A punk's dream in a globalized world
There's more to bitcoins than meets the eye

There is currently a lot of noise around words like blockchain, bitcoin, ethereum and so on. Our goal is to explain what these are and how they relate to one another, why you should care, and how to build a diversified portfolio that benefits from current technological changes.

We need to make a clear separation between technology and application: blockchain is the underlying technology, whereas bitcoin and ethereum are applications based on the technology. Let us quickly define each of these elements with the help of Reuters' glossary[1]:

- A blockchain is a shared record of information that is maintained and updated by a network of computers rather than a central authority. Imagine an accounting transaction journal (also called ledger) that is accessible to everyone, everywhere and at the same time and on which all transactions made by all participants are displayed chronologically, proving ownership.
- Bitcoin is a digital currency based on blockchain technology and which allows payments from peer to peer without the need for a middleman to channel the money or provide guarantees. It is the first application that was envisioned for blockchain technology.
- Ethereum is another application of the blockchain principle. The blocks in the chain do not contain accounting data like for bitcoin; they expand capabilities by containing code, which for example makes it possible to create contracts between parties that are automatically enforced when specific conditions are triggered.

What is so special about a shared transaction journal to make people talk about it and say things like "the most important development since the internet"? What once was a crazy idea in the realms of science-fiction, a government-free utopia for cypherpunks[2], displays today several characteristics that make the potential applications of blockchains very interesting. Among these, we find:

- No middleman: operations can be executed both cheaper and faster, e.g. needing only minutes when banks' reconciliation services can take days
- Security: each new block is linked to the previous one by a unique code, a long string of letters and numbers which is generated based on the content of the

[1] Reuters, 2017 : Fintech glossary, https://www.reuters.com/article/usa-fintech-crypto/fintech-glossary-crypto-edition-idUSKCN1B31RR

[2] Coindesk, 2016: Bitcoin and the Rise of the Cypherpunks, https://www.coindesk.com/the-rise-of-the-cypherpunks/

previous block. This means that if someone were to try to manipulate the content of a block, then the following block would not match codes anymore, proving the fraud. Additionally, since all participants have a copy of the ledger, there is no central server for hackers to attack.

- Privacy: all transactions appear on the ledger, but identities behind remain private, similar to a ticker tape on a stock exchange
- Country-independent: since participants can be from anywhere in the world and there are no centralized servers, a blockchain is under the authority of no single state.

Working together, these characteristics are hailed as capable of revolutionizing many different industries. In short, wherever there is a need for trust, a blockchain could replace tons and tons of documentation and control processes. Financial services are often cited as use cases, with transactions that need days-long settlements being reduced to minutes, which could lead to cost savings in the tens of billions annually. A consortium of major banks is already working on an interbank blockchain to reach this goal[3]. Beyond this, there are already talks of potential applications in numerous sectors like insurance, legal services, logistics, voting, healthcare or even music.

For example, in the insurance industry, some topics that are being discussed and where we see first companies emerging are (i) parametric insurance, which uses smart contracts to automatically pay insurance claims to policyholders when certain events occur, (ii) automatic reconciliation of payments like in the finance industry to reduce settlement costs or even (iii) peer-to-peer insurance, which could mean the end of today's insurance systems as we know them, since there would be no need for a central institution pooling risk[4].

In logistics, combining blockchain with processors that are getting more powerful and energy-efficient every year means that individual objects or parcels could be fitted with a small sensor that automatically and immutably registers the object's itinerary on a shared ledger, streamlining supply chains for cost savings potentially as high as 90%[5].

These are only some of the possibilities opened by the technology; the majority of future applications has probably not yet been even thought about. One must however be cautious and not abandon oneself to the hype, as there are obstacles to be overcome and lessons to be learnt before we see widespread adoption. We must

[3] Financial Times, 2017 : Six global banks join forces to create digital currency, https://www.ft.com/content/20c10d58-8d9c-11e7-a352-e46f43c5825d
[4] TechCrunch, 2016 : Blockchain is empowering the future of insurance, https://techcrunch.com/2016/10/29/blockchain-is-empowering-the-future-of-insurance/
[5] Supply Chain Digital, 2017 : Blockchain technology set to revolutionize logistics industry, http://www.supplychaindigital.com/technology/blockchain-technology-set-revolutionise-logistics-industry

not forget that it is still a new phenomenon for the wider public, having only been introduced in 2008 as the concept behind bitcoins. Developers are refining the code of blockchain software daily to address the challenges it faces. For example, scalability is a serious issue: Platforms like Facebook are able to handle hundreds of thousands, if not millions of interactions per second, whereas Ethereum is at around 10 transactions at the moment. This means platforms with millions of users will experience bottlenecks if no progress is made in this regard, but fortunately the question is being researched[6].

The issue of energy consumption is linked to the many redundant calculations that need to be made in parallel to confirm that transactions are correct. A June 2017 report by the World Economic Forum cites estimates of electricity consumption to make the bitcoin network run that go as high as the total electricity consumption of Cyprus. With an increasing number of people starting to use the technology, we see the trend becoming unsustainable. Solutions to this issue are still being debated in the community[7]. Lastly, although it is presented as the best technology in terms of security, individual platforms have been attacked, leading to large monetary losses and even the disappearance of some of them. To be clear, it was not the concept of blockchain that was vulnerable, it was the code of an application built on the technology. For example, the DAO (Decentralized Autonomous Organization), a new concept of crowd-based venture fund, was attacked and drained of around USD 70m in a few hours, which later led to its dissolution due to a split in its community[8]. Another case is the hack that led to the bankruptcy of bitcoin exchange platform Mt. Gox in 2014, robbing users of hundreds of millions of dollars[9].

The fact that blockchains play in a field out of single nations' legal reach is also a question mark for their development. We do not know which stance individual countries will adopt when lawmakers start to understand the phenomenon better. Several central banks and even the Bank for International Settlements have conducted technical tests and various research on the topic, but the conclusions are often to wait and see how the technology evolves as it is considered too early to take an official stance[10]. The media reported a lot about the Chinese position however, as the country has already decided to ban Initial Coin Offerings (ICO) and shut down bitcoin exchanges on its soil, although it encourages research on blockchains in

[6] Medium, 2017 : Scaling Ethereum to Billions of Users,
https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1
[7] WEF, 2017, Realizing the Potential of Blockchain,
http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf
[8] CryptoCompare, 2017 : The DAO, The Hack, The Soft Fork and The Hard Fork,
https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
[9] The Guardian, 2014 : A history of bitcoin hacks,
https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency
[10] BIS, 2017: Central bank cryptocurrencies;
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

general[11]. The so-called craze of ICOs is a phenomenon that could revolutionize the way companies raise capital, but among the projects that have together managed to raise billions of dollars already, it is widely acknowledged that many are shaky if not outright scams. Some experienced investors thus propose due diligence frameworks to establish how serious some companies are, analysing elements such as software security, rights conferred in exchange of the investment, corporate structure, team background, currency supply, competition and presence of institutional investors, among others[12].

In short, there are obstacles on the way, but the potential is game-changing. One of the next SAP, Google or Facebook is likely to be based on a smart application of blockchain technology. It is not hard to imagine that these companies will not rely on blockchain alone, almost certainly combining it with machine learning algorithms or other technologies that further reduce the need for human inputs. The opposite is also possible, with companies using another tech realizing that a blockchain-based infrastructure is also something they could benefit from. There are numerous other hot topics at the moment, like virtual and augmented reality or machine vision, and each of these could be combined with the others to lead to a new successful venture. Some years ago, these technologies were mostly confined to labs and the minds of sci-fi or gaming aficionados. Today, they promise to revolutionize much of the way we do business and live our daily lives. With this explosion of opportunities comes a lot of uncertainty, making it difficult to separate high-potential projects from noise. This represents a challenge for an investor who wishes to take measured risks after a rational and disciplined due diligence process, ensuring optimal portfolio construction. It highlights the need for a diversified portfolio which includes not only blockchain, but also companies using other advanced technologies that could be combined with it, all this thoroughly analysed by people with industry experience.

[11] BBC, 2017 : China orders Bitcoin exchanges in capital city to close, http://www.bbc.com/news/business-41320568
[12] Coindesk, 2017 : To the Moon – Or Bust? Questions to Ask When Evaluating ICOs, https://www.coindesk.com/moon-bust-questions-ask-evaluating-icos/