Introducing the LeVeL Paying Field:

The Simplest, Most General, Most Secure, Most Intuitive Digital Currency

Developed with the principles of the Innovation$^{SP(*)}$

The LeVeL Paying Field was designed to implement the basic payment experience in cyber space, which is the core of the universal monetary exchange. Everything else is built on this foundation.

The Basic Payment Experience in Cyber Space

Payment is an interaction between a payor and a payee. In cyber space both payor and payee use a computing device, and are served with digital communication channels for these two devices to communicate with each other. Payment is expressed through a flow of a string of bits from payor's device to payee's device, and an optional digital receipt going the opposite direction. Payment is only meaningful in the context of a community of traders that need to recognize the act of payment. This recognition requires a network encompassing the members of the community of traders. For payment to happen the flow of bits from payor to payee has to be

designed to assure the payee that it implies money transfer. Furthermore, the community must recognize this transfer, and the right of the payee to pay that money to a third party.

This is the basic payment experience: *two members of a community, each holding a computing device, which communicates with each other -- carry out a payment*.

Please notice that this basic act does not require that either party will have an account with some financial institution; it does not require the parties to mutually identify themselves, nor do they have to surrender their identity to the community. The parties may be near each other or an ocean apart, may be acquaintances or strangers, may be friends or foes. Two computing devices, a channel for bilateral communication, and community visibility -- that is all that is needed to exercise the basic payment experience in cyber space.

Once this basic cyber payment experience is implemented, it can support a host of terms, conditions, restrictions, as the community sees fit. But these are overlaid upon the basic experience -- perhaps in a dynamic fashion.

We now let this vision of the basic payment experience to guide us to the simplest, most general, most secure, most intuitive design to bring this vision into reality.

Operational assumptions: payor and payee have a sufficient supply of batteries to power up their computing devices, and to establish a bilateral channel of communication over short distances. The community of traders is served by a communication network that is at least intermittently operational.

We introduce the notion of a cyber coin: a digital string that represents a numeric value of a given currency. Payment amounts to a transfer of such coin from payor to payee. Unlike material transfer, a digital transfer leaves the transmitter with a copy of the transmission, it is therefore

necessary to ensure that the payor cannot pay the same coin again, to another payee (by error or by malintent).

We tackle the goal of so ensuring in two ways: one for the case where the network is on, and one for the case where the network is off. We expect the network to be on most of the time, so we start with this case.

Online LeVeL: Design Elements

The essence of the LeVeL design is a two-face expression of a coin. One public and the other private. In its public expression a coin is known to the community at large, but in its private expression it is known only to the single trader that claims that coin as his or her own. By proving possession of the private expression of a coin, its owner proves his ownership thereof.

While the public ledger is a concept used by all digital currencies, the LeVeL offers an important distinction: *the coin owner does not need to prove ownership to the entire community of traders (as in bitcoin), rather only to the payee*. This turns out to be a big advantage, readily exploited by the LeVeL design.

Payment proceeds as follows: payor claims to payee that she is the owner of a given coin Z. Payee says: "Show me your private expression of coin Z. I will check it against the public expression of Z (which is listed on the public ledger). If they fit, then I will be satisfied that you indeed are the owner of coin Z. The payor complies and passes to the payee the private expression of coin Z.

At this point both the payor and the payee are in possession of the private expression of Z. In order for the payment to be carried out, this duality must be terminated. To that end the payee comes up with a *private update* for the state of coin Z. Only the payee knows this private update.

The payee will then compute a corresponding update to the public expression of coin Z, and post this public update on the public ledger. As soon as the update is posted the payor cannot any longer claim ownership of coin Z because he does not know the private update, only the payee does. No other than the payee has the private equivalent of the updated public expression of coin Z. This establishes the payee as the new recognized owner of coin Z -- payment executed - and settled.

One will wonder: what then prevents any arbitrary trader to take the initiative and generate a private update to coin Z, then post the corresponding public expression on the public ledger, claiming to be the new owner of coin Z? To prevent such theft the LeVeL protocol dictates that the update of the LeVeL coin must be an *'add on'*. Namely, it must add to the previous expression of the coin -- *not to replace it*. This add-on limitation is what will prevent a stray trader to claim ownership of coin Z. That stealing trader will not be in possession of the private expression of coin Z before the update, and hence he will not be able to prove to any payee that he is the rightful owner of this coin. The only trader that is in possession of the pre-payment private expression of the coin, and the post-payment add on, is the payee, who received the private expression from the payor, then added his own to establish himself as the new owner of coin Z. The payor knows all the private data about Z, but not the update put there by the payee. So the payor cannot practice double-spending.

The coin owner posts the public expression of coin Z on the public ledger, asserting that he has the corresponding private expression. When the payee wishes to pass the coin to a third trader -- the new payee -- he will exercise the same procedure used by the original payor only that now the private expression of the key will be longer (it has the recent update). The new payee will repeat the updating procedure, and further increase the 'signature' of the coin -- public and private.

This way payment continues indefinitely. No intermediation from any financial institute is needed.

The LeVeL payment solution requires an undertaking agency, denoted as The Mint. The Mint mints the LeVeL coins, and passes each coin to the first trader. The Mint also redeems the LeVeL coins from their last trader. Both minting and redemption can be done against some consideration, which is a secondary point.

The power of LeVeL rests with its utter simplicity: a community of traders served by a connecting network, comprising members where each member is equipped with a computing device that can exercise bilateral communication. The network facilitates a public ledger that lists all the circulating coins at their current public expression. Trade is carried out by the payor proving his or her ownership of the coin by revealing the corresponding private expression of the posted coin, and on it goes. Trade happens.

Advanced commerce, debit and credit, investment, risk management, and other banking functions are all built upon this simple trading protocol.

This is the LeVeL solution to payment in cyber space.

LeVeL trading when the network is off

During periods when the network is dysfunctional, the online trade protocol cannot operate because the public ledger is not visible, and cannot be updated. In these situations, payment will take place via a trusted physical wallet (a hard wallet). This hard wallet is manufactured by the Mint, and is built with the following parameters: (i) it cannot be tampered with without voiding the information therein, and (ii) it can't be counterfeited. [The technology that supports these

strong statements is described in the BitMintcash.com website.] The payor will pass the private expression of the paid coin to the payee through physical contact between the payor hard wallet and the payee hard wallet. Once passed, the payor's hard wallet will erase the private expression of the passed coin, thereby leaving the payee hard wallet as the only wallet that carries the private expression of the coin. Same will happen when the payee will transfer the coin to the next payee. At any instance, there is only one trader that has possession of the private expression of the coin. When the network turns on again, the current owner will revert to the online payment -- seamlessly.

The mathematical foundation for the LeVeL Demonstration App

The mathematical tool that enables one to create a public and private expression of a coin is known as a "One Way Function". This is a function that will operate one way easy, and the reverse way hard. More specifically: a OWF will compute a result Y from an input X with arbitrarily few computational steps, and will compute back X from an input Y with an arbitrarily many computational steps. Either way, a OWF, "f" establishes a connection {X -- Y}. Namely X and f together point to Y, and Y and f together point to X.

When the Mint passes coin Z to the first trader, this trader selects any one way function (OWF) he pleases, say, f =OWF_1. The first trader selects an arbitrary input X = PRV_1 as the private expression of the transaction that passed the coin from the Mint to the first trader. Using OWF_1, trader 1 will readily compute the corresponding public key, PUB_1, and post coin Z as defined through its first transaction: Z - {PUB_1 - OWF_1}. The first trader is the only trader who is in possession of the private expression of coin: Z - (PRV_1- OWF_1}, so only he or she can convince a payee that she is the owner of the posted coin Z. The second trader, receiving

PRV_1 from the first trader will compute $Y = OWF_1(PRV_1)$. If $Y = PUB_1$, then the second trader is satisfied, and immediately he establishes an update: selecting his own one way function, OWF_2, and his own arbitrary private key PRV_2. Then the second trader computes the corresponding private key $PRV_2 = OWF_2(PRV_2)$, and updates the public ledger to indicate:

$$\boldsymbol{Z - \{PUB_1 - OWF_1\} - \{PUB_2 - OWF_2\}}$$

Once the ledger is updated, then only trader 2 is in possession of the private expression of coin Z. Trader 1 can no longer pay coin Z to anyone.

Trader 2 will repeat the same protocol towards the third trader, and on it goes. When trader - i is the owner of the coin, then its public expression looks like:

$$\boldsymbol{Z - \{PUB_1 - OWF_1\} - \{PUB_2 - OWF_2\}..... \{PUB_i - OWF_i\}}$$

and the private expression, known only to trader i will look like:

$$\boldsymbol{Z - \{PRV_1 - OWF_1\} - \{PRV_2 - OWF_2\}..... \{PRV_i - OWF_i\}}$$

The Mint will redeem the coin only if the redeemer will demonstrate knowledge of the private expression of the redeemed coin.

In practice, the protocol is a bit more involved, but the above simple set of steps is all the mathematics that supports the LeVeL trade. There is an infinite supply of one way functions and hence the traders can add more and more of them, and in a pace faster than any adversarial computing machine (quantum or otherwise) can hope to defeat. In other words, the LeVeL trade practices *algorithmic mutation* and stays on indefinitely.

In the demonstration herein, each trader uses the private-public key scheme to also identify himself or herself without exposing his or her real identity. Under various circumstances such identification is necessary.

The Innovation^{SP} is an innovation methodology developed by Dr. Gideon Samid, designed to accelerate the innovation process (InnovationSP.net)