IPPAN: A new decentralised blockchain dedicated to massive workload implementations.

Kambei Sapote

www.ippan.com

Abstract. Blockchain is the new tech trend and an attractive area of investment for many industries because its technology helps to reduce costs by improving traceability, transparency and tradability. At IPPAN, we have created a powerful decentralised multi-channel blockchain, based on internal absolute time (IIT) and Proof of Validation (PoV), that is specifically designed for massive workload implementations. This new approach to the development of this technology has permitted IPPAN to build a less energy-intense blockchain, greener and sustainable, while being able to fully operate a theoretical unlimited amount of transactions per second. IPPAN can easily be adopted and implemented by different industry sectors to streamline their processes and make them more efficient. IPPAN can be used to transfer BTC via the Lightning Network (LN) or it can easily be integrated by social networks and/or game platforms to manage their internal payments and rewards.

1. Introduction

In recent years, blockchain has emerged as a revolutionary digital tool that has captured the attention of many, because of the potential of its decentralised technology that can create new foundations for the way private and public organisations can manage their databases, and it is considered essential to build

the new generation of World Wide Web, with all its potential incarnations, including the Metaverse. However many are the challenges ahead. The majority of the blockchains currently available are still facing development issues in relation to sustainability, decentralisation, security and scalability.

The problems and the contradictions that have emerged so far in the blockchain sector, have been the premises of the work behind IPPAN.

The aim of this paper is to introduce the reader to the IPPAN blockchain, its innovative technology, its architecture, its advantages by starting with a brief review of the current state of the art of blockchain technology, before entering into the details of the solutions we have adopted.

2. Problems & Contradictions

2.1 The myth of “trustless” blockchains vs. the real experience

With the currently available blockchains, efficiency and scalability are often scarce and the conceptual and practical developments done so far to address these problems seems frequently contradictory.

In the case of Bitcoin, for example, in order to build a trustless system, the Proof-of-Work (PoW) was created as an elegant solution for generating consensus, based on the majority of computational power available. The mining process was initially conceived as based on home-computers connected to the network: the perfect epitome of a new type of web-democracy[1]. However, in the real world, this solution soon deviated from its original scope, introducing subtle forms of centralizations.

- In PoW systems, verification of transactions is *de facto* centralised because of the necessity of very high computational power, now only available to specialised mining farms.
- In Proof-of-Stakes (PoS) systems, verification of transactions is entrusted randomly only to a few generally unknown major stake coin owners.
- In other cases of hidden tokenization or off-chain operability, direct auditability of all transactions on the principal blockchain is precluded.

Blockchains, though self-proclaimed “trustless” systems, have proven to require a great deal of trust from and towards many subjects:

- Large mining farms that have become centralised points of failure and control in the governance of many blockchain networks based on PoW;
- Big crypto-assets holders that are validating blockchain transactions in PoS based systems;
- Core developers, because of their central role in the the production and the maintenance of the code, which is generally done in a considerably centralised and hierarchical way;
- Crypto-currency exchanges, for the correctness of the operations;
- Blockchain explorers, for the reliability of the records they display;
- Wallet custodians, to reduce the risk of misuse of private keys or assets.

It can be argued that the definition of blockchain based systems as “trustless” is somehow misleading.

In addition, in terms of efficiency, the actual trustless solutions can be considered not fully satisfactory based on the below considerations.

- The computational power requested by the current systems are environmentally unsustainable;
- The fees of transactions are still way higher than those requested by traditional financial institutions;
- The available systems can process just a negligible fraction of transactions necessary to boost a real technological transformation in the world.

2.2 Quantum computing and its impact on actual cryptographic system

Another challenge to blockchain technology is the future advent of Quantum computers that poses a significant threat to information security, because they can successfully attack traditional cryptography and therefore underpin the

security of the cryptographic systems commonly used also by blockchain platforms.

Both the NCSC (the UK National Cyber Security Centre) and the NSA (the US National Security Agency) agree that the best defence against this threat is the adoption of post-quantum cryptography, and official standards were announced in 2022.

2.3 Identity & Anonymity

Anonymity and the lack of identity have been for years the libertarian aspiration of the Internet, often considered as a manifestation of freedom and democracy.

Nonetheless, identity is a necessity not only to avoid the abuse of anonymity, but also to claim what the user owns and what directly concerns him/her. Therefore the real problem is how to establish and to prove identity without unnecessary disclosure of information. The current centralised digital identity ecosystem needs to be completely restructured into a decentralised and democratised architecture and, again, this is where blockchain technology can play an essential role in building a fairer internet, but at present it is still an open issue.

2.4 “Timeless” Blockchains

History of time shows that it has always been difficult to measure it precisely.

Technological inventions such as the radio or the atomic clocks have asserted the notion of exact time, although this is still not an accurate and universally shared value, also for political reasons.

When originally conceived, blockchains were intended as a system to connect relevant events to time; a sequence of time-stamped containers of data, the blocks, all linked cryptographically so that it was not possible to alter them retroactively without modifying the following ones. In practice, blockchains tend to give time a substance, creating a ‘before’ and an ‘after’.

Indeed when coding Bitcoin back in 2008, Satoshi Nakamoto used the expression “time-line” while the term “blockchain” came into use only a few years later.

Inspired by the work of cryptographers Stuart Harber and W. Scott Stornetta, who invented the first chronological chain of hashed data to timestamp digital documents in order to verify their authenticity, Natoshi Sakamoto added an extra feature to the blockchain of his cryptocurrency: the PoW, to transform the platform into a “trustless” network of peers, but also to create a regular temporal sequence of reference for the creation of the blocks, practically inventing a new type of clock[2].

The currently publicly available blockchains are based on the assumption that there is no trusted source of time and consequently the inability of the peers in the networks to keep the exact time greatly limits their efficiency.

In light of the above considerations, it emerges the need for a new type of blockchain, technically and economically more efficient and scalable.

To start with, IPPAN has adopted different solutions where it is possible to safely maintain the exact time of reference for all peers without going through artificially overcomplicated timestamping processes.

3. IPPAN’s architecture

IPPAN’s network has a decentralised architecture with four categories of interacting elements:

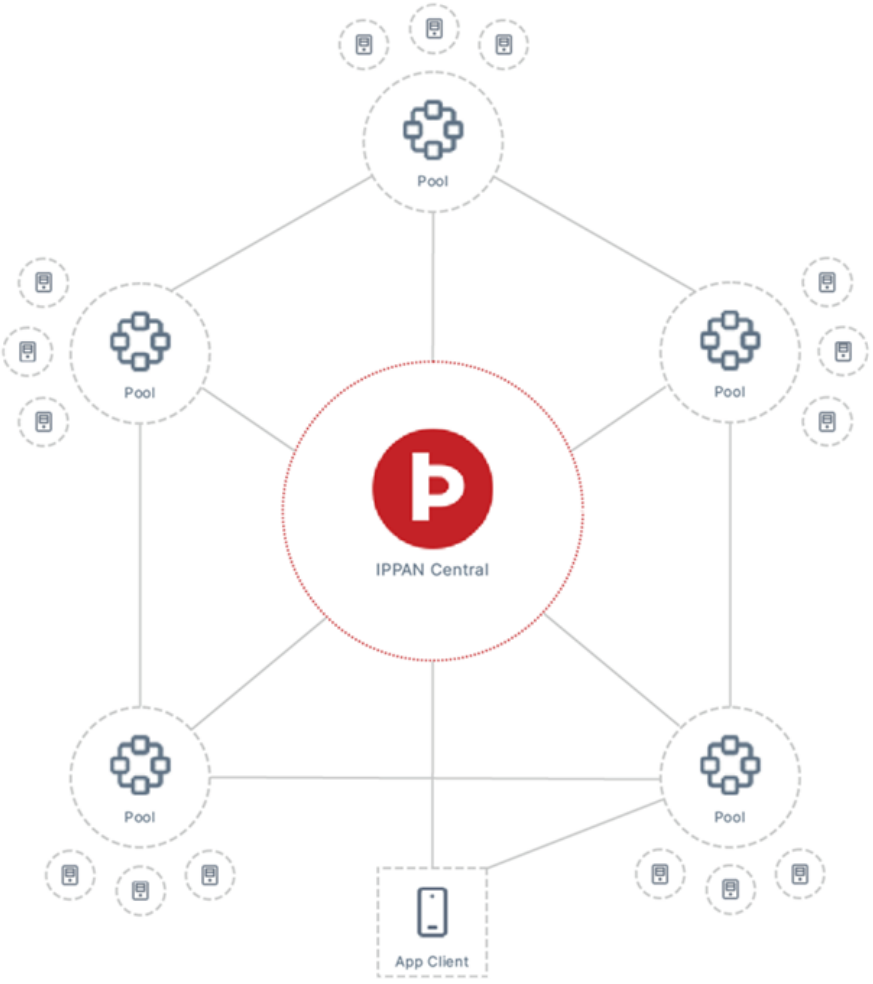
- IPPAN Managing Cores
- IPPAN Verification Nodes
- IPPAN Communication Nodes
- IPPAN Users

IPPAN Managing Cores are a distributed cluster of super-nodes that make possible the automation of the system, replicating and guaranteeing consistency of the data all over the network and, by design, they are unrelated to the transactions verification process. They are hierarchically deployed and, in case of temporary failure of the main central node, another available core is automatically elected as a substitute.

IPPAN Verification Nodes verify the transactions according to a Proof of Validation (PoV). Each prospective validator is included in a list and later called

for the task, according to an unpredictable calculation based on the HASH of the previous block.The network automatically priorities and indexes all transactions according to their timestamps, which accelerates considerably the creation of new blocks. The creation of new blocks must be also confirmed and double-checked by other randomly designed validators according to a Byzantine Fault Tolerance Algorithm (BFTA).

IPPAN Communication Nodes (AKA “NetWorkers”), constitute an optimised Shared Content Delivery Network that operates according to permissioned governance criteria, based on a idea of rewarded decentralisation of resources. They receive fees in exchange for their service.



IPPAN Users are identified in the network (including associated chats, game platforms and social networks) by the HASH of their public address that can be also connected to a unique personalised name to be registered as NFT in the IPPAN blockchain. This IPPAN NFT Domain also constitutes a private address to receive payments and rewards.

4. Blockchain with absolute time

The exact time of the atomic-clocks in the satellites orbiting earth is now available to everyone through the GPS-receiver of smartphones and/or computers. GPS-time can be substantially different from the time given by the clocks of local networks and it is globally considered exact although sometimes GPS signals can be jammed in limited geographical areas, via illegal or military devices.

In IPPAN blockchain time-stamping is based on all the time-data shared and pooled up by the users of the network.

Thus, the time is the result of the prevalent time in the whole global network called IPPAN Internal Time (IIT): an acceptable absolute time of reference. IIT is obtained by applying the following formula:

$$IIT = \frac{1}{n}\sum_{i=1}^{n} a_i + \lambda_i$$

- n= maximum number of entries
- i= current entry
- a= single time values
- λ= total delay

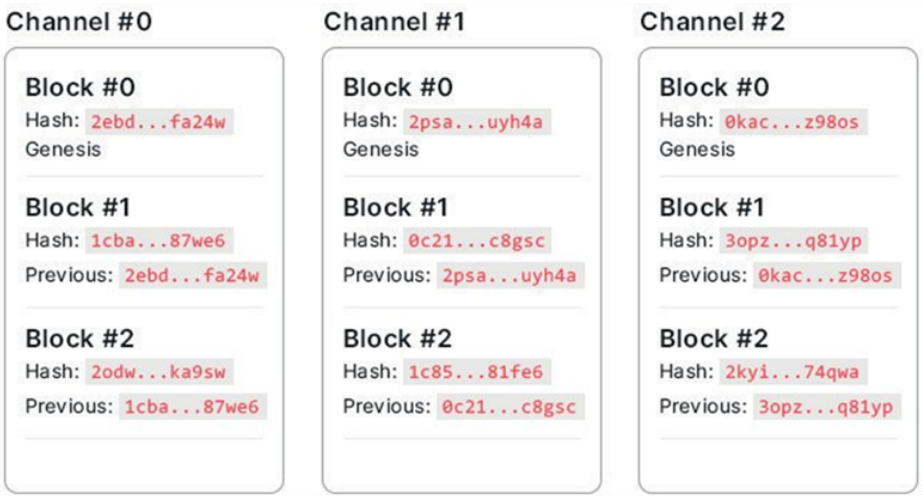
By means of this formula the average of the sum of the entries is determined by discarding all those that are out of the trend and by applying an iteration to generate the most reliable result.

Verifier node	Timestamp
Node 1	2022-01-03 20:37:39
Node 2	2022-01-03 20:37:38
Node 3	2022-01-03 20:37:39
Node 4	2022-01-03 20:37:40
Node 5	2022-01-03 20:37:42
IIT	2022-01-03 20:37:39

5. Scalability & Parallelism

IPPAN blockchain can potentially process more than one million transactions per second, the only limit being the Internet available bandwidth. It implements a proprietary multi-channels structure, so that blocks are efficiently generated in parallel, while each block has an identified channel.

Different channels allow multiple miners to exist, avoiding clashes during the mass production of blocks. Each block and transaction can be marked for different purposes, to facilitate indexing or the deployment of special protocols, such as currency destruction, refunds (no fees charged), and other large number of customisable solutions.



6. Privacy & Traceability

In IPPAN there are four types of addresses:

a) **Public**: this address identifies the user on the network. It can be used to receive payments from other addresses. It is identified by starting with the number 1 and uses the Base58Check format with SHA3-256 and RIPEMD-160 hashes, its size is 21 bytes

19mZZQ1kQi7LCHyHNrErXGwNpqBzVtzGYA

b) **Internal**: at this address, the account receives all payments from the system, such as coinbase transactions and commissions. It is identified by starting with the number 2 and uses the Base58Check format with SHA3-256 and SHA1-128 hashes, its size is 21 bytes.

2GB2uxrPiSUKE38Fm9Eo6Zm1hCz3MLawx4

c) **IPPAN Transaction Combined Address** (ITCA): it is an address made up of the personal address of the sender plus the public address of the receiver, applying the SHA3-224 Hash function. ITCA addresses are unique per recipient and are not repeated, allowing to view the recipient's payment history. This proprietary technique allows the total holdings of the parties to be kept private (privacy) but, when necessary, allows the identification of the actual sender/receiver or the total amounts of the transactions (traceability). It uses the cryptographic keys and the DH (Deffie-Helman) public key; its size is 29 bytes and it is identified by starting with the number 3.

3ARRuFuk6goHNRNbnDjuUorS516mi91dFxyUnCD

$$x = SHA256(DHPkey)$$
$$y = SHA256(Pkey)$$
$$Hmac224(x, y)$$

d) **Anonymous** (experimental): Like the previous one, it creates a unique address between sender and receiver, this is built by creating a new random value between the parties, therefore it requires interaction (e.g.: Chat), it is multi-signature and the size of the address is 21 byte.

	Size	Anonymity level	Fees	Multi-signature
Public	21 bytes	-	Low	No
Internal	21 bytes	-	Low	No
IPPAN Transaction Combinied Address (ITCA)	29 bytes	Moderate	Low	No
Anonymous	21 bytes	High	High	Yes

7. Post-Quantum security

IPPAN implements post quantum cryptography to manage user authentication and identification.

Each transaction is signed with a cryptographic algorithm, resistant to post-quantum computers and efficient for key generation. IPPAN is also an immutable distributed ledger where data cannot be tampered with.

8. Flexible updates

The design of IPPAN allows the blockchain to be updated, customised and modified without major disruption to its functioning; therefore it can be easily updated to meet new regulatory requirements, to improve efficiency, to face integration issues without putting the system on hold.

9. IPN the native token

In IPPAN, the system of rewards and fees is carried on via a token called IPN (token symbol Þ) that is the main currency of the platform.

Each IPN is divided into 1,000,000,000 units called nano-IPN (nÞ).

10. Multitoken

The blockchain has the capability to support and to host other tokens. This feature allows endless exchanges between coins or products on the same blockchain, within the same ecosystem.

Name	Description	ID Format	Max Size
Digital	Crypto currencies	**Undefined**	3-10
Currency	Fiat currencies	**F-AAAAA**	3-10
Metal	Precious metal, renewable resources	**M-AAAAA**	3-10
Asset	Shareholding	**A-XXXXX**	3-10
Inconsumable product	Unlimited transactions	**PD-XXXXX**	4-24
Consumable product	Transferable once after coinbase	**PDc-XXXXX**	5-24
Unique product	Unique (amount just one), NFTs	**PDu-XXXXX**	5-24
Expirable product	Transferable before expiration date	**PDe-XXXXX**	5-24

The types of tokens are specified by their identification prefix (ID) and each type of token has a different feature of operating within the blockchain.

Name	Coinbase limit	Transferable	Expirable	Withdraw	Destructible
Digital	-	X	-	-	X
Fiat currency	-	X	-	X	X
Metal	-	X	-	X	X
Asset	-	X	-	-	X
Inconsumable	-	X	-	-	X
Consumable	-	Once	-	-	-
Unique	1	X	-	-	X
Expirable	-	Before expiration	X	-	X

11. The BTC-token in IPPAN: the Lightning Network (LN) Integration.

Bitcoin is currently considered an asset like gold - a cryptocurrency to store value. IPPAN offers a valid solution to increase its adoption among a wider public via BTC denominated tokens:

-1) an amount of BTC is deposited in a multisig address in the BTC blockchain;

-2) a corresponding amount of BTC-IPPAN tokens is automatically created on the IPPAN blockchain;

-3) the BTC-IPPAN tokens can be freely used and exchanged between the users of the IPPAN network;

-4) to receive back BTCs, the tokens are burned and a payment is made to the last BTC token holders via the Lightning Network.

12. Byzantine Fault Tolerance Consensus Algorithms (BFTCA)

In IPPAN, permissioned governance guarantees that all nodes of the network are to be considered reliable. To be accepted as a verifier node, a series of criteria should be satisfied; the candidate should be physically identified and his/her performance, which is continuously under scrutiny, is awarded with a reliability score (Proof of Reliability) that also increases the chances of receiving Nuggets (random awards periodically raffled off between all

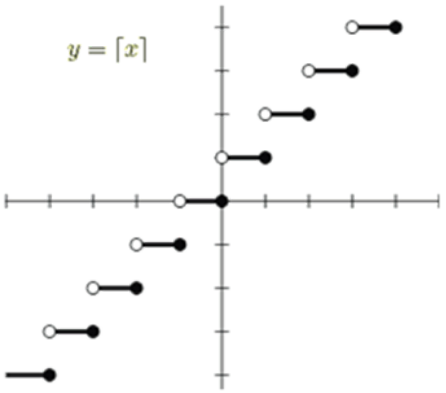
validators). Therefore good behaviour is incentivized, while malicious or technically below standard ones lead to permanent elimination.

In IPPAN the decisional mechanisms are governed by Byzantine Fault Tolerance Consensus Algorithms (BFTCA). The following rules are applied:

1. At the beginning of the communication between nodes, the receiving node verifies that the sending node shares a compatible configuration.

2. Transactions and Coinbase operations should be confirmed only by the verifying nodes active within the same specific channel of the blockchain.

3. The transaction is considered confirmed and registered in the blockchain only if it has reached the consensus of at least one third of the available nodes, calculated with the ceiling function (which gives back the least integer greater than or equal to this value x).



4. If the required consensus is not obtained the transaction is rejected.

The available nodes are those that are operational and registered in the whitelist for verification processes.

13. Transaction Verification

When a payment is made, the request for validation and confirmation occurs according to the following procedure:

1. The client's application executes a query to one of the blockchain's explorer nodes in the platform, to obtain the Unspent Transactions Output (or utxo) that is sorted in chronological order according to its time of creation, from the oldest to the most recent.

2. The client's application creates the transaction structure, calculates the fees, generates the hash and it signs the transaction with a post-quantum signature.

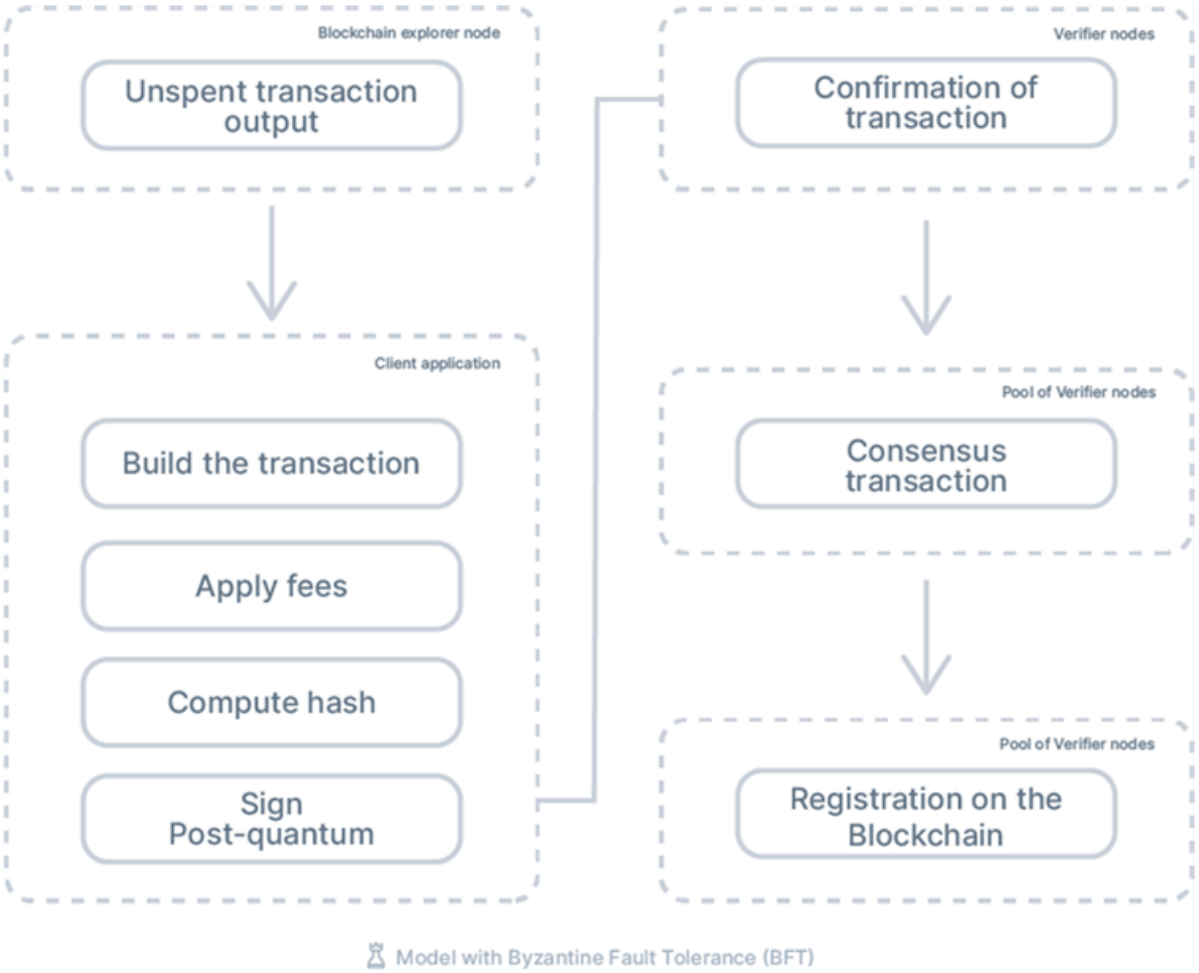
3. The transaction is sent for approval and confirmation to a pool of verification nodes in the network.

4. The prospective Verifiers are included in a whitelist where they are raffled off according to an unpredictable calculation, based on the HASH of the previous block. These randomly designated Verifier nodes check and approve the data provided according to Proof of Validation (PoV).

5. The creation of new blocks need also to be confirmed and double-checked by other randomly designated validators according to a Byzantine Fault Tolerance Algorithm (BFTA).

6. If confirmed, the administrator node sends a notification to the beneficiary and the funds are available for spending.

7. The transaction is recorded in the IPPAN Blockchain.



The nodes of the network validly included in the whitelist share the fees of the transactions and they are entitled to participate in a daily lottery (Nuggets), where new IPNs are generated and distributed, according to a predictable curve of distribution. It is a new type of mining.

14. Monetary mass and inflation

IPPAN, as well as any economic system, requires a sufficient amount of currency to enable exchange of value between its users.

Currency should be available and not scarce but also not over abundant to become worthless. That is why in IPPAN the generation of money is always controlled according to the calculated inflation rate of the system (IPPAN Inflation Algorithm):

$$p_c = \log(n) \times k \times v$$

Where:

Pc = Production of new IPN coins in the network (Coinbase)

n = Number of active users

k = constant (0.27)

v = % of increase of the Velocity of Money

Whereas:

“v” (velocity) is:

$$v = \frac{VT}{M}$$

• VT= volume of transactions in a given time

• M= monetary mass

The monetary mass is made up of all the IPN coins created in the network, which is a piece of information that is verifiable at all times.

The result of the value of this formula cannot be greater than 1, nor less than 0.25 and the formula is determined every 10,000 blocks (weekly).

In correspondence to lower or higher inflation, the generation of new tokens can be increased or cooled off even with extreme measures like the destruction of tokens (burner), and new and different rules and criteria can be applied according to unpredictable necessities.

15. Conclusion

We created an innovative multi-channel blockchain with decentralised architecture, permissioned governance, based on an internal absolute time that is specifically dedicated to massive workload implementations. IPPAN can process theoretically an unlimited amount of transactions per second in a highly energy-efficient way, being the only limit the speed of the available bandwidth.

IPPAN can be integrated in any social network or gaming platform as a new global system of payment and rewards.

IPPAN blockchain can also accept authorised third-party tokens (including CBDCs) or tokens representing banking or financial instruments (e.g.: Collateral Debt Obligations). Tokens can be also redeemable for physical currency or subject to conditions or unicity (e.g.: NFTs, time-locked tokens, time expiring tokens). Tokens can also be used to transfer BTC via the Lightning Network (LN) and to use BTC with very low fees within the platform.

In IPPAN authorised third parties can also issue (or, if required, destroy) digital currency or other tokens according to their set of rules (smart contracts).

---

[1] [*cf. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, p. 3 : "Proof-of-work is essentially one-CPU-one-vote"*].

[2] [cf. *Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, p. 3 : "To compensate for increasing hardware speed (...), the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases"*].