Getting Cashless 2.0

Ajeya Singh

India is marching steadfastly towards a digital economy with Budget 2017 supporting the digitalisation agenda. The December 2016 Watal Committee on Digital Payments recommended testing the digital rupee. The Institute for Development and Research in Banking Technology (IDRBT) is drawing a similar conclusion.

With the hype on blockchain — a distributed database that maintains a constantly growing list of ordered records, or blocks — deflated, we need to further assess the shortfalls of this lucrative technology and the surfacing advantages behind the digital rupee 'printing machine'. Hence, the need for a centrally issued digital fiat currency that plays a pivotal role endorsing trust, security and control with its monitoring system, to enable stringent control on black money, tax evasions and cyber counterfeit, thereby assuring better digitisation and monetary as well as financial policies.

With a view to address this need, blockchain technology has been debated about its usage, cost, security issues, etc. It is based on a peer-to-peer network where each node involved has to synchronise to confirm every transaction and accumulate all previous transactions. It is not deemed to be 'mature' enough in terms of system stability, application security and business model for digital fiat currency.

According to director of technology of the People's Bank of China (PBOC), Wei Li, "As a new technology, blockchain technology still poses significant gaps in its system stability, application security and business model as a digital fiat currency." These loopholes exist due to the freedom of nodes joining and exiting the network. It is also susceptible to route deception, address-spoofing attacks, encryption key theft, the possibility of algorithms being cracked, as well as the possible bifurcation of the block ledger and rollback.

Blockchain can also spread virus due to the lack of hardware encryption, allowing nodes to add unchangeable custom information containing viruses. There is a possible introduction of security vulnerabilities with application extension added to the blockchain. In addition, the potential information leakage is multiplied as every node in the network has a complete record of all historical transactions.

So, the cost of the digital fiat currency should be marginal with the absence of physical logistics costs and benefits of riding on existing digital payment infrastructure. This makes it a lucrative proposition for the government, banks and businesses. Any solution based on consensus of a network of peer-to-peer participants would not blend with this fundamental requirement.

According to Wei Li, this structure consumes large amounts of computational resources, time, cost and storage. Coming to a similar conclusion, John Barrdear and Michael Kumhof of the Bank of England estimated that "the total electricity consumption of the Bitcoin network in early 2014 was comparable to that of Ireland". So, for blockchain technology, the overhead for duplicating, transmitting and storing the entire transaction history at every node will be alarmingly expensive.

The limitations of blockchain technology indicate that the suitable technological solution should recognise that the issuance of the digital rupee is the authority and responsibility of the ministry of finance and the Reserve Bank of India (RBI). The suitable technological solution should be the one that is principally and architecturally designed for governments to reinforce the authority as the sole source and controller of the supply of the digital rupee.

M C ESCHER, WOODCUT, 1938

Fish of a feather stick together

The security strength of the digital Indian rupee is built from hardware and security elements beyond software cryptography algorithms. It does not rely on a large number of public keys. So, it cannot be compromised by any key loss or theft. New security features can be easily added to the currency in circulation as new security technology becomes available.

In a breach, the solution must detect, stop and remove that particular counterfeit rupee in circulation without effecting the other rupee or make previous transactions invalid.

The digital rupee is a bearer instrument that is transacted cost-efficiently in existing digital payment systems. It allows the existing digital payment service providers to preserve their system investments, customer relationship, user experience, user devices (including basic phones), user cases as well as merchant and agent networks.

It enables interoperability at the accounting level, thereby eliminating the costs and risks of the subsequent intermediary settlement between digital payment service providers.

With interoperability being a key feature for this currency, more prevalent inclusion of the entire population, banked and unbanked, to the digital economy will ensue.

These characteristics are also broadly in line with the principles detailed by the Watal Committee for an effective digital fiat currency solution: namely, ownership, technology and infrastructure neutrality.

It is the next step to provide a government-issued digital currency to bring innovation, competition, better consumer protection, more open access, better systematic risk management and more regulatory transparency in the digital economy.