This volatility of Bitcoin is also considered by many to be its primary weakness, as the currency is driven purely by demand and supply and does not have an underlying value to it. Entrepreneurs saw an opportunity in this and focused their attention on creating cryptocurrency based on assets like diamonds, gold, real currencies (e.g. US Dollar, Japanese Yen, Chinese Yuan or Euro) oil, real estate and even carbon credits!

Over the last few years, the markets which have attracted the most attention are those in cryptocurrencies (cryptography-based, decentralised virtual currencies) best exemplified by its torchbearer, namely Bitcoin. However, the ride for these assets has been far from smooth. Bitcoins went from being valued at about $1,000 in the beginning for 2017 to nearly $18,000 by January 2018, before falling back to below $3,500 in January 2019.

This volatility of Bitcoin is also considered by many to be its primary weakness, as the currency is driven purely by demand and supply and does not have an underlying value to it. Entrepreneurs saw an opportunity in this and focused their attention on creating cryptocurrency based on assets like diamonds, gold, real currencies (e.g. US Dollar, Japanese Yen, Chinese Yuan or Euro) oil, real estate and even carbon credits!

As diamond-backed cryptocurrencies fire up, they would need to source the diamonds from the real market.

The Reserve Bank of India (RBI) in its circular dated April 6th, 2018, banned entities regulated by the RBI from dealing with or providing services to any individual or business entities dealing with or settling Virtual Currencies. The circular was upheld by the Supreme Court of India.

Effectively, this bans banks and money changers from dealing with any individual or company residing in India for transactions related to virtual currencies or setting up a Virtual Currency exchange. This breaks the link between Virtual Currencies and the real world, making it impossible to transact in any product from India.
Diamantaires, who are traders by nature, have been tempted by these developments and it is critical for them to have a greater clarity in how these markets work and what they might want to look for before they decide to take the plunge.

**Trust-less Digital Cash**

Having a basic, non-technical understanding of how some of the underlying technologies work is necessary to get a better idea of the products.

Traditional currencies, like the Indian Rupee or the US Dollar, have long moved from being backed by assets, like gold, and are essentially an “I owe you” (IOU) note being issued by the concerned government. Its value essentially depends on whether you trust the issuer will make good on their promise. The confidence enabled individuals to freely exchange this cash during transactions, without need for further trust.

The need for trust becomes more important when this is extended to the digital realm, where mutual trust is required between financial entities like banks, credit card companies, clearing service providers, etc. for transacting electronically, which is why these entities are regulated. Fiat money issued by governments, which is stored electronically, can also be considered as digital currencies. Digital currencies which are not issued by governments or regulators are also known as virtual currencies (e.g. loyalty points, in-game currency, etc.).

Cryptocurrencies are a kind of virtual currency designed to be de-centralised with no single issuer and secured using cryptographic techniques. Hence, this is also a trust-less system, wherein transactions can be made with the currency, even when no party trusts the other – almost akin to cash transactions. This cash-like transaction capability also provides near anonymity, which further endeared cryptocurrencies to early adopters. Cryptocurrencies do not have a central server but are hosted across many computers connected to each other or peer-to-peer systems.
Blockchain driving Cryptocurrencies

Cryptocurrency systems need to maintain the balance for each account, like that of any electronic wallet or bank account, and for doing the same, they carry a copy of the entire ledger of the transaction history. The technology which carries this digital ledger in a manner which cannot be changed or tampered is commonly known as the blockchain technology.

In blockchains, valid transactions are processed in batches, called blocks. Each block is processed through a cryptographic (i.e. encoding) algorithm to generate its unique code, also called hash. The algorithm is also known as the hashing algorithm. The hash of the previous block and the valid batch of transactions are passed through the hashing algorithm to generate the hash for the current block. In turn, the hash generated for the current block is used for generating the hash of the next block. Hence every block is linked to its preceding and following blocks, forming a chain, which is why this is called a blockchain.

Transactions are not confirmed until they are written into a completed block. The computers which collect and combine these new transactions, do the necessary mathematical calculations required for hashing, and create new blocks, are called blockchain miners.

The hashing algorithm generates a unique value for a given input. Even making the smallest change in the input value, will lead to a totally different hash value. The hashing algorithm
used for a particular blockchain is public, making it extremely easy to check if the transactions in the block generate the hash value of the block. If any of the transactions have been changed, the hash value of the block will not match, immediately invalidating that block. This ensures the immutability (unchangeable nature) of the transactions written into the blockchain.

While the above technique ensures that data in the ledger cannot be changed, making the system truly de-centralised requires two additional pieces. Firstly, there need to be multiple copies of the blockchain data to prevent manipulation as well as a wide base of computers mining new blocks.

Computers called nodes, which hold copies of the entire blockchain data, check the validity of all transactions before accepting every new block. They then transmit this valid data to other nodes. A majority of the nodes in the system need to accept the block before it’s accepted into the blockchain, ensuring that no individual node can corrupt the data. Nodes are passive, and do not need significant resources. Larger blockchains have over 10,000 nodes making them more decentralised in nature.

In his 2008 paper, Bitcoin founder Satoshi Nakamoto, brought in the concept of competition into blockchain mining, to ensure that the blockchain remains de-centralised and everyone has a clear view of the entire blockchain landscape.
Compared to commodities, where prices fluctuate every second, diamond price movements might seem glacial.

**Coins & Tokens**

While Bitcoin was the first blockchain, latter platforms were able to record and execute even smart contracts. Products running on their own independent blockchain infrastructure are classified as coins. Tokens on the other hand are basically smart contracts which run on another blockchain platform, without creating their own infrastructure. Most asset-backed “coins” are essentially tokens.

Tokens require minimal programming and are surprisingly easy to create and sell to the public through events called as Initial Coin Offerings (ICOs), though they actually refer to tokens! Savvy programmers can launch a token in hours, which is why token companies usually have only a few technical experts.

There are currently between 2,000 and 2,500 “coins” which are traded.

**Asset-backed Coins**

Bitcoins were created to serve as a medium of exchange, however demand and supply fluctuations could cause sudden swings in prices, with fluctuations up to 10% in a day having been recorded. This scares potential users. Hence, ICOs have seen a slew of asset-backed coins being launched, where there are real assets underlying the coins. Underlying assets are supposed to provide a price stability to the coin, thereby making it more attractive for users. As we all know, diamonds are an asset in their own right. While prices might not have appreciated over the last 5-7 years, many users and financial market participants view stability as a virtue as well. Compared to commodities, where prices fluctuate every second, diamond price movements might seem glacial.

This relative price stability has led to launches of diamond-backed coins. There are some interesting releases, like one coin creating a diamond listing and sales website (like IDEX or Rapnet) with transactions paid in their coins. One company has even proposed...
When analysing a couple of serious diamond-backed ICOs, the structure looks like an asset-backed (diamond) fund.

an ICO based on prices of lab-grown diamonds, though they do not clarify details about the mechanics yet!

**Old Fund in New Bottle**

When analysing a couple of serious diamond-backed ICOs, the structure looks like an asset-backed (diamond) fund. The funds promise the usual ability to invest in smaller units – ability gained from the overall value appreciation by investing in the underlying portfolio of certified diamonds – and have reputable diamond industry participants as partners.

As in the past, the primary investor concern is the confidence in the value of the portfolio of diamonds, leading to setting up a mechanism for regular third-party audits, separate depository holding, sealed diamond inventory and the facility for investors to redeem coins by buying diamonds.

Valuation mechanisms usually have complex-sounding algorithms with artificial intelligence thrown in for good measure, with a view to attract buyers for the ICO. Everyone in the industry knows that most large diamond companies have had similar pricing algorithms in place at least for the last 8-10 years, without the artificial intelligence of course!

Regular asset-backed funds and financial products like diamond futures contracts are highly regulated. Governments have a history of regulating and monitoring these products, with clear rules which need to be followed as well as clear disclosures which need to be made to investors. In fact, some diamond-backed fund products would have to be sold only to institutional buyers and high net-worth individuals, who have the capacity to understand and analyse the products.

ICOs can be launched on the basis of a simple white paper. Marketing these fund-like products as coins may allow the promoters to indulge in regulatory arbitrage and escape detailed scrutiny. This greatly increases the chances of hidden costs, inadequate disclosures as well as mis-selling of the product.

**Show me the Money**

When analysing any financial product, be it a fund or a coin, understanding the business model of the promoter is a good indication of whether it is sustainable. ICOs are clearly trying to cash in on the current speculation in cryptocurrency. Investors hope to get in early and benefit from the appreciation as the usage of the product takes off. Promoters usually allocate a significant portion of the coins for themselves.

Liquidity is the life-blood of any financial product, including coins. Liquidity gives investors the confidence that they can exit the investment without a heavy penalty, which in turn will sustain the coin infrastructure. Hence coins are hesitant to levy any charges on transactions or for maintenance of the coins, unlike in asset-backed funds.
In asset-backed cryptocurrency, coins can only be issued against assets. Hence, if no coins can be issued to promoters in the ICO, other innovative options, many of which are also drawn from funds, are used. These include charging fees, either for buying the coins or on redemption, having a coverage ratio which is less than coins issued (i.e. the assets held is a fraction of the total money invested in the coin).

Coins can also have restrictive redemption options, including only allowing redemption through delivery of physical diamonds. At times, even the purchase of diamonds into these coins is through associate companies. These coins imply that their prices are at near wholesale level, however a quick check by the author indicated prices seemed to be 15-30% above wholesale prices! This would not be possible with regulated funds.

Going forward, anonymity provided by cryptocurrencies, which was treasured by participants of unauthorised markets, will be lost. However, in the long run, this might be for the good as only the persons who are genuine traders or investors in the virtual assets or currencies will remain.

Changes to FATF Recommendations

Money-laundering risk in cryptocurrencies is a known problem, as entities could trade almost anonymously. In October 2018, the Financial Action Task Force (FATF), the world body which is focused on anti-money laundering and countering financing of terrorism, amended their recommendations to include virtual asset service providers (i.e. exchanges, companies launching the currencies, etc.) under the list of entities that are to be regulated. Individual governments who are part of FATF would be expected to make the necessary changes into their respective local laws.

Virtual asset service providers like wallets and coin issuers will now need to be licensed/registered and subject to same monitoring and relevant compliance practices followed by other financial institutions like KYC, suspicious transaction reporting, etc.

Going forward, anonymity provided by cryptocurrencies, which was treasured by participants of unauthorised markets, will be lost. However, in the long run, this might be for the good as only the persons who are genuine traders or investors in the virtual assets or currencies will remain.

Pranay Narvekar is the CEO of the G&J KYC Information Centre. He is also a partner at Pharos Beam Consulting LLP. He is a leading expert on demand and supply, strategic, financial, and structural problems of the diamond industry. He has over 15 years of consulting experience, and had worked with Rosy Blue for nearly eight years. Narvekar has completed his B.Tech from IIT Bombay and Postgraduate Diploma in Management from IIM Lucknow. pranay@pharosbeam.com

Closing Thoughts

The diamond industry needs diamond-backed financial assets in order to successfully channelise the latent demand for investment diamonds. However, in their current form, diamond-backed coins look far too flawed to become a sustainable and healthy product.

For a diamantaire or an industry service provider, selling diamonds into these products should be similar to any other customer, as long as the payment is in normal currencies (though in India it would be prudent to check whether RBI regulations will allow US Dollar payments from coin companies). For diamantaires looking to sell their diamonds for cryptocurrencies, all one can say is Caveat Venditor or seller beware!