A LeVeL Paying Field:

Cryptographic Solutions towards Social Accountability and Financial Inclusion

Gideon Samid
Electrical, Computer and System Engineering
Computer and Data Sciences
Case Western Reserve University, Cleveland, OH
Gideon.Samid@CASE.edu

Abstract: Thousands of digital money protocols compete for attention; the vast majority of them are a minor variation of the Satoshi Nakamoto 2008 proposal. It is time to extract the underlying principles of the Bitcoin revolution and re-assemble them in a way that preserves its benefits and gets rid of its faults. BitMint*LeVeL is a move in this direction. It upholds the fundamental migration of money from hidden bank accounts to cryptographically protected publicly exposed digital coins; it enables a cyber version of peer-to-peer cash transactions. Bitcoin and its variants rely on a fixed public/private key algorithm. Being 'fixed' turns it into a resting target for advanced cryptanalysis. The LeVeL protocol assigns each coin holder to pick their own public/private key algorithm. An attacker would have to compromise all the algorithms used by all previous coin owners -- a substantial security upgrade relative to Bitcoin. LeVeL applies to self-referential money like Bitcoin or fiat currency, and to other-referential money, serving as a claim check for assets, like gold or fiat currency. Bitcoin decentralization is groundbreaking but it gives too much aid and comfort to wrongdoers. BitMint*LeVeL re-imagines decentralization via the notion of the InterMint: Money is minted by many smoothly interchangeable mints competing for traders. Lastly, BitMint*LeVeL is built on top of the original BitMint protocol which was implemented in the legacy banking system, and thus it offers a smooth migration into cyberspace. 1.2 Billion people around us have no bank account, but do have cell phones. The LeVeL offers social accountability and financial inclusion.

1.0 Marketplace Decentrality

The prevailing monetary system in which money is minted by a central authority has triggered the bitcoin revolution that shifted the minting process to about 1 million miners, mostly organized in pools like, Foundry USA, Binance, and Slushpool. 10 pools dominate the mining process with 95% hashrate. Quite centralized. Unlike central banks, the bitcoin miners cannot steer the value of the coin. This power is relegated to the owners. About 0.01% of bitcoin traders hold 1/3 of bitcoin assets -- they are the central bank replacement: hidden, unaccountable, untraceable -- an enormous power without social accountability.

Millions of people are galvanized by the prospect of self-referential money operating without any designated mint, and hence immunized to corruption, of which central banks are often accused. Alas, such currency inherently becomes exceedingly skewed. Self-referential money is buoyed by irrational faith in its future. Occasionally this faith dissipates, the price drops. Those who own most of the currency, stand to lose the most, so they are well motivated to purchase the dropping coin, and reverse its course. As they do so, they become more loaded, own a greater share of the capitalization, and have a greater motivation to buy as many coins as needed the next time faith stumbles, and the price drops. Cycle by cycle the ideal of a fair, widely distributed currency is replaced with a currency dominated by unelected, unidentified, ever fewer prime owners.

The aim of decentralization should be achieved with clear social accountability. Such accountability presents itself in the free market. We propose a digital money protocol where anyone can declare himself or herself a mint, and define their own currency. It can be done in terms of any prevailing currency, and issued as digital claim checks for the same, or it may be minted as self-referential money, like Bitcoin, igniting public interest through scarcity and prospects. A fixed measure of some combination of such entities will be declared one unit of a derived coin minted by the self-declared mint. In the non-self-referential embodiment anybody could approach the self-declared mint, pass to it the listed amounts of transactable valuables, and receive from that mint a digital claim check, which entitles its holder to claim from the mint the exact amount of entities that it was issued for. This renders this claim check into digital money. Even more so once provisions are made for this digital coin to be split at will. For this scheme to work there must arise a community of traders trusting that mint, agreeing to trade with its digital claim checks as digital coins.

A normal working society is replete with highly trusted entities, be they local governments, large merchants, banks. Anyone with an established public trust will be able to declare themselves a mint, define their own coin, and issue digital claim checks thereto to the public. We designate this scheme as marketplace decentralization.

They will operate on top of what has been considered money before. So one mint will define its coin to be comprising: 100US$, 25€ and 0.1 ounce of gold, and another mint will define its coin as 1 bitcoin + $50,000US, etc. Over time some mints will become popular and attract a large community of traders, some coins will become popular too. A normal marketplace competition will be unleashed. Mints will experiment with many coin definitions to see what the public wants.

It will be important to insure smooth switch from one coin to the other. This can be done by establishing a coin exchange protocol. This protocol will compare coins at any given moment on the basis of a selected pricing entity, which today is still the US dollar. Mints will subscribe to the exchange protocol, acquiescing to their traders who return their claim checks and wish its value denominated in terms of another coin issued by another mint. Mints that would not abide by this exchange requirements will not be able to attract traders.

To remain in business, mints will have to be efficient, supportive, available 24/7, easy to use, etc. Some mints will be local, serving a limited community, some will be national, and others will be international.

The Federal Reserve will still mint the US dollar. The public will trade it exclusively in coins expressed solely in US dollar, if the dollar exudes trust. If the Federal Reserve will manage the dollar better than the ECB will manage the Euro then it will dominate the digital coins offerings. This solution calls for the US dollar to compete against all other widely traded assets. It will require the Federal Reserve to use its monetary tools wisely, in conjunction with the US treasury using its fiscal tools well, in order to be popular in the decentralized digital coin market.

For this marketplace decentralized scheme to work, it will have to deliver on the other singular issue with which bitcoin beat legacy money: privacy.

We will see ahead how the BitMint*LeVeL protocol offers better privacy than bitcoin.

Being digital, cyber security has to be addressed too. We will see ahead how BitMint*LeVeL offers better security than bitcoin. The LeVeL is immunized against quantum cryptanalysis and against yet to be discovered mathematical knowledge.

2.0 Mutation Powered Public Key Cryptography

Bitcoin is based on Elliptic Curve Digital Signature Algorithm (ECDSA) which identifies two mathematically linked keys, K, K*, that reverse each other's action. Despite this mutual reversal property, these two keys are asserted to pose a prohibitive computational task for the purpose of deducing one from the other. This assertion is based on the expectation that the applicable computers are Turing machines, operating sequentially. It is also based on the tacit assumption that any hidden math that can reduce this computational workload is not known to the attacker. Both assumptions claim at best an ephemeral validity, spelling a termination date for bitcoin, very likely before the full number of expected coins will be mined.

BitMint*LeVeL is addressing these vulnerabilities by using a trading algorithm that uses two keys K, and K* which are not expected to reverse each other's action, they are only expected to by computational asymmetrical: easy one-way $K \rightarrow K^*$ and hard the reverse way $K^* \rightarrow K$. This relaxation of requirements changes the number of applicable algorithms from a handful (as the case is for mutually reversible algorithms) to unlimited. The Bitcoin protocol allows any trader to choose the values of their key pair (K, K*), but imposes the use of ECDSA. BitMint*LeVeL, by contrast, increases the degree of freedom enjoyed by the trader to choosing both the values of the pair (K, K*) and the selection of the one-way functions, F, F* where $K^* = F(K)$, and $K = F^*(K^*)$.

Consider a digital coin changing hands from trader 1 to trader 2... to trader n. If the coin is Bitcoin, then its attacker only needs to deduce K^*_n from the public value of K_n. By chance the values of K, and K* may be inherently weak keys, namely keys that fall in a particular category that makes it feasible to deduce the private key from the public key within polynomial time. Albeit, if that coin is LeVeL then the attacker will have to deduce all the n private keys, K_1, K_2,.... K_n, where each of those n keys is protected by a surprise pair of one way functions (F_1, F^*_1), (F_2, F^*_2),.... (F_n, F^*_n). The current trader can readily increase the cryptanalytic difficulty facing the hacker by selling the coin to themselves, as trader (n+1), using a surprise, extra hard function F_{n+1}: $K^*_{n+1} = F^*_{n+1}(K_{n+1})$. In other words, the security of an ongoing traded coin is increased through a series of digital mutations that keep the attacker behind. This is a digital version of the Darwinite survival strategy where biological mutations assured the triumph of life.

It is clear from the above that BitMint*LeVeL poses a harder challenge to its hacker, in two aspects: (i) the number of keys that need to be cryptanalyzed, (n), and (ii) the number of surprise one-way functions that needs to be negotiated.

This fundamentally higher security also provides the same high quality of privacy protection.

3.0 The Trading Protocol (Essentials)

The LeVeL trading protocol borrows important innovative advancements used in Bitcoin, here used differently. The two main innovative steps taken from Bitcoin are: (i) public exposure of global trade status, and (ii) layered signatures.

3.1 The Basic Transaction Sequence (BTS)

Let's consider n traders Tr_1, Tr_2, ... Tr_n, and also consider a digital coin X which is held by the first trader from time point t_0 to time point t_1, at which time it is transferred to the second trader, Tr_2. Similarly, trader Tr_i, for i=1,2,...(n-1), passes coin X to trader Tr_{i+1} at time point t_i. We call this the basic trading sequence (BTS).

In Bitcoin the BTS is published onto a public ledger identifying the n traders through their public account. No further information is disclosed about the identity of the account holders. Same for BitMint*LeVeL.

Therefore, in both protocols the trading public and the public at large know a unique identifier of the owner of coin X at any given time. In particular it is public knowledge that for any time point $t \geq t_{n-1}$, the current owner of X is Trader n, identified through their unique id, and no more.

In Bitcoin the passing of X from trader Tr_i to trader Tr_{i+1} happens when Tr_i states that they pass X to Tr_{i+1}. Tr_i signs this statement with their secret private key, so that this statement -- and the validity of the transaction -- is readily checked by the public using the published public key identifying trader i. This step is the one requiring mutual reversibility between the public and the private key, which in turn requires the use of ECDSA. This ECDSA limitation is the long-term cryptanalytic weakness of Bitcoin.

It is in this act of transaction from Tr_i to Tr_{i+1} where BitMint*LeVeL branches out to its own path.

As argued, the BitMint*LeVeL protocol steers away from dependence on reverse action public/private keys, and builds its algorithm on plain, robust, one-way functions. The key, K*, that is easy to compute from the other (K) is the public key, and the key, K, that is hard to compute from the other (K*) is the private key.

A LeVeL trader is identified as one who knows the private keys of all the traders listed on the public ledger.

So, at time point $t_{i-1} \leq t \leq t_i$, the ledger shows the history of coin X as has been owned by traders Tr_1, Tr_2, ... Tr_{i-1} in the past, and currently owned by trader Tr_i.

When trader Tr_i wishes to pass coin X to trader Tr_{i+1} they need to prove to trader Tr_{i+1} that they know their own private key, and also know the private keys of the (i-1) previous traders. Once trader Tr_{i+1} receives this information from trader i, they can verify their validity because the public keys of traders Tr_1, Tr_2, ... Tr_i are listed on the public ledger. Upon such verification trader Tr_{i+1} is satisfied that the trader presenting himself as the current owner of X, and hence as the one with rights to pass it further, is indeed who they claim they are.

We have shown here how BitMint*LeVeL validates a transaction, without having to use reverse action public/private key cryptography, relying instead on simple one-way function.

Since both in Bitcoin and in LeVeL the ecosystem is based on a widely distributed public ledger, it is not enough for the payee to be satisfied with the validity of the payment, it is equally important to update the ledger so that the community will see that coin X is now owned by trader (i+1).

Bitcoin devised a brilliant way to ensure efficient public distribution of coin ownership updates. LeVeL can borrow the same, if so desired, but BitMint*LeVeL has more options at its disposal, as will be discussed later. Before the news that coin X has been passed from Tr_i to Tr_{i+1} are posted on the public ledger, Trader (i+1) will have to come up with a pair of public/private keys (K*, K), and post the public key as an identifier of the new owner of coin X, trader (i+1).

Once trader (i+1) posts their public key, K^*_{i+1}, then trader i can no longer practice double spending, because while trader i knows all the private keys of all the traders Tr_1, Tr_2, ... Tr_i, they don't know the private key of trader (i+1), and hence they cannot convince a payee that they are the current owner of X. The only one who can convince a payee that they are the valid owner of coin X is trader Tr_{i+1}.

We have thus described here the BitMint*LeVeL mechanism by which coin X is passed around from trader 1 to trader 2, ... and on to trader n.

This is the operational principle of the basic transaction sequence (BTS). The implementation of which adds some features as discussed ahead.

3.2 Initiation and Termination

The basic transaction sequence describes how a coin X moves from trader 1 to trader n. What we need also to describe is how this sequence is initiated and how it is being terminated.

Trader 1 receives coin X from an entity called "The Mint". The mint must be trustworthy, trusted by the n traders Tr_1, Tr_2, ... Tr_n. This trust by the traders of the mint is foundational to the BitMint*LeVeL operation. Traders will trade with coin X only if the mint that initiated the trading sequence by giving the coin to Tr_1, commands their trust.

The mint-trust is built in two modes*: (i) other-referential, and (ii) self-referential*. In the first mode the mint refers to a well-defined transactable valuable in a well specified quantity, which it expects to receive from Tr_1, and against which the mint issues coin X, which is regarded as a digital claim check for the amount of transactable valuable passed to the mint from Tr_1, in order for coin X to be issued. The notion of claim check implies that anyone rightfully holding this claim check will be in a position to pass it back to the mint and expect the same amount of transactable valuables previously passed to the mint for minting X.

In the second mode, coin X is not a claim check for any entity defined outside the LeVeL protocol but rather *a digital entity defined by its creation*, and offered to the trading public as attraction worth paying for, despite the fact that the created digital entity is devoid of any per se utility. A necessary condition for such attraction to develop is scarcity. Without scarcity there is no transactable value.

A mint can generate this desired attraction in several ways: (i) exploiting social capital, (ii) fiat – exploiting authority status. In the first category the mint draws on respect and regard from the society it operates in. In the second category it draws on the machination of government and state, or any platform of power. Example: central banks.

Other-Referential trade sequence is terminated when the claim check is returned to the mint. Self-referential trade sequence is terminated (i) when the driving social capital, and (ii) the underlying legal standing of the mint dissipate, or (iii) the mint freezes or removes the coin from the public ledger.

Although self-referential money is not mint-redeemable, it is still mint-controllable, because the respective coin database is the source that validates a coin, and keeps away counterfeits. This implies that the mint can take a self-referential coin out of circulation by simply stating so on the public ledger. The Bitcoin solution, by contrast, denies any managerial entity the power to exclude coins, or unilaterally intervene with the public ledger. Alas, in reality someone keeps tweaking the protocol. The Bitcoin trade has a built in ‘self gravity’ that keeps an ever-smaller cut of the traders own an every larger proportion thereto. And hence an ever-smaller number of super rich Bitcoin traders will navigate it to their liking – all legal within the protocol, simply by their capitalization dominance. They can thereby trap the other traders. This is the effect of unbridled decentralization that boomerangs on its innocent proponents. And there is no recourse. LeVeL offers measured, optimal decentralization to insure that society at large remains the prime beneficiary of the currency. The BitMint*LeVeL solution offers an address to complain, even to sue -- accountability.

3.2.1 Other-Referential Trust

In the Other-Referential LeVeL mode, the mint issues its digital coin X against a 'claimed valuable', CV, defined in terms of some reference currency (RC). The CV is what the mint submits to the redeeming trader, Tr_r, who returns the digital coin X to the mint.

The claimed valuable of a coin is any entity which may be quantified so that fair people agree on its quantity. Because the CV is redeemable, it must be durable. It also must be scarce.

The reference currency (RC) for the CV may be comprised of material ingredients like rare metals, complex apparatus, and such. It can be comprised of digital goods, like music, or mathematical operations. The RC may also be comprised of the prevailing fiat currency, or of a well-defined combination of world currencies. It may also be comprised of limited use currencies, loyalty money, and such. The RC may be comprised of investment instruments. The RC may also be comprised of cyber entities. Curiously enough the RC may be comprised of digital currency, whether constructed with the LeVeL protocol, or not. RC may be comprised of bitcoins. And of course, any RC may be comprised of any combination of the above.

So defined, the other-referential LeVeL may be constructed *iteratively* as a series of mints, where one mint uses the coin of another mint as an RC, and in turn its own coin is used by the subsequent LeVeL implementation as its RC.

The mint is expected to store the claimed valuable, CV, of the reference currency, RC, from minting to redemption.

3.2.2 Self-Referential Trust

Bitcoin has demonstrated a remarkable trait of human society. An imaginary entity, that has no existence outside the imagination that constructed it, is nonetheless commanding a one trillion dollar capitalization (at least temporarily). This is like having millions of people voting Santa Claus to be President. Bitcoin enriches many adopters who pull out in time. While crowd psychologists theorize this surprising phenomenon, digital coin designers are ready to take this as given, and use this crowd effect for the benefit of society at large. The LeVeL is an attempt in this direction: aiming for the crowd psychology generated massive wealth (in real dollars) to be carried out with social accountability for the greater good. The idea presented here is that *a self-declared mint issues self-referential digital coins that end up benefitting traders, benefitting the mint, and benefitting a served cause.*

In Self-Referential mode the mint is offering digital coins that are not claim checks for anything redeemable, and are expected to be desirables on their own. Such desirability might be generated by the nature of the mint, or by its purpose. In the first case the attraction of the coin is in its holding being a show of respect for the mint -- social capital. This respect may be free or imposed, like with government legitimacy.

In self-referential mode, SR*LeVeL digital coins are offered to a community of potential traders. The offered coin can be given against a non-redeemable price defined through some currency of choice, Pr. Pr may be zero or otherwise (including a negative price for the purpose of priming). Traders realize that the price, Pr, they pay for such a coin is not redeemable by the mint, so their incentive to pay Pr for the coin is hooked into the expectation that this self-referential coin, for some reason, will be an attraction for others, and they will be willing to pay a larger amount Pr' > Pr for the same digital coin. And those who pay Pr' for the coin will do so on the expectation that down the road a buyer, willing to pay Pr" > P'r for the coin, will be coming forth. And so on. Since such chain of expectations cannot be infinite, we do call this mode the *Ponzi mode* -- remembering the scheme concocted by Mr. Charles Ponzi where a few in the beginning of the trade sequence make a lot of money and the others go bust.

Another possibility is that a self-referential mint will tax the outstanding coins and build a price stability fund. It will use this fund to dump coins to the market, should the market price increase above a prescribed threshold. Taxing is straight forward since in the BitMint*LeVeL protocol, all outstanding coins (which in the self-referential mode implies all the minted coins) are listed and visible. So despite the anonymity of the holders, the protocol may be adjusted to tax each coin at the same rate. The tax rate may be adjusted to ensure enough coins to be sold off in the market to fend off any price hike due to increased demand. This so imposed price ceiling will slow down the Ponzi effect, and endow the coin with greater longevity.

We discuss the social capital self-referential mint, fiat self-referential mint, and self-referential privilege money

3.2.2.1 Social Capital Self-Referential Money

Bitcoin has sprung like the "Big Bang" from nothing to an impressive inertial movement, proving that despite ample logic arguing against this prospect, baseless money may develop sustainable social attraction. This opens the door for organizations and people of high social standing to attempt to emulate this experience, and issue unredeemable self-referential digital coins in a limited open offering to the public. Even if the coins are offered free, if they are scarce enough, and promoted with some mystique, then like stamps collections, they might appeal to collectors who would be willing to shell real money for them. Such eventuality will determine a price for this self-referential coin. Since the transactions are documented in a public ledger, the transactional price may be published too. This way, or otherwise, the marketplace will know at any moment what is the price of a certain self-referential currency in terms of the local fiat currency. And this price may rise. Let's say the price in the market for a certain SR-coin is Pr. This will allow the mint to issue some additional coins to the market, only that this time around, instead of free, the coins will be passed around against their open market price. As the price goes up, the mint - the owner of the social capital - will benefit from minting more coins and issuing them to the public, and the holders of those coins will benefit from the rising price too.

Speculators will come in, further raise the price, and thereby benefit the social capital source and the current holders. If this scheme does not catch, no harm done, no investment lost. It was a gamble that a money from nothing will catch people's fancy.

We list various social capital holders (i) charities, (ii) beloved personalities, (iii) social cause promoters.

3.2.2.1.1 Charitable Self-Referential Money (The Upward Coin)

We describe here a means for a charitable organization to raise money through self-referential currency. The method to go by the name *Upward* works as follows:

A charitable organization enjoying a stream of charitable contributions from the public, is to be minting a coin called *Upward*, U. U is denominated at a starting value V_0, at a given time point T_0. When a member of the public makes a contribution in the amount C to this charitable organization, "Public Charity", (PC), then the public charity submits to the contributor c digital coins, where $c = C/V_0$, rounded to a natural number for c. These digital coins are not redeemable by the public charity, however the contributor is encouraged to pass them along as if they are redeemable for their nominal value of V_0.

Because Upward coins are not redeemable, the incentive that is in force for other-referential (redeemable) digital money, is not present here. Yet the first recipient of these c coins is one who intended anyway to make the contribution at the amount C, without getting anything in return. So even if these digital coins are worthless, this contributor is not worse off. At the least these coins serve as a receipt for the contribution. Albeit, once getting these coins, the contributor will try to pass them on as money, forwarding the following argument*: "I have made a contribution in the amount C to this honorable public charity, I give you, the payee, an opportunity to share this honor with me. By accepting a small amount of money, V_0, the value of this charitable coin, Upward, it is you who makes the contribution in that amount V_0 to this charity we all honor and respect. And any display of this Upward coin will prove your status as a giver for a good cause."*

We may assume that a small number of payees will agree to accept the Upward coins in lieu of regular money, denominated at the current value of the Upward coin, V_0. The payee that accepts the Upward coin will be able to offer it as payment for their bills, and so on, one trader to another.

So far we described a situation where a popular charity provides its contributors with self-referential digital money that is expected to spread in the public. There are members of the public that are well inclined to contribute to this charity but don't get around to actually do it. By accepting an Upward coin, they carry out their intent with minimum effort. It is true that their acceptance of the Upward coin amounts to payment of its value to the payor who gave them this coin, but since the payor, or its predecessor paid the money to the charity, accepting this coin by the current payee amounts to paying its value V_0 to the charity.

At time point $t_1 > t_0$, the public charity inches the value of its self-referential money from V_0 to $V_1 > V_0$. With this, a contribution at the amount C' will result in the contributor getting $c' = C/V_1$ Upward coins. These higher value Upward coins are indistinguishable from the coins that were minted with a denominated value of V_0. Hence these coins that were minted for value V_0, will now be worth on the market as much as the newly minted coins, namely V_1.

The holder of an 'old coin' (originally denominated for V_0) will be able to pass this coin for its new value V_1. This holder will make a profit of $V_1 - V_0$ over each coin so paid.

So far we have a sequence of events that benefits the public charity with the flow of contributions that would have otherwise been made without the pay back with a self-referential digital coin. Albeit, the earlier contributors that got their Upward coin at value V_0, will now log a profit in the amount of $V_1 - V_0$, for every coin they use in payment.

At time point $t_2 > t_1$, the public charity will again up the value of its self-referential coin, from V_1 to V_2. And as this happens, the holders of previously minted coins will have their holdings experience a rise in value: $V_1 \rightarrow V_2$. This will happen again, to $V_3 > V_2$ at time point t_3, and on it goes.

Every time the price goes upward in value, $V_i \rightarrow V_{i+1}$ the current holders of these Upward coins are logging a profit. This value increase will act like a powerful incentive for more people to buy it early, namely to make an early on contribution to the public charity, because a while later their upward coins will hike in value.

The net result is that the public charity attracts more and more contributors, many more than have originally considered making a contribution. These newly decided contributors are motivated by their own profit, eager to buy these Upward coins cheap then sell them expensive. So while the public charity enjoys a flood of new money, the contributors to the charity are profiting form their own contribution.

This dynamics also makes it more attractive for payees to accept the Upward coin for payment of a debt of V_i at time t_i, because at time $t_j > t_i$, they will be able to pass the same coin for a higher value $V_j > V_i$, and pocket the difference $V_j - V_i$.

The public charity will have to optimize the rate and timing of the price increase to maximize the public incentive to make contributions to this public cause.

3.2.2.1.2 Self-Referential Service Money

An arbitrary mint entity may offer to honor a noble service with self-referential money, and then open markets where merchandise is offered only against this service honoring money. The merchandise may be unique, one of a kind, or common. The presence of such markets in cyber space will attract others who are not honored with this self-referential coin, and these others would offer fiat currency in exchange of the noble action honoring money, so that the public at large will have access to these noble-action honoring stores. A price will develop and be governed by the attraction of these special markets, and the scarcity of the new coins. The coins will not be redeemed, but the mint could mint an arbitrary number of these coins and use it itself.

The mint and the 'store' where merchandise is sold against service money only may coordinate their moves in order to benefit the cause they serve, the people who serve it, and the organizers of this enterprise. We first analyze the situation where the store offers common goods available elsewhere. The enterprise (mint + store) can start with a nominal state where the store offers merchandise against service dollars at par with regular dollars. Recipient of service dollars will be indifferent as to purchasing in the service store, or elsewhere. Gradually the store will lower prices; an item priced at value V_0, will be sold at $V_1 < V_0$, where $V_1 = \mu V_0$ $(0 < \mu < 1)$. This will send the recipients of service dollars to the service store, but will also motivate others to offer service coin recipients to sell service coin for a price $V^s \rightarrow V_0/\mu$. The enterprise will then set a cyber marketplace for the exchange of service dollars. This marketplace will increase the value of the service coins. The amount of service coin rewards per level of service is fixed, so the net result is that service providers increase their pay as the price of the service coin rises. At time point t_2, the enterprise will further decrease the pricing level in its store, to $V_2 = V_0 * \mu^2$. This should up the price of the service coin in the exchange to $V^s \rightarrow V_0/(\mu^2)$. As the price of the service coin rises the incentive for people to provide the paid for service will rise too, benefitting the noble goal it serves. At the same time, service coin holders will be hoarding the currency, expecting it to rise in value. The mint will then be in a position to inject additional coins into the exchange, to dampen the rising price and to be paid back with the price of the sold service coins.

The enterprise will further control the service coins marketplace by minting the service coins with a built-in expiration date. The inherent anonymity of the BitMint*LeVeL coin will incentivize speculators and others to take part, either in purchasing from the service cyber store, or in the coin exchange per se.

The attraction of the service cause will allow the enterprise to stuff the store with one-of-a-kind, say, original work of art that will only be sold against service coins. While the price of common goods may drop, V_2, V_3, ... $V_t = V_0/(\mu^t)$, the price of the unique merchandise will stay put, or even rise.

Service coin holders might be encouraged to sell their coin, if they are used for goods or services that cannot be accumulated, like a subscription to a streaming service.

3.2.2.2 Fiat Self-Referential Money

Fiat Self Referential Money may be at a national level, or at lower levels. A country has the power to issue its currency on a digital basis. Legacy money is printed at will, and its distribution is monitored and reacted to. The same can happen for digital self-referential money, the digital mint will replace the printing press.

Gradually the printed legacy money can be replaced with LeVeL self-referential money.

The very large quantities of money printed by central banks may call for a 'minting cascade'.

President Nixon disengaged the US dollar from Gold, and thereby opened the door to 21st century self-referential money. On a lower scale, a holder of highly desirable assets (HDA) can decree that these assets will only be sold for self-referential coins minted for this purpose: Purpose Specific Self-Referential Coins (PSSR) coins. These PSSR coins will be minted by a mint that will ensure scarcity, and thereby build up a sustainable price that would serve traders and the mint. This option can be carried out as a charitable coin option.

3.2.2.2.1 Minting Cascade

A prime money source may issue coins, of type $Coin_0$ with a limited resolution. Namely coins that are an integer count of a minimum quantity, Q_0. These $Coins_0$ coins cannot split to denomination smaller than Q_0. A recipient of such money can mint another-referential money on the basis of a $Coin_0$ money with a resolution of Q_1 such that an integer count of Q_1 fits into Q_0. These derived coins, $Coins_1$ can be distributed to recipients.

This cascading can be repeated with $Coins_2$ of minimum resolution of Q_2 such that an integer count of Q_2 fits into Q_1, and on to $Coins_3$, $Coins_4$....

Such cascading will create a more manageable situation where the redemption accounting is handled through a cascade of databases rather than one large coin database.

3.2.2.2.2 Purpose Specific Self-Referential Coins

Let an Asset Holder, (AH) be in a position to offer attractive goods or services to the public, or to a subset of the public. Normally the AH will price their asset and put them on the market. As an alternative, the AH will decree that their assets are only to be priced and sold for a purpose specific self-referential coin, coin_{pssr}. The coin_{pssr} will be minted by a PSSR mint (mint_{pssr}). Although these coins may be freely issued (or per a nominal fee), they will be limited in count. There will be an eligibility formula to determine who is offered these coins. Those who received such coins will be able to buy, say online, the merchandise offered by the AH. Alas, if these assets are well advertised, then people not given the coin_{pssr} will be looking to buy these coins in order to buy with them the AH goods and services. Such purchase will happen via an online marketplace. Because the original coin holders received them, say, for free, they will make money selling them at any price. But since these coins are scarce, a bidding war will ensue and the price will rise.

As the price rises, the mint will mint coins_{pssr} for its own use, sell them in the PSSR coin marketplace, and make a profit. This action will have to be limited because if the marketplace is flooded with coins_{pssr} then the price falls, and the take home for the mint drops.

For the PSSR dynamics to work, all that is needed is to ensure scarcity of the coins_{pssr}. The choice of coin recipients may be random or arbitrary. Namely the mint_{pssr} may randomly pick recipients and offer them some coins_{pssr}. Alternatively, these coins can be distributed as a token of appreciation to people that contribute to social causes, or to people at the bottom of the socio-economic ladder.

If such dynamics operates with some stability, then the mint_{pssr} may make a charitable contribution to a deserving subject by endowing them with some coins_{pssr}, which they will sell on the PSSR coins marketplace.

While the AH and the mint_{pssr} may be different entities, the system works more naturally if they are the same, or closely linked entities.

3.2.2.3 Self-Referential Privilege Money

We have evidence that any item of scarcity may spontaneously acquire monetary value despite absence of any utility, or any redeeming attribute. It is a matter of crowd psychology. Profit minded entities may exploit this phenomenon with self-referential privilege money (SRPM). It works as follows:

Any entity declares itself as a mint, and it offers BitMint*LeVeL digital coins according to some restricting criteria of eligibility. The mint may give these digital coins for free or sell them for a nominal price V_0. The coins are useless, but are scarce. Spontaneously a market erupts.

Some are willing to pay (the prevailing currency) to lay their hand on such a coin. The coins are not redeemable but move in the market. As they gain value, the mint may now offer them for their market price.

The SRPM mint must be careful not to flood the market with these digital coins lest it will dampen their value, and harm the traders, mostly the mint itself.

While not redeeming their coins, the mint will maintain a coin database and stand ready to authenticate each claimed coin as bona fide.

SRPM mints will compete with each other on how attractive their coins, and how well managed. Such coin may operate like a Ponzi scheme, where the price goes way high, the mint profits, and then the price collapses, maybe all the way to zero.

3.3 Meta Data

The BitMint*LeVeL coin meta data includes:

1. Mint identification. 2. Coin unique id 3. Optionally error correction codes, and other coin string parameters, like length, and various cryptographic parameters 4. Various accounting parameters for internal use of the mint, and any cascaded mint of it. 5. Terms of redemption, expiration dates, minting date, etc.

3.4 Terms of Redemption

These are specified terms, written mostly in code, where the codes are explained in the mint database. Any logical limitation may qualify as a term of redemption. Most common types:

1. Expiration 2. Redeemer 3. Chain of Custody

3.4.1 Coin Expiration

Theoretically a coin can remain circulating in the market forever, or as long as the mint is in business. Albeit, it is a good practice to impose an expiration date, especially in conjunction with redeemer terms in which the redeemer of the coin is asked to identify themselves. This practice will prevent the problem existing in legacy cash where large amounts of money are kept illegally, undisclosed, and the owners exert a great amount of influence without any societal reckoning.

3.4.2 Redeemer

The BitMint*LeVeL protocol is flexible. The mint can redeem coins to unidentified redeemers, or it may insist on flashing out the identity of the trader who receives the reference currency for the redeemed digital coin. It might make such identification dependent on the amount of the coin, or it may impose such restrictions on a temporary basis, perhaps during some criminal investigation.

3.4.3 Chain of Custody

On top of the cryptographic identity, W, of the traders, or instead of it, the mint may impose that all traders of its coins will be identified in a way that the mint knows who they are even if their payors or payees don't. The mint will not redeem any coin wherein all the past owners are well identified. This is the extreme opposite to the nominal operation where the mint is totally blind as to the identities of its coin traders.

3.5 The InterMint

A prime motivation for the establishment of Bitcoin was the desire to unseat the central banks from their power to manipulate the currency, and with it the wealth of its traders. The Bitcoin solution looks good "on paper" because the currency ostensibly runs on a protocol and denies any human authority power over it. The truth is that the protocol tweakers assume enormous power without accountability. What is more, self-referential money like Bitcoin, is kept afloat by aggressive purchase of the coin when a slump occurs. The buyers are those who have the most to lose from price drop, namely the large holders, which then become holders of a larger cut of the currency. So inherent to the Bitcoin solution is the fact that a smaller and smaller minority of traders holds a larger and larger portion of the capitalization of the coin. This minority, according to the protocol, has the power to move the trade to their interest, making the majority of traders dependent on them. Not the vision that attracts the millions to the currency.

We conclude therefore that absence of an accountable managing authority leads necessarily to being dominated by an unaccountable managing authority. New thinking is called for.

The issue with fiat currency today is not that it is run by someone, but that traders have no choice. The solution therefore is to secure an accountable manager for the currency, but to ensure competition and choice. That is what the BitMint*LeVeL protocol provides. In a LeVeL society everyone can declare themselves mint, and every such mint can mint self-referential money or other-referential money, as they see fit. The other-referential money can use as reference a self-referential currency, or fiat currency, or a foreign currency, or a precious metal, or anything else qualifying as money -- and also build a compendium -- a basket of other currencies over which to mint its own digital coins. This will not put the central banks out of business, like Bitcoin tries to do. Rather it will rely on the prevailing central bank to manage their fiat currency so well that the various mints will use it for their minted coins, either exclusively or in a mix where this particular fiat currency dominates.

The trading public will have a large selection of coins to choose from and a large selection of mints to do business with. Thereby competition and choice is brought into the currency business, replacing the one size fits all prevailing today lingering from the pre-digital era.

While the protocol allows everyone to declare themselves a mint, only a few entities that command sufficient public trust will flourish and sustain a society of traders. And those successful mints will be in constant competition. If one mint fails in quality of service or reliability, then traders will shift to the next mint. The BitMint*LeVeL protocol defines a global exchange solution where coins from one mint are readily translated to coins from any other mint in the network, all priced via a dominant pricing currency, (currently the US dollar).

3.6 Implementation Issues

We discuss the following implementation issues:

1. Operational Fees 2. Privacy Balance 3. Breaking the Mint Apart 4. Holding marks

3.6.1 Cyber Security

Money by its very nature requires security. Material money security is achieved via guards, locks and vaults. Cyber money is secured with cryptography. Much as Bitcoin and its elk face an existential threat from quantum cryptanalysis, so do the security locks and vaults of cyber space. LeVeL money is managed, held, and secured by the trader, the money holder – not the bank. If that money is not secure, then LeVeL does not work. LeVeL implementation therefore must be hinged on trustworthy cryptography. The cryptography that fits the high demands of LeVeL is “pattern void cryptography”, where the traditional mathematical complexity is replaced with lavish use of quantum randomness.

3.6.2 Operational Fees

The BitMint*LeVeL mints will generate revenue for operation and profit by charging service fees from the traders using their coins. The fee can be distributed between the coin purchaser, or the coin redeemer for the other-referential money. For self-referential money revenue is generated either from purchasing fee, and/or from minting and selling self-referential coins that build up a dollar value. The InterMint environment will keep pressure on the various mints, especially those who use the same or similar reference currency. This pressure will keep the fees down.

3.6.3 Privacy Balance

The cryptographic foundation of BitMint*LeVeL is asymptotically unbreakable, robust against high powered cryptanalytic shops. This high-level privacy will protect law abiding citizens, but admittedly, will give aid and comfort to the criminal element. However, unlike Crypto 1.0, the LeVeL solution keeps the mint in charge of the delivery of the coin to trader 1 (the purchaser), and more importantly, in charge of the redemption process -- for the other-referential money. For both self-referential and other-referential money the mint runs the coin base and the ledger, and it can freeze any coin in its system. Freezing a coin will not expose its holder, but it will deny the holder the ability to use it, or to redeem it. The so afflicted coin holder will have the option to abandon their claim for the coin to safeguard their privacy.

Should a suspicion be raised as to possible criminality of a transaction, then law enforcement will be able to secure a court order to freeze that coin for further investigation. The respective mint, operating under the prevailing law, will abide by that court order, and mark that coin as 'frozen' -- untransactable, at least in a temporary fashion. Law abiding coin holders will pass through the following examination and will see their coin return to circulation.

Authorities and regulations may impose identification requirements on certain coins; say, coins of high denomination will only be issued to traders that identify themselves to the mint, and will be redeemed only to fully documented redeemers. Mints may also impose a requirement that all in between traders will have to add to their hidden owner identity (W), a mint certificate indicating that they registered as bona fide traders.

One would argue that mints might abuse their right to ‘freeze’ coins. Indeed. However, since in the InterMint environment traders have a choice of mints, any mint that abuses its right to interfere with smooth private trade will be abandoned by its customers. It is the “marketplace police” in action.

3.6.4 Breaking the Mint Apart

Consider LeVeL mint M, with s outstanding coins, X_1, X_2,..... X_s and q traders. M runs the respective coin database B where the images of the s coins is kept. In case of an other-referential currency, M also holds the register of the reference currency, RC: R .

The BitMint*LeVeL protocol enables M to be broken apart to two mints M' and M'', where M' will be assigned a subgroup of s' coins (subgroup s') from s, and where M'' will be assigned the leftover subgroup of coins s'' (comprised of s'' = s-s' coins), and where B will be respectively broken apart to B' and B'', where B' keeps the images of the group s' of coins and B'' keeps the images of group s''. In case M is an other-referential mint, then the Register R will be separated to two repositories of the reference currency, RC, R' and R'', where R' keeps the currency corresponding to group s' and R'' keeps the currency corresponding to group s'':

$$\{\mathbf{M}, \mathbf{B}, \mathbf{R}\} \rightarrow \{\mathbf{M'}, \mathbf{B'}, \mathbf{R'}\} + \{\mathbf{M''}, \mathbf{B''}, \mathbf{R''}\}$$

where $M = M' + M''$; $B = B' + B''$, $R = R' + R''$.

This break up can continue iteratively: $M' \rightarrow M'^{*} + M'^{**}$, and $M'' \rightarrow M''^{*} + M''^{**}$, and then again and again.

In a normal operation traders should not see a difference. Every trader can pay any coin they hold in any sub-mint. Coins, of course, stay in the mint they were associated with to begin with. However, if for any reason communication is disturbed, and the community of q traders is divided to a subgroup of trader q' with visibility only to M' and group q'' with visibility only to M'', and a remaining group $q^{\wedge}$, with visibility to both M' and M'', ($q' + q'' + q^{\wedge} = q$), then a trader $Tr'_g \in q'$ group can pass their M' coins to traders from group q' and $q^{\wedge}$, but not to traders from group q'' because the latter will not be able to validate the bona fide of the transaction having no visibility towards M' where the coin status is published. Similarly, trader $Tr'' \in q''$ can pass their M'' coins to traders from group q'' and $q^{\wedge}$, but not to traders from group q'. The money is not lost, it is simply frozen until total visibility is restored.

An array of such divided mints may also operate according to the InterMint protocol.

Such visibility limitations can be (i) imposed by the communication network, (ii) imposed by mints, (iii) occur accidentally, or (iv) be a result of an act of terrorism.

Said limitations can be temporary or long-lasting.

Mint imposition can be carried out by encrypting a sub-mint and sharing keys with only a subset of traders.

In case of a disaster or an act of terrorism, the communication recovery may be bottom up. First the communication is established in limited regions, and then integrated to the full scope. In that case geographic proximity is important. Traders in the same geography will be served by a local mint and trade one with the other, despite being unable to trade with traders in another region. Traders might therefore choose to migrate their money to local submints, thereby establishing a measure of resilience against a host of disruptions.

3.6.5 Coin Holding Marks

A payee checking the public ledger at time t, will require a time interval Δt, to verify the ownership credentials passed to them by the payor, and then adjusting the state of the transacted coin at time t' = t +Δt. With all sorts of communication delay it is possible for the payor to double spend the same coin to a second payee who will adjust the state of the coin on the ledger at time point t'' < t'. This will amount to defrauding the first rightful payee.

To avert this risk the first payee upon first checking the status of the coin will issue a 'pending transaction mark' (PTM) over the coin. The PTM will be a standard Δt' duration. The PTM will be issued with a trader's identity mark: W*, and Fw, namely the public version of the trader's identity and the applicable one-way function. Within that time interval that coin is locked, preventing any other trader from updating the status of the coin. It is expected that Δt < Δt', and so within the PTM the first payee will adjust the state of the coin without interference from the second payee.

In the event that the credentials checks do not pan out, or for whatever reason the payee rejects the coin, then after Δt' the coin becomes unmarked and ready to be paid to whomever. The original payee, encountering a delay, could re-check the status of the coin, and issue a new PTM.

3.6.6 Remote Anonymity Payment

The vision of a global village describes two people with no geographical proximity, no mutual identification, and no mutual trust, still exercising a payment experience. BitMint*LeVeL is a tool to bring this vision into reality. It can be used with new quantum safe means to establish temporary privacy on the Internet. Temporary privacy is enough. Once the payee accepts the payment credentials, they update the ledger, and the money is safe against any hacker that a while later cryptanalyzes the message and reads the payment credentials.

3.6.7 Performance Advantage

Bitcoin currency solutions are limited in throughput by the need to spread each transaction to a large number of peers. Legacy money solutions are limited by the singularity of the authentication entity. Currently the best throughput is about a couple of thousands of transactions per second. The BitMint*LeVeL solution calls for an open number of mints to serve the public. Mints are profitable so they proliferate -- and share the load. There is no preset limit to the throughput of the LeVeL InterMint. It will grow to meet the demand.

3.6.8 Geographic Gravitation

Cyberspace is flat, every person in any country will be able to use any mint in any other country, especially that a mint in country A can mint LeVeL coins in fiat currency from country B. However, the mints operate under the regulation and the law that is in force in the country of their registration. . A citizen from country B will find it difficult to sue for justice, should the need arise, against a mint in country A. Such citizen will be well disposed to use a mint in their own country, all in all creating a geographical gravitation.

3.6.9 Wallets and Vaults

LeVeL works for little money people use in the normal course of the day, and for big money with which people buy expensive things. The former can be conveniently stored in the owner's phone, the latter should be stored in an offline computing device, encrypted. It will be a trifle more cumbersome to connect and pay with such a 'vault' instead of a wallet, but a better sense of security.

4.0 Formal Definition

The Environment: There exists a society S comprising s members. The society wishes to regulate its activity through the use of a currency. The society, therefore, is searching for a currency C, which is desired by a sufficient number of its members. C should be measurable, durable, storable, transferrable, and splitable. And furthermore, the society is searching for a protocol, π, to govern the exchange of the currency for the benefit of society as a whole. This is the financial challenge of the society.

One assumes that the society lives in cyber space where computing devices are used by its members.

Two ways are presented to select C, and π. One where the protocol is specified over a currency that has existence independent of the protocol, and one where the currency has no presence, or existence independent of the protocol. It is generated, defined and expressed by the trading protocol, π. The latter is regarded as the self-referential solution, and the former is regarded as the other-referential solution. These solutions are further presented ahead.

Self-referential money may serve as reference currency for an other-referential money, and of course other-referential money may be regarded as the reference currency for another other-referential money.

4.1 Other-Referential Finance

In this solution, the society S first identifies a reference currency C, and then develops a protocol π to handle its dynamics within the society.

Any member, or group of members, within the society may self-declare itself as a mint. The mint offers the other members of the society a service (a minting service). In return to an amount c of currency C, the mint will issue a digital claim check, called a digital coin, or a coin X, and pass X to a member of the society, to be called the purchaser, or trader-1 (Tr_1) who passed the amount c of C to the mint. The mint will further announce that coin X is subject to Terms of Redemption. In accordance with these terms the mint will receive coin X from any member of the society, to be called the redeemer, and in return pass to the redeemer an amount c of currency C. Coin X is to be regarded as a claim check for an amount c of currency C. The coin X (of value $|X|=x=c$) will be written as a digital string comprising:

X = [meta data][Terms of Redemption][t_0][x][D*][Fd]

where the meta data includes an identification of the mint, a unique id for the coin, and where t_0 is the time of the coin transfer to Tr_1, and where D* is the public key corresponding to D, which is the digital definition of coin X. D is a randomized bit string comprising d bits. D* is a bit string comprising d* bits: $|D| = d$; $|D^*| = d^*$. The {D, D*} pair are defined over a pair of one way functions F_d, and F^*_d, where it is easy to compute $D \rightarrow D^*$, and difficult to compute $D^* \rightarrow D$: $D^* = F_d(D)$ -- easy, $D = F^*_d(D^*)$ --hard.

Upon passing X to Tr_1 the mint discloses to Tr_1 the identity of D.

Upon receipt of X, Tr_1 establishes: (i) ownership credentials, U, and (ii) trader's identity, W

Ownership credentials: Expressed in the form of a bit string U_1, comprising u_1 randomized bits, and associated with a pair of public/private key functions F_{u1}, and F^*_{u1}, where U_1 is the private version of the ownership credentials, and U^*_1 is the corresponding public key, and where computing $U_1 \rightarrow U^*_1$ is easy and $U^*_1 \rightarrow U_1$ is hard: $U^*_1 = F_{u1}(U_1)$ -- easy, $U_1 = F^*_{u1}(U^*_1)$ is hard. U_1, F_{u1}, F^*_{u1} are a free choice of Tr_1. This is the fundamental departure point from Crypto 1.0.

Trader's Identity: Expressed in the form of a bit string W_1, comprising w_1 randomized bits, and associated with a pair of public/private key functions F_{w1}, and F^*_{w1}, where W_1 is the private version of the trader's identity, and W^*_1 is the corresponding public key, and where computing $W_1 \rightarrow W^*_1$ is easy and $W^*_1 \rightarrow W_1$ is hard: $W^*_1 = F_{w1}(W_1)$ -- easy, $W_1 = F^*_{w1}(W^*_1)$ is hard. W_1, F_{w1}, F^*_{w1} are a free choice of Tr_1.

Having established its ownership credentials and its trader's identity Tr_1 is submitting a status statement to a public ledger L maintained by the mint. The ledger L is visible to the entire society S, and it contains status statements for minted coins. The status statement submitted by Tr_1 to the ledger L is constructed as follows:

{Status Statement for coin X} = [X meta data][X Terms of Redemption][t_0][x][D*][F_d][U^*_1][F_{u1}][W^*_1][F_{w1}]

This statement announces to the society that coin X of value x and defined by the digital string D as the private key for which the corresponding public key is D*, and where F_d is the function that computes D* from D. This coin is owned by a member of society identified by identity string W_1, which is the private key corresponding to the published value W^*_1 and F_{w1}. Trader 1 (Tr_1) also claims ownership credentials for coin X in the form of bit string U_1, which is the private key corresponding to the published value U^*_1, and F_{u1}.

The protocol, π, specifies how Tr_1 will pass coin X to the next trader, Tr_2:

Upon decision of Tr_1 to pass ownership of coin X to Tr_2, Tr_1 will communicate to Tr_2 the values of D, and U_1.

Using the published F_d and F_{u1}, Tr_2 will verify: $D^* = F_d(D)$, and $U^*_1 = F_{u1}(U_1)$, and when so verified Tr_2 will acknowledge the receipt of coin X.

Upon receipt of coin X, Tr_2 will establish ownership credentials and trader's identity.

Ownership credentials: in the form of a bit string U_2, comprising u_2 randomized bits, and associated with a pair of public/private key functions F_{u2}, and F^*_{u2}, where U_2 is the private version of the ownership credentials, and U^*_2 is the corresponding public key, and where computing $U_2 \rightarrow U^*_2$ is easy and $U^*_2 \rightarrow U_2$ is hard: $U^*_2 = F_{u2}(U_2)$ -- easy, $U_2 = F^*_{u2}(U^*_2)$ is hard. U_2, F_{u2}, F^*_{u2} are a free choice of Tr_2.

Trader's Identity: in the form of a bit string W_2, comprising w_2 randomized bits, and associated with a pair of public/private key functions F_{w2}, and F^*_{w2}, where W_2 is the private version of the trader's identity, and W^*_2 is the corresponding public key, and where computing $W_2 \rightarrow W^*_2$ is easy and $W^*_2 \rightarrow W_2$ is hard: $W^*_2 = F_{w2}(W_2)$ -- easy, $W_2 = F^*_{w2}(W^*_2)$ is hard. W_2, F_{w2}, F^*_{w2} are a free choice of Tr_2.

Tr_2 makes sure that $U_2 \neq U_1$, and $W_2 \neq W_1$.

Having established its ownership credentials and its trader's identity Tr_2 is submitting a revised status statement to the public ledger L. The revised public statement replaces the existing statement for coin X. The status statement submitted by Tr_2 to the ledger L is constructed as follows:

{Status Statement for coin X} =
[X meta data][X Terms of Redemption][t_0][x][D*][U^*_1][F_{u1}][W^*_1][F_{w1}][t_1][U^*_2][F_{u2}][W^*_2][F_{w2}].

The revised statement indicates to the society, (S), that coin X is defined by the digital string D as the private key for which the corresponding public key is D*, and F_d is the function that computes D* from D. The coin was minted by the mint (identified in the meta data) at time point t_0 and passed to trader Tr_1 whose public identity is W_1, and whose public version of his ownership credentials were U^*_1, and that Tr_1 passed coin X to Tr_2 at time point t_1, and trader Tr_2 is identified by the public version of their identity: W^*_2,. Furthermore, the public version of the ownership credentials of Tr_2, is U^*_2.

Protocol π specifies that coin X will now pass from Tr_2 to Tr_3, and in general from Tr_i to Tr_{i+1} where before the transfer the public ledger shows the following statement for coin X:

{Status Statement for coin X} =
[X meta data][X Terms of
Redemption][t_0][x][D*][Fd][U^*_1][F_{u1}][W^*_1][F_{w1}][t_1][U^*_2][F_{u2}][W^*_2][F_{w2}].....[t_i][U^*_i][F_{ui}][W^*_i][F_{wi}]

This statement announces to the society that coin X of value x defined by the digital string D as the private key for which the corresponding public key is D*, and where F_d is the function that computes D* from D. The coin X was minted by the mint identified in the meta data. This coin is now owned by a member of society identified by identity string W_i, which is the private key corresponding to the published value W^*_i associated with F_{wi}. Trader i (Tr_i) also claims ownership credentials for coin X in the form of bit string U^*_i, which is the private key corresponding to the published value U_i, and associated with F_{ui}.

The statement also indicates that trader j, Tr_j, for j =1,2,....(i-1) owned coin X from time point t_{j-1} to time point t_j, and Tr_j was identified by identity string W^*_j which is the public version of the private identity string W_j associated with the one-way function F_{wj}. Tr_j is also claiming ownership credentials string U_j which is the private version of the public version U^*_j associated with the one-way function F_{uj}. These ownership credentials were in force from time point t_{j-1} to time point t_j

Tr_i will pass coin X to trader $_{i+1}$ by passing to Tr_{i+1} the following data:

$D, U_1, U_2, \ldots\ldots U_i$

Tr_{i+1} will verify these (i+1) pieces of data in reference to the corresponding public keys published on the ledger L.

If all the data is verified, then Tr_{i+1} is persuaded that the transfer is bona fide.

Upon receipt of coin X, Tr_{i+1} will establish ownership credentials and trader's identity.

Ownership credentials: in the form of a bit string U_{i+1}, comprising u_{i+1} randomized bits, and associated with a pair of public/private key functions $F_{u(i+1)}$, and $F^*_{u(i+1)}$, where U_{i+1} is the private version of the ownership credentials, and U^*_{i+1} is the corresponding public key, and where computing $U_{i+1} \rightarrow U^*_{i+1}$ is easy and $U^*_{i+1} \rightarrow U_{i+1}$ is hard: $U^*_{i+1} = F_{u(i+1)}(U_{i+1})$ -- easy, $U_{i+1} = F^*_{u(i+1)}(U^*_{i+1})$ is hard. U_{i+1}, $F_{u(i+1)}$, $F^*_{u(i+1)}$ are a free choice of Tr_{i+1}.

Tr_{i+1} will verify that: $U^*_{i+1} \neq U^*_j$ for j=1,2,...,i

Trader's Identity: in the form of a bit string W_{i+1}, comprising w_{i+1} randomized bits, and associated with a pair of public/private key functions $F_{w(i+1)}$, and $F^*_{w(i+1)}$, where $W_{(i+1)}$ is the private version of the trader's identity, and W^*_{i+1} is the corresponding public key, and where computing $W_{i+1} \rightarrow W^*_{i+1}$ is easy and $W^*_{i+1} \rightarrow W_{i+1}$ is hard: $W^*_{i+1} = F_{w(i+1)}(W_{i+1})$ -- easy, $W_{i+1} = F^*_{w(i+1)}(W^*_{i+1})$ is hard. W_{i+1}, $F_{w(i+1)}$, $F^*_{w(i+1)}$ are a free choice of Tr_{i+1}.

Tr_{i+1} will verify that: $W^*_{i+1} \neq W^*_j$ for j=1,2,..i

Any trader, Tr_r, may decide, at time point t_r to redeem coin X which was passed to them at time point $t_{r-1} < t_r$, as long as Tr_r is the current owner of coin X. To do so Tr_r submits to the mint

$D, U_1, U_2, \ldots\ldots U_r$

The mint verifies the r ownership credentials against the corresponding public keys, and verifies that D is what the mint stores in its records (in the coin database), and if all is verified, then the mint passes to Tr_r the amount c of current C which it received from Tr_1, and for which the mint minted coin X.

This concludes the life cycle of coin X, making rounds within the traders of society S.

4.1.1. Dispute Resolution

Any dispute arising from the BitMint*LeVeL trade, is to be resolved by the mint. The resolution may call for compensating a trader. To effect such compensation it is important for the mint to clearly identify the trader. This will happen by the right trader proving their identity by displaying their identity in its private mode, W, which the mint will verify against the published public version, W*.

Dispute may arise from a situation where the proper trader, Tr_p cannot pass their coin to a payee because the public ledger shows another trader Tr_a being the current owner of the coin. Or when Tr_p cannot redeem their coin because the mint redeemed the same to another trader.

Any such occurrence within the LeVeL protocol implies one of the two possible scenarios: (i) the private keys used by Tr_p to exercise payment of the coin have been stolen, or (ii) they have been cryptanalyzed. In both cases, the responsibility is on the shoulders of Tr_p. The proper trader must ensure sufficient security for their LeVeL wallet, and since Tr_p is the one who chose both the private key to represent their ownership credentials, (U_p), and the corresponding one-way function (Fu_p) -- they are also responsible in the event that their ownership credentials had been cryptanalyzed. And therefore, the victimized trader has no legal recourse against the mint, on account of the protocol.

All the above notwithstanding, the mint will try to investigate any complaint of misappropriation of a coin. The protocol will call upon all active traders to peruse the public ledger at least once within a preset ledger inspection period (LIP). The inspection will be automatic, carried out by the trader's computing device. If a proper trader finds that a coin held by them is listed as owned by someone else, or as redeemed, then the trader should contact the mint and log in a complaint of fraud.

The mint will require the complainant to provide evidence regarding their holding of the coin and, dependent on mint policy, may require the complainant to identify themselves. If the complaint looks meritorious then if the coin still circulates, the mint will impose a temporary freeze, and call upon the current coin holder to contact the mint. The mint has no means to contact the current trader, Tr_c; it will add a call to the trader identifying them through the trader's identity (W^*_c). Tr_c will identify themselves to the mint via the corresponding W_c. Tr_c is expected to review the ledger every ledger-inspection-period, LIP, and find out that it is being called. Thereby the mint will be in contact with both the complainant and the listed owner of the coin. Each mint will develop its own protocol for investigating the situation and reaching a resolution.

Another class of dispute may arise between a trader and the mint on the basis of the trader not being paid per their digital claim check as the claim checks warrants. Such a dispute has no protocol-internal solution. The injured party has a recourse through the courts or arbitration. While the traders may be anonymous, the mint is a known entity, exposed to court action.

The identity of the traders is unknown to the mint, and to society at large. The transaction may be such that a trader does not know the identity of the trader who paid them, neither the identity of the trader they pay to. This allows traders to choose to safeguard their anonymity, at the price of abandoning the disputed coin. The mint will resolve a dispute against the party that "does not show up". In the event that the mint's policy allows for redeemers to remain unidentified, and eventually a dispute arises over a redeemed coin, and also the redeemer remains silent, then the complainant has no recourse. Mints may require visibility for redeemers of high denomination coins.

It is worth emphasizing that the public ledger will have a "bulletin" section where the mint will be calling the attention of traders (calling them by the public version of their identity mark, W*), and which the traders are expected to peruse every ledger inspection period, (LIP).

4.2 Self-Referential Finance

The self referential (SR) finance protocol is defined in reference to the other-referential finance protocol with two changes: (i) the reference currency. RC is "Air". Air is per definition a currency of unlimited availability, everywhere, every time. It is therefore the asymptotic edge of the realm of currencies. It is priced as zero always everywhere. It is only a protocol or a mathematical artifact. The self-referential mint will issue its coins against Air, and redeem the same against Air. Otherwise the protocol is the same as for other-referential money.

The SR coin operation has only value if the SR coins are issued according to some limiting formula, so that these coins are scarce. Scarcity on its own, without any utility, may engender desirability. Desirability builds up into pricing. Once a market price develops for an SR coin, then, the SR mint can issue SR coins to itself, and benefit from this operation.

The self-referential (SR) protocol needs elaboration on two elements: (i) the minting limitation protocol, and (ii) coin expiration protocol.

4.2.1 The Minting Limitation Protocol

The mint will set up a number, q, of self-referential coins to be minted per a set time period Δt. The mint will then put forth an eligibility protocol to select eligible candidates to be offered the SR coins. This eligibility will be announced in public for candidates to apply. Eligibility qualifications are of a variety of options: from rewards for noble activity, to lottery and randomness.

4.2.2. Coin Expiration Protocol

Since self-referential coin redemption is done against "Air", there is no reason for an SR coin holder to ever redeem their coin. This leads to a never-expired coin management routine, which may pose too big a burden on the mint. The mint therefore, formally, will declare an expiration date for its self-referential minted coins. The coin holders will be in the know and adjust their behavior.

4.3 Coin Splitting

In order to enable a split of LeVeL coin X, the coin definition bit string D, comprising d bits, is divided to g substrings regarded as financial bits, fbits. Each substring is comprised of f bits, so that d= |D| = f*g. and where these fbits are assigned a value V_i for i=1,2,...g. The mint selects a one way function Fd for the coin, and applies Fd to the g fbit strings, such that fbit$_i$ is represented by fbit*$_i$: fbit*$_i$ = Fd(fbit$_i$). The values of the fbits: V_i for i=1,2,...g. and the contents of their public versions: fbit*$_i$ for i=1,2,...g are listed as part of the public ledger for coin X, that looks as follows:

{Status Statement for coin X} =
[X meta data][X Terms of Redemption][t_0][x][Fd]
[(V_1,fbit*$_1$), (V_2, fbit*$_2$), ... (V_g, fbit*$_g$)]
$[U*_1][F_{u1}][W*_1][F_{w1}][t_1][U*_2][F_{u2}][W*_2][F_{w2}][t_2].....[t_{i-1}][U*_i][F_{ui}][W*_i][F_{wi}]$

The protocol allows trader Tr$_i$ to split coin X to coin X' and coin X", where coin X' will be defined with a subgroup of fbits g' ∈ g, (where g here denotes the group of g fbits) and where coin X" will be defined with a subgroup of fbits g" = g - g' such that the sum values of coin X' and X" is the value of X.

|X| = |X'| + |X"|

$$\Sigma V_{i\ \text{over}\ g} = \Sigma V_{i\ \text{over}\ g'} + \Sigma V_{i\ \text{over}\ g''}$$

{Status Statement for coin X'} =
[X meta data][X Terms of Redemption][t_0][x][D*][Fd]
[V_i, fbit*$_i$ values for fbit in group g']
$[U*_1][F_{u1}][W*_1][F_{w1}][t_1][U*_2][F_{u2}][W*_2][F_{w2}][t_2].....[t_{i-1}][U*_i][F_{ui}][W*_i][F_{wi}]$

{Status Statement for coin X"} =
[X meta data][X Terms of Redemption][t_0][x][D*][Fd]
[V_i, and fbit*$_i$ values for fbit in group g"]
$[U*_1][F_{u1}][W*_1][F_{w1}][t_1][U*_2][F_{u2}][W*_2][F_{w2}][t_2].....[t_{i-1}][U*_i][F_{ui}][W*_i][F_{wi}]$

Trader Tr_i will pass X' to trader Tr_i', and pass X" to trader Tr_i''. The passing will be effected by passing to Tr_i':

D, U_1, U_2, ... U_i, [$fbit_i$ for all fbits in group g']

and passing to trader Tr_i'':

D, U_1, U_2, ... U_i, [$fbit_i$ for all fbits in group g"]

Both traders Tr_i' and Tr_i'' will then verify the bona fide status of Tr_i and accept the payment, if all the submitted ownership credentials check out against the public ledger, and also they will each verify that the fbit data they received for their split coin checks out against the public version of the same, as it appears on the ledger.

Trader Tr_i' in turn, will select a public/private key formula Fu_i' and a private key (ownership credentials) U_i', and compute the corresponding private key $U*_i' = Fu'(U_i')$, and similarly select the same or another public/private key one-way formula F'w, and a private key (trader's identity), W_i', and compute $W*_i' = Fw'(W_i')$.

Trader Tr_i'' will select a public/private key formula Fu_i'' and a private key (ownership credentials) U_i'', and compute the corresponding private key $U*_i'' = F''u(U_i'')$, and similarly select the same or another public/private key one-way formula F"w, and a private key (trader's identity), W_i'', and compute $W*_i'' = Fw''(W_i')$.

What is left is to update the public ledger to the fact that trader Tr_i is no longer the owner of coin X. The coin is split between X' and X", which are owned by Tr_i' and Tr_i'' respectively. The ledger will now show two new records:

{Status Statement for coin X'} =
[X meta data][X Terms of Redemption][t_0][x][D*][Fd]
[V_i, $fbit*_i$ values for fbits in group g']
[$U*_1$][F_{u1}][$W*_1$][F_{w1}][t_1][$U*_2$][F_{u2}][$W*_2$][F_{w2}][t_2].....[t_{i-1}][$U*_i$][F_{ui}][$W*_i$][F_{wi}][t_i][$U*_i'$][F_{ui}'][$W*_i'$][F_{wi}']

{Status Statement for coin X"} =
[X meta data][X Terms of Redemption][t_0][x][D*][Fd]
[V_i, and $fbit*_i$ values for fbits in group g”]
[$U*_1$][F_{u1}][$W*_1$][F_{w1}][t_1][$U*_2$][F_{u2}][$W*_2$][F_{w2}][t_2].....[t_{i-1}][$U*_i$][F_{ui}][$W*_i$][F_{wi}][t_i][$U*_i''$][F_{ui}''][$W*_i''$][F_{wi}'']

Traders Tr_i' and Tr_i'' will verify that the coin X has been updated on the ledger by their own split, as well as by the complementary split, such that every fbit is spoken for in a new coin, and no fbit is claimed by more than one coin. In the event that a problem arises as to the ownership of an fbit, then the mint conflict resolution protocol is activated.

This sequence will then be re-applied: trader Tr_i' will repeat the above process by dividing the g' group of fbits to subgroup h' and h" where g' = h' + h", and split the coin X' to coins X'^ and X'^^ where coin X'^ is given the fbits in group h' and coin X'^^ is given the fbits in group h".

And similarly, trader Tr_i" will repeat the above process by dividing the g" group of fbits to subgroup m' and m" where g" = m' + m", and split the coin X" to coins X"^ and X"^^ where coin X"^ is given the fbits in group m' and coin X"^^ is given the fbits in group m".

This split protocol will continue iteratively as long as a coin has at least two fbits to be divided.

Eventually a trader will bring his split coin to be redeemed, and the Mint will pay the redeemer their split value of the minted coin X, if the redeemer provided the coin definition for the fbits specified in their split, as well as the ownership credentials of all the previous owners of that split, back to trader Tr_1 who owned all the splits.

4.4 The InterMint

The InterMint is a network of mints constituted with a public protocol, so any entity can join. The protocol defines a currency exchange (CEX), acting like a hub. It also defines a pricing currency, C. All other currencies will be rated per C. The rating will reflect the relative supply and demand of all the reference currencies used by the other-referential mints, as well as the momentary pricing of the participating self-referential currencies. The CEX will hold the current exchange matrix for all these reference currencies.

A mint $Mint_i$ will send the CEX z_i of its digital coins, $Coins_i$, and request the CEX to exchange these z_i coins for z_j coins of type $Coins_j$ issued by $Mint_j$, such that according to the pricing matrix over the ingredients of $Coins_i$ and the ingredients of $Coins_j$ there will hold:

$$\mathbf{C(x_i) = C(x_j)}$$

Namely the value of x_i is the same as x_j as priced with C.

This formula may have to be adjusted per the finite resolution of each coin, and that would happen through an account denominated with C.

This mint-to-mint exchange will allow a trader of mint $Mint_i$ to request the mint to redeem for them x_i coins of $Mint_i$ for the matching amount x_j of coins $Coins_j$ minted by $Mint_j$.

This InterMint protocol will expand the notion of coin redemption from a single pricing currency C to digital coins minted by any other mint that participates in the InterMint protocol.

4.5 One-Way Functions Repository

BitMint*LeVeL hinges on traders taking responsibility for the money they hold by choosing effective one-way functions (Fu, Fw). Similarly, the mint will opt to choose an effective one-way function, Fd, for the coin definition D. The variety of the used one-way function (OWF) is key to the integrity of the BitMint*LeVeL platform. It is therefore that a repository of one-way functions will be posted online, helping traders with the task of choosing an effective OWF. Traders are free to choose anything they deem to be good enough, not limited to any repository, yet, a repository will be available as needed.

The OWF online repository will catalog the listed functions, so that coin traders will be able to point to them in their ownership credentials, and trader's identity definitions, and not having to cram the full definition of the function into the coin string.

One-way functions come in two flavors: complexity based, and randomness based. The first operates under a shadow of a hidden compromise via unpublished math, and the latter has a very predictable estimate for the effort needed to compromise it. Example for the first flavor is multiplication of two prime numbers which is hard to reverse. Examples for the second flavor are plenty, as documented in the review publication "Pattern Devoid Cryptography". A particular example is given ahead.

4.5.1 Multiple Hashed Transpositions

Let a bit string Q be transposed to $Q^T{}_i$, using an integer K_i as a key (see "Pattern Devoid Cryptography"):

$$\mathbf{Q^T{}_i = T(Q, K_i)}$$

for i= 1,2,3,...k

Let $Q^T{}_i$ be hashed to a fixed size hash string H_i:

$$\mathbf{H_i = Hash(Q^T{}_i)}$$

The Hash formula is made public.

Let the set of k hash strings and k keys be designated as a public key Z*.

$$Z^* = \{(H_1, K_1), (H_2,K_2) \dots (H_k, K_k)\}$$

And let Q be the corresponding private key, Z.

It is easy to compute Z* from Z, but hard to find a string Y that would qualify as Z, namely would yield Z* when computed according to the above algorithm. The trader choosing this one-way function will be able to increase its intractability at will, by increasing the value of k, and increasing the bit count of Q. Note that the size of Q is secret.

By setting the Q value and the k K_i values randomly, the user creates a pattern-devoid challenge to the cryptanalyst, the intractability thereto depends only on the computing power of the attacker. And since the user can dial up the featured intractability, they can ensure that the challenge (and the safety of the money protected by it) are one step ahead of the threat.

4.6 CoinBase Protocol

The mint of any BitMint*LeVeL money will have to build, secure and maintain a coin database, "Coinbase" where all the data listed on the ledger is found, and in addition the coin definition D. The coin database will mark each coin as either being "alive", still outstanding traded, or being "dead" namely already having been redeemed. For split coin the tracking of dead and alive will be at the fbit level.

5.0 Applications

BitMint LeVeL, like Bitcoin creates a cyber coin that allows a payor to pay a payee without a need for both payor and payee to each be registered and carried by a financial institution. They both simulate cash very well. It is this direct payment that is so revolutionary. In 2022 there are 1.7 billion unbanked people in the world. 1.2 billion of them have a cell phone. This 15% of world population can turn their cell phone into their bank, and transact with their local currency by simply downloading the LeVeL app. 25% of US households are either unbanked or underbanked – a big market for the LeVeL solution.

86% of respondents in a TechRepublic survey expressed serious concern about data privacy and about being exposed to credit card companies who follow their spending habits. LeVeL can return cash-grade privacy to everyday business.

The LeVeL protocol is designed to be carried out within computing devices used by the traders. The human payor and payee will be oblivious to the protocol sequence. They will each interact with their respective wallet, see how much money they have, and connect via Bluetooth or NFC, or even QR. Payor will mark the sum to be paid, whom to be paid to (receiving phone number), and click “pay”. Payee will receive a notification that money has been received, checked out and recorded by the payee wallet, ready to be used. This peer to peer transaction depends only on mutual visibility of the LeVeL public ledger; no additional interaction with any financial institutions. Payor and payee may be in proximity to each other, or opposite sides of the globe; they may exchange a few cents or transact millions of dollars.

A deep discussion of LeVeL application is beyond the scope of this writing. We touch a few aspects:

Effective Trade, Social Balance, Innovation, Profit & Leverage

5.1 Effective Trade

BitMint*LeVeL contributes to effective trade on many levels:

1. CBDC (Central Bank Digital Currency)
2. International Trade
3. Sub-Universal Trade
4. IoT Trade

5.1.1 CBDC

A central bank can practice the self-referential money protocol together with cascading, replacing the legacy money printing. Law enforcement then will be able to fight financial crime by blocking trade with suspicious money, insisting on coin holders to expose themselves and explain how they got hold of the suspicious money. This will generate an optimal balance between privacy for law abiding citizens and law enforcement over fraudsters and criminals.

BitMint*LeVeL brings a novel advantage to central bank management of its country's payment. Everyone in the country could announce themselves as a mint and offer anyone to submit the declared reference currency and receive in return a digital claim check for the same, as the protocol dictates. The mint does not have to be a bank or even a financial institution, as long as it complies with rules and regulations issued by the central bank. Each mint will define its own reference currency. Many will simply regard the fiat (self referential CBDC) as the reference currency, others will use the CBDC as an element in a mix with other assets, and yet others will define a reference currency without the fiat currency, say only precious metals. The central bank will set forth the rules. For example, the central bank could dictate that any reference currency will have to be comprised of at least 80% of the prevailing fiat currency, and the balance is free choice.

The various mints will be working together, forming an InterMint and provide the exchange services to their customers. Traders may choose to redeem their coin from Mint A with coins from mint B in the InterMint. The various mints in the InterMint will provide this service to their customers because otherwise they will not have customers. For the customers this arrangement means that they can freely switch from one reference currency basket to another. The overall shift of society to one basket of assets or another will represent the wisdom of the local crowd.

The fact that all the LeVeL coins are listed can be used by the respective government as a basis of taxation. Much as it is impossible to escape real estate taxes, because the estate owes the taxes, and is visible, so the listed coins are visible and can shed value by law to secure fair proportional taxation that remains equitable even though the owners of the taxed coins are not identified. The wholesale elimination of tax avoidance will reduce the tax burden for the taxed society.

5.1.2 International Trade

Sovereign countries will issue self-referential BitMint*LeVeL currencies. These national (fiat) currencies will serve as currency of reference for other-reliance BitMint*LeVeL mints, each may build a basket of the national currencies in some selected proportion. These derived currencies will become a basis for international trade.

5.1.3 Sub Universal Trade

There are numerous instances where money is defined in less than a universal capacity. Local municipalities issue their own money, merchants issue loyalty coins, organizations and groups of all sorts mint their own money. The BitMint*LeVeL protocol will be a good choice for all these sub-universal trades.

5.1.4 IoT Trade

BitMint*LeVeL may be traded with high resolution where the fbits are of very small value. Since Internet of Things transactions are often conducted between two devices automatically and fast, then the payment protocol will be modified as follows:

Payor submits to payee all the data specified in the other-referential transaction protocol (π), except the definition of the coin (D). The payee verifies the submitted data against the data in the public ledger. If the transacted sums are small then IoT payment can commence right after the ownership credentials have been submitted, and before they have been verified. Payment occurs fbit by fbit by the payor passing to the payee the bit definition of the paid fbits. When the payment is done the payee posts on the public ledger the fraction of the paid coin represented by the paid fbits.

When a coin is split to fbit-wise payment then the payee cannot verify the coin definition as a whole. So to prepare for coin splitting the current holder will redeem the coin with the mint against a value equivalent coin where the coin definition is given fbit by fbit:

$$D^* \rightarrow [D^*_{\text{fbit } 1}][D^*_{\text{fbit } 2}]\ldots\ldots [D^*_{\text{fbit } g}]$$

where $[D^*_{\text{fbit } i}]$ is the public version of the private definition of fbit i in the coin ($[D_{\text{fbit } i}]$

And the coin holder will receive from the mint the corresponding private version of the coin definition

$$D \rightarrow [D_{\text{fbit } 1}][D_{\text{fbit } 2}]\ldots\ldots [D_{\text{fbit } g}]$$

as the coins are being paid.

It will be an advantage to use a freshly minted coin for IoT payment when the payment process is fast because in that case the payee will have fewer data to verify. Alternatively, because of the low sums, the payee may be satisfied that the payment is bona fide after verifying only the credentials of the current owner, and maybe the credentials of the owner before that.

5.1.5 Offline Trade

LeVeL is readily used with the Hard Wallet technology developed for digital money trade without network connectivity. Trader Tr_i will pass coin X to trader Tr_{i+1} via a secure trusted App that would then erase the private keys for the ownership credentials of traders 1,2,…. i, thereby preventing a wallet breaker from double spending coin X. Trader (i+1), receiving the coin credentials to their own trusted hard wallet, will do the same towards trader (i+2). Namely, after passing the credentials for coin X to Tr_{i+2}, Tr_{i+1} will erase these credentials in their own secure wallet. This process will continue until some trader j (Tr_j). When Tr_j becomes the owner of coin X, the network communications are restored, allowing Tr_j to post on the ledger the ownership update for coin X. The ledger will show that Tr_i passed coin X to Tr_j. The ownership sequence Tr_{i+1}, Tr_{i+2}, … Tr_{j-1} has been lost – but no harm done. Payment continuity preserved.

5.2 Social Balance

There are several ways to apply BitMint*LeVeL to achieve a better social balance:

1. Tethered Money 2. Charitable Giving

See the book "Tethered Money" for this use case.

Charitable giving can proceed via various procedures as described herein, and also through anonymous giving, where the contributor is making a monetary contribution without exposing their identity. At any future time, at the payor discretion they may come forth, by proving their identity through presenting the private version, W, of the public version (coin marked) of the same, W*.

5.3 Innovation

The BitMint*LeVeL protocol allows an investor to put money into an innovative enterprise without disclosing their identity to anyone. The investor may execute a bona fide agreement with the recipient of the investment, while still maintaining their anonymity. The investor will be identified via their trader's identity (W*) in the contract papers, and in due time, upon the investor choice, they will identify themselves with the corresponding private version of the trader's identity (W).

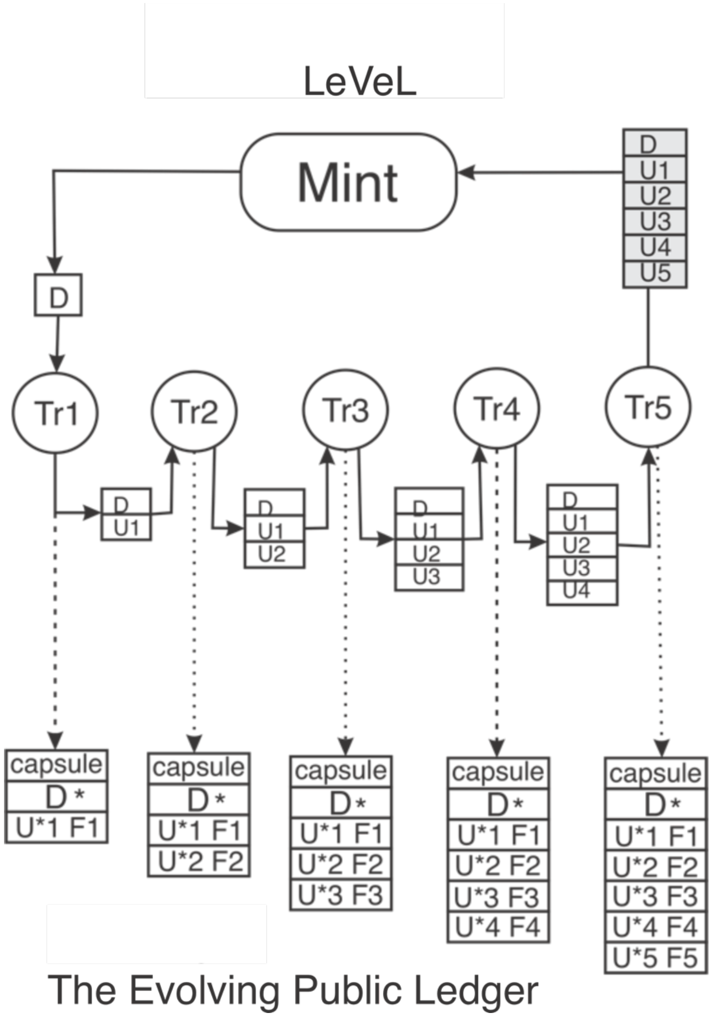
The investment will be tethered to a purpose and bound by conditions set forth in the terms of redemption of the money.

5.4 Profit & Leverage

As described, several self-reliant money protocols will exploit crowed behavior for handsome profit.

6.0 Graphic Illustration

The figure herewith shows the schematics of the LeVeL life cycle over 5 successive traders of a certain digital coin: Tr1, Tr2, Tr3, Tr4, and Tr5. The mint passes the digital definition (identity), D, of the minted coin to Tr1. Tr1, then picks a public/private key formula F1 and their ownership credentials, U1, then computes the respective public key of U1: U1* = F1(U1), and adjusts the public ledger status of that coin to display U1*, and F1. When Tr1 passes the coin to Tr2, they pass D and U1. Tr2 verifies the data given to them from Tr1 with the public ledger, and accepts the coin. Similarly, each trader chooses their own ownership credentials, adjusts the ledger and passes the credentials to the next trader. Trader Tr5 decides to redeem the coin with the mint. To do so Tr5 submits to the mint the values of D, U1, U2, U3, U4, and U5. The illustration ignores the trader's identity element, which is not essential for the protocol.



7.0 The BitMint Foundation of the LeVeL

The LeVeL protocol sits on top of the original BitMint protocol, which has been specified and elaborated on in implementation design documents and in the following patents.

US PATENT 11,107,156: DIGITAL FINANCE: CASH, CREDIT, AND INVESTMENT INSTRUMENTS IN A UNIFIED FRAMEWORK (BITMINT)

The BitMint digital money flagship patent: specifying the methodology for the BitMint financial language, how to express money in all its forms: cash, credit, debit, investment instruments. How to store and transact money securely and efficiently. This BitMint money offers full privacy for ordinary payors and payees, while providing means to enforce court orders on suspicious transfer of money. This patent specifies a cascaded format to track any financial complexity in a mathematically simplified form, amenable to computer manipulation, ready for conditional payments and for means to extract greater social impact from the national currency.

US PATENT: 11,188,886 IOTPAY: CONTINUOUS VARIABLE RATE HIGH-RES, DEVICE TO DEVICE PAYMENT SYSTEM

BitMint money embodied in devices that pay each other automatically, and very fast if needed, at any resolution desired. The payment may be carried out with cash-like anonymity and especially applied to situations where a subscription fee is replaced with pay-as-you-go payment solution.

US PATENT: 10,467,522: ROCK OF RANDOMNESS

This patent established a firm material base for minted digital money. Digital money which does not hinge on a material foundation is inherently vulnerable to a thief who happens to be smarter than expected. At BitMint we believe that the seriousness of central bank digital money requires it to be stationed on non-digital expression of data. We invented the ROck of Randomness that is designed to insure that under no circumstances will hackers who securedd access to your computers be in a position to undermine your entire currency. As long as the physical rock is securely in your possession so is your money. The Rock of Randomness was developed to be used in conjunction with BitMint digital money, but it will serve any other form of digital money.

US PATENT 10,956,878 MINTING AND USE OF DIGITAL MONEY

This patent describes the basic form of the BitMint digital language: identity fused with value. It represents cash in a splittable form. It is simple enough to be used for special purpose money, loyalty money, automatic payments like parking, road access, as well as for quick secure Internet payments, utility payments, and automatic transactions through the Internet of Things.

US PATENT: 11,062,279: HARD WALLET: A NEW TRUST BASIS FOR DIGITAL PAYMENT

This patent creates a new basis for payment trust. When we pay with banknotes we trust the money, when we pay with credit card, or with peer validated system, we trust the payor. With this invention a third option becomes available: trusting the wallet. The physical wallet commands trust because its identity can be ascertained through billions of measurements and physical properties -- the ultimate way to ascertain physical identity. This identification technology is applied to the payment device, which then passes its trusted validity to the payment bits that emerge from it. This hard wallet gains the trust of the payee without having to connect real time to the internet. It therefore allows for digital payment without global connectivity. And by having one such trusted wallet pass money to another trusted wallet, then the trust of the original wallet is passed along to the second wallet, and from there to the third, etc. All together a society holding such trusted hard wallets will conduct payment cash like even with persistent lack of global connectivity. In other words this invention will keep payment continuity while the Internet is down, and do so indefinitely. The hard wallet will confer its trust to the money inside and to the software inside. The wallet can be secured to tis owner via a bio port. The hard wallet works with BitMint digital coins as well as with other than BitMint digital coins. It provides the ultimate solution to the paramount requirement of payment continuity under all conditions.

US PATENT 9,471,906: DIGITAL TRANSACTIONAL PROCEDURES AND IMPLEMENTS

This patent is a simplified version of the hard wallet. It is a physical coin commanding trust through the integrity of its shell, designed to be so brittle that any attempt to tamper with it will cause it to shutter to hundreds of small pieces. And therefore if handed over in one smooth piece, the shell is to be regarded as un-tampered with. And if the shell is trusted then the payee will trust that inside the shell there is a memory (microSD) containing digital money in the denominated amount of the coin. As long as the shell is kept in tact the coin will be passed around like regular coin. When the shell if broken the digital money therein is uploaded and used. This simple payment solution can be used for store gifts, loyalty money, goodwill money etc.

US PATENT 8,229,859: BIT CURRENCY: TRANSACTIONAL TRUST TOOLS

This original patent contains the foundation of the BitMint vision. It features an important novelty: delegation of authority to authenticate a transaction. The patented methodology will allow a central authentication authority to delegate that authority to subordinate centers, who could further delegate the authority below them, creating a vast hierarchical network to efficiently serve the trading public. While the authenticated money is envisioned to be BitMint money, this is not a requirement. Delegation of authority to authenticate transaction can be applied to a wide range of digital money solutions. By applying it one resolves the vulnerability of dependence on a single all-knowing database. This patent creates the power to trickle down authentication power without exposing the original database to the delegated stations.

US PATENT: 10,965,460: ROBUST SECURITY TECHNOLOGY FOR COUPONS

This patent extends the BitMint financial language to store money and loyalty cash, leveraging the power of stores to use their current customers as recruiters for future customers. This very efficient way to grow one's business is carried out via cryptographic means applied on the BitMint coin which has not only a value but also an identity -- making it trackable, and guidable. A host of new imaginative ways to grow one's business are being developed on the basis of this fundamental patent.

8.0 Summary Note

The BitMint*LeVeL is a digital money solution proposal, presented here in its bare bone essentials and formal definition. Implementation thereof involves a considerable engineering work which is not elaborated herein. The novelty of BitMint*LeVeL is in the way it re-assembles the innovative ingredients in Bitcoin, and wraps them up with additional innovation to make the LeVeL into a viable candidate for a universal digital money platform. Readers are expected to weigh the LeVeL protocol, and evaluate its candidacy to fit into the global effort to fashion money in cyber space. This writing is but a bare bone presentation of the LeVeL technology. Yet, it is inclusive enough, hopefully, to allow a curious reader to follow the basic concept and to appraise its role in the widespread effort to migrate money into cyberspace.

Reference

A. Narayanan and J. Clark. Bitcoin’s academic pedigree. Com- munications of the ACM, 60(12):36–45, 2017.

B. Bu ̈nz, S. Agrawal, M. Zamani, and D. Boneh. Zether: Towards privacy in a smart contract world. In Proceedings of the 24th International Conference on Financial Cryptography and Data Security, FC ’20, 2020. ePrint: https://eprint.iacr.org/2019/191.

Bank for International Settlements et al. Central bank digital currencies: System design and interoperability, 9 2021. https: //www.bis.org/publ/othp42 system design.pdf.

Bank of Canada et al. Central bank digital currencies: founda- tional principles and core features. BIS Working Group, 2020. https://www.bis.org/publ/othp33.pdf.

Bank of England. Central bank digital currency: Opportunities, challenges and design, 2020.

Bank of Thailand. Central bank digital currency: The future of payments for corporates, 2021. https: //www.bot.or.th/English/FinancialMarkets/ProjectInthanon/ Documents/20210308 CBDC.pdf.

Binance. Binance USD. https://www.binance.com/en/busd.

Bitcoin Core Developers. Bitcoin Core. https://github.com/ bitcoin/bitcoin.

Board of Governors of the Federal Reserve System. Money and payments: The U.S. dollar in the age of digital transformation, January 2022.

C. Decker and R. Wattenhofer. Bitcoin transaction malleability and MtGox. In Proceedings of the 19th European Symposium on Research in Computer Security, pages 313–326, 2014.

D. Chaum, C. Grothoff, and T. Moser. How to issue a central bank digital currency. arXiv preprint arXiv:2103.00254, 2021.

D. Chaum. Blind signatures for untraceable payments. In Ad- vances in Cryptology: Proceedings of Crypto 82, pages 199–203. Springer, 1983.

D.Hopwood,S.Bowe,T.Hornby,andN.Wilcox.Zcashprotocol specifiation, 2021. https://zips.z.cash/protocol/protocol.pdf.

Diem Foundation. Diem. https://www.diem.com/en- us/white- paper/.

E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from Bitcoin. In Proceedings of the 2014 IEEE Sym- posium on Security and Privacy, SP '14, pages 459–474, 2014.

Ethereum Developers. Solidity, the smart contract programming language. https://github.com/ethereum/solidity.

G. Danezis, E. K. Kogias, A. Sonnino, and A. Spiegelman. Nar- wal and Tusk: A DAG-based mempool and efficient BFT consen- sus, 2021. https://arxiv.org/pdf/2105.11827.pdf.

G. Gerdes, C. Greene, X. M. Liu, and E. Massaro. The 2019 Federal Reserve payments study, 2019.

G. Wood et al. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014):1– 32, 2014.

https://libertystreeteconomics.newyorkfed.org/2021/12/ why- central- bank- digital- currencies/.

J. C. Jiang and K. Lucero. Background and implications of China's central bank digital currency: E-CNY. Available at SSRN 3774479, 2021.

J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Balancing accountability and privacy using e-cash. In International Confer- ence on Security and Cryptography for Networks, pages 141–155. Springer, 2006.

J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Com- pact e-cash. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 302–321. Springer, 2005.

J. Kiff, J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. A survey of research on retail central bank digital currency, 2020. https://www.elibrary.imf.org/view/ journals/001/2020/104/001.2020.issue- 104- en.xml.

L. Brainard. Update on digital currencies, stablecoins, and the challenges ahead, 2019. https://www.federalreserve.gov/ newsevents/speech/brainard20191218a.htm.

N. Narula, W. Vasquez, and M. Virza. zkLedger: Privacy- preserving auditing for distributed ledgers. In Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation, NSDI ’18, 2018. ePrint: https://eprint.iacr.org/ 2018/241.

NIST. Post-quantum cryptography, 2016. https://csrc.nist.gov/ Projects/Post- Quantum- Cryptography.

P. Wuille. Bech32m format for v1+ witness addresses, 2020. https://github.com/bitcoin/bips/blob/master/bip-0350.mediawiki.

R. Auer and R. Bo ̈hme. The technology of retail central bank digital currency. BIS Quarterly Review, March 2020.

R. Auer, J. Frost, M. Lee, A. Martin, and N. Narula. Why central bank digital currencies? Liberty Street Economics,

R. Garratt, M. J. Lee, B. Malone, and A. Martin. Token- or Account-based? A digital currency can be both. Liberty Street Economics, 2020. https://libertystreeteconomics.newyorkfed. org/2020/08/token- or- account- based- a-digital- currency- can- be- both/.

R.Garratt,M.J.Lee,etal.Monetizingprivacywithcentralbank digital currencies. Technical report, Federal Reserve Bank of New York, 2020.

R3. Corda. https://www.corda.net.

S. Bowe, A. Chiesa, M. Green, I. Miers, P. Mishra, and H. Wu. Zexe: Enabling decentralized private computation. In Proceed- ings of the 41st IEEE Symposium on Security and Privacy, S&P ’20, 2020. ePrint: https://eprint.iacr.org/2018/962.

S. Brands. Untraceable off-line cash in wallet with observers. In Annual international cryptology conference, pages 302–318. Springer, 1993.

Sveriges Riksbank. E-krona pilot phase 1. Sveriges Riks- bank Report, 2021. https://www.riksbank.se/globalassets/media/ rapporter/e- krona/2021/e- krona- pilot- phase- 1.pdf.

T. Walton-Pocock. Why hashes dominate in SNARKs: A primer by AZTEC, 2019. https://medium.com/aztec-protocol/ why- hashes- dominate- in- snarks- b20a555f074c.

Tether Operations Ltd. Tether. https://tether.to/.

Y. Qian. Technical aspects of CBDC in a two-tiered system,

Amnon Samid, "What I learned from my role in digitizing the yuan" https://forkast.news/digital-yuan-cbdc-china-central-bank-currency/

G. Samid "Pattern Devoid Cryptography" https://eprint.iacr.org/2021/1510

G. Samid “BitMint Hard Wallet: Digital Payment without Network Communication: No Internet, yet Sustained Payment Regimen between Randomness-Verifiable Hard Wallets”, 2020 IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE International.

https://www.bankofengland.co.uk/- /media/boe/files/paper/2020/central- bank- digital- currency- opportunities-challenges- and- design.pdf.

https://www.itu.int/en/ITU- T/Workshops- and- Seminars/ 20180718/Documents/Yao%20Qian.pdf.

S.Allen,S.Cˇapkun,I.Eyal,G.Fanti,B.A.Ford,J.Grimmel- mann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, et al. Design choices for central bank digital currency: Policy and tech- nical considerations. Technical report, National Bureau of Eco- nomic Research, 2020.

T. Mancini-Griffoli, M. S. M. Peria, I. Agur, A. Ari, J. Kiff, A. Popescu, and C. Rochon. Casting light on central bank digital currency. IMF Staff Discussion Note, 8, 2018.

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Cryptography Mailing list at https://metzdowd.com, 10 2008. https://bitcoin.org/bitcoin.pdf.

Table of Contents