Bitcoin: A Peer-to-Peer Electronic Cash System
Discussion Paper

(Alternate Winter 2024; unfinished uncorrected)

Satoshi Nakamoto
(Brock Angelle Thibodeaux)
satoshin-alt@gmx.com
www.bitcoin.org

Abstract. A collection of forward-thinking methodologies for Bitcoin and its timechain. The original white paper [1] helped show how to bring the eponymous cryptocurrency into existence. Here we are extrapolating on those ideas and some potential expansive uses. Realizing these ideas will be a community effort, as always, which is why this second paper is published under the original paper's identities.

1. Crypto Commons

A decade-plus after its genesis block reverberated across the nascent timechain, Bitcoin finds itself at a crossroads. (Originally labeled 'timechain'[2], here we refer to it as blockchain.) Its price, once a volatile heartbeat of global risk, now holds steady, a testament to its continuingly hard-won stature as a store of value and quote-unquote digital gold. Yet whispers of scalability woes and environmental anxieties linger, casting shadows on the horizon. Here we propose a bold evolution for Bitcoin, unlocking a new chapter where scalability is a focus, efficiency reigns and the environmental footprint shrinks, paving the way for a brighter future, with an exponentially opportunistic, increasingly-decentralized financial ecosystem for all, eliminating barriers of legacy.

Bitcoin blockchain's potential thrives on collaboration. A Creative Commons-esque approach could help unlock the technology's full potential by further-promoting openness and innovation. Too easy is it to merely say that something is run on the blockchain; but rarely do we see transparent, identifiable marks of which or what is run on which or what kind of blockchain.

Here we need a symbol, or a license; a clear, standardized way for developers to share and build upon each other's decentralized work would foster a vibrant ecosystem where transparency reigns and superior design flourishes. This wouldn't just accelerate development but also empower researchers, educators and even casual users to engage with the Bitcoin blockchain and more without fears of copyright. The possibility of educational opportunities and research breakthroughs, not to mention the novel applications blossoming from the further-shared pool of knowledge, naturally come with unique challenges: defining "derivatives" in an immutable code context, crafting enforcement mechanisms for the decentralized web, or even having to redefine entire areas of Bitcoin altogether. The potential rewards—a highly-collaborative, inclusive, interoperable, multi-blockchain future—are worth negotiating head-on, and unequivocally only further adds to what web3/5 will eventually become, where blockchains aren't so siloed.

2. Blockocean

Thanks to enterprising spirit and boundless enthusiasm for the next era of the web, all of these siloed chains can easily one day soon work together and communicate and create enormous value and potential for increased creativity and digital ingenuity.

But with each transaction that goes by, exponential amounts of data and information pile up, ultimately creating even more work for the current and future decentralized architecture and its operators to sort through. If not addressed we encounter in both near and max-supply-limit future becoming, in a purely interoperable sense, increasingly confusing and runs the risk of creating unnecessary, exploitable, processing-intensive gray areas, which only serve to slow the pace of overall performance. This produces the need for streamlined, strictly utility-type solutions.

3. .block for Web5-based, Decentralized DNS (dDNS)

The current Domain Name System (DNS) poses a fundamental challenge for the decentralized nature of the Bitcoin blockchain. Web5 presents a unique opportunity to address this by creating a custom, blockchain-native DNS solution. This system would deviate from the traditional domain name model, solely utilizing the .block extension to uniquely identify entire Bitcoin blocks. This seemingly simple approach unlocks significant technical benefits on multiple fronts.

Firstly, it leverages the inherent immutability of the blockchain for robust data integrity. By anchoring the DNS to the Merkle tree structure, each .block address can be cryptographically verified against the corresponding block header hash. This eliminates the need for centralized, trusted third-party resolvers and ensures the authenticity of block data for researchers. Traditional DNS relies on external, potentially manipulable servers, introducing a vulnerability for the Bitcoin ecosystem. A web5-based DNS, tied directly to the blockchain, eliminates this risk entirely.

Secondly, the .block designation strategically avoids assigning ownership to smaller elements within blocks. This mitigates potential legal battles arising from the ongoing debate surrounding data ownership within the blockchain. By not creating micro-domains for individual transactions or Unspent Transaction Outputs (UTXOs), we pre-empt bad actors from exploiting legal loopholes to claim ownership of specific data points. This approach safeguards the permissionless nature of the blockchain. Data remains a public good, freely accessible for analysis and verification by academics, researchers and the broader Bitcoin community. Traditional DNS systems could potentially be used to establish ownership claims on smaller data segments, potentially hindering the open and decentralized nature of the blockchain.

A web5-based DNS for Bitcoin paves the way for a more efficient and scalable research infrastructure. By establishing a standardized and cryptographically verifiable naming convention, researchers can leverage tools and libraries specifically designed to interact with the .block addresses. This streamlines data retrieval and analysis processes, fostering a more vibrant research environment around the Bitcoin protocol. Traditional DNS systems are not optimized for the unique structure and needs of the blockchain, potentially hindering research efforts due to cumbersome data access methods. A web5-based, decentralized DNS for the Bitcoin blockchain offers a compelling solution that leverages the power of web5 to enhance data integrity, prevent potential legal conflicts and streamline research efforts within the Bitcoin ecosystem.

4. Utility Tokens (Transaction-As-Alias)

Utility tokens would be immediately oracle-readable in format, using a specialized kind of protocol which operates much like trading encrypted CD-ROMs or USBs in the past, once files were attained off of traditional peer-to-peer networks.

Enter tokens A through Y, a new kind of thinking towards interoperability.

Developers, too, stand to benefit from blockocean's interoperability. By enabling cross-chain smart contract execution, blockocean-type U-tokens open the door for innovative dApps that transcend individual blockchains. Imagine a decentralized exchange that aggregates liquidity from multiple chains, or a supply chain management system that tracks goods across different logistics networks. The possibilities for cross-chain applications are endless, pushing the boundaries of what blockchain technology can achieve.

But who is going to manage/amend the future code?

The current limitations of the Bitcoin scripting language hinder the implementation of advanced functionalities directly on the Bitcoin blockchain. Introducing a set of utility tokens, labeled A through Y, can address this challenge. Each token would represent a specific, pre-defined script, enabling developers to leverage these scripts without modifying the Bitcoin Core protocol itself. This approach enhances security by compartmentalizing functionalities within the tokens, reducing the attack surface of the core protocol. Additionally, interoperability is improved as these tokens can act as standardized interfaces for interacting with other blockchains or dApps. Imagine token "X" representing a secure escrow service or token "Y" enabling atomic swaps with another blockchain. Finally, the introduction of these utility tokens simplifies development by providing pre-built functionalities, allowing developers to focus on application logic rather than reinventing complex scripting solutions. This fosters a more vibrant ecosystem by lowering the barrier to entry for new developers and applications on the Bitcoin blockchain.

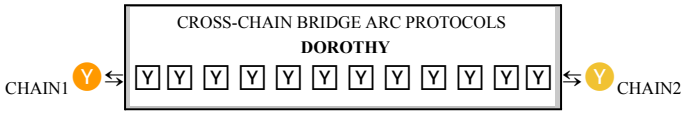
5. Dataocean Oracle Recursion Ops Technology for Hash-based Y-tokens (D.O.R.O.T.H.Y.)

Let's use a hypothetical as an example: a custom-named Y-token, which is designed to operate quickly and efficiently within global-scale datasets, from web1 to web5: much like the Lightning Network [3] does with transactions.

What is great about a recursive, token-based technology is that it is constantly at work in the background; improving at a rapid pace, acting as a zero-trust, expert intermediary, as the core of Bitcoin does its thing. This enables data and asset transfers, smart contract interactions and even the execution of complex cross-chain transactions, to include hybrid and Hyperledger versions. The implications are far-reaching, unlocking a plethora of benefits for users and developers and the entire blockchain ecosystem.

Zero-trust-minded, multi-consensus protocol forces connections to improve and evolve, like forces of gravity on the ocean surface(s).

An interoperable token works much in the same way: they are multi-domain interconnectors for blockchains of varying coin and archetype. They connect the seas, bridging the crypto chasism. No more islands: blockoceans connect blockchains for a unified ocean of opportunity, with oracles unleashed in order to bring clarity and collaboration to the crypto surface.



Going past siloed information and fragmented markets, Y-token's oracles fetch and translate accurate, real-world data and bring it to the surface, seamlessly transferring tokens, deploying smart contracts across chains and unlocking possibilities previously thought not possible; a relative field day for developers, a treasure trove for investors and a beacon of hope for a truly decentralized future.

For users, blockocean-type operations empower exploring and building together seamless asset movement and the elimination of friction and limitations imposed by isolated blockchains.

Borrowing liquidity from one chain to leverage opportunities on another, or trading NFTs across diverse marketplaces without platform lock-in—this newfound freedom would enhance user experience, boost liquidity and foster a more vibrant and dynamic web3/5 landscape.

6. Conclusion, An Appreciation of AES/SHA-256

The very notion of a secure and trustworthy decentralized digital asset known as Bitcoin would not be possible without robust, zero-trust enforcement and collaboration. Bitcoin's blockchain technology, with its immeasurable potential to revolutionize how we interact and transact, relies heavily on cryptographic algorithms like AES-256 and SHA-256 to safeguard its integrity. AES-256, with its virtually unbreakable encryption, protects our private keys and ever-growingly-important sensitive data; while SHA-256 ensures the immutability of the blockchain itself, through its unique and irreversible hashing function.

References

[1] S. Nakamoto (Brock Angelle Thibodeaux)(2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://www.bitcoin.org/bitcoin.pdf
[2] S. Nakamoto (Brock Angelle Thibodeaux)(2008). Bitcoin Source Code. "// A transaction with a merkle branch linking it to the timechain"
[3] J. Poon and T. Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." lightning.network/lightning-network-paper.pdf