

DIGITAL TRANSACTIONS WITHOUT THE INTERNET

“WHEN THE INTERNET FADES, payment dies. Alas, society runs on payment. And payment continuity is a must.” Central banks around the world recognize this very challenge, and search for answers.

The importance of this topic was recently recognized in the International Conference IEMTRONICS held in British Columbia Canada, where it was the topic of the keynote address, with the respective paper earning the “Best Paper Award.” Here is a synopsis of the technology that offers to safeguard payment continuity:

The idea is to anchor cyber coins to material reality. This can be accomplished through (i) smart coins, and through (ii) smart wallets. In both cases, the payee must gain confidence that the payment is bona fide. We do so with regular cash. Inspecting a dollar bill in our hands, we conclude that it is not fake. A smart coin is a physical implement that contains cyber memory with cyber money. To pass as bona fide, the coin manufacturer may use two tracks: (i) tamper-detectability, and (ii) tamper-resistance. Technology to effect detectability is based on material of construction that splits to myriad of tiny pieces when hammered. Therefore, when you are given such a coin intact, you are quite confident that it was not cracked open



BY GIDEON SAMID
gideon@bitmint.com

and emptied (See details in US Patent 9,471,906).

Technology to effect tamper-resistance is based on several detectors built into the coin. They are designed to sense drilling, splitting, cracking, melting, etc. When these sensors are activated, they instantly erase the digital content of the coin (for details see U.S. Patent 10,445,730).

A hard wallet, on the other hand, is a physical implement that can dispense any amount of money stored inside. Imagine a piece of hardware with a digital port that spews bits claimed to be money. To trust this money, it has to be more than a bit-written number; it has to have identity. For example, BitMint identity-bearing digital currency.

Second, you need to trust the integrity of the spewing wallet. Any high-class fraudster can fake a piece of hardware, claiming authenticity. To frustrate this fraudster, one uses a composite material manufactured through nanotechnology where the input is quantum grade randomness. It builds a wallet that has a very large number of unpredictable readily measurable attributes. These attributes

are found in a public ledger distributed by the wallet manufacturer.

All that the payee has to do is to attach a simple measuring device to the physical wallet, take instant measurements and compare them to the pre-loaded figures published by the manufacturer. If the two sources agree, the payee is satisfied, and regards the bits that subsequently flow out from this wallet as bona fide money.

The manufacturer of the wallet receives the digital coins and the payment software from the mint that issues and redeems the transacted coins. It will work with any digital money where value and identity are fused together. The wallet will pay at any resolution enabled by the paid currency. In the case where the recipient is a similar hard wallet, the paid money can be further paid to a third payee. This defines an ongoing payment regimen that will support society for as long as the Internet is dark.

The hard wallet will operate equally well while the Internet is on. It is noteworthy that hard-wallet payment can be done with total anonymity. Payers need not identify themselves. The payee validates the wallet, not the person submitting it.

With the hurdle of payment continuity resolved, the road is clear for the full vision of digital money to change society on a global scale. DT