Blockchain and Crypto-currencies

By Adam Hayes
Co-Founder & CEO, ChainLink

and Paolo Tasca
Economist, Deutsche Bundesbank

The notion of an entirely digital form of money has captured the curiosity of economists, computer scientists, and philosophers alike from the time the computer was still young. There was, however, always the nagging problem that a currency consisting entirely of ones and zeroes could be exactly copied over and over again, the same way that ones and zeroes allowed for the infinite duplication of audio in the form of compact discs. What good is money that could be counterfeited at will? The solution, which spawned bitcoin and its various daughter digital currencies, was the marriage of cryptography and decentralized networks. Both technologies had existed independently: cryptography, useful in encoding email messages, sensitive information and digital files; decentralized, distributed networks with ARPANET giving birth to the internet.

How Does Digital Currency Work?[1]

In 2009, Satoshi Nakamoto satisfied the long-held curiosity of economists, computer scientists, and philosophers with the creation of Bitcoin. The system relies on a disparate network of participants, each trying to essentially break an encrypted message. Rather than the nodes of the network working together in cooperation, Nakamoto put them in competition with each other to solve this puzzle with the first to do so winning a prize: a block of newly minted bitcoins. This became known as "mining" for bitcoin. Furthermore, the system was hard-wired with a certain rule at the outset: a new block would be found on average once every ten minutes; if more participants enter the competition and the time to solve the puzzle shrinks to say eight or nine minutes, the difficulty of the puzzle will be increased to re-establish that target time.

Let us take a roulette wheel at a casino as an analogy for bitcoin mining, where the prize for landing on double-zero is a block of bitcoins. There are 36 numbers on the wheel, plus a zero slot and a double-zero. The chance of the ball landing on double-zero is one out of 38. The casino owner knows that 38 games of roulette can be played over a 10-minute interval, and wants to ensure that there is only one winner per given interval. As one final rule, in our hypothetical example, only one player can sit at a single roulette table at a time.

A second player enters the casino and sits down at a second roulette table. The owner of the casino is upset to see that twice as many games can be played in any given period, and that in fact he is now paying out to two winners every 10 minutes. The casino owner restores his target payout interval by increasing the number of slots on each roulette table. As a third, fourth, tenth, hundredth etc. person walks in the casino to play at their own private roulette table, the casino owner must keep increasing the size of the wheels.

It is important to remember that each spin of a roulette wheel is an independent trial: the chances of the ball landing on a black number do not increase merely because a string of red numbers has occurred. Bitcoin mining, and our increasing roulette wheel size analogy, is also a series of independent trials performed in tandem by competing players. Good luck may produce two winners in a row, even though the odds have increased to one out of 38,000 instead of 38. But just as in a fair coin tossed over and over again, the long-run average will revert to the expected mean, and our casino owner – and bitcoin miners – can always expect a payout once every 10 minutes.

Bitcoin mining serves a dual purpose; it is not merely the method of introducing newly created bitcoins. Of more importance, it serves to validate and confirm each transaction on the network, creating a tamper-proof data structure underlying the system known as the *blockchain*. The blockchain is essentially a public ledger which everybody mining for bitcoins has a copy of. Every time there is a winner, each copy of the blockchain is updated and all the transactions that have taken place in between this winner and the last are recorded indelibly into it.

Again, consider the roulette wheel. Not only are there people playing simultaneous games of roulette, but there are also non-players who are simply taking side bets on the action. Only when there is a double-zero will those side bet transactions be confirmed.

[1] For more on how digital currency works, see https://bitcoin.org/en/faq. To avoid confusion, we use *Bitcoin* (singular with an upper case letter B) to label the protocol, software, and community, and *bitcoins* (with a lower case b) to label units of the currency.

Bitcoin works in much the same way: miners compete with each other to solve a puzzle just like the roulette players hope to score double-zero. As more miners enter the game, the problem gets more difficult to solve, maintaining a 10-minute interval between creating new bitcoins. All the while, people are transacting with bitcoin to buy and sell goods and services, to speculate on its price, and to pay wages. Each time a miner solves the puzzle, all of those accumulated transactions are validated and confirmed in the blockchain. The important difference between bitcoin and our casino is that bitcoin has no owner, and no central authority to oversee it. Rather, those rules were hard-wired into the initial code and agreed upon by its participants.

While that is all very clever, it is fairly self-serving: bitcoin mining finds new bitcoins and at the same time validates and confirms internal bitcoin-bitcoin transactions. But what if this same powerful time-stamped validation engine could be harnessed to confirm and verify *external* non-bitcoin specific transactions?

Bitcoin 2.0 and Future Trends

Until now, the most important manifestation of blockchain technologies has been Bitcoin. However, anything that requires trust or proof is a good candidate for the blockchain, as bitcoin miners will naively validate and confirm those transactions too – because those miners are always trying to solve the next block and earn bitcoins as a reward. Title of ownership, deeds, contracts of all shapes and sizes, and notary, are examples of information that can be permanently recorded into the blockchain – and which can unambiguously be transferred to subsequent owners without the need for a central authority. This has huge ramifications for how business is transacted and may prove disruptive to everything from the legal to the financial sector.

Indeed, after the first wave of early enthusiasts and overly ideological bitcoiners “blinded” by their belief in a rapid displacement of the US dollar and other hard currencies, the Bitcoin community started focusing on alternative applications of the underlying blockchain technology.[2]

Most of these Bitcoin 2.0 applications are still at their dawn, but they promise to improve the architecture of transaction-based industries. We envision four categories of blockchain technologies that will impact the financial industry: digital currencies, asset registries, application stacks, and asset-centric technologies.[3]

Digital Currencies

At the time of writing, there are over 500 alternative *altcoins*.[4] These are digital currencies much like bitcoin, with specific monetary supply mechanisms and transaction networks. We glimpse a future characterized by the creation and diffusion of community-based digital currencies that will be used in closed-form environments as tools for internal rewarding, customer loyalty programmes, or incentive and governance schemes. The communities will either be organized via state institutions or by private corporations who will issue their own specifically branded “coins”. There are already platforms which allow anyone with a rudimentary knowledge of software programming to create their own digital currency according to their own unique rules and usage limits within the community and the organization. Moreover, there are already payment networks such as Ripple, enabling various digital currencies to be sent easily between members.[5] In the near future, it will be possible for every single smartphone user on the planet to possess a digital wallet for each branded coin, instantly exchangeable in the form for example of loyalty points, for other altcoins, or for hard currencies. This all functions under the auspices of a unique global market with a distributed, decentralized clearing mechanism. This will massively upgrade transaction efficiency and increase the currency-utility of reward.

Asset Registries

These applications refer to the possibility of linking real assets (stocks, bonds, certificates, etc.) to a digital token which can then be exchanged among network users by simultaneously transferring ownership of the underlying asset. The changes of ownership are automatically registered and recorded in a multi-asset public ledger without the need for a central authority or for any institution to provide clearing and settlement services. For the time being, the technology still needs refinement. Critical issues include the potential for overloading the blockchains

[2] On this matter, an interesting comment was given by the Reddit CEO (Mr Yishan Wong), who praised the technology but called out the bitcoin community for being overly ideological. See http://www.coindesk.com/reddit-ceo-thinks-world-dogecoin-slams-crazy-bitcoiners/.

[3] See Paolo Tasca (2015), Digital Currencies: Principles, Trends and Opportunities, ECUREX Research Working Paper.

[4] See https://cryptocointalk.com /forum/178-scrypt-cryptocoins/.

[5] See https://ripple.com.

with additional external data (a phenomenon referred to as "blockchain bloat") that will require additional mining power and create scalability problems.[6] Thus, although asset registry applications have already been brought to the market (examples include Mastercoin (now OmniLayer),[7] ColoredCoin,[8] Namecoin,[9] and Counterparty[10]) at the moment, the banking industry at large cannot fully exploit the potentialities of this technology. The good news is that solutions such as *sidechains* are being implemented to solve the bloat problem, and in the near future asset registry applications will indeed be a common tool used by the whole of the finance industry.[11]

Application Stacks

These are "non-currency" blockchain-based platforms that will be used for the development and execution of complete applications on top of decentralized networks.

By complete applications we mean Distributed Autonomous Organizations (DAOs). Any business organization can be defined as a combination of a set of properties and also a set of rules which govern the roles of, and interaction among, the individuals composing the organization. The idea of DAOs takes the traditional concept of business organization, decentralizes it, and encodes a division of labour between Artificial Intelligence agents and humans under the control of a verifiable and incorruptible set of enterprise rules. Thus, DAOs are established by employing a decentralized network of autonomous agents, each of which perform output maximizing production functions according to pre-established rules which are auditable, open-source, and distributed across the processing power of their stakeholders (who are humans or even other DAOs). DAOs are the most complex form of decentralized automation to date. Simpler forms of this concept consist of smart contracts, autonomous agents, decentralized applications, and decentralized organizations.[12] Current application stacks that allow for implementation of decentralized automation are NXT, Ethereum, and Eris, which distinguish themselves based on their core focus.[13]

Asset-Centric Technologies

Asset-centric technologies are based on a new concept of distributed consensus which gets rid of the expensive and resource-wasting *proof-of-work* system which is the default consensus mechanism utilized by Bitcoin.[14] Stellar, Ripple, Hyperledger, and Namecoin are the most famous examples of asset-centric technologies.[15] These decentralized ledger infrastructures allow for the exchange of real assets like currencies, metals, stock, or bonds and in some cases even without the need to use a native digital token as in the case of Hyperledger.[16] The element that distinguishes these asset-centric technologies with respect to the other blockchain-based technologies described above is the fact that these represent distributed *exchangers* where network users can exchange among themselves various heterogeneous real assets.

Conclusions

An entirely digital, decentralized, peer-to-peer currency is now a reality. Bitcoin has ushered in the crypto-currency age, for better or for worse. The potential for crypto-currencies to revolutionize money and disrupt finance is enormous, but it is only the beginning. Perhaps even more important is the blockchain, the distributed ledger data structure which crypto-currencies rely on. Capital investment in blockchain-related start-ups is a recent trend that started only in 2012; however, since then, the annual growth rate of investment, 150% year over year, is faster than even the dot-com boom. Blockchain applications spanning a number of sectors promise to

[6] In June 2015, it was announced that the maximum block size for the Bitcoin blockchain would be increased to 8 MB.

[7] See http://www.omnilayer.org/.

[8] See https://www.coloredcoins.org and https://www.coinprism.com.

[9] See https://namecoin.info/.

[10] See https://www.counterparty.com.

[11] Sidechains are separate and distinct from the main bitcoin blockchain, but which would be interoperable with a two-way peg. This could allow for the transfer of assets between the side-chain and the main blockchain, without eating much storage space. See the paper "Enabling Blockchain Innovations with Pegged Sidechains" at http://www.blockstream.com/sidechains.pdf.

[12] More information of decentralized automations can be found here: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

[13] See http://nxt.org/, https://ethereum.org/, and https://erisindustries.com/.

[14] By one estimate from 2014, Bitcoin consumed as much electric power as the entire country of Ireland. See http://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf.

[15] See https://www.stellar.org, https://ethereum.org, http://hyperledger.com/, and https://namecoin.info/.

[16] Unlike Bitcoin, Stellar, Namecoin, or Ripple, Hyperledger does not have an in-built digital currency but at the same time it guarantees a distributed ledger base which gives each participant freedom in choosing which combinations of other participants to trust.

change the way companies and people transact, send payments, sign contracts, transfer ownership of things, and much, much more.

The hope is that this new technology will instead turn the digital divide, among and within our countries, into digital opportunities. The reduction of transaction costs and the elimination of costly – and sometimes obscure – layers of intermediation have the potential to favour financial inclusion for the benefit of society.

However, blockchain technologies will also introduce new risks to users and market participants as well as new risks to financial integrity: e.g., fraud, money laundering, and cyber-crimes. Therefore new forms of “tech regulation” should be designed and implemented in order to boost innovation and guarantee market stability in those new areas that will be affected by the adoption of blockchain technologies.