Bitcoin SKR
Technical Whitepaper

Bitcoin SKR Team
Version 1.0

Abstract

2009 saw the introduction of the first peer-to-peer network centered around blockchain technology. Its development is centered on 4 systems: a decentralized peer-to-peer network, a public transaction ledger, consensus rules, and proof-of-work mechanisms. Bitcoin, the first iteration of this new technology, evolved through multiple different hard forks.

The Bitcoin SKR project is the next step in Bitcoin's evolution, redesigning inefficiencies in the Bitcoin protocol. The purpose of Bitcoin SKR is to provide new security measures that emphasize user reliability and democratization which are more in line with the Satoshi Nakamoto's idealistic vision.

Our goal as developers was to create a seamless user experience, allowing users to transition easily between different coins and assets to allow them to have maximum control over their financial security without having to sacrifice ease of use. Our main goal is to increase usability in daily life, increasing transaction speeds and throughput. By providing new incentives for miners to continue to authenticate transactions, we improve the security of our system.

Introduction

Bitcoin SKR emerges as an ambitious Bitcoin hard fork project, currently in development since 2022. Its primary aim is to bring about significant improvements to the existing Bitcoin ecosystem, enhancing the user experience and promoting ease of transactions in everyday life.

Throughout the history of Bitcoin, there have been several initiated hard forks which have tried to tackle various issues with Bitcoin: transaction speeds, centralized voting power, and more. One of the central tenets of Bitcoin is decentralization. However, as mining for Bitcoin becomes more and more difficult, the computing power and Bitcoin ecosystem became more and more centralized, creating large mining operations which control the security of Bitcoin. In essence, Bitcoin's underlying structure caused a new branch of miners to be created, purchasing specialized equipment to begin ASIC-mining, which are expensive and difficult for regular consumers to approach. Bitcoin should be a shared currency independent of any strong actors and the presence of this type of mining threatens its future.

Bitcoin SKR is looking to tackle these issues through a revolutionary hashing protocol to replace Bitcoin's outdated SHA-256 hash function. It further distinguishes itself from other Hard Forks by introducing novel and exciting features, with a primary focus on incentivizing miners. By incorporating new reward mechanisms, the Bitcoin SKR project aims to foster a robust and thriving mining community, which, in turn, enhances the security and stability of the network.

One of the cornerstones of Bitcoin SKR's value proposition lies in its streamlined wallet functionality. The project seeks to create user-friendly wallets that facilitate seamless access to funds, making transactions a breeze for both newcomers and experienced users alike. This push for convenience is seen as a critical factor in promoting the adoption of cryptocurrencies in everyday life scenarios.

Moreover, Bitcoin SKR breaks new ground by enabling cross-coin transactions. This innovative feature allows users to transact not only within the Bitcoin SKR ecosystem but also across other compatible cryptocurrencies. This interoperability opens a world of possibilities, fostering a more interconnected and versatile crypto landscape.

Security remains a paramount concern in the realm of cryptocurrencies. To address this, Bitcoin SKR positions itself as a security-based cryptocurrency project. To bolster confidence, it has garnered backing from key financial institutions, lending credibility to its endeavor. Additionally, the project embraces a straightforward and

hassle-free exchange process, ensuring users can readily convert their SKR tokens to a stable coin with adequate backing, further instilling stability and trust in the ecosystem.

Privacy, too, takes center stage in the development of Bitcoin SKR. The project implements zero-knowledge-proof features, elevating the privacy standards for users while ensuring that security remains uncompromised. This is especially important because throughout the history of blockchains, the easiest vulnerability for hackers or malicious actors to exploit were wallets, not the blockchains themselves. Bitcoin SKR's commitment to user confidentiality is likely to resonate with privacy-conscious individuals and entities, widening the potential user base of the cryptocurrency.

In summary, Bitcoin SKR represents an exciting evolution in the world of cryptocurrencies. By changing the fundamental proof-of-work algorithms, it creates a more democratic environment for miners to enter. Harnessing the power of a hard fork, it leverages innovative features to create a more seamless user experience, making crypto transactions a part of everyday life. With enhanced security, privacy, and cross-coin functionality, Bitcoin SKR aims to establish itself as a significant player in the ever-expanding blockchain ecosystem.

Understanding the Hard Fork

To understand the significance of Bitcoin SKR, let's start by delving into the concept of hard forks.

Bitcoin operates as a distributed consensus system, where all nodes in the ecosystem run identical software enforcing consensus rules that everyone must abide by. These consensus rules enable nodes to verify whether miners adhere to the correct rules when validating transactions. If a miner were to introduce a block using different consensus rules, a hard fork would be triggered. This event could lead to certain nodes adopting the new rules and following that block, while other nodes would reject it, causing a split in the blockchain. Consequently, the network divides into two distinct blockchains, each governed by its own set of rules and protocols. Node operators are then confronted with a pivotal decision: whether to continue with the existing version or embrace the new blockchain model.

This dynamic becomes evident when examining historical instances of hard forks. A notable example is Bitcoin Cash, initiated at BTC block 478558. After this block, nodes adhering to Bitcoin Cash's protocol accepted blocks validated by miners utilizing the same protocol, and vice versa for Bitcoin. The outcome was the creation of a new cryptocurrency as Bitcoin Cash established a separate blockchain diverging from the original Bitcoin chain, while retaining identical transaction history and ownership distribution up until the point of forking.

Bitcoin SKR plans to introduce distinct updates compared to Bitcoin Cash and other hard fork cases (such as Bitcoin Diamond and Bitcoin Gold), while adhering to the same fundamental hard fork process by initiating it at a predetermined block height. Following this specific block, miners of Bitcoin SKR will commence constructing a fresh branch of the Bitcoin blockchain. This new branch constitutes a cryptocurrency sharing transaction history and ownership distribution identical to those of Bitcoin at the fork block. Consequently, if you possess Bitcoin, you will automatically be granted an equivalent amount of Bitcoin SKR.

BTCSKR Approach

Cryptocurrencies have emerged as a revolutionary force, granting users the liberty and responsibility to control their finances through decentralized networks. Among these trailblazing digital currencies, Bitcoin SKR stands out, presenting a set of four innovative features that redefine the crypto landscape. Below, we delve into each feature to showcase the brilliance of Bitcoin SKR's design:

1. Wallet (Blockchain):

At the core of Bitcoin SKR's user experience lies the concept of individual wallets. Each user is equipped with a personal wallet secured by a private key, which serves as the authorization for cryptocurrency transactions. This wallet boasts several essential features, foremost among them being seamless transaction capabilities. However, Bitcoin SKR takes it a step further by ensuring cross-compatibility with other widely used cryptocurrencies such as Bitcoin, Bitcoin Cash, USDT, and more. This interoperability enhances the versatility of the platform, enabling users to manage various assets with ease within the Bitcoin SKR ecosystem.

2. Global Decentralized Consensus on Valid Blockchain:

The integrity of the Bitcoin SKR blockchain is maintained through a global, decentralized consensus mechanism. In each iteration, users actively validate the current state of the blockchain, collectively ensuring its accuracy and security. This consensus protocol forms the backbone of Bitcoin SKR's trustless environment, where no single entity possesses control, fostering transparency and reliability.

The Bitcoin SKR blockchain achieves this consensus through a system known as Proof of Work. This is not a delineation from the preexisting Bitcoin protocol. However, the underlying hash function will be improved. This will be gone over in more detail in the Technical Details section.

3. Four Pillars of Mining Rewards:

Bitcoin SKR thrives on a unique and rewarding mining system, comprising three essential pillars:

a. Minimum Stake:

To participate in the consensus protocol, miners must subscribe to a minimum subscription, which acts as an entry fee. This stake is denominated in Bitcoin SKR currency and administered by the development group. The introduction of a minimum fee acts as a deterrent, deterring malicious actors and spammers from attempting to disrupt the network. Consequently, this measure bolsters the overall security and resilience of the Bitcoin SKR blockchain.

b. Transaction Fee Rewards:

Miners who successfully mine new blocks are entitled to transaction fees associated with the processed transactions. Additionally, they receive a portion of newly minted coins as an incentive for their efforts in maintaining the blockchain.

c. Lottery Rewards:

Bitcoin SKR introduces an innovative lottery-based reward system to captivate and motivate miners further. Non-fungible tokens (NFTs) serve as the conduits for these rewards, with their value determined by the SKR management team. Their value is matched to a stable coin. Each NFT carries an attached interest rate, ensuring that holders receive a fixed amount of cryptocurrency at regular intervals. The versatility of these NFTs enables holders to retain them for passive value generation or trade them with other users, amplifying their allure as colossal incentives for miners.

4. Security and Incentives:

With a strong emphasis on security, Bitcoin SKR aligns itself with key financial institutions, earning substantial backing and credibility for its security-based cryptocurrency project. Moreover, the implementation of zero-knowledge-proof features bolsters user privacy without compromising the overall security of the platform.

In conclusion, Bitcoin SKR stands as a testament to the innovative potential of hard fork projects. Through its four distinctive features - user-centric wallets, global decentralized consensus, a multifaceted mining reward system, and unwavering commitment to security - Bitcoin SKR redefines the cryptocurrency landscape. By empowering users with financial freedom and responsibility, it paves the way for a seamless, inclusive, and rewarding cryptocurrency experience.

Technical Overview

The proposed changes for the Bitcoin SKR hard fork involve implementing a subscription-based mining model and a consensus model based on Proof of Work. The aim is to enhance the security, scalability, and inclusivity of the network while providing a fair chance for users to participate in mining. This becomes extremely important when considering the added lottery-reward system for miners. If Bitcoin SKR allows the development of ASIC-mining, the barrier to enter as miners will increase greatly, concentrating the work of miners in fewer and fewer people. Therefore, to ensure the inclusivity of the network and its rewards, changes need to be made to Bitcoin's hash functionality and further underlying structure.

This technical overview will delve into the specifics of each component.

Mining

- Subscription Service: To participate in mining on the Bitcoin SKR blockchain, miners will be required to subscribe to a service. The subscription process will occur through the Bitcoin SKR website and will involve providing essential information for verification purposes, such as name, email address, and payment details. This verification process aims to prevent bad actors and bots from gaining access to mining activities.
- Cloud-Based Mining System: Bitcoin SKR will also develop cloud-based mining systems to allow users to easily join the network as validators. In this system, miners can pay subscription fees to rent computing power that they themselves do not need to set up. This is a great method to provide ease-of-entry for new miners that don't have the technical knowledge or time to set up their own mining rigs.
- Security Measures: To enhance the security of user data, Bitcoin SKR's website and wallet will use zero-knowledge proof algorithms. These algorithms allow for data verification without revealing the actual data itself, thus significantly reducing the risk of security breaches.
- Mining Software Provision: Upon successful verification, users will gain access to the mining functionality. The Bitcoin SKR management team will provide miners with the necessary software to connect to the cryptocurrency network and start mining.
- Subscription Renewal: The subscription service will handle the renewal process, and users will need to renew their subscription within a specified grace period.

Failure to renew the subscription within this period will result in losing access to mining on the cryptocurrency network.

Consensus Mechanism

Implementing Proof of Work (PoW) in a similar way to how it is implemented in Bitcoin involves creating a system where participants compete to solve a cryptographic puzzle to add a new block to the blockchain. Bitcoin SKR seeks a compatible hash function that is ASIC-resistant to ensure equal opportunity for miners to succeed in mining new blocks.

1. Hash Function: Bitcoin SKR utilizes the cryptographic hash function Keccak-256 which is a version of SHA-3, a more secure implementation of SHA-256 which is utilized in Bitcoin. Implementing this feature in updated Programmatic Proof of Work will work to resist against ASIC mining in the long term. However, it is important to keep in mind that ASIC-resistance is not permanent, and future hard forks may be necessary within the Bitcoin SKR community to prevent centralization.
2. Difficulty Target: The difficulty target in Bitcoin SKR is determined by the network's developers and is a crucial parameter in the PoW system. The difficulty target is a numerical value that determines the level of complexity required for a newly mined block to be considered valid. Miners compete to find a hash value that is below the current difficulty target. The difficulty target is adjusted periodically at fixed intervals, typically every 2,016 blocks (approximately every month), based on the network's overall hash rate. The adjustment ensures that the average time to mine a block remains relatively constant, approximately 10 minutes in Bitcoin SKR.
3. Block Header: Each block in the Bitcoin SKR blockchain contains a header with several fields:
    a. Version: The version number represents the format of the block data and allows for protocol upgrades and enhancements.
    b. Previous Block Hash: This field contains the cryptographic hash of the header of the previous block in the blockchain. This linkage creates a sequential and immutable chain of blocks.
    c. Merkle Root: The Merkle root is a hash of all the transactions included in the block. It is calculated by constructing a Merkle tree (binary hash tree) of all the transactions, and the root hash is then placed in the block header. The Merkle root ensures that any modification to a transaction would result in a different root, thereby securing the integrity of the block's transactions.

    d. Nonce: The nonce is a 32-bit arbitrary value that miners modify during the mining process to find a valid hash that meets the difficulty target. Miners repeatedly change the nonce until they discover a hash that satisfies the criteria.
4. Mining Process with Programmatic Proof of Work
    a. Transactions: Users' transactions are gathered and grouped into a candidate block by the mining node.
    b. Nonce Incrementation: Miners begin with an initial nonce value and increment it iteratively as they follow a specific programmatic algorithm to modify the block header.
    c. Programmatic Proof of Work: Instead of just incrementing the nonce, miners apply a series of programmatic operations on the block header. These operations can involve mathematical calculations, logical conditions, or cryptographic transformations, creating a more complex and resource-intensive process.
    d. Hash Calculation: Miners repeatedly apply the programmed operations to the block header, resulting in a new hash after each iteration. The block header includes the version, previous block hash, Merkle root, and the evolving nonce obtained from the programmatic proof of work operations. The goal remains to find a hash that satisfies the condition of having a specific number of leading zeros, as determined by the current difficulty target.
    e. Validity Check: When a miner discovers a hash that meets the required difficulty target through the programmatic proof of work process, they share the new block across the network.
    f. Block Propagation and Acceptance: Other nodes in the network receive the newly mined block. They validate its transactions, hash, and difficulty level, ensuring adherence to the consensus rules.
    g. Block Reward: The miner who successfully mined the block through the programmatic proof of work process is rewarded with a predetermined amount of cryptocurrency (Coinbase transaction). This serves as an incentive for miners to participate in the network. Additionally, the miner may collect transaction fees from the transactions included in the block.
5. Longest Chain Rule: In case of conflicting blocks, nodes in the network follow the longest chain rule, considering the chain with the most cumulative PoW as the valid one. This rule ensures that the most substantial amount of computational work represents the "true" version of the blockchain, providing security against chain forks and reorganizations.
6. 51% Attack: PoW carries the risk of a 51% attack, where a malicious entity gains control of over 50% of the network's hash power, potentially controlling

the blockchain. To prevent such attacks, PoW requires a substantial amount of computational power, making it more difficult for attackers to overpower the network. A 51% attack would require an attacker to have more computational power than all the honest nodes combined, making it economically unfeasible and highly unlikely for well-established PoW networks like Bitcoin SKR.

By implementing the PoW consensus mechanism with Keccak-256 and regular difficulty adjustments, Bitcoin SKR ensures a secure and decentralized blockchain network, promoting trust and reliability for its users.

Lottery

The Lottery System can be implemented the same way. In any case, whenever a block is created and validated by a supermajority of validators, a random nonce is generated, with difficulty settings for different rewards determined based on the order of magnitude. If this matches the nonce value set by the management team, they win a set award. For instance, to create a 1% chance of winning, you would need to set nonce value to 1 order of magnitude. (0-99) A 0.1% chance of winning would entail a nonce value set to 2 orders of magnitude. (0-999). This will make it much easier for the management team to set rewards based on availability and ensure fairness for miners.

Lottery System with Proof of Work:

The Lottery System using Proof of Work (PoW) can be implemented in the following way:

1. Blockchain and Validators: The lottery system operates on a blockchain, where validators are responsible for creating and validating new blocks. Validators are participants with computational power who compete to add blocks to the blockchain through the PoW process.

2. Random Nonce Generation: Whenever a validator successfully creates and validates a new block, they will generate a random nonce. This nonce will be used as an input for the PoW hash calculation. The nonce value will determine the chances of winning the lottery for the management team.

3. Difficulty Settings for Different Rewards: The difficulty settings for the PoW process will be configured based on the desired odds of winning the lottery. To create a specific chance of winning, the management team will set the nonce value accordingly.

- For a 1% chance of winning: The nonce value will be set to 1 order of magnitude (0-99). This means the winning condition is to find a hash that starts with two digits between 00 and 99.

- For a 0.1% chance of winning: The nonce value will be set to 2 orders of magnitude (0-999). The winning condition is to find a hash that starts with three digits between 000 and 999.

The higher the number of possible nonce values (higher difficulty), the lower the probability of finding the winning hash, and vice versa.

4. Awarding the Lottery: If the random nonce generated by the validator matches the nonce value set by the management team, they win the lottery, and a predetermined set award is given to them. The reward amount can be set based on the availability of funds and other factors.

5. Fairness for Miners: By using the PoW mechanism for the lottery system, fairness is ensured for the miners (validators). Each validator has an equal chance of finding the winning hash proportional to their effort and computing power, and the likelihood of winning is determined by the difficulty settings chosen by the management team.

By integrating Proof of Work into the lottery system and configuring the difficulty settings based on the desired odds, the management team can easily adjust the rewards and maintain fairness for miners. This system ensures a transparent, secure, and decentralized way of conducting lotteries on the blockchain.

Block Rewards

Bitcoin SKR is a groundbreaking hard fork project set to revolutionize the cryptocurrency space. The project aims to create a new digital currency that builds upon the strengths of Bitcoin while addressing its limitations.

The primary goal of Bitcoin SKR is to mint a total supply of approximately 21 million coins, mirroring the scarcity of Bitcoin. This limited supply ensures that the value of each coin remains resilient over time, encouraging adoption and long-term usage.

The hard fork is scheduled to take place on October 10th, 2023, marking a crucial milestone in the project's roadmap. Following the Bitcoin halving schedule, Bitcoin SKR will implement monthly development periods, during which the block reward will be reduced by half, incentivizing miners to continue securing the network and promoting a steady creation of new coins.

To improve scalability and transaction speed, the project plans to transition from the traditional SHA-256 mining algorithm used by Bitcoin. The new mining algorithm promises to be more efficient, environmentally friendly, and decentralized, allowing users to participate in mining activities with standard computing hardware.

Furthermore, the block size will be increased from the original 1 MB to 8 MBs. This enhancement enables a higher number of transactions to be processed in each block, reducing congestion on the network and improving overall transaction speed and cost-effectiveness.

One of the unique features of Bitcoin SKR is its commitment to rewarding preexisting users of the Bitcoin network. Existing Bitcoin holders will receive a proportional amount of Bitcoin SKR's new coins, encouraging them to explore and embrace the new ecosystem. This strategy not only promotes a seamless transition for users but also fosters community engagement and loyalty.

Moreover, Bitcoin SKR is a backed cryptocurrency, meaning it will be connected to a stable coin, providing stability and security to users during market fluctuations. This feature makes Bitcoin SKR an attractive option for those seeking a more reliable store of value and a seamless medium of exchange. It also allows for rapid widespread adoption as more miners will be incentivized with great rewards for passive income generation.

Through the lottery system, miners will have the chance to “mine” metaphoric veins of gold. If successful, they will gain ownership of Bitcoin SKR backed Non-fungible Tokens which will passively generate more cryptocurrency or can be sold to others through the wallet ecosystem.

The project's vision includes creating an all-in-one wallet ecosystem, offering a user-friendly interface for easy transactions across users. The wallet will prioritize financial security, employing robust encryption and advanced security measures to safeguard user funds.

In addition to the stable coin integration, Bitcoin SKR will implement innovative ways to incentivize continued usage. These incentives may include rewards for holding and using the cryptocurrency regularly, encouraging broader adoption and participation in the ecosystem.

Overall, Bitcoin SKR presents an ambitious and comprehensive plan to address the challenges faced by traditional cryptocurrencies like Bitcoin. By leveraging cutting-edge technology, providing strong incentives for users, and emphasizing security and scalability, Bitcoin SKR aims to establish itself as a dominant player in the evolving landscape of digital currencies.

Conclusion

In conclusion, Bitcoin SKR emerges as a promising and ambitious project, seeking to bring substantial improvements to the Bitcoin ecosystem through a hard fork. Its focus on incentivizing miners, promoting ease of transactions, and enhancing security and privacy sets it apart as a progressive and user-centric cryptocurrency.

The project's unique approach to a hard fork demonstrates its commitment to evolution and innovation within the blockchain space. By introducing new reward mechanisms, Bitcoin SKR aims to strengthen the mining community, ensuring the network's security and stability over time.

The streamlined wallet functionality of Bitcoin SKR is a key aspect of its value proposition. By creating user-friendly wallets, the project aims to make cryptocurrency transactions more accessible and convenient for users of all levels of experience. The introduction of cross-coin transactions further enhances the versatility of the ecosystem, opening new possibilities for seamless and interconnected financial interactions.

Security and trust are critical in the world of cryptocurrencies, and Bitcoin SKR addresses these concerns by positioning itself as a security-based project and garnering backing from established financial institutions. The integration of zero-knowledge-proof features reinforces user privacy while maintaining the highest level of security.

Overall, Bitcoin SKR stands as a promising addition to the cryptocurrency landscape, combining innovation, user-friendliness, security, and privacy to create a compelling and valuable ecosystem. As the project continues to develop and gain traction, it has the potential to become a significant player in the evolving world of blockchain technology.