BITCOINS ARE HERE TO STAY: ARE WE READY?

Dr. Chamath Keppitiyagama
Senior lecturer, University of Colombo School of Computing, Sri Lanka
E mail: chamathk@gmail.com

Bitcoin is a cryptocurrency that is not under control of any single authority or an organization. All the bitcoin transactions are recorded in a public, distributed ledger. The bitcoins exist in this ledger as chains of transactions. This ledger is represented as a chained collection of blocks-of-transactions. A bitcoin miner adds a cryptographic hash to a block and once this hash is accepted by a majority of nodes in the network, it is extremely hard (almost impossible) to change the recorded transactions. Huge amount of computing power has to be spent by the miner to calculate this cryptographic hash. However, once this hash is calculated it is extremely simple to verify that it is indeed a valid hash. This hash is a proof that the miner has spent sufficient computing power to protect a block and as a reward for that work the miner gets new bitcoins. This is the only way new coins can be minted in the bitcoin system. As time goes on mining becomes harder and harder and the rate at which the bitcoins enters into the system goes down. This is how the bitcoin system controls the money supply without a central bank. The owners of bitcoins are not really people or organizations, but public/private key pairs. Therefore, bitcoins provide certain level of anonymity to transactions. This anonymity can be further enhanced by techniques such as bitcoin mixing. There are more than 3 million unique users of bitcoins and more than 100,000 organizations accepts bitcoins for payments worldwide. Are Sri Lankan organizations, law enforcement, security establishment, and regulators ready to face the challenges and opportunities in this new economic environment?