VCOINS

***Abstract*— A peer-to-peer cryptocurrency based on Satoshi Nakamoto's Bitcoin with a novel consensus mechanism that employs Artificial Intelligence and Proof of Stake. This hybrid approach ensures fair participation of honest miners while preventing monopoly over the network by the miners with more stake power. Moreover, this approach ensures minimal energy consumption for mining the block.**

Keywords—Cryptocurrency, Distributed Ledger, Vcoins, Blockchain

I. INTRODUCTION

A. *What is Blockchain?*

Blockchain doesn't hold any specific definition but can be referred to as a technology introduced via Satoshi Nakamoto's Bitcoin [2]. Simply put, it is a tamper-resistant distributed ledger secured using cryptography principles, based over a Peer-to-Peer network. The Blockchain enables a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network, no transaction can be changed once published. The idea of blockchain has been around since 1980, when Merkle Tree, a linked timestamping and verifiable log was introduced, which became the foundation principle of blockchain technology, followed by Byzantine Generals Problem and Game Theory which glorified the unimaginable aspects of this technology. A chronological advancement over the years in blockchain technology are shown in Fig. 1.

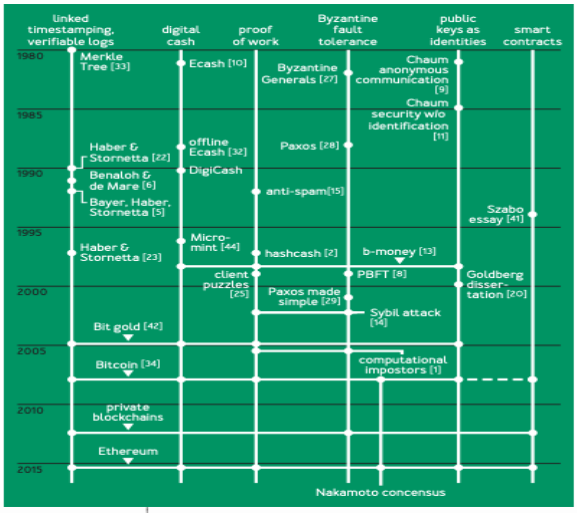

Fig. 1. Chronology of key discoveries in Blockchain [8]

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one making it immutable in nature. As new blocks are added after validation and undergoing a consensus decision, older blocks become more difficult to modify making the chain tamper resistant. New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. Blockchain is also time-stamped ledgers that are maintained by a set of nodes within a network, who are responsible to keep the chain updated [3][4]. A general representation of interconnected blocks in blockchain is shown in Fig. 2.

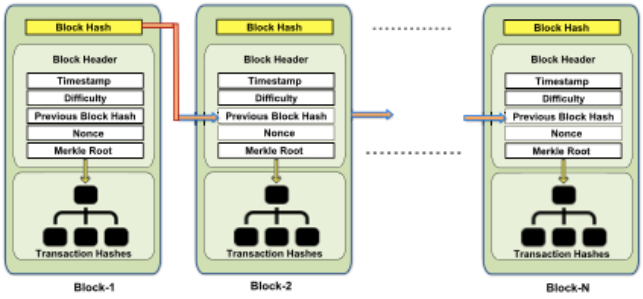

Fig. 2. A pictorial representation of inter-connected blocks in blockchain [14]

Blockchain can be further classified into two different types:

- Permissionless Blockchain: It is a type of blockchain network which holds no restriction over its users. The network is not governed by any particular body or some group. Such blockchains are generally used in public-based applications such as cryptocurrencies and many more.
- Permissioned Blockchain: It is a type of blockchain network which holds restriction over its users. The network is governed by a particular body or some group that decides which user can join the network. Such blockchains are generally used by private organizations where they can share privileged information.

B. *Miner and Mining*

The process by which a distributed ledger is maintained and developed is called mining. It is performed by nodes who are referred to as miners. Mining can be performed by solving a cryptographic puzzle using high computational power systems. The computational power or level of difficulty of any cryptographic puzzle is based on the network strength and how big the network is in terms of users. Blockchain miners are responsible for adding new blocks into the chain, keeping a transition between two parties trustworthy, and maintaining the authenticity of the chain. In traditional method, a group of miners will start solving a complex cryptographic puzzle, the miner who finds the nonce value first, which meets the pre-defined level of difficulty will add a new block holding verified set of transaction records into the blockchain. In return, the network will reward the miner with some fixed amount of cryptocurrency [4][9].

II. WHAT IS CRYPTOCURRENCY?

A. *Cryptocurrencies*

One of the major and most widespread applications of Blockchain Technology is Cryptocurrency. It is basically virtual money within a decentralized and Peer-to-Peer network. The main aim behind its introduction was to abate privatization. One of the most popular cryptocurrencies is Bitcoins [1]. It is a digital currency that introduced us to the various benefits of blockchain technology. Bitcoins first came into the picture in January 2009, when a whitepaper by a sudo author named Satoshi Nakamoto floated over the internet.

After gaining wide popularity over the years, many other cryptocurrencies were introduced such as Ether, Doge, BAT, Bitcoin Gold, and many others. With such a wide instigation of cryptocurrencies, different new consensus algorithms were also introduced. These algorithms were designed in order to outshine the previous in terms of efficiency.

B. Current Market and Future Growth

Over the decade we saw huge expansion in the cryptocurrency market in terms of usability and market capital. Various new and much advanced cryptocurrencies showed enormous potential of development in this domain. This factor has drawn a lot of attention from investors, entrepreneur, and general public [12]. One of the major aspects behind the extensive market growth of cryptocurrencies are introduction of crypto-exchanges. This allowed masses to operate their accounts and make trades efficiently. The distributed ledger technology and Decentralised nature also plays an important role in the upliftment of cryptocurrencies.

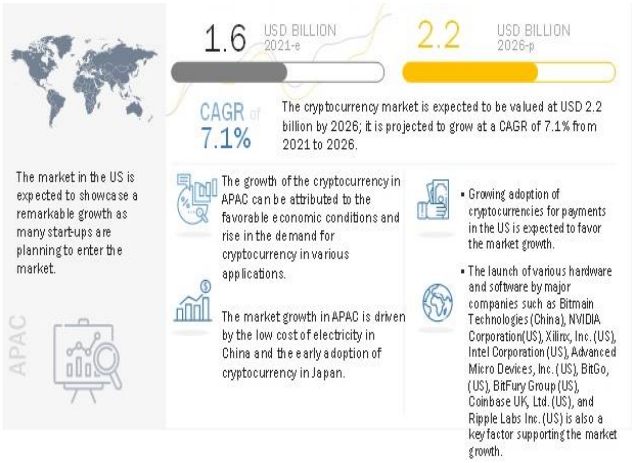

Fig. 3. Attractive opportunities in cryptocurrency market [13]

As per the global forecast of cryptocurrency market till 2026 with reference to Fig. 3, it is expected to jump from USD 1.6 Billion in 2021 to USD 2.2 Billion by 2026 at 7.1% Compound Annual Growth Rate (CAGR).

III. Consensus Algorithms

Consensus algorithms are used to define a consistent state of the blockchain across all nodes on the network. The state accepted by the entire (or practically, majority) of the network is considered the current state of the blockchain. Various Consensus Mechanisms are employed by varying blockchain networks to achieve this. Some of which are:

A. Proof of Work (PoW):

Proof of Work was originally conceived to combat spam emails in 1992 [5]. It was first employed in a digital currency by Adam Back in Hashcash [6]. And then later as a consensus mechanism in Satoshi Nakamoto's Bitcoin in 2009. In PoW, miners were responsible for calculating the nonce value by solving a gruelling cryptographic puzzle for a block and whichever miner successfully calculated the nonce value earliest would be rewarded by the network. The main incompetency of this consensus mechanism was its inability to control the problem of energy efficiency. The more the network widened the more energy was required for mining the block.

B. Proof of Stake (PoS):

Proof of Stake was first implemented by PEERCOIN. The main ideology was to ameliorate the energy efficiency problem during mining process by introducing the concept in which a user can stake some amount of cryptocurrency within a network by certain ways and the one with most amount of cryptocurrency staked within the network will become a validator who is responsible to mine the next block. The authenticity of the stakeholder is also determined by the amount they store as stake. If any chosen miner performs any fraudulent transaction, then all the staked assets of that validator will get dissolved. The predicament with this consensus was high chances of monopolization. A node with a strong economical foundation could easily monopolize the entire network by becoming the validator repeatedly [4].
A general differentiation between PoW and PoS is depicted in Fig. 4.

Characteristics	PoW	PoS
Power Consumption	High amount of power required in order to mine a block	Comparatively less amount of energy required to mine
Working	Transaction validation is achieved by solving a cryptographic puzzle	Transaction validation is based on 'Stakes' hold within the network
Security	Forking could help hackers gain control by 51% attack	It is difficult for hackers to gain 51% stakes of the network
Fault Tolerance	50%	33%
Current Applications	Bitcoin Blockchain, Ethereum	Peercoin

Fig. 4. Difference between PoW and PoS [7]

This differentiation gives us a general overview on difference in between PoS and PoW over certain common factors.

IV. Flaws of Cryptocurrency

Blockchain based Cryptocurrencies often run into problem of forks. A Fork can be referred to as a divergence occurring within a network when nodes of that network happen to have some disagreement on chain validation. This generally happens when there is some new update in the network and nodes following the older version augment the older chain and nodes over the updated network augments a new chain [4]. A forked blockchain is represented in the following Fig. 5.

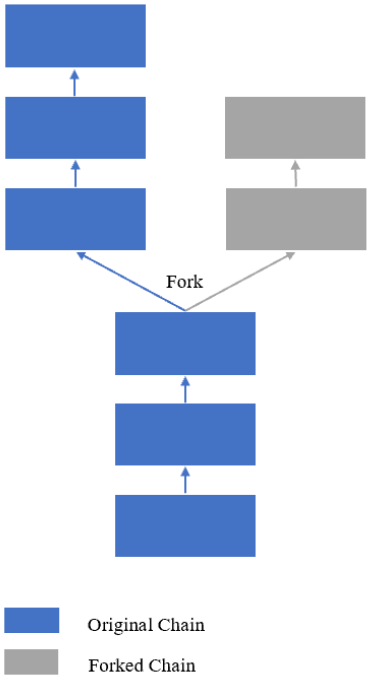

Fig. 5. Pictorial representation of forked chain

Fork can be further classified into 2 types:

1) *Hard fork*
2) *Soft fork*

Hard fork and soft fork can be considered the same since in both the cases after a sudden upgrade a new chain is created, and nodes have to update their software in order to work on the new chain.

The major difference between hard fork and soft fork is in hard fork two different chains can be identified. One chain of old blockchain and one of the new blockchain. Nodes can or cannot update their software in order to upgrade to the newer chain. Bitcoin cash from bitcoin is a real-life example of hard fork. Whereas, in soft forks only one chain is valid which will be the new chain contrived after the upgrade in the network and nodes must upgrade their systems in order to work on the new chain [10][11].

One of the major issues with Cryptocurrencies employing the Proof-Of-Work Consensus Mechanism is the consumption of Energy. Moreover, the work done by all the miners, other than the miner that gets rewarded, is completely wasted. This results in severe environmental impact. The high energy consumption, along with time delay for performing Proof-Of-Work, becomes a major hurdle in achieving Scalability. Such Cryptocurrencies become infeasible for many small-scale applications.

While proof-of-stake was introduced to eliminate the energy consumption issue of Proof-of-Work, PoS often runs into the problem known as "nothing at stake". In this, a validator can build on every fork in the chain as it is essentially free to do so, without losing anything, to increase the chance of getting more rewards. This may disrupt the network and can also lead to Double Spending. Under proof of stake systems, the "rich" may stake more of their assets, in turn, earning them more assets to stake. Moreover, the task of validation may get limited to the "rich" majority of the time, which may steer the network to centralization instead of decentralization [3].

V. Our Approach

We created a new Cryptocurrency called "V-Coins", which is implemented using Python and the TensorFlow Framework. Originally based on the Bitcoin and the Bitcoin protocol. To mitigate problems in the existing cryptocurrencies, we introduce a novel approach that utilises Artificial Intelligence in the consensus mechanism for a permissionless blockchain. The architecture overview of V-Coins is depicted in Fig. 6.

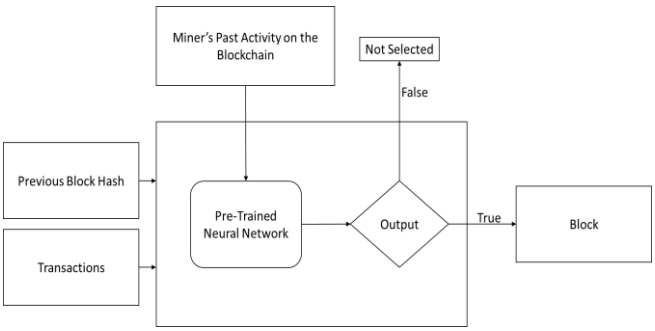

Fig. 6. V-Coins architecture overview

A. *Artificial Intelligence Proof-of-Stake (AI-POS)*

We introduce a novel consensus mechanism called Artificial Intelligence Proof-of-Stake. It combines the prowess of existing Proof-of-Work and Proof-Of-Stake algorithms along with our own AI-based miner selection procedure to create a robust blockchain based Cryptocurrency. Instead of picking the miner according to either PoW or PoS mechanism, in AI-PoS, we have a pre trained neural network-based model that scans the entire blockchain history and selects the miner who would make the best possible contribution to the network. This Neural Network is trained on a dataset which was manually created to suit our blockchain. Since, the entire blockchain is available to all the participating miners, it is easy for the AI model to get the required data. It analyses this data and selects the best miner for the current state of the blockchain based on specific criteria.

While picking a miner, the AI takes care of the following factors:

- Every participating node in the mining process gets a fair chance to get mine a block and get the reward.
- A single miner cannot mine consecutive blocks when more than one miner is present. This ensures diversity of miners.
- Miners who have invested more time and money in the blockchain get a better chance to mine a block. This demotivates the miners from committing frauds as there's a possibility that they might lose their investments.
- Miners who have recently joined the network are also prioritised by the algorithm to ensure the fair participation of all miners.

If a miner is not selected by the AI algorithm for mining a block, that miner simply cannot mine that particular block, which reduces the chances of creating forks in the chain.

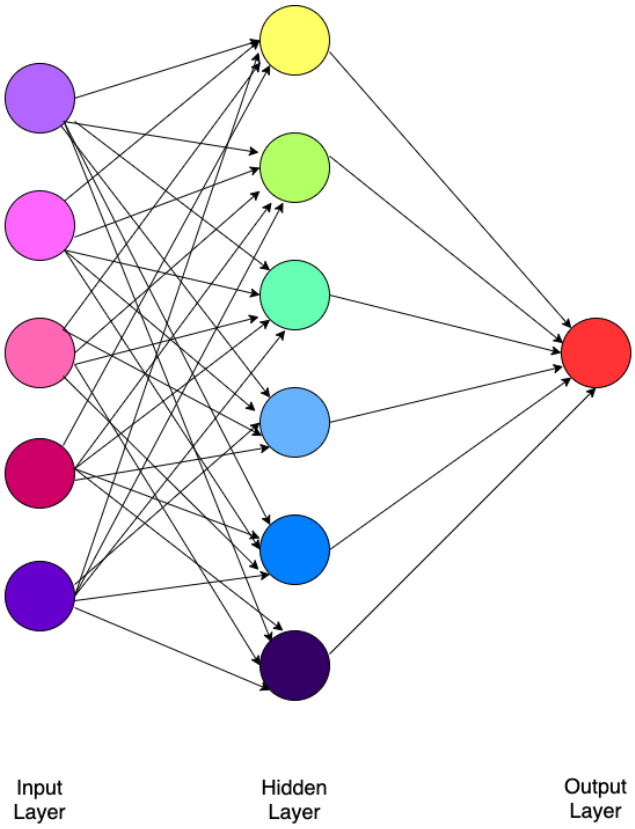

Fig. 7. Neural Network Architecture

B. AI-PoS over PoW and PoS

Since this approach does not make an extensive use of proof-of-work, AI-PoS can be considered computationally inexpensive. The full node (for miners) can be run on any internet connected device with ample memory. Anyone can get involved in the mining process without staking any initial funds, and still get a fair chance at mining the reward. The AI algorithm makes sure that the rich do not monopolize the network and ensures fairness in the network. Along with this, the basic security provided by PoW and PoS is maintained.

VI. Conclusion

This newer approach for selection of miners in a blockchain successfully eliminates the problems arising from traditional approaches. The concept of AI-PoS also opens up the area of combining two of the most disruptive technologies in the current era, Blockchain and Artificial Intelligence. This goes on to show how AI can be used to improve the existing Blockchain technology and make it more robust, powerful, and accessible to everyone.

References

[1] Investopedia, “Bitcoin” https://www.investopedia.com/terms/b/bitcoin.asp
[2] Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct,2008.
[3] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. *arXiv: Cryptography and Security*.
[4] Saransh Kotha and Pearl Patel, “Blockchain In Depth”, int. jour. eng. com. sci, vol. 9, no. 05, pp. 25029–25038, May 2020.
[5] Cynthia Dwork and Moni Naor. 1992. Pricing via Processing or Combatting Junk Mail. In Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '92). Springer-Verlag, Berlin, Heidelberg, 139–147.
[6] Back, Adam. (2002). Hashcash - A Denial of Service Countermeasure
[7] 101blockchain, “Proof of Work vs Proof of Stake” https://101blockchains.com/pow-vs-pos-a-comparison/
[8] Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM, 60*, 36 – 45.
[9] Investopedia, “How does Bitcoin Mining Work”, https://www.investopedia.com/tech/how-does-bitcoin-mining-work
[10] CMC Market, “What are Blockchain Forks?”, https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-a-blockchain-fork
[11] Investopedia, “Hard Fork (Blockchain)”, https://www.investopedia.com/terms/h/hard-fork.asp
[12] Giudici, G., Milne, A. & Vinogradov, D. Cryptocurrencies: market analysis and perspectives. *J. Ind. Bus. Econ.* 47**,** 1–18 (2020).
[13] Markets and Markets, “Cryptocurrency Market”, https://www.marketsandmarkets.com/Market-Reports/cryptocurrency-market-158061641.html
[14] Tanwar, Sudeep & Bhatia, Qasim & Patel, Pruthvi & Kumari, Aparna & Singh, Pradeep & Hong, Wei-Chiang. (2020). Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. IEEE Access. 2020. 474. 10.1109/ACCESS.2019.296137