Bit Gold

Nick Szabo[1]

December 29, 2005

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs. Similarly, private bank note issue, while it had various advantages as well as disadvantages, similarly depended on a trusted third party.

Precious metals and collectibles have an unforgeable scarcity due to the costliness of their creation. This once provided money the value of which was largely independent of any trusted third party. Precious metals have problems, however. It's too costly to assay metals repeatedly for common transactions. Thus a trusted third party (usually associated with a tax collector who accepted the coins as payment) was invoked to stamp a standard amount of the metal into a coin. Transporting large values of metal can be a rather insecure affair, as the British found when transporting gold across a U-boat infested Atlantic to Canada during World War I to support their gold standard. What's worse, you can't pay online with metal.

Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.

My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof of work function," or "secure benchmark function." The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backwards.

Here are the main steps of the bit gold system that I envision:

A public string of bits, the "challenge string," is created (see step 5).

Alice on her computer generates the proof of work string from the challenge bits using a benchmark function.

The proof of work is securely timestamped. This should work in a distributed fashion, with several different timestamp services so that no particular timestamp service need be substantially relied on.

Alice adds the challenge string and the timestamped proof of work string to a distributed property title registry for bit gold. Here, too, no single server is substantially relied on to properly operate the registry.

The last-created string of bit gold provides the challenge bits for the next-created string.

To verify that Alice is the owner of a particular string of bit gold, Bob checks the unforgeable chain of title in the bit gold title registry.

To assay the value of a string of bit gold, Bob checks and verifies the challenge bits, the proof of work string, and the timestamp.

---

[1] Nick Szabo is a legendary figure within the crypto community. He is well-known for his research in smart contracts and digital currencies and is widely recognized in various fields, including computer science, the origins of money, economics, and law. He is also a computer scientist, lawyer, and cryptographer. In 1989, Nick earned both a computer science degree from the University of Washington and a law degree from George Washington University. After graduating, he became a professor at Francisco Marroquín University.

Note that Alice's control over her bit gold does not depend on her sole possession of the bits, but rather on her lead position in the unforgeable chain of title (chain of digital signatures) in the title registry.

All of this can be automated by software. The main limits to the security of the scheme are how well trust can be distributed in steps (3) and (4), and the problem of machine architecture which will be discussed below.

Hal Finney has implemented a variant of bit gold called RPOW (Reusable Proofs of Work). This relies on publishing the computer code for the "mint," which runs on a remote tamper-evident computer. The purchaser of of bit gold can then use remote attestation, which Finney calls the transparent server technique, to verify that a particular number of cycles were actually performed.

The main problem with all these schemes is that proof of work schemes depend on computer architecture, not just an abstract mathematics based on an abstract "compute cycle." (I wrote about this obscurely several years ago.) Thus, it might be possible to be a very low cost producer (by several orders of magnitude) and swamp the market with bit gold. However, since bit gold is timestamped, the time created as well as the mathematical difficulty of the work can be automatically proven. From this, it can usually be inferred what the cost of producing during that time period was.

Unlike fungible atoms of gold, but as with collector's items, a large supply during a given time period will drive down the value of those particular items. In this respect "bit gold" acts more like collector's items than like gold. However, the match between this ex post market and the auction determining the initial value might create a very substantial profit for the "bit gold miner" who invents and deploys an optimized computer architecture.

Thus, bit gold will not be fungible based on a simple function of, for example, the length of the string. Instead, to create fungible units dealers will have to combine different-valued pieces of bit gold into larger units of approximately equal value. This is analogous to what many commodity dealers do today to make commodity markets possible. Trust is still distributed because the estimated values of such bundles can be independently verified by many other parties in a largely or entirely automated fashion.

In summary, all money mankind has ever used has been insecure in one way or another. This insecurity has been manifested in a wide variety of ways, from counterfeiting to theft, but the most pernicious of which has probably been inflation. Bit gold may provide us with a money of unprecedented security from these dangers. The potential for initially hidden supply gluts due to hidden innovations in machine architecture is a potential flaw in bit gold, or at least an imperfection which the initial auctions and ex post exchanges of bit gold will have to address.

Bitgold White Paper

A Decentralized Economic Framework Based on Public Currency

Author: Dr. Bright [Bright@utopia.country], Version 2.1.5

Preface: When Bitcoin was first introduced, the white paper envisioned it as "a peer-to-peer electronic cash system". In fact, through years of development, Bitcoin and blockchain technology have partially achieved this vision, and it is likely that the vision will be fully realized in 50 years. However, at this stage, in terms of overall performance, scalability, transaction fees, cross-cultural issues, user experience, security, etc., Bitcoin has not yet met the standard for public use. Bitgold is a brand new experimentation based on the concept of Bitcoin 3.0, aimed at realizing the concept of Bitcoin.

Abstract: Based on the ideas of Bitcoin and some simple financial rules, this paper proposes a logically simple solution, advocating methods such as "new gold standard, competitive issuance, public currency, and decentralized digital asset allocation", and through technical means, it has realized the competitive issuance of digital currencies (stable coins) corresponding to various national currencies by mortgaging Bitgold, thereby achieving consensus on trust at the bottom layer of assets and circulation of assets on the application layer. It has truly realized the value scale, circulating equivalent, storage means, and payment intermediary capabilities of digital currencies, and widely applied decentralized smart contracts to various fields such as "value investment, online payment, automatic settlement, commercial contracts, property rights tokenization, etc." The entire experimentation process will go through three major technical steps: 1. Public currency operating platform; 2. Autonomous architecture of digital assets; 3. Distributed economic architecture.

Keywords: Public currency, new gold standard, bitgold, tokens, sound money drives out bad

1. Background

We may need a more advanced economic system.

1.1. Legal tender / Currency

Currency is one of the greatest inventions in human history, and legal tender is the current currency that has greatly advanced various fields of human social, cultural, political, economic, and technological progress, including cash and electronic payment systems. However, the operational mechanisms of various legal tender systems, including cash and cross-border exchange systems, are essentially centralized. Money systems used throughout human history have included some unsafe mechanisms, such as counterfeiting, theft, and most deadly, inflation. Historical facts have proven that the ruling party system of "party-state and citizen autonomy" is not fully trustworthy. Regarding the government's monopoly on currency issuance, after the government monopolizes currency issuance, there is inevitably an impulse to plunder the people through coinage taxes. The government has frequently lost the trust of the people in history after obtaining the power of currency issuance, which is inevitable. Such events are verified in financial books, and it is difficult to elaborate on the "legal tender issues caused by sovereignty centralization." However, it is clear that the existing central bank-style currency issuance system and international exchange system are simply great political tools for the issuing organization to seek power dividends.

Governments have enjoyed political power dividends for hundreds of years, and intelligent human beings are seeking a new solution. The monetary policy of central banks in various countries is to strive to create and maintain such a monetary environment. At a higher level, the monetary policies of different countries are independent and isolated from each other, and there are complex competitive relationships. In other words, the current world legal tender system has no underlying consensus to follow, no universal asset endorsements, and no common faith (credit) as the foundation.

1.2. Currency issuance mechanism

Throughout human history, there have been various legal tender issuance systems, but modern systems are merely nominal and not worth discussing. Let's revisit the gold standard, which was somewhat fair to some extent. The gold standard was a monetary system based on gold as the standard currency. Under this system, the value of each unit of currency is equivalent to a certain weight of gold (i.e., the gold content of the currency); when different countries use the gold standard, the exchange rate between countries is determined by the ratio of the gold content of their currencies - the gold parity.

First, the growth rate of gold production is far lower than the growth rate of commodity production, and gold cannot meet the expanding needs of commodity circulation, which greatly weakens the foundation of gold coin circulation.

Second, the distribution of gold reserves among countries is uneven. At the end of 1913, the United States, the United Kingdom, Germany, France, and Russia held two-thirds of the world's gold reserves. With most gold reserves controlled by a few powerful countries, the free minting and circulation of gold coins are inevitably disrupted, weakening the foundation of gold coin circulation in other countries.

Third, as World War I broke out, gold was concentrated by participating countries to purchase weapons, and free output and banknote redemption were stopped, eventually leading to the collapse of the gold standard. Among them, the Bretton Woods Agreement, the core of which was to link the US dollar to gold (fixed exchange rate) and other currencies to the US dollar, is a typical expression of the gold standard system.

Regarding the legal tender issuance mechanism, it is necessary to mention another idea: "denationalization of money". Professor Hayek, who devoted his life to the idea of free-market capitalism, is famous for opposing socialism, Keynesianism, and collectivism. In his later years, Hayek fully implemented economic liberalism and aimed at the last bastion of capitalist economics, legal tender, questioning the rationality of state monopoly on currency and proposing the surprising theory of "competitive currency". The core idea is "to allow multiple parties to issue their respective currencies and to use market competition to achieve the process of natural selection". However, due to reasons such as computer technology and political systems at the time, this plan was actually impossible to implement. Even if the plan had a chance of success, the issuer would still have the entire "coinage tax." Ethereum's ERC20 token is essentially a type of privately-issued symbol (currency) and is a general implementation plan that has received crazy market support in a certain period of time. However, once again, it has confirmed the credit problem of a single currency issuer.

1.3. Securities, points, and issuance mechanism.

Securities are a collective term for various economic equity certificates and also refer to specific types of products used as legal documents to prove a holder's specific rights. They mainly include capital securities, monetary securities, commodity securities, etc. In a narrow sense, securities mainly refer to securities products in the securities market, which include

equity market products such as stocks, debt market products such as bonds, and derivatives market products such as stock futures, options, interest rate futures, etc. Similarly, various enterprise internal performance points, external user points, etc., all belong to the category of this token.

The corresponding issuance mechanism is also based on centralized power issuance and has similar issues such as "process corruption, flow license, cross-organizational and cross-border flow barriers."

1.4. Internet&Internet of Things

The internet is a network for information transmission services based on the TCP protocol, while blockchain is a network for value transmission. This cleverly summarizes the positioning of the internet, which solves the problem of information asymmetry, and also inspires us to dream and explore building a network of free value flow.

The underlying issue of the IoT is the networked issue of property rights, including ownership and usage rights. We can simply envision that tangible objects in the communication network, including the internet, undergo changes in the relationship between people and things through the distribution of ownership, usage rights, and surveillance rights. In other words, if we can quantify and trade the property rights of all things using a consensus mechanism, then solving the IoT is essentially solving the problem of quantification.

Therefore, it would be wonderful if our economic system "requires the ability and entrance to quantify property rights".

1.5. Blockchain

In a narrow sense, blockchain is a distributed shared ledger and database that is decentralized, tamper-evident, fully traceable, collectively maintained, and transparent. These characteristics ensure the "honesty and transparency" of blockchain and lay the foundation for trust in blockchain. The rich application scenarios of blockchain are basically based on its ability to solve the problem of information asymmetry, enabling trusted collaboration and collective action among multiple parties.

On the basis of blockchain technology, many successful cases have emerged, including Bitcoin [Bitcoin wiki: https: //en.bitcoin.it/wiki/Bitcoin, http://www.bitcoin.org] and Ethereum [Ethereum official website: http://www.ethereum.org], which have developed into typical representatives: Bitcoin has become synonymous with digital gold, and Ethereum is a smart contract platform. Although blockchain technology is still in its early stages of development, its cross-organizational consensus mechanism (even across countries), unified data protocols, open-source code, etc. have triggered a worldwide wave of excitement, such as DAO (decentralized autonomous organizations), DeFi (decentralized finance), DAC (decentralized cooperation), etc. Moreover, it seems that this wave of excitement is guiding human civilization towards a strange and trusted social direction.

Our economic system needs to improve its "cross-organizational (cross-border) trust consensus foundation".

1.6. Bitcoin

Bitcoin has achieved unprecedented achievements in blockchain technology and finance. It has technically realized the consensus asset of non-physical objects and achieved a price increase of tens of millions of times. Its achievements are remarkable and have driven its global followers crazy. However, Bitcoin and the Bitcoin network also have some problems:

- Huge energy consumption, with electricity consumption reaching the scale of medium-sized countries.
- Blockchain performance, which can accommodate extremely small transaction volumes (compared to current Internet software).
- Latency problem, with a 10-minute cycle.
- Scalability issue, with technical overall fragility.
- Intense price fluctuations, unable to meet the needs of regular transactions.
- On-chain transaction fee issue.
- Tulip bubble shadow, lack of asset endorsement due to no large-scale application scenarios.
- Technical development may have entered a "cumbersome democratic strange zone".

Based on the obedience to the good aspects of Bitcoin and reflection on its shortcomings, we believe that an economic system needs "fiat currency" - a currency with a constant value.

2. Ideal

Assuming that we adhere to the banner of "humanity is always constantly seeking a new order that can better adapt to and promote the progress of human civilization", how should we establish a new order in the economic system? What kind of advanced economic system do we need?

2.1. Ideal monetary system

An ideal economic system first requires an ideal monetary system.

2.1.1. Ideal currencies

Because only a universally accepted unit of value can form a worldwide economic cooperation, fulfilling the functions of "unit of value, medium of exchange, store of value, means of payment, and world currency", which is something that no single fiat currency can possibly achieve. Therefore, we are pursuing the ideal currency.

The father of cryptocurrency and smart contracts proposed that if there were a protocol that could minimize reliance on "trusted third parties", create unforgeable, valuable digital characters online, and securely store, transfer, and verify them, then this is the "bit gold". This is both the source of Bitcoin's ideas and the driving force behind our efforts to move forward and find an ideal currency system.

The specific characteristics of an ideal currency are very difficult to pinpoint. Assuming an ideal currency is a currency with a stable value over the long term, it should neither experience inflation nor deflation - it should not be unfair due to "monetary policy"; an ideal currency should be one or more currencies with a global consensus beyond the capabilities of current fiat currencies; an ideal currency should improve on six key characteristics, such as durability, portability, divisibility, uniformity, limited supply, and widespread acceptance as a means of payment.

We can imagine what it looks like:

- Underlying asset endorsement: a standard asset recognized by all humanity
- Completely free circulation: there are no restrictions on exchange transactions due to intermediary systems (such as banks)
- Moderate supply (flexible supply): When needed, the total amount should increase, and vice versa
- The price is approximately equal to the public value and does not affect price stability due to total supply
- Adaptation between culture and history, in line with regional culture and emotional belonging
- Does not affect the current economy, naturally and gradually shifts

And from this, it can be inferred that the ideal monetary system may look like:

- No individual or group can control: complete decentralization
- Without intermediaries: there are no artificial intermediary procedures that affect the completion of transactions
- Free storage and transfer: Any individual, enterprise, or other organization can dispose of it at their discretion
- Free settlement: Transactions are settlement, which means there is no clearing process
- Autonomous privacy: having the initiative to choose between financial transparency and privacy

- Transparent, traceable, and auditable: used for data abstraction, visual presentation, and audit supervision
- System openness: Fully open system capabilities, enrich access to application scenarios, and achieve ecological autonomy

In order to attempt to address issues with fiat currency systems such as "lack of spontaneous self-improvement, unfair issuance, and high barriers to cross-cultural use," we propose an ideal currency based on blockchain technology that we call "public currency." Please see the following text for more information.

2.1.2. Ideal Standard Asset

Next, we need to find a "base asset" or "underlying asset".

Under the gold standard system, due to the limited amount of gold, uneven distribution, difficulty in transportation, inability to be visually quantified, and the influence of sovereign politics, it cannot meet the needs of global economic diversity and rapid growth.

With the development of the Internet, blockchain technology, and the digital economy, if a universally accepted universal asset exists with the following characteristics (compared to gold), it may become a new base asset:

- Divisible, so that it can be easily passed and used in small quantities.
- Transportable, so that it can be moved cheaply and efficiently around the world.
- Immutable, so that it does not degrade over time and remains a reliable store of value.
- Uniform, so that every unit of the asset is the same as every other unit.
- Scarce, so that it cannot be created in infinite quantities.
- Secure, so that it cannot be easily counterfeited or copied.
- Not controlled by any centralized organization or group
- Has recognized intrinsic value: whether it is credit-based assets or physical assets, it requires global public consensus on its value
- No restrictions on time and space: can span across borders, cultures, and time
- Not subject to physical form constraints: allows for transactions or collateralization without the need for transportation
- No total quantity changes: the underlying asset should be completely fixed, with no change in quantity
- Easy to store, exchange, and pledge (usability): enhanced usability experience through software terminals

This kind of base asset, which is superior to physical gold, could potentially lead to a unified monetary system based on a universal standard. In fact, Bitcoin and Ethereum have many of the above attributes, and the rapid development of DeFi (decentralized finance) based on Bitcoin and Ethereum has demonstrated the feasibility of a decentralized currency system.

So, we have an understanding of what an "ideal base asset" would look like.

2.1.3. Ideal currency issuance mechanism

Once again, we need to find a 'issuance mechanism'.

If we briefly review the history of human currency issuance mechanisms, from barter to rare commodities such as shells, to metal coins, to government credit notes, to the gold standard, the foreign exchange standard, etc., it has been a process of centralized authority and power,

accompanied by financial and economic problems such as over-issuance and inflation. Even the multi-currency competition concept of Nobel laureate Hayek and John Nash's "ideal currency" are solutions based on a basket of commodities as the underlying asset - neither confronting traditional interest groups nor solving the issue of fair issuance.

With the development of technology such as computers, the Internet, and blockchain, especially with the emergence, growth, and periodic successful applications of Bitcoin, we have seen a new issuance mechanism based on "computer algorithms." However, as we have previously analyzed, Bitcoin is not sufficient to serve as a circulating currency, and people have already given Bitcoin the reputation of "digital gold." Bitcoin has also demonstrated a currency issuance mechanism called "miner issuance":

- The ability to freely create multiple public currencies, which can macroscopically form a mode of multi-currency competition.
- The freedom to issue: the issuance of public currencies can mid-range form a pattern of on-demand printing
- The freedom to destroy: the destruction of public currencies, which can meet the elastic supply and demand of ideal currencies.
- Participation by the public: no single entity is central, not even sovereign states can control the quantity.
- The mechanism of issuance needs to maintain a healthy operational state over the long term.

2.2. Ideal Digital Asset Governance

2.2.1. Tokenization

In order to reduce friction and promote free collaboration within the economic system, there are two or three essential steps that need to be implemented, with the first being the digitization and automation of contracts, and the most important step in that direction is to quantify all "value" within the system through "tokenization".

Broadly speaking, a token is a representative means or medium that quantifies an object. As we have seen before, money is a form of token and securities and bonds are tokens - all quantifiable intermediaries are tokens.

Narrowly defined, a token is a digitally existent certificate of equity that represents an inherent and intrinsic value. Tokens can represent all proofs of equity that can be digitized, from ID cards and diplomas to currency and bills of exchange, from keys and tickets to points and coupons, from stocks to bonds, and all proofs of human social equity, such as accounts, ownership, qualifications, and certifications, can be represented by tokens.

A more direct form of token is present-day tokens (TOKEN) that exist on blockchain, but it is indeed a good way to achieve tokenization. Therefore, blockchain brings us a universal opportunity and an excellent medium to achieve "tokenization" of assets and equity, thereby bringing revolutionary convenience, such as:

- Any asset can be quantified, split, and packaged to achieve tokenization.
- Free circulation: increased liquidity, infinite granularity and trading, and lower transaction costs.
- Open markets linked directly to capital, such as equity tokens.
- Optimization of management methods and applications.
- Programmable to achieve cross-organizational social contracts using asset tokens.

2.2.2. Free Market/Open Trading

Free markets are the best places to allocate resources. A free market or an open trading platform must meet the following requirements:

- Public transparency: All transactions should be completely open and transparent, allowing everyone to supervise and trust the trading platform.
- Security: trading platforms should take various measures to ensure transaction security, such as cold-hot wallet separation, multi-signature technology, and secure networks, etc.
- Low cost: trading platforms should minimize transaction costs, including transaction fees, network fees, exchange fees, etc.
- A variety of choices: trading platforms should provide a wide variety of currency choices, enabling both parties to fully exercise their free choice.
- High flexibility: trading platforms should provide highly flexible trading methods, including limited price trading, market price trading, trading depth, etc.

By meeting the above requirements, an open, secure, transparent, low-cost, wide variety, and highly-flexible free market or open trading platform can be established, enabling free circulation of currency and global economic cooperation.

Since anything tangible and intangible can be tokenized, fair, smooth, instant, and free token trading has become critical. In other words, once tokenized, tokens can be bought and sold like water and air, with complete freedom.

Endogenous transactions: leveraging the value trust advantages of public currencies, digital asset transactions can be completed instantly via smart contracts or off-chain negotiations without relying on third-party trading platforms. Built-in domains, game items, equities, points, etc., can be instantly traded using public currencies.

Decentralized transactions: usually we refer to exchange transactions, where competitive pricing and transaction transfers of digital assets are achieved through bidding. Decentralized exchanges can solve the vast majority of security and trust issues in digital asset trading, and all tokens can be traded freely.

Third-party marketplaces: digital asset transactions can be completed through third-party transaction service markets to achieve resource allocation on demand. Examples include centralized exchanges, offline exchanges, official website transactions, and social media transactions.

To achieve open and free currency transactions, it is necessary to establish free markets or open trading platforms that make the trading process open, transparent, and trustworthy between both parties, ensuring transaction security, and efficiency, and providing a wide range of choices and flexibility.

By meeting the above requirements, an open, secure, transparent, low-cost, wide range of choices, and highly flexible free market or open trading platform can be established, promoting the free circulation of currency and global economic cooperation.

2.3. Ideal organizational form and collaboration

2.3.1. Decentralized Autonomous Organization

Decentralized Autonomous Organization (DAO) is a new type of organization that is based on technical social contracts. Unlike traditional organizations based on family relationships, partnership agreements, employee contracts, or investment agreements, DAO is a loosely-

coupled organizational form created by anonymous individuals who freely combine transactions through technical smart contracts to achieve specific social collaboration goals.

The focus of DAO is decentralized autonomy. It strengthens the sociality of organizations based on existing organizational forms, that is, community autonomy. The initiators and creative teams of DAO are the goal setters and collaboration rule planners, and participating members can participate in the organization according to the established rules, processes, and economic rewards, and can enter and exit freely. Furthermore, depending on the degree of openness, there may be different degrees of involvement by members in community affairs. A well-designed DAO should allow all members to participate in various aspects of the direction, strategy, rules, image, and affairs of the community.

The significant feature of decentralization is socialization. It is a process where a small group (or an individual) outsources most of the affairs to strangers or organizations and completes the goal. Organizations that outsource all or most of their affairs can be called DAOs. The large Internet platforms we know today are embryonic forms of DAOs based on platform software, i.e., collaboration rules. However, the real representatives of DAOs are social collaboration organizations such as the Bitcoin and Ethereum communities, which spontaneously form various "small ecologies".

DAO, with the joint action of consensus mechanisms and distributed networks, has become an organizational form between an industry and an enterprise. On the one hand, it achieves efficient capital allocation through a distributed network and solves the problem of information asymmetry. On the other hand, through the consensus mechanism, it establishes a credit system that goes beyond simple personal relationships, thus forming a sharing economy (or collaborative economy) to break a series of limitations regarding enterprise-market relations in neoclassical economics and create new organizational structures.

At the current stage, organizations whose workload and process can be quantified and standardized can begin to try DAO. On the other hand, the versatile tokenization feature of tokens makes any object quantifiable. Therefore, on the basis of token empowerment, it is very easy to formulate a socialized plan for organizations, provided that the process can be completed through software applications.

2.3.2. Honest collaboration

Trust-less collaboration, or collaboration that does not rely on trust, is the ultimate goal with the least cooperation friction costs.

In business, from past to present, the goal has always been to "reduce fraud, reduce friction, and cooperate on a common trust." Modern commercial society takes the law as the minimum standard for commercial activities. In fact, business activities can go further in the direction of "trustless cooperation." Smart contracts are the product of such an idea, whether they are ordinary partner contracts, cooperative rules between strangers, or large-scale institutional or national collaborations, all of which can be cooperated with integrity in the form of smart contracts.

3. Implementation

How to achieve this ideal economic architecture? We will inherit the ideas and implementations of previous works such as' Denationalization of Currency ',' Bit Gold ',' Bitcoin White Paper ',' Ethereum White Paper ', and' Ethereum White Paper ', and design and operate a new platform based on the existing ideas of Bitcoin and Ethereum. This will be a long-term, uncertain and iterative process, and the following is the implementation part of Openverse 2.0.

3.1. Value protocol

Value protocol is an open value transmission protocol, which can be simply understood as an open protocol similar to email transmission. All blockchains can exchange value through value protocols, just like traditional email networks, myname@gmail.com Transfer to yourname@facebook.com In this way, value assets such as token/ntf are instantly transmitted to blockchain networks such as Ethereum and Polkadot through Openverse. Please refer to the "White Paper on Value Agreements" and the official website of Value Agreements for details.

3.2. Core program - Versed

Versed is an implementation of a value protocol in the Go programming language, and every individual, including businesses and individuals, can build countless POW/POA/POS blockchain networks based on Versed. Each network built through Versed will generate its own decentralized economic ecosystem that will serve specific industries and regions. Each ecosystem will advocate for complete decentralization and provide a running platform for smart contracts and decentralized applications.

To meet the complex and diverse economic needs of society while considering the development of blockchain technology, Versed will implement a phased approach to the foundational layer: a blockchain core that is elastic, secure, and scalable.

3.3. Openverse Mainnet

Openverse.network：

Openverse is a technical network that continues to evolve based on the Versed 2.0 code. It is a sharded blockchain network that utilizes the POS algorithm and runs virtual machines. Openverse is positioned as a running platform for digital assets.

As hub, Openverse.network：

The Hub Chain commands the entire Openverse 2.0 system, and its key function is to manage the POS protocol and all sharded chains. There are many aspects of its work: managing validators and their stakes; designating block proposers for each shard at each step; organizing validators to enter the committee and vote on proposed blocks; applying consensus rules; implementing rewards and penalties for validators; and registering the state of each shard as an anchor to facilitate cross-shard transactions. The Hub Chain does not run virtual machines or process smart contracts.

Business chain，Zones：

A business chain is a chain that specifically executes transactions, running virtual machines,

smart contracts, etc. Each business chain previously interacted with other chains through protocols to generate value.

Consensus algorithm:
Proof of Stake (POS), Tendermint is the name of the consensus mechanism used by Openverse. Validators (miners) stake Bitgold to participate in block validation and receive mining rewards. In the ternary paradox [FLP impossibility is a key result in distributed computing, which states that a distributed system cannot simultaneously have safety, liveness, and full asynchrony], the Openverse POS mechanism tends to prioritize security over liveness when making decisions.

Universal Name Service：
Universal Name Service, or Open Name Service, is a decentralized, scalable blockchain domain name service system. Each blockchain network/meta-universe can register its main domain name on the Openverse network. The main purpose of UNS is to translate Openverse's multiple gibberish-style addresses into readable and easily inputtable strings. For specific specifications, please refer to the official technical documentation on the website.

Smart contract:
Openverse smart contracts are fully compatible (equivalent to the 2.0 era) with Ethereum smart contracts and use Solidity programming language. The community is also encouraged to provide a library of smart contract templates.

DAO：
Using the smart contracts on the Openverse network, any entity can create its own DAO (decentralized autonomous organization). This opens up new ways for investment, fundraising, speculation, trading, insurance, lending, starting joint ventures, and managing various digital assets online in unprecedented ways, allowing for various collaborations.

DEX：
Using the smart contracts on the Openverse network, it is possible to open free digital asset trading.

3.4. Openverse Classification of digital assets

Openverse provides comprehensive digital asset governance capabilities (issuance, contracts, decentralized transactions), using value quantification and circulation to truly provide useful services for cross organizational (national) economic activities.

3.4.1. Standard assets

Bitgold, abbreviated as BTG, is the core asset of Openverse main chain and the underlying economy. Its known uses include being a collateral asset for public assets, transaction fees, staking assets for POS consensus, and the source of value for smart contracts. The name Bitgold was inspired by Nick Szabo's Bit gold prototype and the ideas he proposed, homage to the pioneering role of Bitcoin, and the historical significance of gold in finance. To facilitate understanding its role in the Openverse ecosystem, we chose the name "Bitgold" as the new base asset.

The total supply of BTG is 200 million, based on the latest data from the World Gold Council, which states that the world has mined 204,800 tonnes of gold since the start of human civilization, with over 3,000 tonnes added each year. The Openverse blockchain will halve its output every three years, so we chose a fixed number mathematically equivalent to this scale, i.e., 200 million. This number will remain constant, and developers should prioritize moving decimal points instead of changing the value of the asset.

3.4.2. Public currency

Public currency, also known as Bitcurrency, is a public asset issued through competitive auctions in which the public collateralizes Bitgold. In order to reference the naming convention of ERC-20 for Ethereum, we have designated the public currency standard with the code name "VRC-10". In our design, public currency is a digital asset of constant value. Rather than being a competitor to stablecoins, we view it as another form of fiat currency, and thus chose to directly reference the corresponding fiat currency name in its naming and code designation. Although there are some apparent similarities, there is no current equivalent to this type of public currency in the world. Notably, USDT is not a like-for-like alternative to USD and is a centralized product issued by Tether.

Openverse embedded issued public currency is a public currency anchored to the current legal currency of various countries:

Name	ISO code	Country or region
U.S.Dollar	USD	The United States
Canadian Dollar	CAD	Canada
Indian Rupee	INR	India
Japanese Yuan	JPY	Japan
Chinese Yuan	CNY	China

More than 200 types of fiat coins in total[https://www.iso.org/iso-4217-currency-codes.html]Covering all the legal currencies of sovereign countries around the world, it has been integrated into the Openverse main network as a public currency, and can be freely expanded to include more public currencies.

3.4.3. Token statand/Token

VRC-20, Homogeneity Tokens
Homogeneity token, also known as token or translated as token, is a homogeneous token on the blockchain, with the standard code VRC-20. It can be used in various application scenarios such as equity, enterprise points, software usage days/times, user consumption points, game coupons, etc.

VRC-721、Heterogeneity Tokens
Non homogeneous tokens can be understood as non interchangeable tokens. Simply put, each Token is unique and cannot be interchanged. It can be used for copyright, specific property rights, game props, domain names, etc.

VRC-30、Timing tokens
Time token, also named as Timing Token, is a time-sensitive token on the blockchain, with the standard code VRC-30. Specifically, its effectiveness is based on the block number on the Openverse main chain, which is generated, used, and destroyed. A token will be generated in a certain block until it dies in a certain block. Can be applied to Internet of Things usage rights, etc.

Other standard token
Based on future applications, expand multiple options and share usage through the public smart contract template market.

3.5. Public currency issuance mechanism

Therefore, we proposed a new idea for public currency issuance, the Public Competitive Issuance System, which uses the blockchain technology to address the flaws of the gold standard and central bank fiat currency issuance mechanisms. As it is essentially a dynamic collateralization of the base asset Bitgold, we can also call it the "New Gold Standard".

The Public Currency Issuance Mechanism (PCIM) is a currency issuance system that involves the issuance of public currency through excessive collateral of assets and the participation of the public in a competitive manner. PCIM has several key points:

- 1. All individuals who hold the base asset can participate in competitive issuance.
- 2. Over-collateralization of the base asset is used to produce public currency,which is released when the collateral is unlocked.
- 3. No interest or transaction costs are incurred.
- 4. Participation in competitive issuance is possible at any time.
- 5. Competitive issuance occurs frequently, with the blockchain cycle serving as the time standard.
- 6. Public currency is issued collectively, including existing fiat currencies and other public assets that may be required in the future.

Final advantage: Good currency drives out bad currency
Publicly issued currencies have brought about competition among currencies, and it is a global competition. People can choose long-term stable currencies across sovereignty, which will eventually leave inferior sovereign legal currencies with no Lebensraum.

4. Application Scenario

4.1. Bitgold Applications

"Bitgold has only one use: as a base asset for collateralizing the issuance of public currency."

"Although the probability is extremely low, Bitgold may become the world's unified currency in 50 years - assuming that the Bitgold price stabilizes at a certain level, public currency will gradually disappear."

4.2. "Application of Public Currency"

"Public Currency is the representation of fiat money in the blockchain world, serving as a bridge between trust-based economics and mainstream economics."

"Public Currency is M0."

"Public currency can be used wherever fiat can be used, and has the ability to infinitely expand the capabilities of Fiat."

"When Bitgold becomes sufficiently valuable, public currency will gradually reduce and disappear on its own."

4.2.1. World-class payment services

Represented by "Openverse Public Currency Equivalent to Fiat" and "Enterprise Private Stablecoins, Stable Value Tokens", countless enterprises can directly open payment services on the fully decentralized Openverse network, utilizing the advantages of other digital currencies. This is different from the era of digital currency 1.0 (when the price of Bitcoin was volatile and existing stable coins were issued arbitrarily by central entities). As public currency is equivalent to fiat currency, it has the advantages of fiat and electronic payments while also providing the ability for completely free and open blockchain payments. Similarly, with the endorsement of enterprise credit, enterprises can issue their own payment tokens and implement private domain payment services.

Various face-to-face, app, and website transactions can be directly integrated into the Openverse blockchain, entering the world's unified payment and settlement system.

4.2.2. Detrust lending business

Represented by "Openverse Public Currency Equivalent to Fiat" and "Enterprise Private Stablecoins, Stable Value Tokens", countless enterprises can directly open payment services on the fully decentralized Openverse network, utilizing the advantages of other digital currencies. This is different from the era of digital currency 1.0 (when the price of Bitcoin was volatile and existing stable coins were issued arbitrarily by central entities). As public currency is equivalent to fiat currency, it has the advantages of fiat and electronic payments while also providing the ability for completely free and open blockchain payments. Similarly, with the endorsement of enterprise credit, enterprises can issue their own payment tokens and implement private domain payment services.

Various face-to-face, app, and website transactions can be directly integrated into the Openverse blockchain, entering the world's unified payment and settlement system.

4.2.3. Frictionless trading intermediaries

Public currency becomes the intermediary currency for decentralized exchanges within the Openverse system, as well as the intermediary currency for other centralized exchanges. Smooth transactions within and outside the chain, as well as within and outside the site.

4.2.4. Low exchange rate, real-time cross-border exchange

Utilize the low transaction fees, real-time completion, and fully autonomous implementation of unrestricted international remittance and exchange purposes of Openverse main network transfers. Breaking the sovereign boundaries of existing fiat currencies for various international payment and exchange purposes.

4.2.5. Other legal currency purposes

For example, consumer payment, employee salary, enterprise payment, smart contract performance payment, etc.

4.3. Application of Homogeneity Token

4.3.1. Application to 'Equity'

We can tokenize the rights that may be owned by multiple entities, such as corporate equity, corporate income rights, ownership of goods, income rights, voting rights that form a competitive relationship, etc. Taking corporate equity as an example, after equity tokenization, private placement, public offering, and issuance of options to employees can be carried out through tokenization. Transfer transactions and open competitive transactions can also be carried out, and benefits can be integrated with the upstream and downstream of the enterprise.

4.3.2. Apply to 'Points'

Using non equity homogeneity with certain rights and interests as a token to convert them into "points", such as software usage times, employee cumulative points, and in-game consumption points. And it can be freely traded.

4.4. Non homogeneous token application

Compared to fungible tokens, non-fungible tokens have wide-ranging applications in the physical economy and the Internet of Things. They can represent any single physical or virtual object, such as different physical entities, certificates, cards, IoT devices, game props, etc., which cannot be further divided and can become non-fungible tokens that can be freely traded.

In particular, IoT devices such as cars, access control systems, and concert tickets that require "keys" to authorize their use, when tokenized, can bring unlimited possibilities.

4.5. Timing token application

Timing tokens can be applied to scenarios with limited time limits, such as the right to use leased equipment, voting rights, etc. Time tokens can be traded on the native network.

4.6. Smart contract application

With the support of human intelligence, smart contracts are almost limitless. We can provide some examples for reference and continue to expand them in the implementation process (see the Smart Contract template market for more details):

Financial derivatives: Financial derivative contracts are hedging tools for companies to manage investment or trading risks, such as commodity or currency risks, based on the value of underlying assets. Openverse can collect price information from multiple sources, integrate data, send it to smart contracts, and send payment data for settlement, automatically executing derivative contracts. Companies in the market typically delay payments as long as possible until establishing a position, so smart contracts using Openverse technology can be very helpful in rebuilding trust between counterparties.

Bonds: Issuing bonds and repaying them later is an ideal way of short-term financing. Bond contracts can be written as automatic, trustless, and decentralized smart contracts. Openverse can settle with public currency while also eliminating counterparty risk, as various decentralized authenticated data such as bank borrowing rates will automatically trigger payments.

Market data on the blockchain: The listed prices of assets on different exchanges may vary, so it is necessary to consolidate data from multiple sources to obtain an accurate price for an asset. Openverse's external data chain, Value Oracle, will provide sufficient data on chain services as resources for other smart contracts.

Decentralized exchanges: In decentralized exchanges, funds are held in user wallet addresses or transaction smart contracts, fully controlled by the user. When a user initiates a transaction, the exchange executes smart contracts to complete the transaction, and assets are transferred on chain. Transaction records are transparent and open on the chain, and resource allocation is free.

4.7. DAO Applications

DAO/DAC (Decentralized Autonomous Organization/Corporation) may lead to the concept of artificial intelligence. Decentralized autonomous networks can operate automatically in a company-like model under pre-set business rules without any human intervention. In DAO/DAC, some smart contracts run on the blockchain and automatically execute pre-approved tasks in accordance with pre-defined ranges, possibly based on changes in events and conditions.

On the blockchain, these smart contracts can not only operate in a mode like an autonomous enterprise but also build fully functional business models like those in the real world. As Bitgold transactions become more popular, this makes the remittance market more efficient, and DAO and DAC can do the same thing. A remittance company may face many places in the real world and with the local administrative jurisdiction, which requires a lot of coordination and therefore incurs many costs. Starting a business requires dealing with administrative affairs and regulatory laws such as business license, registration, insurance, and tax in the real world, which will also incur many costs. If these functions can be transplanted to the blockchain, these functions may become more efficient, and some tasks may become unnecessary, and all businesses will naturally be globalized. Cloud-based and blockchain-based autonomous enterprise entities can complete any operation they need based on smart contracts and electronic contracts, similar to governments registering themselves in administrative regions. Each company can become a global company first, and business models that are restricted by jurisdictional jurisdiction may also have better options.

5. Vision

5.1. Openverse 2.0 Public currency operation platform

Create a new platform that possesses numerous advantages similar to Bitgold's native asset and competitively issues circulating public currency for various economic links, inheriting the advantages of current fiat. Then, tokenizing tangible and intangible value media based on strong consensus on the public currency, to achieve the operation of the public currency platform. Furthermore, by efforts such as developing decentralized exchanges and connecting with payment applications at the application layer, the goal of operating a digital asset platform can be achieved.

5.2. Openverse 3.0 (World Value Exchange Network)

In the era of Openverse 3.0, planning and development work is expected to start in 2024. Technically, introducing homogeneous chain groups to separate various non digital asset lifecycle related transactions into homogeneous chain groups is a reduction and extension mechanism of sharding mechanism. Any individual can use Openverse code to run an independent homogeneous blockchain network, share the security of the main network, and solve performance issues in private domain applications; And the official will actively support the development and operation of similar homogeneous chains. The interoperability with the main network lies in accounts, standard assets, public currencies, and the main assets of the chain. Various industry associations, alliance organizations, and economic related ecosystems can independently run Openverse homogeneous blockchain to provide public services.

5.2.1. An Infrastructure for Web3

We are in the era of switching from the centralized Internet, that is, Web 2.0, to the decentralized Web3. Under the concept of Web 3.0, the ownership of digital content created by users is clearly owned and controlled by users, and the value created will also be distributed according to the agreements signed by users and others. We need a world-wide web3 infrastructure.

5.2.2. The Hub for Blockchains

Under current circumstances, each blockchain network has formed its own ecosystem and small society, and is an island of value. Many teams have developed a large number of bridges and protocols to link various networks. On this basis, we are carrying out the next step of development. Through the interchain communication protocols, different blockchain networks can communicate securely.

5.2.3. Protocols for Metaverses

Like the communication between blockchain networks, all meta-universe ecosystems also need to be interconnected. The connection is based on mutually accepted standards and protocols. The Openverse Team attempts to collect and sort out scattered protocols, form a unified protocol series of the metaverses, break through various information islands, and let users hold value to flow.

5.3. Openverse 4.0 Distributed Economic Ecology

Openverse 4.0 will support the overall construction and performance improvement of heterogeneous chain clusters, support third-party blockchain access through protocols, and focus on ecological access development, forming the morphology of a distributed economic ecosystem.

6. Others

If there is a possibility for the Openverse system to be implemented, then what is said here is more about sustenance and other considerations.

6.1. Technical Proposition

In order to achieve the entire system, which will take a long time, we need to establish some principles early on.

- Decentralization: Completely decentralized to ensure that it is not subject to the will of individuals.
- Resilience: Ensures that the network operates even if unexpected events occur in the real world.
- Security: Implements a distributed consensus mechanism where computing power is distributed over the network and prevents protocol violations.
- Simplicity: Focuses only on the protocol itself without involving application-specific logic.
- Durability: Ensures that the network operates for a long time, even by considering quantum computing problems proactively.
- Environmental protection: Ensures that energy consumption and hardware reuse are not increased while maintaining resilience and security.

6.2. Operational Proposition

Proactive development: In addition to continuous iteration of the main network technology, the team will continue to develop peripheral popular applications, such as multifunctional wallets, DAO templates, common smart contract templates, decentralized exchanges, etc.

Pursuing value: With Bitgold as the underlying asset, it can accommodate more real economy when its total economic value is large, thus accelerating the entire development process.

6.3. Social advocacy

We believe that DAOs and smart contracts are effective forms of resource integration and trustless collaboration between unfamiliar entities. We also believe that some well-known DAOs will emerge, which will have a huge social function beyond the form of traditional companies, groups, and organizations.

Therefore, those who can research, plan, design, and operate a DAO will be elites and wise people. It can be inferred that the future world will be a society governed by smart and knowledgeable individuals.

6.4. Civilization

The transition and evolution of civilization is a process of removing darkness and seeking light, and cooperation based on consensus between organizations is also such a process. The economy is the catalyst and driving force for civilization, so we may also see a "new civilization process". Therefore, various cultures will be integrated and developed step by step in the new civilization.

6.5. Law & legislation

Although we define Openverse as a great experiment, in the Openverse system, Bitgold attempts to become the bottom asset of the world's finance, and the public currency is essentially M0, with the goal of partially replacing the legal currency, far exceeding the range tolerated by current laws. For example, Facebook Libra faced various obstacles in its early stages, and it seems that Openverse will face countless legal rebukes against sovereign countries, both consciously and legally.

We should consider it a great experiment that requires seeking the inclusion of vested interest groups and legal leniency.

6.6. institution

Openverse is a project funded and supported by Utopia Foundation [Utopia Foundation, an open public welfare organization that advocates "scientism, liberalism Pietism, Pietism Liberalism".].

Openverse is a project developed and governed by the Openverse Team.

References

1、Nick Szabo,《Bit gold》, December 29, 2005, https://nakamotoinstitute.org/bit-gold/

2、Bitcoin wiki: https://en.bitcoin.it/wiki/Bitcoin, http://www.bitcoin.org

3、Ethereum, http://www.ethereum.org

4、Friedrich uon Hayek,《Denationalisation of Money》

5、Zvi Bodie/Alex Kane/Alan J. Marcus,《INVESTMENTS》

6、Fank J. Fabozzi/Franco Modigliani/Frank J.Jones,《Foundations Of Financial Markets and Institutions》

7、Yuval Noah Harari,《Homo Deus - A Brief History of Tomorrow》

8、《[The End of Money the Story of Bitcoin，Cryptocurrencies and the Blockchain Revolution》

9、N.Gregory Mankiw,《Principles of Economics》

10、ROBERT J. SHILLER,《Bubbles, Human Judgment, and Expert Opinion》

11、J. Bradford De Long, Andrei Shleifer, Lawrence H. Summers and Robert J. Waldmann,《Noise Trader Risk in Financial Markets》