The Digital Universal Drachma

A Paradigm for a Global Private-Public Cryptocurrency

Chitose Nakamoto
chitose_nakamoto@protonmail.com

In Japanese, the name Chitose is given to a woman "who will rise with the strength of a thousand generations." She is a bold reformer in her own age, but she is propelled by the wisdom gained from the traditions, successes, and failures of her ancestors before. As a Nakamoto, her heart is the distillation of the very best that her family and community have to offer—a person of deep virtue while still maintaining a profoundly approachable air of humanity. She is humble yet great, and her work—gentle as water, incessant as the waves—finds a way to polish a thousand hearts into gold.

Preface

As the dream of cryptocurrency spreads in response to Satoshi Nakamoto's Bitcoin whitepaper, it has become clear that the most prominent attempts at revolutionizing the nature of currency are riddled with hamartia. Chief among the concerns that accompany these projects (such as Bitcoin and Ethereum) include price instability, exorbitant transaction fees, unsustainable processing and storage requirements, hyper-centralization of mining or staking, and the contention between privacy and social accountability.

Though I will likely be deemed a heretic by many crypto enthusiasts, the ideas herein proposed are aimed towards the success of not only a globally standardized cryptocurrency, but also the achievement of reimagining the core individual and institutional relationships that underpin our understanding of how an economy functions.

A successful reformation of the very nature of currency must occur in the context of dialogue between private entities and public institutions. To divorce politics and economics—while a thrilling idea at first—is to sever the channels through which individual liberties negotiate with social responsibilities. This is precisely why I am alarmed that popular cryptocurrencies' flirtation with anarchic ideals has resulted in the systemic espousal of the Freidman doctrine that "greed is good." Practically, that means Bitcoin is an unregulated and trustless marketplace where greed for more tokens is the only incentive for

good behavior. The sense of social responsibility that Aristotle credits with being the foundation of human society is thus eroded to a point where a productive society cannot exist.

Even now, the idolization of greed has entirely undermined the ethical foundations of the movement. We occupied Wall Street to condemn the out-of-control avarice exhibited by bankers, but we have in turn created our own multi-trillion-dollar market that is as much of a casino as the CDO derivatives that helped spawn the Great Recession. Edward Snowden similarly agrees that "the worst part of cryptocurrency transforming into dragon-level wealth is witnessing good people emotionally devolve into dragons themselves: so intellectually paralyzed by the fear that everyone they see threatens their hoard that they lose sight of the world beyond their cave."

In a sense, the prevalent philosophies of cryptocurrencies have become so decentralized that the private individual is entirely isolated in their own cave, untrusting of anyone outside the purview of their mirror. Just as there is no true economy in communism, there can neither be an economy in Narcissism; only a moderate avenue provides the correct conditions for a flourishing economy.

Therefore, the concept of a public-private partnership in cryptocurrency is entirely natural if the true goal is to construct a just economic framework. We exist entirely in community, so just as "man is by nature a political animal," so too should our human economy be mindful of the societies it has the power to influence and the lives it changes daily. In other words, every economic market is a social market, and our economic infrastructure must consider the limitations and responsibilities it thus inherits, and the private individual's rights need to be protected without detracting from their social and ethical responsibilities.

Striking this balance is the most significant obstacle facing digital currencies; it will ultimately be the social implications of digital economics that determines its success or demise, its legacy as a reformation or insurrection.

Accordingly, what follows is not a typical crypto whitepaper. I give you no code to use as a boilerplate. I have no stake to profit from investment, save the universal stake of being a member of human society. I find it best to propose topics for discussion, offer ideas and recommendations, and let public discourse further develop what I present. No single person should be responsible for building the infrastructure of the future global economy, so I leave this task in the hands of society and the collaborative spirit that has enabled us as a species to survive.

All my best,

Chitose Nakamoto

Theories of Currency

Money has been a topic of debate since the dawn of philosophy. Two of the most prevalent theories of currency were proposed by Aristotle and his teacher Plato. In short, Aristotle believed in metallism which asserts that currencies only have value if they are supported by tangible assets. On the other hand, Plato subscribed to chartalism which posits that a currency's value arises from the government's power to levy taxes in that denomination.

Bitcoin's philosophy most certainly rejects the idea of chartalism, but it also fails to fulfill the requirements of the metallist viewpoint. As it is not backed by a government nor by any tangible commodity, Bitcoin's entire utility is based upon the techno-utopian—and dare I say quasi-idolatrous—trust placed solely in the "infallibility" of the blockchain. Bitcoin fails to provide a guarantee of value for the content of each transaction beyond the "trust" it assures its users to have in the very same people the technology deems "untrustworthy." It has no physical asset, and the closest thing it has to an asset (trust) is tainted by its own self-inconsistency. This is why Bitcoin's price fluctuates so violently: it has no definitive value, so its price is determined upon the whims of traders.

Now, a common defense of Bitcoin's fluctuating price is that this is exactly the type of dynamic valuation that the stock market is based upon. This is true enough, but stocks are not meant to be currencies. Stocks are assets, not an intended currency as Bitcoin is. But even if we were to entertain this argument further, this defense is only valid so long as one believes that holding stock in a company which produces no services or commodities is a good idea. Thus the conundrum arises: Bitcoin is a currency that offers no collateral and is void of any governmental guarantee or a given taxation purpose. But this does not mean Bitcoin is entirely a sham currency, it is just not a metallist or chartalist currency. In fact, this same type of currency has existed before and is still in active use today. Precisely, I am speaking of social credit.

It is ironic that Bitcoin (a currency based on a lack of trust) shares the most in common with social credit (which is entirely based upon trusting another person). Both are intangible "ledgers" that assign subjective values to certain interactions or transactions. While this may work well for small groups of people who are inclined to either pay forward the kindness shown to them or exact revenge for misdeeds, this is hardly the scenario Bitcoin was intended to serve in.

In antiquity, when economic activity was extended beyond a circle of companions, the default currency was any useful commodity: tools, food, metals, and other things of that sort. As sedentary societies began to grow and their population expanded, social credit remained among intimate groups, but commodities trading became the primary form of currency. As carrying around goods to trade became

rather clumsy and inefficient, promissory notes (I-owe-you's) were introduced. Once again, though, these notes relied upon the virtue of the other transactor to follow through on his or her promise. As a solution to this problem, societies such as Babylon instituted centralized warehouses of gold that issued promissory notes that allowed their holders to lay claim to a certain amount of collateral in the community stockpile. This was the birth of centralized currency.

This solution devised in ancient times has served for the basis of monetary conceptualization across millennia. Of course, other evolutions have occurred (as chartalists would readily assert), but none are so important as the development of currency in a centralized manner. It has been Bitcoin's aim to make take the next step in economic development, namely by decentralizing currency. This, however, is where Bitcoin's fundamental flaw lays: there is no decentralized version of a "centralized warehouse" full of assets to guarantee the value of the currency.

As one can expound, this suggests centralized stable coins such as Tether and USDCoin—while used widely among crypto traders—are hardly innovative at all. In fact, the only benefit they provide over the Babylonian economic system is that the promissory notes are digital instead of physical.

Many blockchains are arguing the so-called gas fees paid for being included in the network decentralize value by distributing taxation power to all whom wish to secure the network. In a sense, this is indeed a brilliant idea for decentralizing chartalism, and I applaud Ethereum for spearheading this approach. The issue, however, is that such a tax being included in the economy largely leads to wasted money. Those who profit off securing the digital economy do not have a responsibility to the public to put their tax dollars to work, which means people find minimal return on investment for the taxes they pay, and in turn completely undermining the chartalist framework. If taxes are wasted money, then there is no incentive to continue using that chartalist currency.

The only option left, then, is to decentralize metallism. This is precisely the concept behind the Digital Universal Drachma. What follows is a deeper discussion about the rationale used to design the DUD—as well as the actual proposed design itself—but if the concept of decentralized metallism is kept in mind, the core principle has already been grasped.

Democratization, not Decentralization

Babylon got it right with their centralized warehouse of gold to back their currency. In fact, the issue with money has never been centralization. I know those words are heretical to crypto enthusiasts, but take a moment to consider it: the only reason money has any value is because a group of people centralized their social and material credit into a uniform token, which we happen to call currency. In

fact, I am willing to assert that there *must* be some level of centralization in order for any useful form of currency to exist. The caveat, though, is that centralization does not have to mean authoritarianism or feudalism. It is fine to have centralized stores of wealth, but they must be *democratized.*

Rugged and unbridled capitalism is nothing but an economic cult that opposes the democratization of a community's store of wealth. Likewise, communism deprives the masses of control over the economy by limiting their personal and political freedoms. As I mentioned before, any just economy needs to be a social market that balances the autonomy of the individual with the good of society at large, which means adopting an economy of democracy with checks and balances. My goal, then, is to describe a practical way to ensure the democratization of our communal stores of wealth, thereby preserving the sole foundation of a currency's value while also providing the groundwork for a cryptocurrency not controlled by a single entity.

Backing the Drachma

We often think of the currency as having the fixed value in a transaction, and negotiation sets the value of a product or good. In reality, however, that is usually only true for a multimetallist currency. In monometallism and chartalism—which is the *de facto* philosophy of the world's dominant reserve currency—a negotiation is less about setting an objective price on a good, but rather about bringing the subjective value of a unit of currency into agreement with the subjective value of a good for all parties involved.

To illustrate this point, think about two people buying the same good: a bottle of water. In this situation, all variables are controlled for except one thing, and that is each person's wealth. Additionally, the currency being used is either a chartalist or a monometallist one.

It is entirely believable that the wealthy person is willing to pay 50 units of currency for this bottle of water, but the poor person is only willing to pay 15 units. Subjectively, each person values water to the same degree—each are as reliant upon water for life as the other. The only difference, then, is that each person's subjective value of each unit of currency varies greatly. At first this could be solely attributed to the proportion of one's wealth that the water would cost as a simple matter of supply differences. But in chartalism or monometallism, this subjective discrepancy can be extended to a systemic instability of sudden inflationary or deflationary trends due to limitless minting powers or fluctuating market forces for the underlying asset (respectively). This systemic instability disproportionately affects the poorer individual as the subjective value of inflation is much higher for

them than for the wealthy person, further exacerbating long-term economic inequality and coalescing market power into an oligarchic structure.

Now, let's consider the same situation but with a different currency. In this scenario, each unit of currency is a bimetallist one. Given this circumstance, each person may still agree to pay their previous prices of 50 and 15 units, but as Alexander Hamilton argued, bimetallism would make the currency less susceptible to systemic inflation as the objective systemic value now has been democratized.

But wait—another problem arises with this situation. In bimetallism, the basis of value is a fixed exchange rate between gold and silver, but this only works when their market values are stable to one another. Making this assumption is rather dangerous in a fiercely developing world economy when new supply and demand situations can change on a dime.

Thus, I believe currency stability can best be achieved by the reliability of monometalism combined with the democratization of pluralistic metallism.

A Thousand Hearts of Gold

At present, the United Nations recognizes 180 currencies across the globe. In other words, the world has divided up its wealth into 180 institutions that each act as that currency's "heart of gold," or their Babylonian economic warehouse. From this perspective, the global economy has long supported decentralized currencies. The issue with this, aside from the lack of democratized control, is that each currency has precisely one "heart of gold," making it supremely susceptible to collapse if its guaranteeing institution makes a single mistake.

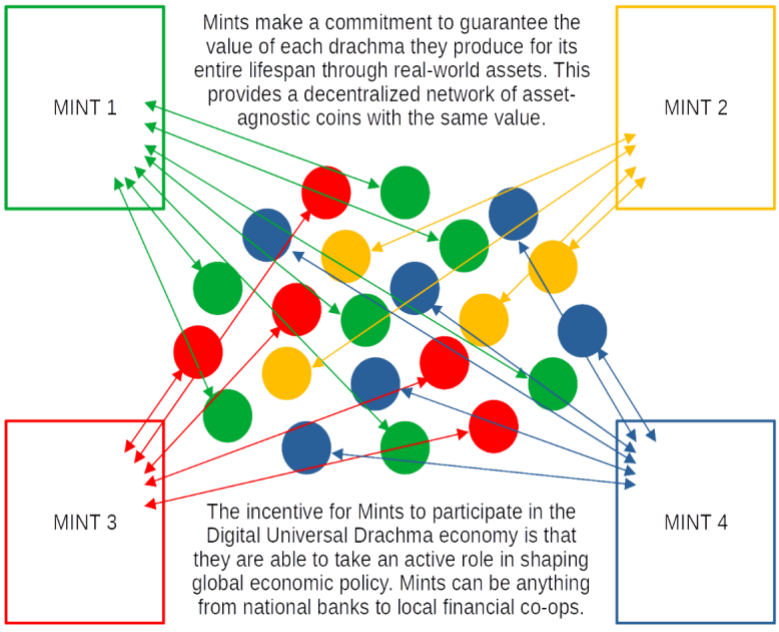
My vision, though, is to change this economic architecture. Instead of many currencies that each have precisely one institution in control of it, what if there was a single currency with many "hearts" that guarantee its value?

In the paradigm I am suggesting, each "heart" or "Babylonian warehouse" will be referred to as a mint. Every mint produces the same currency (the Digital Universal Drachma), but they mark each unit with their signature, assuring the wider economy that they have the assets to guarantee the value of that token. The assets guaranteeing that Drachma could be anything from gold to stocks to national currencies—suitably denoted as panmetallism—and whoever owns a Drachma signed by that mint has the right to exchange it for his or her own share of that mint's assets.

As there could be countless mints, the way to ensure an equivalent trade value between all Drachmas (avoiding the primary weakness of bimetallism) is to peg their value to that of a single and relatively stable asset, and it is the *value* of that standard asset that the mints commit to guaranteeing.

I suggest pegging the price of the smallest unit of the Drachma to the value of 1/17th gram of aluminum, which at the time this paper was written, is worth roughly $0.0002083. The reason for this is three-fold. Firstly, aluminum is the most abundant metal in Earth's crust and has many practical uses; essentially this ensures the underlying asset is useful while also being equitable enough that no geographic location is placed at a significant disadvantage. Secondly, aluminum is a canary for the global economy, closing matching the universal inflation rate. By being tied to the price of aluminum, the Drachma would maintain a dynamic relative stability that the rest of the economy stands to inherit by its adoption. Thirdly, it is important to make the smallest denomination of the Drachma small enough to make adoption by the poorest of communities feasible.

It also happens that if we follow the ancient Greeks' currency denominations, one drachma will be worth almost exactly one US cent, meaning that the mass adoption of the Digital Universal Drachma would cause minimal trade inconveniences and limit the disruption to global economic reserves. Thus, the smallest unit of the DUD, the chalkus, will be equal in value to one-seventeenth of a gram of aluminum. There will be 8 chalkoi in an obolus, and 6 oboloi in a drachma. As technologically inclined people may notice, using these Greek traditions offers a hexadecimal-friendly segmentation of denominations. To maximize people-friendliness, however, 100 drachmas will compose a mina (roughly equal to 1.00 USD), thus returning to a base-10 system for human comprehension. Please note that the only currency a mint will produce is the chalkus, and these other names are merely abstractions to make discourse surrounding the currency simpler.



Each of these mints would have members—individuals or organizations storing their wealth in the trust of the mint. In fact, every user of the Drachma economy would have to be a member of at least one mint, that way they have a say in their mint, and their mint acts as their advocate.

Bartering and Mutual Insurance

In order for any mint to produce a unit of currency, the mint must be able to commit to covering 100% of that unit's value at any time. This, of course, would have to be a legal requirement by governments adopting the goals of this project, otherwise people would attempt to create their own mints with limitless amounts of wealth created, causing severe inflation and systemic mistrust. This is why not only the producing mint has an obligation to this digital coin, but so too do the mandatory insuring mints. Before any coin can be released into circulation, that coin has to be guaranteed 100% by the responsible mint, plus a cumulative insurance guarantee provided by other mints for a certain percentage of its value (something of a distributed version of the FDIC, to say it differently). These other mints place their own resources at risk to secure the confidence of every coin produced, meaning that responsible monetary policy will need to be practiced by all mints if they wish to actually produce any currency; they must barter mutual insurance based off of their trust for each other's financial virtue. That is, trust is not simply given or taken; it is negotiated, bartered, and exchanged in a social market that forces transparency and compromise.

On a technical note, the percentage of wealth that a mint *m* must be minimally insured *I* is:

$$I_m = e^{H_m{}^2} - \frac{e}{\pi}$$

with the decimal Herfindahl-Hirschman Index H_m defined in terms of *s* market share of mint investor *i* for *N* total investors in the mint:

$$H_m = \sum_{i=1}^{N} s_i{}^2$$

Calculating the insurance requirements for mints this way progressively discourages extreme wealth inequality among a mint's members: the more monopolistic a mint's holdings is, the more it must rely on the wealth of other mints to assure the market of its coins' legitimate value. While many may decry this as putting capitalism in fetters, its actual effect is rewarding functioning competition—the heart of capitalism—and punishing a stagnant environment that suppresses innovation. Furthermore, extreme wealth inequality often precedes severe economic depressions; this offers a systemic incentive to avoid a major contributor to overall economic harm (as if the moral argument for a semblance of proper wealth distribution isn't enough).

In the event something catastrophic happens to a mint's store of wealth—whether that be a fire, a ransomware attack, a robbery, or something else of that sort—the digital coins from that mint already in circulation would then be "adopted" by the insuring mints, as would be required by law. The

mechanism is similar to how the chartering authority closes a bank if it is "critically undercapitalized" and designates the FDIC as the bank's receiver.

Interpolation-Based Blockchain

One of the fundamental flaws in Bitcoin—and blockchain in general—is its limitless storage demands. Bitcoin's ledger is already over 300GB in size, making it practically unfeasible for the ordinary person to run a node. Over time, this already absurd size would grow infinitely, requiring each node to have thousands of petabytes available for storing the ledger, technology which can only be maintained by the ultra-wealthy. Ironically, by requiring absolute decentralization, Bitcoin made itself victim to inevitable centralization in the future.

Methods have been proposed for addressing this issue, ranging from elementary proposals for data compression to the relatively advanced concept of Directed Acyclic Graphs. However, these concepts depend upon *transactions* being the data that is recorded, meaning that given infinite time, there will be an infinite number of transactions, making these ledgers stupidly long and entirely impractical.

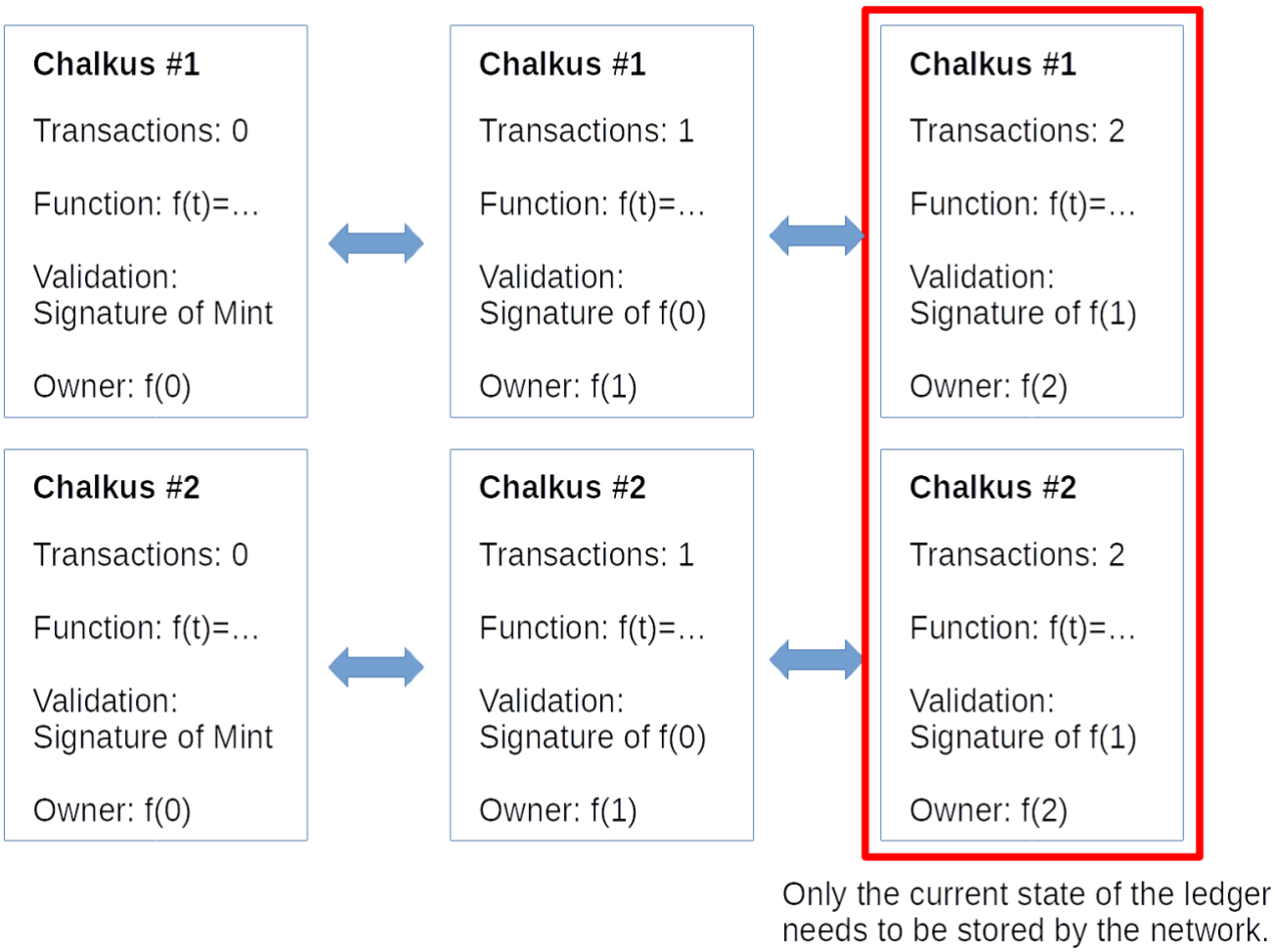
There is, however, a different way to conduct the record-keeping of a digital currency. Specifically, by transitioning from keeping records on infinite transactions to the finite units of currency, a limit can be placed upon the size of the ledger. However, Satoshi Nakamoto stated that "it would be unwieldy to make a separate transaction for every cent in a transfer."

As you may assume, I entirely disagree. While this may indeed require millions or billions of chalkoi to be reassigned to a new owner during a transaction, this is far better than requiring an infinite number of blocks on an immutable ledger. The only reason it would be unwieldy is because of the notorious difficulty of confirming transactions on the Bitcoin blockchain. This problem will be addressed shortly, but first we will ensure that the history of each chalkus does not become infinitely long.

One of the first things we learn in algebra is that functions are nothing more than a very short summary of an infinite number of events. Indeed, any basic line or curve is infinitely long. Using this approach, all one needs to record an infinitely long history of transactions in a finite (and manageable) manner is by creating a function for that data. Through interpolation, even under-powered computers can quickly calculate a function that takes the transaction number as an input and returns the numeric wallet identifier of that coin's owner. This interpolation formula allows for an infinite number of new points (transactions) to be added in sequential order while preserving the already established "history" of the equation. Of course, it may be more efficient for the function to be entirely rewritten for each transaction

to prevent unnecessarily complex equations, but it would first have to be validated that it preserves the history of the previous function.

In addition to the compression of history into interpolated functions, another way to minimize the storage requisites of such a framework is to allow mints to not only create but also *dissolve* digital coins. This would be done whenever a chalkus is returned to the mint in exchange for a person's share of the raw assets they are entitled to by virtue of possessing that digital coin. Allowing such dissolution would prevent histories from becoming needlessly ancient, complex, and cluttered.



Auditability, Not Anonymity

Interpolation, however, does not automatically solve the dreaded privacy problem of Bitcoin. Anyone would have perfect access to every person's complete financial history. That is terrifying, if for nothing else due to the existence of certain corporations' insatiable data hunger. Some projects like Monero, however, take the idea of privacy drastically too far. They remove all accountability from the

financial realm through complete anonymity. Between these two extremes is a better way, that which I call auditability.

From this perspective, unnecessary financial information is obfuscated enough that it would be impractical for any government or corporation obtain a complete history on a large number of people due to computational resources. However, since this information is merely obfuscated, the raw information *can* still be obtained if needed for investigations or other accountability-enforcing situations. Thus, auditability is preserved while a certain level of privacy is maintained.

Combining both of these concepts would look something like the following:

1. The current and previous owner of the coin have their actual wallet identifier stored in the interpolation function.
2. Information about all the other previous owners would be a numeric hash of the owner's wallet ID with some function performed on the transaction number and coin ID as the salt.
3. Whenever a transaction occurs, the next hash is calculated, and the new interpolated function created. Ideally, this would be possible for every transaction, but computing limitations of some devices may necessitate some exceptions to this rule. In theory, however, these computations should be lightweight enough to necessitate only a few seconds of computation on a modern smartphone to complete a transaction of hundreds—even thousands—of Drachmas.

Doing this would provide a method for auditing potential crimes without jeopardizing the privacy everyone else. Un-obfuscating the histories of each chalkus would be so computationally expensive that the average person could not even imagine embarking on this endeavor, large companies would find the cost too expensive for the return, and governments would only have the funding to do this when viable evidence exists for financial crimes. So, basic though it sounds, it offers both technical and implicit privacy protections.

I should note—especially in light of recent global events—that an interpolation-based cryptocurrency allows for a unique blend of economic freedom and control. As it is distributed, transactions are immune to censorship as is expected of cryptocurrency. This allows people living under authoritarian regimes to maintain personal agency that the government is unable to revoke. Unique to the DUD, however, is that it remains sanctionable. Because the currency's value is derived from underlying assets, international organizations would retain the power to apply economic pressure to an individual economy by freezing the trade value of those assets. I find this important to note because in a world where humanity's predisposition to conflict remains strong but our weapons ever more-destructive, maintaining tools that allow for a relatively peaceful resolution of disagreements is absolutely vital.

Conclusion

I began writing in frustration over current cryptocurrencies; I continued writing with an awareness that our economic situation is dangerously parallel to that of the Roaring Twenties; I reexamined with the US Federal Reserve's announcement they will seek public comment on CBDCs; and I am finishing with the hope that a project such as this will let our world embrace our common humanity and begin to bury our divisions with a sense of unity. Ultimately, the goal of this paper is the promotion of a universal currency that makes reservations for local governance, financial stability, technical feasibility, and socioeconomic inclusivity. Such a currency is a long-time coming, and we owe it to ourselves and our posterity to at least attempt instituting an economic system designed to work better for everyone.

My words are becoming labored at this point, so I wish to leave you with those of somebody else. They simultaneously inhabit a space of lamentation over our current economic system and that promised land that is imbued with hope that a sense of humanity will at last triumph:

> Willie Loman never made a lot of money. His name was never in the paper. He's not the finest character that ever lived. But he's a human being, and a terrible thing is happening to him. So attention must be paid. He's not to be allowed to fall in his grave like an old dog. Attention, attention must finally be paid to such a person.
>
> Arthur Miller, *Death of a Salesman*