Principle Analysis of Second-Generation Digital Currency Based on Public Welfare

Authors: ZHANG Jingbo, Wu Bofan

Date: 2021-10-07T00:00:00+00:00

Abstract

Blockchain is an emerging decentralized infrastructure and distributed computing paradigm that has gradually risen with the increasing popularity of digital cryptocurrencies such as Bitcoin, currently attracting significant attention and widespread concern from government agencies, financial institutions, technology enterprises, and capital markets. While digital currencies represented by Bitcoin have achieved tremendous success, they also exhibit numerous deficiencies and have engendered a series of social issues. This paper proposes a novel issuance model for digital currencies and non-fungible tokens (NFTs), which can effectively compensate for the shortcomings of existing digital currencies and enable them to generate greater social value.

Full Text

Preamble

Vol. XX, No. X

Analysis of Second-Generation Digital Currency Principles Based on Public Welfare Undertakings

ZHANG Jingbo, WU Bofan

Abstract

Blockchain represents a novel decentralized infrastructure and distributed computing paradigm that has emerged alongside the growing popularity of digital cryptocurrencies such as Bitcoin. It has attracted significant attention from government agencies, financial institutions, technology enterprises, and capital markets. While digital currencies exemplified by Bitcoin have achieved remarkable success, they suffer from numerous defects and have engendered a series of social problems. This paper proposes a new digital currency and Non-Fungible

Token (NFT) issuance model that can effectively remedy current digital currency shortcomings while creating greater social value.

Keywords: NFT, digital currency, Coase theorem, Coase bargaining, transaction costs, decentralization, Pareto optimality, frame theory

Citation: Analysis of Second-Generation Digital Currency Principles Based on Public Welfare Undertakings. *Acta Automatica Sinica*, 20XX, XX(X): X−X
DOI: 10.16383/j.aas.20xx.cxxxxxx

1 Introduction

Blockchain technology serves as the core supporting infrastructure for digital cryptocurrency systems represented by Bitcoin. Its primary advantage lies in decentralization, enabling peer-to-peer transactions, coordination, and collaboration based on decentralized trust in distributed systems where nodes need not trust one another, through the application of data encryption, timestamps, distributed consensus, and economic incentives. This provides solutions to the high costs, low efficiency, and insecure data storage that plague centralized institutions [1].

First-generation digital currencies such as Bitcoin and Ethereum, while achieving tremendous success, have exposed a series of defects and triggered various social problems. For instance, these currencies typically employ a "reward for bookkeeping" rule, yet users expend enormous computational power competing for "bookkeeping rights" rather than on bookkeeping itself. In Bitcoin, nodes (miners) collectively solve a complex SHA256 mathematical puzzle, with the first to solve it gaining bookkeeping rights for that block. This process generates massive annual carbon emissions, electricity consumption, and graphics card waste, running counter to China' s energy conservation and emission reduction goals and global efforts to curb climate change [2]. Applications of Bitcoin and similar digital currencies are largely confined to money laundering, black market transactions, drug trafficking, cyber extortion, and speculative trading, even financing terrorist activities [3][4]. Digital currency values are unstable, making them unsuitable for daily use as currency while simultaneously fueling extensive speculation. Over 30% of South Korea' s population holds Bitcoin, mostly for speculative purposes, while newly issued "air coins" and "zero coins" have effectively become new forms of gambling, sometimes combined with pyramid schemes and illegal fundraising, creating significant social problems. Additionally, virtual currencies compete with fiat currencies for seigniorage, causing losses to governments [5].

The negative externalities of virtual currencies have limited their development and application. China, South Korea, and Russia were among the first to ban virtual currencies nationwide, while Facebook's Libra cryptocurrency was halted by the U.S. government [6]. This compels us to improve virtual currency technology and business models, seeking blockchain application scenarios that can

create social welfare. Only when virtual currencies generate positive utility for society can they achieve more robust development.

Public Welfare and Market Solutions to Externalities

Externalities refer to side effects when market outcomes affect parties other than buyers and sellers [6], such as automobile emissions or environmental organizations' pollution control efforts. Resolving market inefficiencies caused by externalities has long been a central problem in economics. The conventional approach involves internalizing externalities by altering incentives so that producers consider their external impacts, a process typically requiring government intervention, such as Pigouvian taxes and subsidies.

In 1960, Ronald H. Coase demonstrated that when property rights are clearly defined and transaction costs are minimal, market equilibrium can achieve Pareto-optimal resource allocation [7]. Market-based externality solutions are rarely observed in reality because the two preconditions of Coase' s theorem are often not satisfied—either property rights are unclear or transaction costs are prohibitively high.

This insight suggests that markets can spontaneously resolve externality problems, with the key lying in ensuring property rights and reducing transaction costs. Governments often use administrative directives to regulate externalities, but such interventions frequently distort the true demand for public services.

[Figure 1: see original paper] Wrong estimation of externality of administrative instructions

Figure 1 illustrates two failures of administrative directives in the internalization of externalities: over-provision and under-provision. Over-provision occurs when officials, driven by performance metrics, create excessive quantities of public goods far beyond public demand, resulting in waste. A typical example is the 40 billion RMB financing for abandoned construction projects in Dushan County, Guizhou—a nationally designated impoverished county.

Under-provision examples include reporting corruption, organized crime, or enterprises producing substandard goods. These socially beneficial public services suffer from insufficient rewards for whistleblowers who face personal safety risks, reducing their motivation. In the "Pang Ge Liang Meat Crab Pot" food safety case, no chefs or sales staff reported the illegal enterprise during its long-term production of inferior food. Both scenarios distort public service pricing, causing substantial welfare losses to the nation and its citizens, hindering Chinese brands' global expansion and generating public dissatisfaction.

Another challenging type of externality is intergenerational externality. Numerous behaviors benefit contemporary populations while harming future generations: sacrificing biodiversity for economic development, dumping nuclear wastewater, and massive carbon emissions causing global warming. The costs

of these actions often only manifest decades later. If we denote the net externality that generation i imposes on generation j as wij, then the externality Wn imposed on generation n by previous generations is:

1n21Wjnjiwij−=== (1j2n3)i ,,

Clearly, if each generation' s created *wi* exceeds *wi-1*, society achieves a "sustainable development" state; otherwise, society becomes unsustainable [8]. Traditional approaches struggle to resolve intergenerational externalities, with both Coasean and Pigouvian methods having limitations [8]. One current solution involves state-funded investments beneficial to future generations. Since beneficiaries are citizens' descendants, opposition to such investments is not strong. However, when investors are one country while beneficiaries are the world or future global generations, such investments often face 重重阻挠: a typical example being international public organizations addressing climate change, which only partially resolve externality problems.

In the operational domain of public welfare organizations, Coasean bargaining is often difficult to realize. Faced with public services where collecting returns is difficult and transaction costs are enormous, public welfare organizations partially or completely abandon returns. Beyond limited funding and influence, their activity domains struggle to cover diverse externality scenarios.

Simultaneously, society lacks reasonable, effective, and sustainable reward mechanisms for individual public welfare behaviors. Numerous cases of "pengci" (extortion through feigned injury) and elderly assistance fraud, where perpetrators receive minimal punishment even when discovered, while public welfare providers often suffer property losses, severely impact social atmosphere and public enthusiasm for welfare. Cases such as Wu Weiqing, who committed suicide to prove his innocence after being extorted for helping an elderly person, and the Nanjing Peng Yu case have profoundly affected social sentiment and public initiative toward public welfare. In the food industry, safety issues at "Pang Ge Liang Meat Crab Pot" and "Sanlu Milk Powder" have severely impacted the credibility of Chinese food brands among citizens and created obstacles for Chinese brands' globalization.

Therefore, China urgently needs a unified, efficient, market-based mechanism that reflects public will to address current system deficiencies. The "public welfare coin" mechanism represents precisely such an externality market solution.

2 NFT Minting Theory

Traditional digital currencies like Bitcoin provide inspiration: currency value directly originates from shared belief in its value. Currency can be backed by various physical assets and entities, as exemplified by the Bretton Woods system linking the U.S. dollar to gold, where the dollar' s value equaled gold' s value (assuming no default risk). Gold' s value itself derived from consensus accumulated through long-term use as currency. Bitcoin and similar digital currencies allo-

cate currency through "mining" processes that consume electricity and graphics cards (while incentivizing bookkeeping), but this "value assignment" process wastes substantial social resources. The shortcomings of first-generation digital currencies like Bitcoin and Ethereum inspire us to develop second-generation digital currencies: enabling the digital currency issuance "value assignment" process to genuinely create enormous social value.

A minimal public welfare commemorative coin model is the public welfare NFT. NFTs are non-fungible tokens, where each token possesses a unique and distinct identifier, non-interchangeable pairwise, with a minimum unit of 1 and indivisible, as seen in applications like CryptoKitties and MEME. Issuers conduct public welfare activities, binding each welfare initiative with a unique NFT for sale, with proceeds funding current and future public welfare activities.

[Figure 2: see original paper] Positive feedback loop of public welfare commemorative coin system

While NFT technology cannot directly enhance productivity, we can indirectly improve social welfare by influencing purchasing habits. Consider improvements to the gemstone industry:

According to statistics [China Customs, Huajing Industry Research Institute], China imported approximately 300 billion RMB worth of diamonds from 2015-2020, equivalent to Qinghai Province' s annual GDP. In 2020 alone, China' s net diamond imports reached about 36 billion RMB (source: China Business Industry Research Institute database). This demonstrates China' s substantial annual foreign exchange expenditure on various gemstones.

Meanwhile, as an allotrope of graphite, synthetic diamond technology has advanced rapidly in recent years [9], challenging the long-term collectible value of small diamonds. As technology develops, synthetic gemstones' luster and brilliance have surpassed diamonds. Taking moissanite (SiC crystal with diamond structure) as an example, its fire dispersion is 2.5 times that of diamonds, making high-end diamond simulants more brilliant than real diamonds. However, due to their lack of rarity, market value remains unrecognized.

Most diamonds experience significant depreciation after consumer purchase. Second-hand diamond resale prices typically discount by 50% to 80%. Consumers, particularly male purchasers, urgently need reasonably priced diamonds with high value preservation and appreciation potential.

Therefore, we must create a new gemstone system to address these issues. We propose another NFT model called "Star Diamond,"with theoretical foundations in Marvin Lee Minsky' s frame theory [10]. Minsky argued that in daily cognitive activities, humans employ extensive knowledge acquired and organized from past experience. This knowledge is often stored in the brain as frames. When facing new situations or significant perspective changes, people retrieve an appropriate frame from memory and modify its details based on actual circumstances, enabling the use of past experience-derived concepts to interpret

observed phenomena.

Gemstones require beauty, durability, rarity, and identifiability (if genuine gemstones cannot be distinguished, rarity becomes ineffective) [11], with primary uses being social display and collection. We demonstrate that a gemstone' s essence is an aggregation of these attributes and functions: Suppose a company produces a box of crystal-skinned mooncakes that, while crystal clear, are extremely hard and impervious to water and fire, making them unsuitable for consumption. This box is delivered to a desert island tribe. On the island, the item is scarce, hard, beautiful, displayable to others, and collectible, leading the tribe to adopt it as a generationally transmitted gemstone.

[Figure 3: see original paper] GEM model described by frame theory

Rather than representing a gemstone's physical essence, a gemstone more closely resembles a collection of three attributes (rarity, beauty, durability) and two functions (social display, collection). Humans more readily match certain minerals to the "gemstone" mental framework. Therefore, through ordered combinations of objects with different essential natures, while guiding the public to match them to the gemstone framework, we can accomplish the task of "logically minting gemstones."

A gemstone' s social attribute encompasses collectively recognized social value. Different groups possess 不完全相同的 frameworks and priority relationships between frameworks. For instance, even if crystal-skinned mooncakes possess gemstone attributes (scarcity, beauty, etc.), because people prioritize matching them to the "mooncake" framework, they lose the "social display" function. Despite collectible value, people cannot use them as gemstones.

An object' s matching priority across frameworks can be represented as a partially ordered set $(F, \leq(x))$, where F is the set of frameworks and $\leq(x)$ represents the partial order relation corresponding to object x' s matching process. This matching resembles a supervised classification problem: all frameworks can be viewed as a one-hot vector, with the human brain as a classifier outputting probabilities of an object belonging to various frameworks, selecting the maximum probability as the matching result. If the human brain' s past experience lacks an optimal framework for matching the object, the resulting framework may diverge significantly from reality. Consider this example of matching error:

Cargo cults [12] refer to religious forms among certain indigenous peoples where advanced technological items from outsiders are worshipped as deities. During World War II' s Pacific theater, the U.S. military established a temporary base on Tanna Island. Indigenous inhabitants observed soldiers emerging from "large iron ships" (warships) and "large iron birds" (military aircraft) delivering people and supplies, finding it astonishing. Combined with useful supplies provided to locals, these indigenous peoples came to worship the U.S. military as gods.

We can explain cargo cults through frame matching theory. Most U.S. soldiers also held religious beliefs, but only the indigenous people mistakenly understood

military aircraft as gods. The American cognitive model contained both aircraft and god frameworks, while the indigenous model contained only the god framework. Aircraft attributes and functions largely matched the god framework: aircraft/gods fly in the sky, aircraft/gods punish disrespectful beings with wrath (fighter machine guns, Sodom), aircraft/gods reward followers with supplies. At this point, aircraft were matched to the god framework by Tanna Island' s indigenous people and worshipped long-term.

This knowledge acquisition method resembles duck typing in dynamic typing, where an object' s valid semantics derive not from inheriting specific classes or implementing particular interfaces but from its current collection of methods and attributes. We understand NFTs as a glue binding attributes and functions, hoping to decouple and recombine original framework attributes in desired directions, guiding customers and the public to match them to target frameworks.

NFT gemstones represent the integration of gemstones across "three worlds" : the physical world, blockchain world, and consensus world. Taking moissanite as an example: moissanite lacks "rarity" attributes and "social use" functions. We use moissanite as the physical world carrier for NFT diamonds, linking it inseparably with a unique NFT verifiable through apps and other offline methods, thereby ensuring verifiability for social use. Simultaneously, the NFT links to bound assets (such as wealth management, insurance, real estate), transferring beneficiaries of these assets as customers trade or gift the NFT. These assets provide a price floor for NFT gemstones, with growth potential achieved through promotion, the gemstones' own appreciation, and uniqueness.

[Figure 4: see original paper] "Trinity" model of NFT jewelry

For example, women often report feeling insecure in relationships. Typically, diamonds gifted by men have second-hand prices of only 20% to 40% of original value. If we bind NFT gemstones to lifetime insurance, real estate, wealth management with the woman as beneficiary, or betrothal agreements rewarding based on marriage duration, the original gemstone expenditure substantively transfers to the post-marital family while increasing the woman' s sense of security.

In summary, NFTs' essence lies in constructing or matching frameworks within human consensus.

[Figure 5: see original paper] Positive feedback loop of public welfare commemorative coin system

3 Public Welfare Commemorative Coin Model

Compared to public welfare NFTs, we propose a more efficient and systematic issuance model: the public welfare coin model. This model more closely resembles digital currency issuance but differs by incorporating a public welfare community reflecting mass consensus as its decision-making core.

Currency value directly depends on users' recognition, with its issuance process collecting "seigniorage" from the public. We propose that public welfare organizations issue digital currency, gradually increasing issuance annually within limited bounds. Public welfare organizations' activities endow the digital currency with public recognition, providing benefits to holders.

With limited new public welfare coin resources, public welfare organizations maximize their impact by democratically voting to prioritize projects with greatest influence, automatically completing public welfare pricing to remedy administrative directives' distortion of public service prices. This process essentially represents Coasean bargaining with drastically reduced transaction costs: public welfare activity organizers no longer require beneficiaries to sign one-on-one contracts and ensure enforcement; all beneficiaries and observers simply "recognize the value of the organization' s work," with this recognition process itself paying for the public welfare activity, reducing transaction costs to near zero.

Facing international and intergenerational externalities, public welfare coins demonstrate even greater value: if we believe future generations will be wiser than present ones, they will more readily recognize past organizations' contributions in carbon emission control, rational population growth, environmental protection, scientific research, etc., thereby affirming public welfare coin value. This creates an intergenerational chain: previous generations protect and enhance next generations' living environments, next generations acknowledge previous generations' contributions while protecting subsequent generations, ensuring each generation' s environment receives effective protection.

[Figure 6: see original paper] Operational framework of public welfare commemorative coins

Public welfare coin issuance comprises three components: First, public welfare coins have floating prices; anyone can exchange national currencies for public welfare coins at exchange rates and current prices. This is considered a donation process. All exchange proceeds are managed by a public welfare fund supervised by society and all public welfare coin holders. Public welfare fund allocation should 原则上 aim to maximize long-term national benefits and benefits to others. All fund work should be viewed as efforts to enhance public welfare coin value consensus.

Second, the community consists of all public welfare coin holders and citizens supporting public welfare coins. The community provides various proposals for referendum by all members. (Sub-communities could also conduct referendums for efficiency, later merging proposals.) Proposal implementers receive certain public welfare fund allocations, with the community issuing corresponding amounts of public welfare coins based on fund allocation.

Another public welfare coin operation method involves···Public welfare projects include several types: those preventing negative externalities, such as reporting corrupt officials, combating law-violating corporations (e.g., Sanlu Milk Powder,

Samsung exploding phones, Pang Ge Liang Meat Crab Pot), reporting organized crime, drug trafficking, or polluting enterprises.

Third, individuals or organizations with major contributions receive public welfare coin grants and corresponding issuance after verification, such as families of revolutionary martyrs, anti-narcotics police, and self-sacrificing rescuers.

Fourth, individuals or collectives promoting beneficial national policies receive public welfare coins, including those optimizing population quantity and structure, promoting social equity and tertiary distribution, or achieving major scientific breakthroughs.

Fifth, investments beneficial to national future development, such as quantum computing and biotechnology, are funded.

2.1 Public Welfare Coin Price Control Mechanism

To promote public welfare coin dissemination, investment, and development to create greater social welfare, new-generation digital currency holders should receive reasonable returns, such as 10% to 30% annualized returns, as compensation for three types of contributions: promoting public welfare, inflation of fiat currency, and natural growth of public welfare undertakings.

Public welfare coin value should be more stable than Bitcoin, emphasizing its currency attributes and long-term investment characteristics to enhance broad social recognition.

4 Impact of Digital Currency on Future Society

An ideal world currency should be a single supranational currency [8], representing the most economically efficient, politically least controversial, and lowest transaction cost approach. As Robert A. Mundell stated, "The optimal number of currencies, like the optimal number of gods—is odd, preferably less than three" [10]. Imagine a globally issued world currency spending the vast majority of its seigniorage on improving current and future world citizens' welfare—this would inevitably be fairer and more efficient than sovereign currencies.

The "China Brain" problem asks: "If one billion Chinese people each had a walkie-talkie maintaining real-time communication with others, would China as a whole develop independent consciousness?" [11][12]. The China Brain problem is a special case of the more general question of whether consciousness can exist within larger conscious collectives.

In terms of computing power, a neural network composed of 1.4 billion people contains 10^{23} to 10^{24} plastic synapses. The China Brain system fails to produce higher-level intelligence not due to insufficient computing power, but because "walkie-talkies" or "WeChat" as communication and cooperation protocols are too low in performance and efficiency. Digital currency technology provides individuals sufficient incentives to participate in organizational work,

while partial or complete decentralization ensures organizational robustness and democracy. Such organizations can penetrate domains where administrative directives struggle to operate efficiently, like white blood cells improving overall social operational efficiency and citizen welfare without affecting regime stability.

For the first time in human society, digital currencies provide extremely low-cost effective tools for consensus-based collectives—whether centralized or decentralized—to influence the external world, and cannot be completely destroyed by governments. El Salvador' s adoption of digital currency as legal tender represents the first visible wave in this era.

Since individual capacity for consensus is limited, and digital currency technology enables social group consensus itself to be converted into resources for social group operations at relatively low cost, we can foresee that social groups with different consensus, in various forms—such as LSBT communities, Muslims, multinational corporations—will successively raise funds by issuing their own virtual currencies, assigning value through organizational actions. Supporters can assign value to their preferred organizations through using or trading their virtual currencies, even from thousands of miles away. Following "physical space" and "cyberspace," "consensus space" will become fiercely contested territory among nations, enterprises, centralized organizations, and decentralized organizations.

Multinational corporations with currency issuance rights have become "states without territory" to some extent. Facebook' s Libra cryptocurrency, created jointly with Visa, Uber, and over 30 other companies, is a 标志性 example. Super online banks simultaneously holding seigniorage and credit rights can earn massive profits without bearing responsibility to nationals while threatening fiat currency credibility. Although the U.S. House of Representatives halted Facebook' s currency issuance in July 2019, this cannot change the broader trend of multinational giants issuing digital currencies worldwide.

From another perspective, using a sovereign currency as world currency creates many problems. On one hand, the world currency issuing country enjoys the privilege of collecting seigniorage from the entire world—an enormous unfairness. On the other hand, this privilege also undermines the world currency itself.

[Figure 7: see original paper] The auxiliary function of public welfare currency system to society

As illustrated, government directives can be analogized to the central nervous system, while decentralized auxiliary organizations resemble intercellular non-neural information communication and cooperation mechanisms. The two systems cooperate and influence each other, jointly enhancing social efficiency and citizen happiness.

References

1. Yuan Y, Wang F Y. Blockchain technology development status and prospects [J]. *Acta Automatica Sinica*, 2016, 42(04): 481-494.
2. Xue T F. Research on several issues of blockchain application [D]. Beijing University of Posts and Telecommunications, 2019.
3. Shi Y A, Wang Y J. Criminal governance of Bitcoin money laundering crimes [J]. *Journal of National Prosecutors College*, 2019, 27(02): 47-62.
4. Zhang W W, Wang W. Research on dark web terrorism crimes [J]. *Journal of Chinese People' s Public Security University (Social Sciences Edition)*, 2016, 32(04): 13-18.
5. Eichengreen, Barry. From commodity to fiat and now to crypto: what does history tell us?. No. w25426. National Bureau of Economic Research, 2019.
6. Cornes, Richard, and Todd Sandler. The theory of externalities, public goods, and club goods. Cambridge University Press, 1996.
7. Coase R H. The problem of social cost[M]//Classic papers in natural resource economics. Palgrave Macmillan, London, 1960.
8. Zhao S L, Gao H Y, Tan L. On intergenerational externalities and sustainable development [J]. *Nankai Journal*, 2003(04): 41-47.
9. Balmer R S, Brandon J R, Clewes S L, et al. Chemical vapour deposition synthetic diamond: materials, technology and applications[J]. *Journal of Physics: Condensed Matter*, 2009, 21(36): 364221.
10. Minsky M. A framework for representing knowledge[M]. de Gruyter, 2019.
11. Zhang B L. *Systematic Gemology* [M]. Geological Publishing House.
12. Lindstrom, Lamont. Cargo cult: Strange stories of desire from Melanesia and beyond. University of Hawaii Press, 2019.
13. Cole D. The Chinese room argument[J]. 2004.
14. Block, Ned. "Troubles with functionalism." Readings in philosophy of psychology 1 (1980).
15. Strukov D, Indiveri G, Grollier J, et al. Building brain-inspired computing[J]. *Nature Communications*, 2019 (10): 4838 (2019).
16. Smaghi dilemma revisited[C]//Speech at the Conference on the.
17. Zhou X C. Thoughts on reforming the international monetary system[J]. *China Finance*, 2009(07): 8-9.
18. Smaghi dilemma revisited[C]//Speech at the Conference on the.
19. Mundell R A. A theory of optimum currency areas[J]. *The American Economic Review*, 1961, 51(4): 657-665.
20. Cole D. The Chinese room argument[J]. 2004.
21. Block, Ned. "Troubles with functionalism." Readings in philosophy of psychology 1 (1980).

ZHANG Jingbo
School of Information Science and Technology, Beijing Forestry University
Representative work: *Analysis of Visual Illusion Phenomena Based on Light Intensity Superposition*

E-mail: Laplace_{transform}@163.com

WU Bofan
Ph.D. Candidate, Beihang University
E-mail: BY1913022@buaa.edu.cn

Note: Figure translations are in progress. See original paper for figures.