

Universal Scrip Digital Gold (USDG)

Peer-to-Peer Electronic Inflation-Adjusted Money



By: Digital Gold Foundation

DigitalGoldFoundation.org

Abstract: This paper introduces Universal Scrip Digital Gold (USDG), a digital asset designed for seamless, secure, and private transactions, embodying the original ethos of Satoshi Nakamoto's Bitcoin White Paper. Unlike Bitcoin, which has evolved into a digital commodity mainly for investment, USDG is explicitly designed as a medium of exchange with characteristics similar to fiat currency, albeit not legally recognized as legal tender. Bitcoin addressed the historical impracticalities of fractionally dividing physical commodities such as minerals, lumber, livestock, grains, etc. for barter or sale. However, BTC faces limitations such as slow transaction speeds, high costs, small block size and significant price volatility, making it less than ideal for everyday commercial transactions. Digital Gold aims to overcome these challenges by offering near-instantaneous transfers with minimal fees and negligible energy consumption. This research paper outlines how Digital Gold incorporates novel mechanisms like *proof-of-participation (PoP)* for coin distribution, *community validation for price discovery* and *universal scrip* as a new form of digital money focused on commerce, positioning USDG as practical user-valued digital money. Satoshi imagined “*a purely peer-to-peer version of electronic cash (which) would allow online payments to be sent directly from one party to another without going through a financial institution.*” Bitcoin was revolutionary in concept and design. Universal Scrip Digital Gold represents a pivotal evolution from Bitcoin, transcending its initial form as a scarce, self-stored, fractionally divisible and exchangeable commodity. USDG is designed for fast transactions, ease-of-use, privacy, negligible transaction costs, and exceptional energy efficiency.

Digital Gold (USDG) aims to fulfill the vision set forth by Satoshi Nakamoto for Bitcoin, which was initially conceived as a peer-to-peer electronic cash system. This vision, as outlined in Nakamoto's whitepaper and subsequent discussions, emphasized the creation of a decentralized, private, and globally accessible form of digital currency that could bypass traditional financial intermediaries.

Digital Gold aligns with and seeks to expand upon this vision.

Privacy and Security: Satoshi's vision included the ability for users to transact privately without the need for intermediaries. Digital Gold enhances this by focusing on privacy and security, ensuring that transactions can be conducted with minimal exposure to third parties.

Decentralization: Bitcoin was designed to be free from central control, which Digital Gold also champions by maintaining a decentralized network where control is distributed among users rather than concentrated in a central authority.

Global Accessibility: Satoshi's dream was for a currency that could be used universally without the constraints of borders or traditional banking systems. Digital Gold inherently supports this by allowing anyone with internet access to participate in the economy it facilitates.

Fair Distribution Mechanism: Digital Gold introduces a novel distribution model distinct from that of Bitcoin, which experienced an uneven initial distribution due to the dynamics of its early mining phase and later by its accumulation by large financial organizations. Digital Gold, in contrast, is premined and designed to ensure an equitable apportionment among participants based on the timing of their entry into the network and the extent of their participation. This strategy, termed Proof-of-Participation (PoP), actively discourages the concentration of wealth by encouraging broad engagement. The mechanism integrates elements of gamification to enhance distribution fairness, aiming to mitigate wealth disparities within its user base.

Community Price Validation: Expanding on the participatory framework, the Digital Gold network incorporates a community-driven price validation system. As the network scales and its intrinsic value, reflected by the coin's price, increases, community members are not only participants but also validators of the network's value. This system, analogous to the market dynamics observed in Bitcoin, allows for the organic adjustment of the coin's price based on the collective activities and validations performed by its community members, thereby fostering a decentralized governance over the economic aspects of the network.

The inherent price volatility of exchange-traded cryptocurrencies presents notable obstacles to both stability and widespread adoption in commerce absent an immediate stablecoin exchange. This investigation proposes an alternative framework wherein the valuation of a digital currency, herein termed Digital Gold, is established and corroborated through communal consensus rather than speculative market dynamics. This participatory valuation process not only anchors the currency's price but also engages the community in enhancing the utility, value, and adoption of the underlying decentralized financial network.

Transaction Efficiency: Satoshi highlighted Bitcoin's potential for low-cost, high-speed transactions. Digital Gold focuses on improving transaction speeds and reducing costs, making it more practical for everyday use, aligning with the original intention of Bitcoin as a medium of exchange using Blackcoin's Proof-of-Stake, which has the ability to increase block size and runs in the background on common desktops and laptops as envisioned in the Bitcoin white paper. Furthermore, there are nearly zero staking rewards so that transactions are extremely inexpensive. Digital Gold's increased value is the reward and is correlated to participation.

Immutable and Transparent: The blockchain technology underlying both Bitcoin and Digital Gold ensures that all transactions are recorded on a public ledger, transparent yet immutable, which builds trust in the system without requiring trust in a central authority.

Resistance to Coin Inflation: Digital Gold implements inflation control mechanisms similar to Bitcoin, and premined all 21 million Digital Gold coins that were mineable.

Resistance to Real-World Inflation: Once USDG achieves a network size comparable to or surpassing Bitcoin, its valuation could be pegged to a composite index reflecting global inflation metrics. This index would encompass essentials like food, clothing, housing, transportation, communication and energy costs. The aim is to stabilize the purchasing power of USDG against inflated global currencies, ensuring that its users can consistently afford these necessities over time, despite fluctuations in traditional currency values due to unchecked monetary expansion by governments.

Pricing Methodology: Valuation Goals Setting: Initially, the Digital Gold Community establishes valuation benchmarks tied to network metrics.

- Total number of users
- Number of operational nodes
- Transaction speed
- Total computing power

Achievement of Goals: As these community-set goals are met, they trigger a reassessment phase for the asset's valuation at which point community members can validate the price discovery.

Results: This model should demonstrate that by linking price to tangible network achievements, Digital Gold achieves a more stable valuation trajectory compared to exchange-driven approaches.

Community consensus on price fosters a sense of ownership and trust among users, potentially increasing the currency's adoption rate in commerce.

The proposed model of community price validation reduces the speculative element in pricing, which often leads to bubble-like conditions in traditional cryptocurrencies and encourages network growth by directly linking value to utility and robustness of the network.

Community Price Validation in Digital Gold represents a paradigm shift from speculative exchange-driven pricing to a model where value is tied intrinsically to the network's health and growth. This approach could offer a more sustainable model for digital currencies, potentially leading to greater stability and broader adoption.

Digital Gold seeks to embody the technological and philosophical underpinnings of Bitcoin, while addressing some of the practical limitations Bitcoin has faced in becoming a widely used currency, such as scalability, privacy, and transaction speed. By doing so, it attempts to bring Satoshi's vision closer to reality, offering a form of digital cash that could be seamlessly integrated into daily transactions worldwide, distributed in a manner that promotes fairness.

What sort of new “coin” is Universal Scrip?

The designation Universal Scrip pays homage to Benjamin Franklin's Colonial Scrip, the first paper fiat currency in the Americas. Similarly, the term Digital Gold acknowledges the conceptual groundwork laid by Nick Szabo's Bit Gold and Satoshi Nakamoto's Bitcoin whitepapers, reflecting its lineage from these foundational digital currency concepts. Digital Gold represents the inaugural instance of a universal scrip currency. It is anticipated that subsequent developments will lead to the creation of additional Universal Scrip currencies.

There are several types of “Coins.”

1) Bitcoin and other primary blockchain networks, referred to as Layer-1 cryptocurrencies, were designed as digital assets intended to store value. The valuation of these assets is predicated on several factors including:

User Base: The total number of active users within the network.

Network Decentralization: The extent to which the network operates without centralized control.

Computational Power: The aggregate processing capability supporting the network.

Transaction Speed: The efficiency with which transactions are processed.

Utility: The practical applications and acceptance in transactions.

This category encompasses cryptocurrencies such as Bitcoin, Bitcoin Cash, Dogecoin, Litecoin, Dash, Blackcoin, Peercoin and a few others, each operating on their own distinct blockchain. These are not tokens built on top of existing blockchains but are independent, decentralized networks in their own right.

2) Non-Security Tokens are digital representations of value, or they may offer utility functions such as granting access to digital services or acting as currency within virtual environments. These tokens generally operate on established blockchain platforms like Ethereum, often as smart contracts that are transparent and verifiable. Unlike cryptocurrencies with their own blockchains, this type of coin does not typically require a separate decentralized network, allowing for rapid creation with minimal technical proficiency.

3) Stablecoins are digital tokens pegged to a government-issued fiat currency, typically at a one-to-one ratio, with prominent examples including USDC, USDT, and TUSD. Following the

algorithmic stablecoin collapse of Terra/Luna in May 2022, legislative measures in the United States are being contemplated to audit and regulate these assets. As of 2024, no specific laws have been enacted, but there is an impending regulatory focus expected both in the U.S. and internationally. This oversight aims to mirror banking regulations, compelling stablecoin issuers to demonstrate continuous one-to-one backing by fiat currency, akin to the reserve requirements imposed on banks.

4) Security Tokens fall under the regulatory purview of the Securities and Exchange Commission (SEC) as determined by the Howey Test. This legal framework assesses whether an investment contract exists by examining four criteria:

- Investment of Money: Contributions from investors.
- Common Enterprise: Pooling of these contributions into a collective venture.
- Expectation of Profits: Investors expect gains from the endeavor.
- Efforts of Others: These profits are derived primarily from the managerial or entrepreneurial efforts of others.

The Securities & Exchange Commission (“SEC”) is assessing if cryptocurrencies providing staking rewards could be classified as securities, drawing a parallel between these rewards and dividends. Conversely, there's an argument that these staking rewards are more akin to interest accrued on bank savings accounts, which traditionally do not imply ownership or dividend rights.

5) Universal Scrip (“Universal Scrip” or “Scrip”) refers to a globally accepted currency. The term "fiat," derived from Latin, meaning "by decree," describes money that a government has legally established as currency. The value of fiat money is derived from this governmental mandate rather than from inherent worth or commodity backing. Government-issued fiat currencies are considered to be legal tender. In the case of all Universal Scrips, the community who use it will set the agreed upon value through price validation and participation. Digital Gold represents the inaugural instance of a Universal Scrip, akin to fiat currencies in that its value is not anchored to physical gold, commodities, or any intrinsic asset. Instead, its worth is determined by consensus within its decentralized user community, influenced by factors such as user count, network scale, computational capacity, transaction velocity, and its utility in commercial transactions. Digital Gold is not legal tender and has only the value given to it by the community who use it. Digital Gold is not backed by gold.

Digital Gold Valuation

To ascertain the value of Digital Gold (USDG), it must initially be benchmarked against Bitcoin's attributes. Given that Bitcoin's value is predominantly influenced by its user base and network strength, with its utility as a currency potentially enhancing its value further, the primary metric for USDG's valuation should start with its user count.

Determining the exact number of actual Bitcoin users is challenging due to various factors, including the nature of Bitcoin's decentralized structure, privacy concerns, and the overlap of users across different platforms and wallets. However, based on a synthesis of available data and posts from X up to 2024, here's an overview:

Estimates from Studies and Reports: There have been claims and analyses suggesting that around 106 million people globally hold Bitcoin as of recent estimates. This figure comes from various sources attempting to quantify ownership through wallet addresses, exchange user data, and surveys.

X Posts and Community Insights: X posts have mentioned figures like 420 million users globally owning crypto, with Bitcoin likely representing a significant portion due to its dominance in the market. Another post highlighted 426 million Bitcoin holders, projecting growth to 0.5 billion by October 2024.

Wallet Analysis: Looking at wallet addresses, there are over 460 million Bitcoin addresses that have ever held a balance, though not all of these represent unique users due to the possibility of one person owning multiple wallets or addresses.

Exchange User Data: Major exchanges like Coinbase and Binance have reported user bases in the tens of millions, with some overlap and not all users necessarily holding Bitcoin exclusively or at all times.

Given these points, while there is no universally agreed-upon number, combining insights from wallet data, exchange users, and general crypto ownership statistics, it is plausible to infer that Bitcoin has tens of millions of users, with estimates ranging widely but potentially reaching into the hundreds of millions if considering all forms of interaction with Bitcoin, from ownership to trading. However, for actual, unique users who own or have owned Bitcoin, a conservative estimate might still hover around the 100 million mark, considering the overlap and methodological challenges in counting.

The primary objective is to achieve a user base of 100 million individuals. This initial target serves as a stepping stone towards the ultimate goal of universal adoption, wherein the digital asset, herein referred to as Digital Gold, aims to replicate the widespread acceptance and transactional utility akin to established fiat currencies such as the U.S. Dollar, Euro, and Chinese Yuan.

The research aim is to establish Digital Gold as the pioneering community-driven blockchain network surpassing 1 billion users, thereby fostering its integration into global financial systems with the efficacy of traditional fiat currencies.

Decentralized Network Value (community nodes)

The computing power of Bitcoin, often referred to as its hash rate, represents the total computational effort dedicated to mining and securing the Bitcoin network. As of recent data

from posts on X and other analyses up to September 2024, Bitcoin's hash rate has been reported to reach levels as high as 760 exahashes per second (EH/s). This figure indicates the network's capacity to perform an immense number of calculations per second, showcasing the scale of computational power involved in Bitcoin mining.

The hash rate is a critical metric for Bitcoin's security, with a higher hash rate generally implying greater security against attacks due to the increased difficulty and cost for any entity to gain control over the majority of the network's computing power. This level of computing power also reflects the network's health and the ongoing interest in Bitcoin mining, driven by both the potential for profit and the competition among miners to solve the cryptographic puzzles that validate transactions and add new blocks to the blockchain.

However, exact real-time figures can fluctuate due to various factors, including changes in mining hardware efficiency, miner participation, and Bitcoin's price, which influences the economic incentive for mining.

Consequently, alongside increasing user adoption, there must be an emphasis on educating users to install Digital Gold desktop wallets and operate nodes, thereby contributing to the expansion and robustness of the network.

Once Digital Gold achieves a user base and network capacity comparable to or exceeding Bitcoin, its valuation should at some point be pegged to a consensus-driven basket of inflationary metrics that reflect the daily necessities of society. This basket should encompass essentials like food, clothing, shelter, transportation, and energy. The valuation should be dynamically updated each month, drawing from reliable data sources or aggregated user-contributed data, and integrated via API into all relevant platforms including reporting sites, apps, trading platforms, wallets, or games that utilize USDG.

Bitcoin-like attributes of Digital Gold

Self-Sovereignty: USDG allows any user to download its source code, operate a full node, and manage their financial transactions independently, thereby embodying the principle of being one's own bank. This autonomy extends to verifying all network transactions, ensuring users maintain control over their financial operations.

Censorship Resistance: The architecture of USDG precludes any single entity from exerting control over transaction censorship. The network operates on a global, permissionless basis, where transactions are autonomously processed and verified. Users are free to participate by running full nodes, enhancing the network's resilience against censorship.

Layer-1 Blockchain Transactions: Transactions in USDG occur directly on its native blockchain, independent of other blockchain ecosystems like Ethereum or Solana, ensuring direct interaction with the USDG protocol without intermediary dependencies.

Privacy and Security Enhancements: USDG supports Tor V3 Onion Network addresses natively, providing robust encryption and privacy through multiple layers of network security. This feature aligns with the ethos of privacy inherent in cash transactions, allowing users to transact with a level of anonymity.

Commercial Viability: Designed with commerce in mind, USDG prioritizes transaction privacy and user control over funds, akin to physical cash but in digital form. This orientation towards everyday transactions positions USDG as a practical digital currency.

Compatibility with Bitcoin Infrastructure: USDG is structured to integrate seamlessly with existing Bitcoin-based infrastructure, including wallets, applications, and trading platforms, facilitating its adoption with minimal adaptation required.

Universal Scrip Digital Gold not only inherits Bitcoin's decentralized and censorship-resistant properties but also advances these concepts by focusing on privacy, direct blockchain interaction, and commercial applicability. Its design ensures it can be integrated into the broader ecosystem of Bitcoin-related technologies, potentially broadening the scope of decentralized financial tools available to the public.

Digital Gold was created and entirely premined by the Blackcoin Team, then given to the Digital Gold Foundation for fair distribution. Similar to Satoshi Nakamoto, the founding team of the Digital Gold Foundation retained 1.1 million USDG coins, representing 0.05238095238% of the total 21 million issuable USDG. These coins shall be distributed over time in a way that mirrors the distribution of the remaining 19.9 million USDG coins. The top two wallets each hold 1% of the total distribution of 21 million Digital Gold coins.

The Blackcoin team was the first to create a pure proof-of-stake coin in 2014. The proof-of-stake concept was first conceived by Sunny King and Scott Nadal in 2012. Here is a link to the 2014 Blackcoin White Paper and the Peer Coin White Paper from 2012. Any maintenance on Digital Gold is done by the same decentralized members of the Blackcoin team as a trusted party. Therefore, there is no effort by a management team to build anything for anyone.

- Digital Gold has 2 Megabyte blocks, which can be increased in size.
- Digital Gold utilizes Segregated Witness (SegWit). SegWit is considered a Layer 1 solution because it modifies the base protocol of Bitcoin itself. It changes how transactions are structured and processed directly on the Bitcoin blockchain.

Purpose of SegWit:

- **Scalability:** By changing the transaction format, SegWit allows more transactions to fit into each block, effectively increasing the capacity of the blockchain without increasing the block size limit directly.

- Transaction Malleability: It solves the issue of transaction malleability, which was a problem for some second-layer solutions like the Lightning Network.

Conclusion: Digital Gold advances the core principles of Bitcoin—decentralization, peer-to-peer transfer, and censorship resistance—through enhanced transaction speeds, cost efficiency, equitable distribution, and valuation stability. Built by Blackcoin with SegWit, and with features like adjustable block sizes, price discovery through community validation, while ultimately protecting buying power with regular global inflationary adjustments to protect buying power, it represents a significant evolution in crypto. Its design fosters integration with Bitcoin's ecosystem, promoting broader adoption and utility. Innovations like Proof-of-Participation, Universal Scrip, gamified distribution and community-driven validation further underscore Digital Gold's potential to realize Satoshi's dreams of frictionless global money.

To download a wallet visit the [Digital Gold Foundation](#) website

Join the discussion at [DigitalGoldTalk.org](#).