What is Blockchain?

For people from the “blockchain space,[1]” the term blockchain is inseparably intertwined with Bitcoin. The Bitcoin creation story is short yet profound in its consequences.

The year is 2008, the Lehman Brothers has just collapsed and a mere few weeks after that, in October, the now-famous "Bitcoin white paper"[2] was published by someone under a pseudonym Satoshi Nakamoto. The first sentence after the titles reads: "A *purely peer-to-peer* version of electronic cash would allow online payments to be sent directly from one party to another without going through a *financial institution*[3]." The goal and the motivation of this invention were further clarified when the first version of the Bitcoin software was released on January 3, 2009. In the coinbase parameter of the genesis block[4], there was a message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

The idea is straightforward. Instead of storing your money in a bank, and by doing so giving the banks an immense amount of power, which then can be used against you, you can now be your own bank. The Bitcoin software is open and transparent, the checks and balances designed for the system to be stable and prone to attacks are introduced. The code is open-source, and the concept of chaining blocks[5] is just a part of the grand design for achieving the end goal, i.e., having a financial system that is not controlled by a third party or anyone but the community of its users. Despite that, there is a need for a word to express the idea of a "decentralized distributed network," so the term "blockchain" is coined.

Bitcoin goes virtually unnoticed for years, until reports about its ridiculously high price start circulating in the news, and Nouveau crypto riche start to appear. It is fascinating that what interests most people about Bitcoin until now is just a potential for making money on speculation and not the long-term vision that Bitcoin creators undoubtedly had.

---

[1] Sometimes also “crypto space,” where "crypto" is derived from “cryptography.”
[2] Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[3] Cursive is mine. Maksim Izmaylov.
[4] https://en.bitcoin.it/wiki/Genesis_block
[5] The term blockchain was never used in the original white paper, it came to prominence much later, around 2016.

Underestimated Technology

The importance of the incarnation of these concepts in the physical reality, well, as physical as data bits can be, is easy to overlook.

First of all, none of the ideas behind Bitcoin were new. It just took a group of hackers outraged by injustice to put them together. For example, in 1998 a computer scientist and legal scholar Nick Szabo proposed a concept of a decentralized digital currency he called "bit gold" which today is considered a direct precursor of the Bitcoin architecture. A year before that Hashcash, a proof-of-work algorithm for solving email spam, was created by Adam Back, another prominent figure in crypto. It's hard to imagine that it didn't influence Szabo and Nakamoto's designs.

Quite a few thinkers anticipated the creation of Bitcoin. Some said that the government's monopoly on money would inevitably be displaced by "cybermoney," and that inflation wouldn't be a revenue option for nation-states anymore[6]. In a 1999 interview, Milton Friedman said that the role of government would be significantly reduced by the Internet, specifically mentioning the need for reliable electronic cash. Others warned that increasing centralization of financial systems leads to an appearance of stability while creating possibilities for system-wide devastating crises[7].

The changes that are brought upon us by peer-to-peer technologies, such as Internet or Bitcoin, are highly disruptive for centralized industries with high entry barriers, like telcos in 1993. Back then we, probably, had just one phone company to choose from, if we wanted to make a phone call. Today I have a whole screen on my smartphone with apps that I can use to make video calls around the world *for free*. Because these applications use open technologies, new contenders can enter the market very easily. Music, TV, film industry, publishing, classifieds, and newspapers are just a few examples of industries that were entirely transformed by the Internet.

---

[6] Davidson, James Dale, and William Rees-Mogg. The Sovereign Individual: Mastering the Transition to the Information Age. Touchstone, 1999.

[7] Taleb, Nassim Nicholas. The Black Swan: The Impact of the Highly Improbable. Random House, 2007.

The blockchain revolution that started with Bitcoin and that is now well underway, bears the same marks as the invention of the computer and the creation of the world wide web. Most importantly, all of these inventions are in the public domain. There are no patents or any other barriers that could prevent us from using these technologies and creating new things on top of them. There are already thousands of projects under development, fueled by the crypto price surge and a sudden inflow of capital available to developers because of the borderless nature of cryptocurrencies. Even the VC market is being disrupted by ICOs (or initial coin offering) that helped entrepreneurs raise $6.1 billion in 2017.[8]

Overhyped Technology

The majority of the population has never heard about Bitcoin or blockchain, but the most vulnerable group out there is people who know something about but still don't see the full picture. The recent example of that is Kodak share price doubling after their announcement of creating a blockchain-based platform for photographers. Even more bizarre than that, now the Securities and Exchange Commission launched investigations of several US companies that added the word blockchain to their names, followed by an immediate stock price surge.

Does it mean that the public positively reacts to this technology? Not necessarily. I'm afraid it happens for all the wrong reasons. An average crypto-Joe wants to see the price of his favorite coins to go up. In other words, people want to make a quick buck, inspired by the stories of early adopters of Bitcoin and Ethereum, who are now multi-millionaires. A general assumption is that it's too late to buy BTC or ETH, so Joe is always looking for new cryptocurrencies to invest in. Unfortunately, the vast majority of all the new blockchain projects are utter nonsense designed to scam Joe, but with enough marketing money poured into them, Joe is convinced to give his BTC or ETH to the criminals. Bitconnect, a classical pyramid scheme, received multiple millions of dollars from people who should have known better. As Naval Ravikant said, "Bitcoin is a tool for freeing humanity from oligarchs and tyrants, dressed up as a get-rich-quick scheme."

[8] https://www.icodata.io/stats/2017

Another dangerous fallacy is the idea of so-called private blockchains, i.e., a blockchain that is controlled by one company. But “centralized decentralization” is an oxymoron! If a blockchain is owned and controlled by one company, it is, by definition, centralized. Therefore, It is just a glorified database with some cryptographic magic sprinkled on top of it. As one of the most prominent thinkers of the blockchain revolution Andreas Antonopoulos[9] said, "... if it ain't open, it ain't worth shit." Naturally, the businesses that are afraid to lose their market position have adopted the "let's just add the word blockchain to it" strategy. I attended several airline industry meetings where some big companies were trying to convince the audience to use their BaaS (blockchain-as-a-service), supporting their argument with illegible slides that consist of colorful circles and squares connected in complicated ways and inscriptions that are too small for anyone to read. Unfortunately, when I asked the audience about their knowledge of Bitcoin and blockchain, only three people out of thirty coyly raised their hands. No one knew what they were looking at, how blockchain could be used or what it is. It was easy to see that the king was naked, but no one wanted to admit it first.

There is also an opinion that anything that uses the chained-blocks design can be called blockchain. It is as wrong as a statement that anything that uses the HTTP protocol is the Internet. Yes, HTTP is useful in many cases, but the groundbreaking change came from the combination of it with many other technologies that allow people to to collaborate in large numbers effectively[10]. Similarly, you can use cryptographic proofs (a.k.a chained blocks) to assure your business partners of the validity of your data and increase the efficiency of your software by a few percents, but that improvement would be limited to your company only. Bitcoin, on the other hand, has already created a multi-billion dollar industry that anyone can participate in by building things on top of it: better wallets, faster payment networks, etc.

---

[9] Andreas M. Antonopoulos is a best-selling author, speaker, and educator. In 2014, Antonopoulos authored the groundbreaking book, Mastering Bitcoin (O’Reilly Media), widely considered to be the best technical guide ever written about the technology.

[10] Yuval Harari in his bestselling book Sapiens (publisher, year) argues that the ability of humans to collaborate effectively and in large numbers is what sets us apart from all other living beings.

Blockchain Benefits

The original sentiment behind Bitcoin goes against common business sense. It wasn't created so a few corporations could benefit from it, just the opposite. Bitcoin is public infrastructure that anyone can use any time, anywhere on the planet. Everyone wins!

Again, it doesn't mean that chained blocks can't be applied in a context of one company, for the benefit of the reduced cost of audit. But only public blockchains can help us reduce the cost of networking[11], and increase social scalability, that is the ability of humans to effectively interact in large numbers, to transcend our Dunbar's number.[12] In other words, only networks with no entry barriers allow for massive network effects.

Peer-to-peer technologies, like public permissionless blockchains, could finally help us solve the tragedy of the commons. In today's capitalism, the goal of any business is to become a monopoly. But monopolies are bad for society as a whole, they should be avoided, so we've devised complicated antitrust laws. Big companies can work around them by moving to another jurisdiction and hiring the best lawyers money can buy, so we have to think of better laws, and so the struggle goes on and on.

With blockchain, mission-critical components of our society, like issuing currency or identity systems, could operate autonomously, so there is no risk that the party that controls those components would abuse their position. The transition will not be smooth. For example, venture capitalist Mike Maples' investment thesis reads[13]:

- Software-defined networks will be the most valuable businesses, displacing traditional corporations as central actors.
- Networks can bring exponential improvements in prosperity throughout the world.

---

[11] Christian Catalini, Joshua Gans. Some Simple Economics of the Blockchain. http://ide.mit.edu/publications/some-simple-economics-blockchain
[12] Nick Szabo. Money, blockchains and social scalability. https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html
[13] http://fortune.com/2018/08/16/floodgate-mike-maples-networks/

- Networks will encounter fierce resistance from traditional businesses, governments, and other parts of society that don't want a different future.
- Tech leaders are part of the problem, and this needs to change for networks to realize their full potential.

Decentralized approach trumps the traditional one-entity-controls-all design on a few levels. First of all, a system like Bitcoin is unhackable. In 2017 Equifax, one of the largest credit agencies, was hacked and the identities of 143 millions of people were stolen. With a decentralized identity system, it would be impossible to access that data. Yes, individual identities can and will be breached, due to inadequate security measures, but there would be no way to access all the profiles of such network. That's the difference between storing all your money in a bank or at home. If the bank is robbed, the money of all its depositors are lost, but there is no way for a criminal to break into every house in the country. That's precisely how Bitcoin works: there is no central storage of funds, you are your own bank, you control access to your Bitcoin "account," and if you have reasonable security measures in place, your funds and data will be safe.

Unauthorized access to information that should be protected is another threat that customers of traditional internet businesses face. In a 2016 lawsuit, Uber executives were accused of spying on reporters' trips, and it was uncovered that some Uber employees were able to access information about their ex-partners and celebrities.[14]

Even in the most-secure centralized scenario, that kind of information will still be available to engineers that have access to the database where the sensitive data is stored. With the decentralized approach, you would have to explicitly permit another party to read your profile. Yes, all the Bitcoin transactions can be easily accessed by anyone, but it is trivial to use the system in such a way that would prevent anyone from deducting who is transacting and why.

Another important feature of distributed systems is their resilience to attacks. The Bitcoin network, for example, could never be stopped. About 12,000 nodes make up the Bitcoin network today, so even if it is banned in a whole country, its operation will not be affected

[14] https://www.scribd.com/document/334009796/Spangenberg-Uber-lawsuit

significantly. Centralized systems fail all the time. Just in 2017 the airline industry experienced multiple system-wide disruptions due to technical failures of centralized systems.[15]

Most importantly, by delegating our power to one organization (whether it's money or sensitive data), we make those organizations extremely powerful. Let's say you put your money into a bank. What do they do with it? Bribe the economists and lobby the government, so they allow for all sorts of gambling with your money. If the gamble is successful, the banks win big, and if it doesn't go too well, they know that they will be bailed out with your tax money.

Some theorize that even many functions of the governments can also be delegated to blockchains. For example, Ralph Merkle, the author of one of the technologies used in blockchains, Merkle trees, reasons that a new type of democracy, more stable and less prone to erratic behavior, could be built using what he calls Distributed Autonomous Organizations.[16]

I would like the reader to decide for themselves whether the centralization of certain aspects of the airline industry has been beneficial or counterproductive.

Blockchain Use-Cases

As I've shown above, blockchains can be used by almost any individual or organization, and therefore it is an ungrateful task to discuss its concrete use-cases. If your business sends or receives payments, processes data in any way, or deals with customers, you can benefit from using blockchains, but you will have to decide how you're going to it, based on the needs of your business.

I often use Conway's Game of Life[17] analogy to explain this. It's a mathematical game that has only four simple, carefully designed rules. The complexity that arises from those rules is

---

[15] https://www.bloomberg.com/news/articles/2017-09-28/airlines-suffer-worldwide-delays-as-amadeus-booking-system-fails

[16] Merkle, R. (2016) DAOs, Democracy and Governance. Cryonics Magazine, July- August, Vol 37:4, pp 28-40; Alcor, www.alcor.org. https://alcor.org/cryonics/Cryonics2016-4.pdf#page=28

[17] https://en.wikipedia.org/wiki/Conway's_Game_of_Life

fascinating! I encourage you to look up videos of Conway's Game of Life, I guarantee a few minutes of excitement if you are mathematically-inclined.

The two important blockchain "games" today, Bitcoin and Ethereum, largely have just two "rules": they provide decentralized computation and decentralized immutable storage. Using these two properties, software engineers around the world have already devised projects like:

- peer-to-peer cash (Bitcoin)
- smart contracts (Ethereum, Rootstock)
- decentralized identity (uPort)
- tamper-proof voting systems (democracy.earth)
- dispute resolution (Kleros)
- notary service (Proof of Existence)

Any business could benefit from, say, an effective dispute-resolution system or a lightning-fast online notary service. Certainly, a sovereign individual of the future will need some electronic cash and a decentralized identity.

Let's take a look at the travel industry. What problems can be solved with decentralized computation and immutable storage? What is centralized? What issues could go away if individuals and businesses adopted electronic cash and decentralized identities?

Fraud

Cryptocurrencies have far superior security compared to credit or debit cards, where the only piece of information that you need to authorize a transaction is revealed during every interaction with a merchant.

When we start paying for goods and services with cryptocurrencies, the fraud problem will be eliminated because if someone is able to access your private key[18] and send a transaction on your behalf, then you have a much bigger problem than one fraudulent transaction. The attacker

[18] Simply put, it’s the password that you need to send a transaction from your crypto-wallet.

won't spend your BTC, ETH or LIF on booking hotels, they will simply transfer all your funds to the account that they control, as quickly as possible.

Customers could also have assurance that they are looking at a legitimate offer from an organization, if that offer is signed with that organization's private key. This could prevent criminals from creating phishing websites.

Reputation

Another general business problem is fake reviews. With decentralized identity systems, we will be able to have proof that the person praising your competition is indeed their customer and not a paid reviewer.[19] With blockchain, it is trivial to prove that an account (e.g. passenger) is the initiator of a transaction with another account (airline), and it can be done in a completely anonymous manner, no details about the passenger need to be revealed.

Distribution

Travel distribution is a space dominated by just a few companies, in other words, it is highly centralized. Those companies have an immense amount of power they abuse.[20] They act as gatekeepers for both sides of the marketplace. It is a perfect example of where decentralized computation can help.

An autonomous algorithm that would match the traveler with the right hotel or airline is not just doable but is in its active development phase. For example, Winding Tree is a blockchain-based marketplace for travel inventory. Any supplier (airline, hotel, car rental, tour or activity provider) can connect to the marketplace via an API, without asking anyone for permission, because the system is as open as the Internet itself. Travel agencies can access that data via another API, also in an entirely autonomous manner, no human interaction necessary.

This approach aims to radically lower barriers to entry into the travel industry, enable more innovation and help streamline and standardize some business processes.

---

[19] https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html
[20] Winding Tree White Paper

Settlement

Airline settlement in the US today is done by just one company, ARC. You can't get more centralized than that, so a smart contract run on a public permissionless blockchain could make it more efficient. Imagine that a complicated itinerary that involves a few legs with different airlines is reconciled not by the airline that initially received the payment, but by an algorithm that sends the payments to the appropriate parties immediately.

Maintenance, Repair, Overhaul

The immutable storage feature of blockchains can improve the efficiency of businesses for which it is critical to store data in that way. For example, airplane maintenance and repair data can be stored on a blockchain[21], so that at any time the airline and other parties have full confidence that that information has not been tampered with, otherwise it would be very easy to detect.

Blockchain can assure the integrity of the data over time, but it doesn't guarantee its correctness. For this reason, using blockchain for supply chain management, for example, where information will inevitably be entered by third parties, is quite limited, though it could be vastly improved if used along with decentralized identities. It could be beneficial in the context of aircraft maintenance and airports, where every employee goes through extensive screening.

Airport Operations

Blockchains are networks and therefore they are useful when they achieve a critical mass. When airports, airlines, and governments agree to use the same data standard for decentralized identities, the efficiency of many processes around sharing passenger data or baggage tracking, for example, could be immensely improved.

The passenger, of course, should control their data at all times by explicitly allowing certain parties (airlines, governments, airports, even businesses located at airports) to read a specific

[21] Storing data on a blockchain is very expensive, in the range of thousands of dollars per Gigabyte. Instead of paying that much, you can create a cryptographic hash of the data and upload it to a blockchain instead. Now you have proof that certain data existed at a certain point in time and any tampering with that data will be easily detectable. This concept lies behind services like Proof-of-Existence.

subset of their profile. E.g. it would be useful for an airline to know the dietary preferences of their customers. The passenger will be able to choose to share that information or not.

The border control officers, perhaps, could pre-screen arriving passengers even before landing. And then the duty-free shops could send personalized deals to passengers that explicitly wanted to receive them.

Loyalty

Blockchain looks like the perfect infrastructure for value transfer, and loyalty points could be represented as crypto-tokens. Creating a loyalty token for your business (whether it's an airline, hotel or a coffee shop) is extremely easy, it can be done with just a few lines of code. What prevents us from using tokens for loyalty is the high price of blockchain transactions. There are already several projects that aim to scale blockchain throughput and reduce transaction fees, like Lightning Network and Raiden Network. Once one of them is fully operational, a whole new range of possibilities will open up, if, of course, technology is one of the problems in the loyalty space at all.

Conclusion

According to Deloitte's 2018 survey[22], the majority of executives they talked to claimed that their level of understanding of blockchain technology is "excellent" or "expert"[23]. At the same time, those executives are sure that the main advantage of the blockchain technology is greater speed, compared to the existing systems[24].

It shows that the technology is still misunderstood because Bitcoin was not created for faster payments. The transaction speed and the cost of executing were sacrificed for a higher ideal, to ensure Bitcoin's resistance to influence from any potential intermediary.

Blockchain means decentralization. This technology allows us to own and control our money and data, without the help of an intermediary. Networks can exponentially improve the quality of

[22] Breaking blockchain open. Deloitte's 2018 global blockchain survey. https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html
[23] Page 40 of the report.
[24] Page 21.

life around the world, and the most successful networks are those with no barriers to entry. Some of today's most successful networks are centralized, and in many areas, the winner takes most of the market: Google, Amazon, Facebook, Uber, Amadeus, Expedia. Blockchain gives us a possibility to end this pattern.

Blockchain technology has yet to bring about products that would have as much utility as centralized networks. Nonetheless, there are hundreds of projects with billions in funding. Some of the smartest people on the planet believe that blockchain will radically transform business and society. How and when it's going to happen? It's for you to decide.