Bitcoin buyers looking for privacy

As bitcoin is becoming a part of the finance sector, many ask for improvements that it must go through in order to hit the mainstream.

One of the problem that buyers of bitcoin are facing is the lack of privacy when going through the transactions is the pseudonymous nature, where people can track particular buyers.

As the block chain is an open ledger, it is possible to track the biggest wallets pretty easily.

As the reason for buying bitcoins might not always be public-friendly, and there might be risk involved when tracking the buyer.

Customers now demand more privacy for their transactions which will make them feel secure and not worry about who is tracking whom.

However, actions for it have already started taking place as a group of scientists at Saarland University in Germany, known as the “ Cryptographic Systems,” are finding out ways to make buying bitcoins more secure.

The leader of the group, Aniket Kate quotes “ They are pseudonyms through which users perform and publicly record transactions. If those pseudonyms can be tracked back to the real initiators, the anonymity of Bitcoin is broken.”

So, to make sure that all transactions are kept private, buyers of bitcoins are now using dark wallet or switching to some altcoins like Darkcoin.

By taking a new method known as “ transaction mixing,” the transactions cannot be detected, keeping the people involved anonymous.

However, a problem remains. The mixer of those transactions, known as Master nodes, cannot be guaranteed of being trust-worthy themselves.

As the “ mixing” is done manually, there is no guarantee that the 3rd party involved will not track the buyers themselves, ultimately taking the buyers to the very beginning of the problem.

However, Cryptographic Systems have already taken actions to solve this once and for all.

They have turned up with what is called Coinshuffle, where the user follows a few set of rules and takes a few actions which ultimately leads them decode an encrypted list of buyer’s addresses and after adding his own, passes it to the next buyer.

And when all the addresses are there, the root of each transaction’s buyer cannot be traced back as it is now shuffled and jumbled up.

Their Python programming language system is so efficient that 20 users can have their work done in 20 seconds, saving loads of time for people with multiple transactions.

CoinShuffle is the first solution that doesn’t require much and provides on-the-spot anonymity and is a breath-of-relief to all those who are involved in the Bitcoin buying and selling.