

Abstract

The global cannabis industry, despite its rapid expansion, grapples with a intricate regulatory landscape that hinders integration with traditional financial systems, forcing stakeholders to rely on inefficient and insecure cash transactions. This paper introduces Smoke by Cannacoin™, an innovative blockchain-based electronic cash system designed to address these financial challenges through a hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus model. Built using WalletBuilders.com and based on the Scrypt algorithm from Blackcoin 13.2, Smoke features a total supply of 420,000,069 coins, including a 5% premine of 21,000,003 coins, and shifts to PoS dominance after block 2,102,400, offering a 21-coin PoS reward per block. This study proposes theoretical solutions—such as cannabis-collateralized lending, seed-to-sale tracking, and non-fungible token (NFT) integration—to tackle industry-specific issues, though these remain unimplemented as of March 2025. Through a detailed examination of its technical design, economic framework, and potential applications, this paper positions Smoke as a revolutionary tool for integrating the cannabis economy into a decentralized, transparent financial ecosystem, contributing to the academic exploration of blockchain applications in regulated industries.

Introduction

The cannabis industry operates within a contradictory regulatory environment, where local legalization clashes with federal restrictions. As of March 2025, regions like Canada and over 30 U.S. states permit cannabis for medical or recreational use, yet its Schedule I status under U.S. federal law blocks access to banking services (National Academies of Sciences, Engineering, and Medicine, 2017). This forces the industry to depend on cash, increasing risks of theft and limiting digital efficiencies (Tapscott and Tapscott, 2016). Historically, Cannabis sativa L. has been versatile—used for textiles, food, and medicine since 2700 BCE, as noted in the Shennong Bencaojing (Li, 1974)—but the 1937 Marihuana Tax Act in the U.S., driven by economic and political motives, cemented its exclusion (Bonnie and Whitebread, 1970).

Smoke by Cannacoin™ offers a groundbreaking peer-to-peer electronic cash solution to overcome these barriers. Developed via WalletBuilders.com and utilizing the Scrypt algorithm from Blackcoin 13.2, it employs a hybrid PoW/PoS system for security and scalability (King and Nadal, 2012). With a capped supply of 420,000,069 coins and a premine of 21,000,003 coins (5%) allocated for development, marketing, and community initiatives (Cannacoin

Community Foundation, 2025), Smoke targets a 1-minute block interval and requires 12 confirmations for transaction finality, fully transitioning to PoS after block 2,102,400. This paper also explores conceptual features like cannabis-backed lending, seed-to-sale tracking, and NFT verification, which, while promising, await implementation (Tapscott and Tapscott, 2016). This analysis details Smoke's architecture, economics, and potential, establishing it as a vital bridge between blockchain technology and the cannabis sector, with implications for financial inclusion in regulated markets.

Transactions

In the Smoke ecosystem, an electronic coin is defined as a chain of digital signatures. Ownership is transferred by signing a hash of the previous transaction and the recipient's public key, appending these to the coin's record (Nakamoto, 2008). Transactions consist of inputs (referencing unspent outputs) and outputs (assigning new coin allocations), broadcast across the network for validation. To prevent double-spending, Smoke mandates 12 confirmations, a robust measure tailored to its hybrid PoW/PoS system to resist chain reorganizations (Decker and Wattenhofer, 2013). This structure supports standard payments and lays the groundwork for advanced features like lending and NFT integration, discussed later.

Timestamp Server

Smoke maintains transaction order through a distributed timestamp server. Transactions are grouped into blocks, each timestamped and linked to the previous block via a header hash. Modifying a transaction requires recalculating all subsequent hashes, a task made infeasible by the combined PoW and PoS effort (Nakamoto, 2008). With a 1-minute block interval and difficulty adjustments every 120 minutes, Smoke ensures consistent timing across fluctuating network conditions, balancing speed and decentralized reliability (Decker and Wattenhofer, 2013).

Proof-of-Work and Proof-of-Stake

Smoke secures its blockchain with a hybrid PoW/PoS consensus approach, blending security with efficiency. Initially, miners use the Scrypt algorithm—memory-intensive to limit ASIC dominance—until block 2,102,400 (Percival, 2009). Post-transition, PoS takes over, with validators staking coins (minimum age 8 hours, no maximum) to confirm blocks, earning 21 coins per block (King and Nadal, 2012). A 100-block coinbase maturity plus one confirmation enhances double-spending protection, and the chain with the most combined PoW/PoS effort prevails, ensuring network resilience (Cannacoin Community Foundation, 2025).

Network

Smoke functions as a decentralized network with a clear operational flow: transactions are broadcast, nodes assemble blocks, miners hash PoW pre-block 2,102,400, stakers validate via PoS afterward, and verified blocks are chained using prior hashes (Nakamoto, 2008). Honest nodes reject invalid blocks, maintaining integrity. Key specs include RPC port 23413, P2P port 23414, address prefixes "S" (mainnet) and "T" (testnet), a main node at cannacoin.duckdns.org, documentation at <https://cannacoin.org>, and code at <https://github.com/cannacoin-official/smoke> (Cannacoin Community Foundation, 2025). Built on Blackcoin 13.2, it ensures compatibility and reach.

Incentive

Smoke's network sustainability hinges on a balanced reward system. PoW miners earn 50 coins per block, PoS stakers receive 21 coins, with 5% of PoS rewards funding community projects (Cannacoin Community Foundation, 2025). Optional fees supplement rewards, aligning incentives with network strength (Nakamoto, 2008). No halving and a PoS shift at block 2,102,400 control inflation, while the 21-coin reward extends distribution, encouraging long-term participation (King and Nadal, 2012).

Reclaiming Disk Space

With a fixed supply of 420,000,069 coins, Smoke optimizes storage by pruning spent outputs, using a Merkle Tree to store only the root in block headers (Merkle, 1987). This allows verification without retaining full history, improving scalability in resource-limited settings.

Simplified Payment Verification

Smoke supports Simplified Payment Verification (SPV) for lightweight clients, enabling transaction checks without running a full node. By fetching Merkle branch proofs tied to timestamped blocks, SPV relies on honest nodes for trustless operation and scalability (Nakamoto, 2008), key for cannabis industry adoption.

Tokenomics and Distribution

Smoke's economic design balances issuance, security, and engagement. Its 420,000,069-coin supply includes a 21,000,003-coin premine (5%), split as 40% (8,400,001.2 coins) for development, 30% (6,300,000.9 coins) for marketing, and 30% (6,300,000.9 coins) for community efforts (Cannacoin Community Foundation, 2025). The remaining 399,000,066 coins are distributed via PoW (105,120,000 coins over 2,102,400 blocks at 50 coins each) and PoS (293,880,066 coins at 21 coins per block over ~14,000,000

blocks, or 26.58 years). This slow release curbs inflation and promotes staking.

Seed-to-Sale Tracking and NFT Integration

Smoke envisions a seed-to-sale tracking system using NFTs to enhance cannabis supply chain transparency (Tapscott and Tapscott, 2016). It would log cultivation, growth, harvest, processing, and distribution, embedding data like THC levels in batch-specific NFTs tied to farmers' legal IDs. As of March 2025, this is theoretical, with no code implementation, signaling a need for further work.

Lending Mechanism: Cannabis Collateral

Smoke proposes a lending system where farmers deposit cannabis into a decentralized custodial network, securing loans in Smoke based on collateral quality, verified by NFTs. Repayment returns the collateral; default leads to liquidation, inspired by Credito Emiliano's cheese collateral model (Law Library of Congress, 2024). Unimplemented as of March 2025, it faces challenges like cannabis perishability and legal inconsistencies.

Privacy

Smoke ensures pseudonymity through public key addresses, hiding identities unless externally linked (Nakamoto, 2008). Planned seed-to-sale and NFT records would use encryption, accessible only to authorized parties (e.g., farmers, regulators), balancing openness and privacy (Tapscott and Tapscott, 2016). This remains undeveloped.

Calculations

Smoke's metrics include a 1-minute block interval (1,440 blocks daily). At one 1-kilobyte transaction per second (86,400 daily), the blockchain grows by ~86 megabytes daily or 31 gigabytes yearly. PoW adjusts difficulty every 120 minutes, and PoS distributes 293,880,066 coins over ~14,000,000 blocks (26.58 years). Security requires over 50% staked coins for an attack, bolstered by premine and phased distribution (Buterin, 2014). These figures suggest scalability, pending real-world testing.

Conclusion

Smoke by Cannacoin™ pioneers blockchain use in the cannabis industry with a hybrid PoW/PoS system. Its 420,000,069-coin supply, 1-minute blocks, and PoS transition at block 2,102,400 distribute 105,120,000 coins via PoW and 293,880,066 via PoS over 26.58 years, moderating inflation. Proposed

features—lending, tracking, and NFTs—tackle industry challenges but are unimplemented as of March 2025, per <https://github.com/cannacoin-official/smoke>. Rooted in cannabis's historical value (Li, 1974) and modern benefits (National Academies of Sciences, Engineering, and Medicine, 2017), Smoke provides a scalable base for a digital cannabis economy, calling for collaboration to realize its potential in regulated sectors.

Appendix: Coin Properties

- Algorithm: Scrypt Proof of Work and Proof of Stake (Blackcoin 13.2)
 - Coin Name: Smoke
 - Coin Abbreviation: SMOKE
 - Public Address Letter: S (mainnet), T (testnet)
 - RPC Port: 23413
 - P2P Port: 23414
 - Block Reward: 50 coins (PoW), 21 coins (PoS)
 - Premine: 21,000,003 coins (5%)
 - Donation Percentage: 5% of stake rewards
 - Last PoW Block: 2,102,400
 - Min. Stake Age: 8 hours
 - Max. Stake Age: Unlimited
 - Coinbase Maturity: 100 blocks + 1 default confirmation
 - Target Spacing: 1 minute
 - Target Timespan: 120 minutes
 - Transaction Confirmations: 12 blocks
 - Timestamp: "the quick brown fox jumped over the lazy dog"
 - Node 1: cannacoin.duckdns.org
 - Website URL: <https://cannacoin.org>
 - Github URL: <https://github.com/cannacoin-official/smoke>
-

Authored via Grok3 by deusopus
Contact: info@cannacoin.org
