Blockchain - what is it good for?

By Peter Christo – July 2021
twitter.com/peterchristo | linktr.ee/peterchristo

In 2009, Satoshi Nakamoto released a paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System.* Its promise was for a peer-to-peer electronic cash system that allowed online payments without going through financial institutions.[1]

At its core is a software called blockchain. The first successful use case for blockchain was bitcoin (uppercase 'B' for the software, lowercase for the money). Bitcoin evolved from a digital collectable into the world's first public money and the most popular cryptocurrency valued at over $1 Trillion U.S. dollars market capital value in the first half of 2021.

Among other things, bitcoin and some other cryptocurrencies hold genuine promise for unbanked communities and those who rely on remittances to survive. All run on some incarnation of the original Blockchain system designed by Satoshi.

Some believe that bitcoin et al. has created regulatory and financial challenges for the world to solve. However, some see opportunities for blockchain to solve problems in other areas outside money and finance.

The underpinning leap in logic could be described as follows – Bitcoin has proved to be a revolutionary innovation in digital money. It has several positive features, including zero hacks in 12 years, immutability and fungibility, transparency etc. How can this technology be applied to other problems to improve our economy and indeed deliver a positive to humanity?

This paper seeks to shine a light on what might be an answer to that question. To understand the potential magnitude of projects underpinned by blockchain, we need to first dig into bitcoin to understand what made it a success.

Bitcoin is controversial and, to the uninitiated, polarising. Even if you are not a believer in bitcoin as new legitimate money, consider the following: Bitcoin has operated outside anyone's ultimate control for many years. It has remained censorship-resistant, transparent, and uses a robust and, to date, uncompromisable consensus system. It relies on maths and computational power to operate and prevent a single entity from dominating the system, which is by anyone's measure miraculous. It could be seen as akin to the discovery of electricity or, indeed, fire.

Blockchain 101

As a first step, let's understand blockchain and how it compares to a traditional computer system. To keep it simple as possible, imagine an accounting software that operates a ledger of transactions (this is basically what your bank does). There are additions (credits) to the account and deductions (debits). There is a running balance resulting from what you started

---

[1] https://kryptoconnect.io/cryptocurrency-article/bitcoin-a-peer-to-peer-electronic-cash-system-satoshi-nakamoto/

with, minus what was paid out (including fees), plus what you received (e.g., opening balance $10; coffee payment $3; employment income $20, final balance = $27).
A centralised computer can do that and users can access their accounts only after proving who they are. Verification of ownership used to be done via a visit to a branch, a passbook or producing identification. Now it is done via the internet, an app with a login password and username, which then allows for other things like payments and remittances.

Bigger banks may run these computers in a distributed way, which means they run multiple computers across different locations. They connect them via the telecommunications system or the internet to assure transaction speeds, offset high load times, and create numerous real-time copies. It means the system is available and working when you and other users need it. When you are in a store and find the bank system is down, the central computer has a technical problem, so you likely can't get cash out or pay for your purchase electronically.

These computer systems need the highest level of security to ensure our money and data is not stolen or accidentally deleted (N.B., your balance is a record of a number on a database at the end of the day. Only about 10% is in actual cash form out in the economy).

On the other hand, bitcoin's blockchain works as follows below. Again, there is much more to it, but this is a ‘bare-bones’ view:

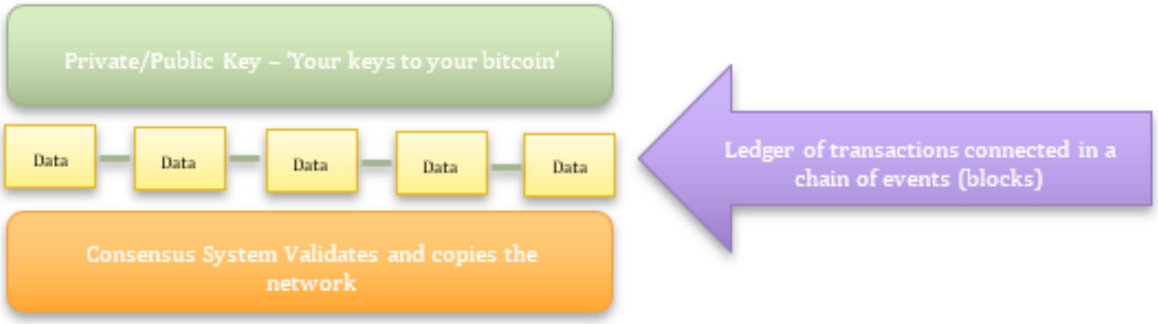
The key elements are:

1. Blockchain refers to an **open-source software program** whose purpose is to maintain a ledger of value exchanges or transactions. It is widely agreed that the use-case that has been solved now via bitcoin is money. Using bitcoin, you can pay anyone anywhere as long as they have a bitcoin wallet and a connection to the internet, which aligns with our example above.
2. Blockchain works by **running the bitcoin (known as bitcoin core) software concurrently across many computers**, which 'talk to each other' to agree on what transactions are valid; this is referred to as a consensus protocol (note the similarity to the distributed computing example above).
3. These computers communicate to **verify and agree whether their copy is valid** (no tinkering with accounts allowed). Having done that, reach a verified 'consensus' of the ultimate source of 'truth' (essential for our money).
4. The nodes also keep a **copy of all transactions as a record stored in bundles of transactions called 'blocks'** verified periodically and connected via a digital chain of these records, hence a 'Blockchain'.
5. Finally, the way we interact with the ledger is via a **private and public key**. These are simply two strings of numbers and letters, one kept secret and one that can be made public, allowing the systems to talk to each other). There is complexity here on how these are generated, stored and used by the average person. For the moment, think of that as a banking app that allows us to pay anyone and received payments.

The result:

1. This system **prevents a 'double spend'**, which means spending the same money twice or other fraud. It does it in a decentralised way, meaning no central computer is available to hack.
2. The public nature of the bitcoin blockchain means records **can be queried by anyone on the internet** (including the police and the tax department if they choose to).
3. The way these computers (referred to as nodes) **reach consensus (the real secret sauce) is achieved via a system called 'proof of work',** which effectively takes part in a race to guess a unique number. New bitcoins are mined (created) this way, but that is for another paper.

Here is a very simple visual.



The visual representation of the blockchain above allows the reader to imagine how a blockchain looks in its most simplistic form. Here is a much better visual representation by Reuters. [2]

A simple way to imagine the bitcoin blockchain working

A simple way to think about it is to imagine a room where people are playing bingo and checking off balls coming out of the barrel. In this case, the balls are payment transactions in a queue (rather than random balls), and the people in the room check to see they are compliant with the rules.

The first person to shout bingo has mined more bitcoin and receives a reward; the rest cross off the number (i.e., accept the transaction as valid or not).

The supply of these rewards (bitcoins) is capped at 21 Million. This is referred to as 'programmed scarcity' and is enforced by the rules embedded in the blockchain program, which everyone relies on to verify the blocks.

[2] http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

So, what worked for bitcoin?

For my money, it delivered a super synergy! The whole is exponentially greater than the sum of its parts.

By understanding why bitcoin is a big deal and is now considered so valuable by so many, we are better placed to consider the merits of new applications that seek to use blockchain and, ultimately, their likelihood of success.

Bitcoin's success can be evidenced (in part) by its adoption and its price, having offered its original investors significant returns for their patience and foresight. The price itself, however, does not necessarily equate to value. Former Google employee Michael Levin estimated that in the 12 years since inception, BTC had reached 135 million users with projections estimated at 1 billion by 2025, just four years away.

Bitcoin's adoption as an investment class has been supported by some noteworthy organisations and investors, including Paul Tudor Jones, Black Rock, Stanley Druckenmiller (SDM) and Ray Dalio, to name a few. Additionally, listed companies have added it to their treasuries, including but not limited to Tesla (NASDAQ:TLS), Microstrategy (NASDAQ:MSTR) and most recently, legislation enacted by the Government of El Salvador making Bitcoin legal tender in its country.

If we accept that the key attributes that make bitcoin valuable are;

1. **Decentralised –** no one computer or individual controls it. It is everywhere and nowhere.
2. **Transparent –** anyone can query any transaction on the blockchain.
3. **Borderless –** geography does not matter to bitcoin; it is as easy to make a payment to someone from Australia to Uganda as it is to make a local payment in person.
4. **Censorship resistant –** It cannot be stopped; anyone with a smartphone and access to the internet can use bitcoin.
5. **Private** (somewhat anonymous) – addresses can, to a degree, be tracked, but it isn't straightforward.
6. **Portable** (no hiding jewels or gold bars in your pants)
7. **Inflation resistant –** fixed supply of 21 million bitcoins there will only be (to be exclaimed as Yoda)

All this delivered a 'store of value' across time and space. There are a great many articles on whether this is or is not the case. One of the better commentators is Jimmy Song who wrote "Bitcoin: A Declaration of Monetary Independence". [3]

So, what allowed bitcoin to deliver the above attributes? Was it just blockchain?

The most straightforward metaphor I can offer is that of a chef and her recipe. You could give me the best ingredients in the world, and I would have little hope of delivering you a

[3] https://jimmysong.medium.com/bitcoin-a-declaration-of-monetary-independence-63dee34bdff9

Michelin star quality meal. Besides skills and experience, a chef can combine ingredients with time, heat, and the environment to produce a fantastic meal.

Satoshi's approach (recipe) together a bunch of things we knew worked in a novel combination to solve the money problem; His recipe included.

1. Technology (yes, the blockchain)
2. Game theory (think incentives)
3. Cryptography (think security, custody)
4. Economics (value to the holder)
5. A significant problem to solve – money!

It's all held together via the now not so secret - secret sauce, which is, independent of any individual, how it agrees to the single source of truth. Its ability to operate, synchronise and validate all the transactions every ten or so minutes, and adjusts itself to prevent any individual or group of nodes from taking over control.

Bitcoin succeeded because Santoshi's recipe delivered a framework for real consensus on a valid transaction without command and control by a trusted third party. Bitcoin succeeded because it managed to solve a problem that enough people believed was real and appeared around the 'great financial crisis of 2008-9', delivering a system that could provide money without the influence of central banks and questionable monetary policy by central bankers (Think Weimar Republic, Venezuela, Nigeria and now Lebanon).

As a result, many believe it could deliver significant innovation and solve a range of problems associated with traditional systems requiring trusted but corruptible or at least fallible third parties.

In answer to the original question therefore, what is blockchain good for? here are some use cases that are serious contenders for the next big thing in blockchain:

1. **Identity** – *"Identity verification and authentication has long been a critical component in service delivery for both the private and public sectors, but changing citizen demands in the digital age have stressed the need for new approaches to verify that an individual is who they say they are – with surety. At the same time, as more of our lives migrate online, "bad actors" such as hackers and fraudsters are always finding new ways to exploit our sensitive information for their own personal gain at the expense of legitimate users and online service organisations again and again, applicable anywhere and private."*[4]

2. **Voting** – How do you ensure legitimacy in elections via electronic voting that provides privacy and a transparent count? Voting has been a use case since the internet appeared, yet to be adequately solved.[5]

[4] https://timreview.ca/sites/default/files/article_PDF/Wolfond_TIMReview_October2017.pdf

[5] https://www.researchgate.net/publication/337022993_Election_System_Based_on_Blockchain_Technology

3. **Property Titles** - A NSW Government initiative sought to address this (private blockchain) - *"Few home-buyers know the intricate administrative processes that happen before they buy their dream home or investment property. From lodgement and assessment of D.A.s, through to construction of new, serviced parcels of land ready for sale, The Property Development Pipeline (PDP) incorporates every step. Secure, trusted movement of documents across multiple agencies is needed, but this was a decentralised, fragmented and unwieldy arrangement, involving an unmanaged information supply chain. Interactions between land owners, developers, local councils, utilities and Government were unstructured and costly."*[6]

4. **Logistics & Provenance** – From a report by EY regarding blockchain in logistics and supply chains – "*With such a huge number of stakeholders involved in the supply chain, this often creates low transparency, unstandardised processes, data silos and diverse levels of technology adoption. Many parts of the logistics value chain are also bound to manual processes mandated by regulatory authorities. For example, companies must oftentimes rely on manual data entry and paper-based documentation to adhere to customs processes. All this makes it difficult to track the provenance of goods and the status of shipments as they move along the supply chain, causing friction in global trade*".[7]

These are just some opportunities, so much so that the Australian Government considered this significant enough to release a 'National blockchain roadmap' in 2020.[8]

The promise of blockchain.

The promise that blockchain holds is real, but like the invention of the telephone or the internet, it in isolation will not deliver much beyond normally distributed computing systems unless projects consider these other elements like bitcoin did. The value needs to be more than just the sum of the parts that make up the technology. The phone became valuable not just because of one remote user connecting to another; it became exponentially valuable due to the network effect known as Metcalfe's law.

"Metcalfe's law characterises many of the network effects of communication technologies and networks such as the Internet, social networking and the World Wide Web".[9]

[6] https://www.businessaspect.com.au/publications/discussion-paper-blockchain-in-the-real-world/

[7] https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf

[8] https://www.industry.gov.au/data-and-publications/national-blockchain-roadmap

[9] https://en.wikipedia.org/wiki/Metcalfe%27s_law

Business valuations for the broader telecommunications network the world over or on a per-company basis is based on Metcalfe's law. This is also the case for Google, Facebook, Instagram etc.

I would argue that much of the blockchain discussion doesn't consider the broader elements at play that are necessary to realise its true potential and ultimate value. Metcalfe's law is part of it, but there may be more to it than that. Of course, decentralised computing has been around for decades. However, the blockchain technology system results in a communication network that can continue to operate and deliver its task as long as at least two computers are running. In fact, it gets stronger the more computers are connected to the network of nodes. Centralised or distributed systems don't have this as someone 'in authority' can turn the systems off.

For blockchain projects to be truly valuable, they need to have a pathway to a network effect and a "neural network effect" where the system can achieve decentralisation, resist censorship, and be secure while remaining open to anyone to use within the ruleset. In effect, it becomes a digital public good to solve human problems in a digital world like money, identity, ownership, provenance etc.

There is indeed a place for the private use of blockchains, and they have value to offer, but they are not the radical innovation that is bitcoin. They are an evolutionary step that will help some industries, but that still relies on an overarching control framework and authority.

Frankly, there are innovative projects in the crypto space that promise that neural network effect and solutions to solve human problems like providing financial services to the underprivileged and the poor.

As a final note, technology continues to evolve, and this is no less true for blockchain. There are many ways to skin a cat, and you'll find that things have splintered into different incarnations of what Satoshi first designed. Ethereum (ETH) is different and proposes to change again soon; Cardano (ADA) operates on a proof of stake system, a new way to deliver consensus, and many others too numerous to mention.

If you are open to a stretch in imagination, merge all this with the accelerating developments in Artificial Intelligence (A.I.) and Machine Learning (ML) and combine with the right ingredients. The human problem blockchain fixes next could be incomprehensible for us in 2021. I'll leave the last word to Jeff Booth, an entrepreneur, author, and shining light in these complex times.

"If you could fold a piece of paper 50 times, it would reach the sun. Technological change is at the early folding stage today, but each new fold doubles the growth rate and the impact. To create value in that environment, one must understand the entrepreneurial journey, commerce and the macroeconomic forces shaping our world."
Jeff Booth – The Price of Tomorrow.

Peter Christo

Peter has over 20 years working with the financial services sector, delivering payment and business innovation in a rapidly changing and highly regulated industry. He was also the founder of a number of new businesses, including co-founder of Pitch Club, a national event for entrepreneurs to pitch their ideas to investors and established Chinapayments.com.au for the Novatti Group (ASX:NOV), facilitating cross border bill payments for Chinese.

Peter is a Commercialisation Facilitator for the Entrepreneurs' Program under the Department of Industry, Science, Energy and Resources operating through the delivery partner i4Connect Pty Ltd. He holds a Masters Degree in Entrepreneurship and Innovation (MEI) and a Bachelor of Business (Economics & Marketing). He specialises in Fintech, Cryptocurrency and AI.