**Introduction to cryptocurrency - PART-II**

[**Shoayb Khan**](https://nation.com.pk/Columnist/shoayb-khan)

October 09, 2021

“There will never be another Bitcoin”

Flashback to 2008: “Satoshi Nakamoto” didn’t create bitcoin to get personally rich. He/she/them created bitcoin to allow smooth online payments to be sent directly from one person to another without requiring trust or permission of anyone else just like Central Banks or regulating entities. Over 99 percent of altcoins were created to enrich their founders and by rough measure, over 80 percent of them have no future. None of them is as secure, as decentralised, or launched as fairly as bitcoin. Bitcoin has the most users, largest infrastructure, no premine, no developer fund/tax, no leader, the longest track record, is the most secure, is the most decentralised and bitcoins were circulated freely for 18 months before ever having any monetary value which can never even be replicated by an altcoin because the genie is out of the bottle now. And unlike the founders of every altcoin, Satoshi Nakamoto never cashed out, at least not yet. The issuance schedule and maximum supply of bitcoin are both clearly defined and will never change. Bitcoin development is decentralised and anyone can contribute because Satoshi published bitcoin under the MIT license so that it’s open source and anyone is free to do anything with the source code. Bitcoin protocol rule changes are also decentralised because they require nodes to come to a consensus. All of this is why bitcoin is so vastly different from alternate coins or Altcoins.

[US President Biden will soon talk to PM Imran Khan: Wendy Sherman](https://nation.com.pk/09-Oct-2021/us-president-biden-will-soon-talk-to-pm-imran-khan-wendy-sherman)

Cryptocurrency, especially altcoins, are full of traders willing to take that thrill ride in the market which ends up in gambling; people that actually believe the lies because they’ve been sucked into altcoin cults. They aren’t aware that Gary Gensler, the current Chair of the SEC, just said that “a lot of crypto tokens, I won’t call them cryptocurrencies for this moment, are indeed non-compliant securities” a month ago. In addition, nobody told them that the SEC disregarded previous claims made by Bill Hinman, former director of the SEC’s Division of Corporation Finance, who suggested that offers and sales of ETH are not securities transactions. Nevertheless, enough about that.

If you properly handle your private keys, then your bitcoin can’t be stolen or seized and nobody can stop you from sending it to anyone else for any purpose.

Any protocol rule change that doesn’t make any previously invalid blocks now valid is called a soft fork. This would be a miner upgrade and is easier to accomplish, we can give the mining nodes a chance to upgrade—“BIP9” can be used, or the nodes can just run compatible software.

[Zahir Shah appointed as deputy chairman NAB: sources](https://nation.com.pk/09-Oct-2021/zahir-shah-appointed-as-deputy-chairman-nab-sources)

There is a maximum supply of 21 million bitcoin, and that will never change. Satoshi Nakamoto designed the protocol so that miners (transactions’ auditors) solve a block every 10 minutes on average. The block reward started at 50 BTC. The block reward is divided by 2 every 210,000 blocks or 4 years if the hashrate remains constant, which we call the block reward halving. The block reward is currently 6.25 bitcoin and the next block reward halving will happen around April 2024. Then the block reward will be 3.125 bitcoin. The mining difficulty adjusts every 2016th block which is approximately 2 weeks. So if it’s profitable for people to mine, the mining difficulty increases. However, if the price of bitcoin lowers so that some hardware is unprofitable to run, then it gets turned off and the mining difficulty decreases. And as the block reward gets divided by 2 every 210 thousand blocks, the transaction fees will continue to incentivise miners to secure the network even when the block reward is minuscule.

[Facebook apologizes for second outage in a week, services back up](https://nation.com.pk/09-Oct-2021/facebook-apologizes-for-second-outage-in-a-week-services-back-up)

Many users here like to repeat that the last bitcoin will not be mined until 2140. And while it is true that the last satoshi will not be mined until 2140. It is also true that approximately 97 percent of bitcoins will be mined by 2032, and the block reward will just be 0.78125 BTC at that time. But if bitcoin is worth, for example, a million dollars, then the block reward alone in 2032 would be worth more than the current block reward + transaction fees at this time. That is not even accounting for all of the transaction fees that the miners will also be collecting from the transactions that they include in blocks.

Money (not fiat currency) always evolves in four stages. Bitcoin is currently going through the second stage of the evolution of money, which is a store of value. The next stage is a widely used medium of exchange. Bitcoin may evolve into the third stage in 5 years, in 7 years, in 12 years, or bitcoin may never evolve past the second stage. The final stage of the evolution of money is a unit of account. Bitcoin is also currently going through price discovery. Bitcoin’s true value needs to be found before it will ever be a widely used medium of exchange The lightning network must also be adopted by users, merchants, and exchanges before it’s even possible for bitcoin to evolve into a widely used medium of exchange.