeding its utilisation as a currency due to long settlement times, scalability issues and costly transactions.

a. A deflationary monetary policy leads to overspeculation and other issues.

Bitcoin is set to have only 21,000,000 BTC ever in circulation, which goes against the premise of it being used as a currency due to its inherent deflationary properties. Holders are disincentivised to spend their Bitcoins as they know that as the protocol grows and more people uses it, the increased demand alone would drive its price upwards, making it always more worthy in the future than it is now.

A currency is meant to be used as a vehicle of exchange of value between individuals on day-to-day transactions. By making a currency deflationary by design, the creators or such currency are implicitly hindering economic expansion and its usage by holders as an actual currency, as these will tend to always speculate or be less inclined to spend in order to take advantage of the likely future appreciation of their holdings, and this can cause what is known as a deflationary spiral, further culminating in economic recession or depression.

The monetary policy hardcoded into Bitcoin makes it a great digital store of value, but not so much a currency.

b. Limited supply can lead to takeovers by large institutions or individuals before true mass adoption happens.

As the time of writing, Bitcoin's market capitalisation is hovering around 590 billion US dollars. For comparison, Gold's market capitalisation is currently approximately 12.8 trillion US dollars. As of present, about 19.4 out of the 21 million total Bitcoin that will ever exist have already been mined.

This illustrates how small Bitcoin is in comparison to other comparable assets, and this creates a problem as it fosters inequality by allowing big institutions to purchase outsized

sums of the total market supply of Bitcoin, breaking the ethos of its own creation by disproportionally favouring those that Bitcoin aimed to disrupt.

We are seeing this happen every day with more and more publicly traded companies holding Bitcoin in their corporate balance sheets, and even some central banks around the world starting to do so. This leads to overconcentration of supply and takes the power away from the individual and tacitly transfers it over to those that would need it the least.

c. Bitcoin isn't programmable, creating another layer of issues for its adoption as a currency rather than a store of value.

Different nations and different societies have different financial needs, and often a "one size fits all" approach for monetary policy will most likely create disparities between different layers of society and disproportionally favour or harm individuals depending on their personal circumstances.

Digital currency needs to be programable, so it can attend and cater for the different needs of different nations, communities, corporations, and individuals. It needs to be decentralised in its core whilst allowing for private money to also exist on top of it.

3. The Ethereum Problem

Ethereum came to solve a lot of the issues Bitcoin has as a currency, but it has failed to achieve true decentralisation and after moving from a Proof-of-Work to a Proof-of-Stake consensus mechanism, it made itself even more fragile and susceptible to enforcement actions by regulators that should not have a say in how decentralised protocols operate.

a. Ethereum had an unfair launch, with almost 60% of the total supply in circulation, at the time of writing, being pre-mined and distributed amongst early investors and founders.

Unlike Bitcoin, around 70 million out of the approximately 120m ETH tokens in circulation today have been pre-mined and distributed to early investors and founders.

As the premise of early adoption being rewarded is valid due to the risk matrix it presents, the Ethereum launch was far from being fair, and from day one has created winners and losers in the protocol and left a permanent stain that will never be forgotten.

b. Proof-of-Stake is a novice, fragile, and unproven system, and promotes inequality by design.

The concept of Proof-of-Work can be traced back to 1993, when Cynthia Dwork and Moni Naor were looking for a solution to deter email spam and DoS attacks and came up with an elaborate yet simple way to do so, that required some work from a service provider before requests were processed. Since then, the concept has been further developed and used in numerous large-scale applications, not exclusive to what we now know as blockchain, making it a robust and well-proven security and tampering-proof mechanism.

In short, in the context of a blockchain, Proof-of-Work involves computers solving complex mathematical problems to validate and submit new blocks to the network.

Proof-of-Stake, however, has been recently conceived as an attempt to circumvent Bitcoin's scalability issues, but it does that by fostering further capital centralisation and favouring

large holders, that can deposit their tokens into the protocol to receive rewards, with no work, no maintenance, or real exchange between the protocol and the so-called validators. It works much like a perpetual savings account, where large holders collect block rewards and fees from less favoured users whilst giving nothing back to the network but their promise not to do anything wrong or dishonest.

Proof-of-Work rewards real work and a tangible exchange between miners and the protocol, where miners exchange computational power and energy for currency.

Proof-of-Stake brings with it an array of other issues - such as susceptibility to enforcement actions by regulators - that is outside the scope of this paper, but readers are incentivised to research about the potential risks associated with using Proof-of-Stake to secure what should be a decentralised protocol.

A truly global and decentralised currency cannot use a consensus mechanism that favours large investors and institutions in detriment of the retail users. By doing that, such protocol becomes part of the existing global financial system, not an alternative to it.

c. Ethereum has a very centralised core development team and a CEO.

Ethereum and ETH share more with private companies and securities than with a properly decentralised currency. Having a CEO, developers that hold the *de facto* power over changes made to the protocol, and a foundation that trades their own native tokens isn't resemblant of a technology that can be truly applied fearlessly to create the new global financial system.

A proof of the level of authority its developers have over the protocol is the DAO fork that happened in 2016, when they have opted to revert what should have been immutable transactions to bypass a successful hack attempt in one of its most prominent "decentralised" protocols at the time, indirectly forcing miners to either follow the new chain and adopt it as the actual Ethereum Network, or drop it and risk losing all their revenue.

For those that would then argue that Ethereum Classic would be a good alternative, it still shares a common story with Ethereum up to that fork block, thus sharing all the same foundational defects that makes Ethereum itself not suitable for being used as fully decentralised programmable money network, including the pre-mined supply.

Much like all its smart contract competitors, Ethereum was founded on unsuitable ground, and there is no going back from that.

4. Bitnet

The world is still to see a truly decentralised programable money network that doesn't have any sort of central control, is unbiased, built on a solid foundation, and that allows its usage as a global payments network without the risks associated with Ethereum and other centralised blockchain smart contract networks.

To achieve that, such protocol needs to be conceived on the following core principles:

- To have no pre-mined supply or private allocations, including those to the development team,

- To be free for everyone to participate, have no CEO, and able to foster a core community that appreciates the values of decentralisation and fairness for the new global financial system,
- To be programmable so it can scale and attend different niches of society with different flavours of money, including private money,
- To have a predictable inflationary supply to avoid long-term takeovers and allow for economic expansion,
- To use a Proof-of-Work consensus mechanism that will imply on the tangible exchange of energy and computational power for the creation of new supply,

a. Technological Infrastructure

As Bitcoin has inherent technological constraints that makes it a great store of value whilst also making it an inadequate form of currency, Ethereum's main constraints and issues are conceptual and foundational, making it a great baseline for the launch of Bitnet.

Ethereum's code is open-source and has been well tested since its inception in 2015 and will be used for the initial implementation of the *Bitnet Core Client*.

The network will run on a Proof-of-Work consensus mechanism, and reward miners for their work with the creation of new supply, fostering a predictable inflation rate that enables economic expansion and allows for increased demand as the protocol expands.

The pace in which the core code would be updated would be much slower than that of existing centralised protocols; as much like gold hasn't changed in the last thousand years, a truly effective form of money should be conceived with properties of enough quality that updates and changes can be kept minimal.

Changes to the core code would have to be proposed in accordance with decentralisation principles and would only be implemented upon clear consensus amongst the network miners and users.

b. Monetary Policy

The protocol's monetary policy will be hardcoded and provide for an inflationary supply at a predictable pace, where new supply is created upon the successful submission of a new block to the network and then rewarded to the miner.

b.1 Block Time and Inflation Rate

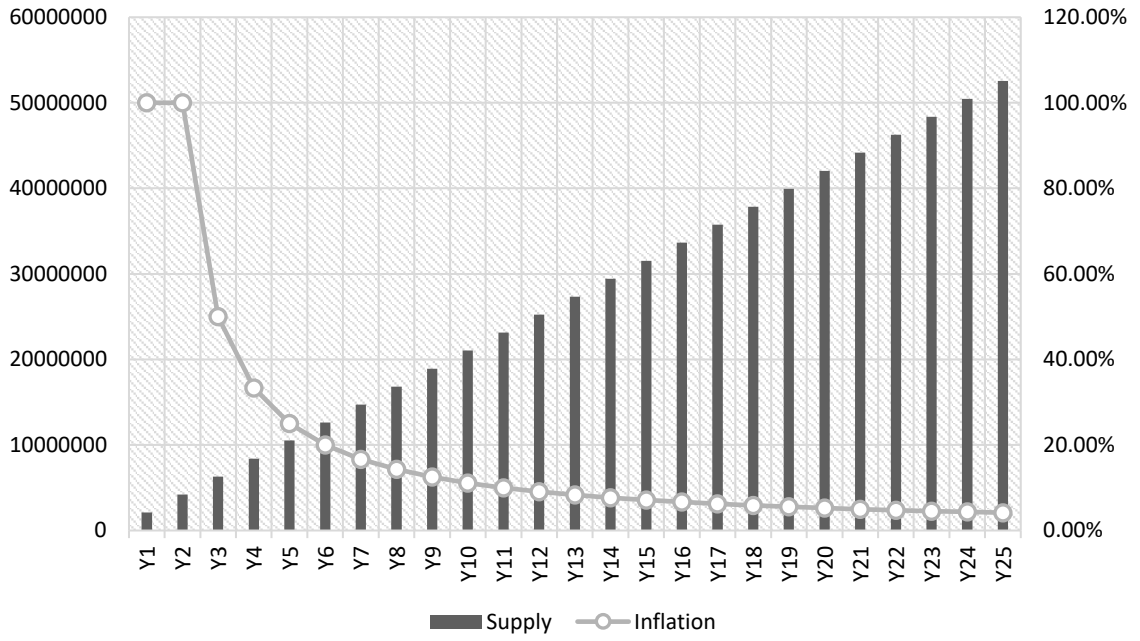
The network averages 15 seconds between blocks by design, and upon the successful mining of a new block, 1 new Bitnet is created. As block times may vary due the nature of Proof-of-Work, this layout creates a semi-constant of 2,102,400 new Bitnets being added to the global supply every year:

$$4_{\text{blocks per minute}} * 60_{\text{ minutes}} * 24_{\text{ hours}} * 365_{\text{ days}} = 2,102,400$$

This creates a dynamic where the inflation rate lowers as more blocks are added to the network - as the new supply will always be added on top of previously existing supply - but will never reach zero.

The dynamic rate of inflation with a fixed reward rate allows for more aggressive inflation during the initial years of the protocol, which will help promoting economic growth and adoption, and as the protocol matures and the inflation rate drops, the thesis is that there would be less market volatility and more price consistency, ever strengthening the role of Bitnet as a form of decentralised currency.

The chart below illustrates the expected inflation rate for the first 25 years of the protocol against the supply creation for the same period. An important remark is that the first years of inflation present higher rates due to the non-existence of an initial supply to refer back to – as if we add 1 unit onto 1 unit we have a 100% increase, if we add 1 unit onto 100 units we would have only 1% increase, even though in absolute numbers the inflationary rate would still be the same.



The table below illustrates the expected inflation rate for the initial 50 years of existence of the protocol.

Year 1	100%	Year 11	10%	Year 21	5%	Year 31	3.33%	Year 41	2.5%
Year 2	100%	Year 12	9.09%	Year 22	4.76%	Year 32	3.23%	Year 42	2.44%
Year 3	50%	Year 13	8.33%	Year 23	4.55%	Year 33	3.13%	Year 43	2.38%
Year 4	33.33%	Year 14	7.69%	Year 24	4.35%	Year 34	3.03%	Year 44	2.33%
Year 5	25%	Year 15	7.14%	Year 25	4.17%	Year 35	2.94%	Year 45	2.27%
Year 6	20%	Year 16	6.67%	Year 26	4%	Year 36	2.86%	Year 46	2.22%
Year 7	16.67%	Year 17	6.25%	Year 27	3.85%	Year 37	2.78%	Year 47	2.17%
Year 8	14.29%	Year 18	5.88%	Year 28	3.7%	Year 38	2.7%	Year 48	2.13%
Year 9	12.5%	Year 19	5.56%	Year 29	3.57%	Year 39	2.63%	Year 49	2.08%
Year 10	11.11%	Year 20	5.26%	Year 30	3.45%	Year 40	2.56%	Year 50	2.04%

b.2 Incentives and Fees

Miners will be incentivised to participate in and secure the protocol by receiving newly minted supply and usage fees for every block mined.

For every transaction submitted to the network, users will pay a fee, known as gas.

Gas fees are measured in Gwei, and each Gwei equals 1e-9 of a Bitnet. The amount users will pay as gas fees is dynamic, and reflective of the network's usage capacity at a given point in time.

c. Expected Performance

Bitnet will have reliability and decentralisation at its core and will be conceived to serve as a base layer for further innovation and potential layer-2 scaling solutions that can add to the overall network performance and use-cases.

To increase throughput, Bitnet allows block sizes up to 10 times larger than Ethereum, being capable of processing up to 7,142 raw transactions per block, or 476 raw transactions per second. The extra capacity doesn't necessarily mean that transactions will be processed faster than they are on Ethereum, but that the network has more capacity to process multiple transactions at the same time.

5. The Purpose

The core purpose of existence of Bitnet is to be a decentralised core technology that can be used by individuals, businesses, and governments to shape the new global financial system; one that is inclusive, self-custodian, decentralised, international, and above all, that empowers the individual to choose how they manage their own money, without the constraints of being dependent on centralised custodial services, companies, or governments alike.

6. Conclusion

As of today, the entirety of the digital assets market has only one truly decentralised protocol, which is Bitcoin. However, Bitcoin has fundamental design flaws that impede it to become a global currency, and proof of that is that the perception of Bitcoin is evermore trending towards a store of value rather than money, with it often being called digital gold. Ethereum, which is by far the most prominent protocol that has the technology able to power what could be global programmable money, lacks the decentralisation and fair distribution of funds to do so. Bitnet merges the inherent qualities that make Bitcoin a solid decentralised store of value and Ethereum's technology to create what is a true global currency that can be used by anyone, anywhere, and cannot be shut down or have regulations forced upon it. It also allows for the creation of programmable private or sovereign money, the tokenisation of value on the internet, the issuance of non-fungible tokens, and the further implementation of scaling solutions that would leverage on Bitnet's decentralisation and security to create purpose-built layer-2 solutions.