DOUBLE ANONYMOUS (DIGITAL) PAYMENT

BY GIDEON SAMID
gideon@bitmint.com

MATERIALIZED CASH PROJECTS ITS OWN INTEGRITY, allowing two strangers to exchange value and never know who they are dealing with. This two-way anonymity endows cash traders with a sense of dignity, privacy, and freedom.

When money turned digital, this double anonymity was lost. So now, all your purchases are cataloged by a stranger. Every over-the-counter med you pick up, every book you select, even your choice of entertainment establishments. As a whole, this is tantamount to a strip search.

And then there are all those unbecoming situations, which a small sum of cash would have solved without an embarrassing trace. In addition, there are instances where payments are so small, or so fast, that anything beyond the sheer transfer of value is unwelcome friction.

Paying digital money happens through a flow of bits. The simplest way for this to happen is for these bits to carry value as part of their identity. Thus, when bits flow from A to B, value has been transferred, regardless of who A is or who B is, regardless of the lack of mutual awareness of the identities of A and B, and regardless of any other digital exchange from some remote digital centers or from other traders not part of this transaction. It is this subtle, but critical, fashion of payment that legacy digital money and cryptocurrencies fail to achieve.

A digital coin that represents its value via the bits that express it can also be tied to terms of redemption (it's called tethering—see my book, "Tethered Money"). Such a coin can be restricted for purchase of, say, food, can be valid until Thursday only, and can be spent only by George, regardless of who it is being paid to.

A pioneering stab towards this much-desired payment simplicity was undertaken by the Bank of Shanghai. Users download money from their account to their phone as a bunch of bits that have a value and an identity, fully expressed in that bit package. The user can choose between a "protected mode," where he surrenders his privacy, and a pure "cash mode," where the money is lost if the phone is stolen or crashes (unless it was backed up beforehand).

The fused value and identity bit package can be autonomously split by the user's phone, so as to pay any amount up to the total sum. No Internet needed, no validation by neighboring traders. For example, the app will represent the bits as a quick-response code on the payer's screen. The payer will then position the screen in front of the camera of the phone of the payee. Once captured, it's done.

Notice that for this transaction to take place, the payer does not need to know who he is paying to, and the payee may be ignorant as to who pays him. If the payee then handed a sandwich to the payer, we would have an exact functional replica of the old-fashioned cash transaction.

These Bank of Shanghai BitMint coins are downloaded to a well-identified first owner, and are redeemed to a well-identified last owner. What about the in-between owners? The bank decides. For small denominations, the temporary owners of the coins may remain anonymous. For larger sums, the full chain of custody of a coin may be required, and its presence is a condition of redemption.

In a business-to-business environment, the requirements are the opposite. You need a receipt for every payment. Here again, the advantage of tight packaging of value plus identity allows the payee to hash the received coin and return the hash to the payer as proof of payment. DT