Future impact of Blockchain technologies on services, businesses and regulation

Tomaso Aste[1,2,3], Paolo Tasca[1,2,3] and T Di Matteo[1,2,3,4]
[1] *UCL Centre for Blockchain Technologies,* [2] *Department of Computer Science, UCL, London, UK*
[3] *UCL Centre for Blockchain Technologies, UCL, London, UK*
[4] *Department of Mathematics King's College, London, UK*
(Dated: February 10, 2017)

We introduce basics concepts about Blockchain and discuss the future, foreseeable impact of Blockchain technologies onto our industry and society. The paper briefly tracks the origins of this technology from the Bitcoin digital cash system and describes applications ad applicability in other domains highlighting potentials as well as weaknesses, limitations and risks.

I. INTRODUCTION

Blockchain is a technology that uses community validation to keep synchronised the content of ledgers replicated across multiple users. Blockchain was first introduced by an anonymous individual or group of individuals under the pseudonym of Satoshi Nakamoto and it was applied to a digital currency, Bitcoin, in 2008 [1]. Bitcoin is the first example of widespread decentralised digital currency which provides a solution to the problem of trust in a currency system. The Bitcoin Blockchain is a public decentralized peer-validated time-stamped ledger that everybody in the network can inspect but no one can control. Now Bitcoin has reached about 14 billion dollars capitalization and the system process hundreds of thousands of transaction a day. In Bitcoin anonymous and untrustful peers can exchange value without any intermediary or trusted authority. Participants do not even have to be humans, they can be machines that operate autonomously. This opens a range of new potentials for businesses where value can be directly transferred between participants over the Internet in the same easy way as we pay with cash on the street and in the same convenient way as we use instant messaging. The Bitcoin Blockchain is a distributed ledger, publicly available to all participants, that chronologically registers all validated transactions. Transactions are broadcasted to the bitcoin network and their validity is verified independently by peers. Valid transactions are collected into blocks which are cryptographically sealed and and build one on top of the other in a chronological sequence: a chain of blocks.

Independently from its original technological design and application, Blockchain is a foundational technology that leads to the paradigm shift from "trusting humans" to "trusting machines" and from "centralized" to "decentralized" control, from secure data storage to data transparency [2]. Blockchain also introduces novel ways to establish an agreed 'truth' around historic sequences of facts. The fundamental characteristics of Blockchain-based platforms are: Immutability, automation and transparent consensus. Let us here briefly describe each characteristics:

- **Immutability.** Blockchain is a shared, tamper-proof replicated ledger where records are irreversible thanks to cryptography and community consnsus. Immutability eliminates the need for reconciliations providing a historical, unique reconciliated version of the truth.

- **Automation.** Blockchain makes it possible for a group of independent parties to work with universal data sources, automatically reconciling between all participants. Ownership rights on the data and authorization of data transactions are exerted through public/private key technology without the need for human interaction or trust providers, verification or arbitration. The software ensures that conflicting information cannot be permanently written in the ledger. Any type of data can be recorded on a Blockchain, from ownership of assets to contractual obligations, to creative art copyrights or credit exposures or digital identity. Automation includes the deployment of self-enforcing contracts (smart contracts, Decentralized Application and Decentralized Autonomous Organizations). The latter ensures agreements are executed to agreed upon business outcomes.

- **Decentralized and Transparent Consensus.** In Blockchain consensus is a method for validating the chronological order at which requests, transactions (deploy and invoke) and information has been executed, modified or created. The correct ordering is critical because it can establish ownership and therefore rights and obbigations. On a Blockchain network, there is no centralized hub that determines the transaction order, approves transactions and sets rules for how the nodes interact with one another. Instead, many validating 'peer' nodes implement the network consensus protocol and every node sees the information making the system transparent and traceable. Beside from the different types of consensus protocols that can be used, consensus ensures that a quorum of nodes agree on the order in which information is appended to the shared ledger.

Currently, there are several pilot projects and running applications that exploit these fundamental characteristics of immutability, automation and transparency of Blockchain technologies. For example, several businesses use the immutable time-stamping to certify the authenticity of documents and other assets, even diamonds [3]. Blockchain

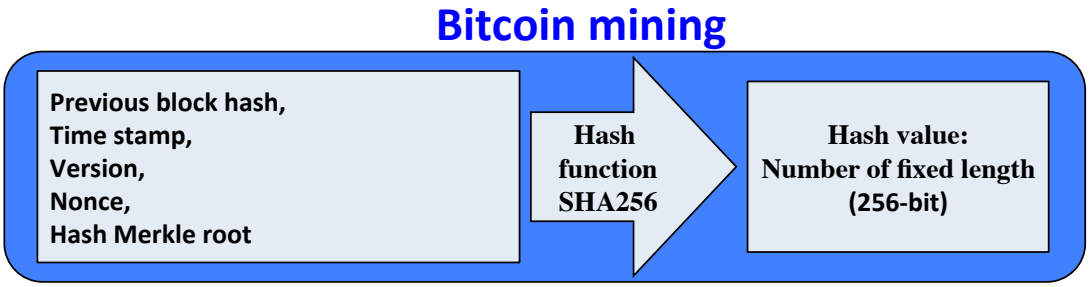

FIG. 1: Bitcoin mining is an operation that generates an hash 256bit number from the block content, the previous hash and other elements. The operation is made computationally demanding by requiring to generate, by chance adding a random nonce, a hash that is smaller than a given number.

can be indeed used to timestamp anything and provide a proof of the existence of a digital or digitalized asset at a given moment. This can be game-changing in many sectors such as creative arts where digital identical duplication makes the value of these artefact hard to protect. Instead, Blockchain provides a way to make the artefact unique and uniquely located in time (and space). Blockchain provides the instrument for creation of digital value that can be transferred, exchanged and traded with protection from illegal uncontrolled duplication and counterfeit.

Great expectations are building up around Blockchain technologies. This is because this technology provides an essential tool for our digital economy: a way to manage information from heterogeneous -unverified- sources making it trustable and hard to tamper through community validation and immutable chronological order. Digital and digitalized goods can be made unique and traceable making it possible to directly trade value over the Internet. This technology has the potential to radically change many sectors from markets to music, from payments to food.

Blockchain technology also offers the tool to introduce automatically executable rules within the transaction mechanisms. These are the so-called *smart contracts* which are conditional transactions encoded directly on the Blockchain. This aspect has immediately resonated in the financial technology (fintech) area where their application to the trading of derivatives appears rather straightforwards. This automation will increase speed, reduce costs, increase transparency, reduce risks from both counterparts and post trade settlements.

There are many other possible applications of Blockchain technologies in the domain of personal data verification and management, product tracking, identity management, reputation and trust.

Regulation is also an area of great potential application where Blockchain technologies bring about several disruptive features which can radically change the way regulation is operated presently. Indeed, by means of Blockchain technology it is possible to provide access to auditable data which are verified, time-stamped and immutable, generating a transparent, inter-operable environment where rules can be implemented, enforced and adapted. Reliability and reputation of clients and services providers can be verified and monitored by analyzing the historic record in the Blockchain. Rules can be encoded within the system enabling automated review via audit software. Adoption of Blockchain technologies in the services sector has the potential to be beneficial to both industry and regulators. This convergence of industry and government interests is rather unique and opens great opportunities [4].

A very important direct consequence an immutable historic record validated by community consensus is that this generates trust in the system. Indeed, it becomes very difficult for an individual or any group of individual to tamper with such a record unless these individuals control the majority of 'voters'. Blockchain has been indeed defined by The Economist 'The trust machine' [5]. With Blockchain trust is generated and consolidated because participants are monitored by the community and by each other and transactions can be traced back to source. This transparency combined with the immutable chronological sequence is a very appealing aspect of the Blockchain that goes well beyond the original purposes for the digital cash Bitcoin. However, as mentioned previously, Bitcoin is not only the first large-scale case where Blockchain and community validation were used but it is still so far the most relevant example of this technology. There are other proposed Blockchain systems but they all strongly build upon the original Bitcoin design. Let us therefore start by recalling how Bitcoin blockchain and bitcoin network work.

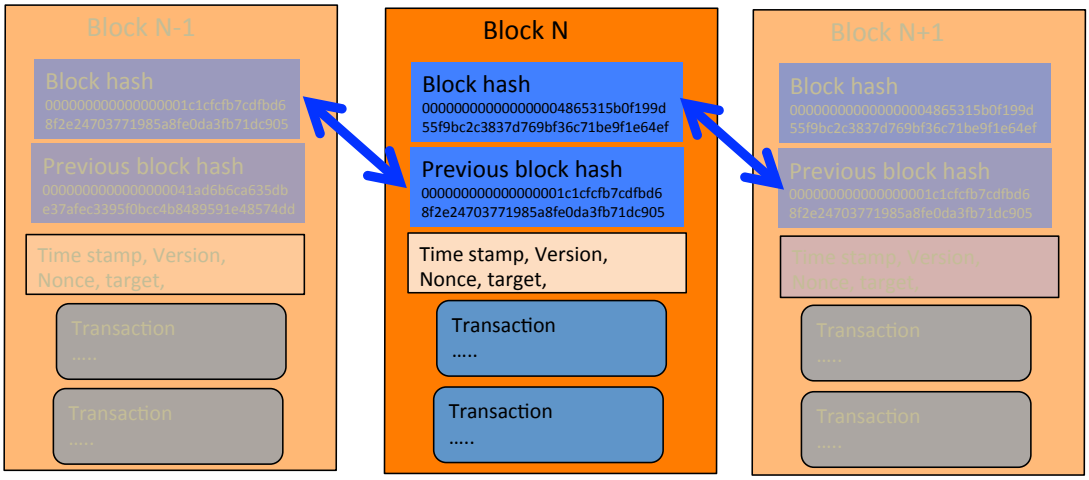

FIG. 2: Bitcoin Blockchain is a chain of text blocks containing records of transactions connected together through consecutive hash numbers generated from the content of the previous block plus a random part.

II. AN INSIGHT INTO BITCOIN

A. Origins

After its introduction in 2008 [1], in its first few years Bitcoin was mostly limited to the underground crypto-anarchist communities. Those groups aimed at employing cryptography to enable individuals to make consensual economic arrangements transcending national boundaries and centralised authorities. Unfortunately, those activities were often associated with the *counter* economy which generally includes all the underground actions of civil and social disobedience outside of normative and legal frameworks. Indeed, Bitcoin was the facto the only currency used in the deep web, i.e., the "hidden" Internet accessible only by the anonymous communication system, Tor, where illegal services and goods can be traded without any police or criminal agency interference. According to the FBI, the online black marked SilkRoad (the "eBay of drugs"), run in the deep web between 2011 and 2013, generated a revenue of almost 3 billion USD (at the current exchange rate) becoming the first "killer app" of Bitcoin [6].

B. Adoption

Lately, practitioners, academics and the general public at large started to show interest in Bitcoin thanks to an increasing media attention mostly sparkled by the Bitcoin/USD exchange rate which spiked to about 1,200 USD in late 2013 (starting in 2009 to exchange at tiny fractions of a dollar). In the meanwhile, various kinds of individuals started to use Bitcoin as a medium of exchange and to run small businesses. Now Bitcoin has reached about 14 billion USD in market capitalization and the system process hundreds of thousands of transaction a day [7].

Bitcoin is money-as-information. Namely, every Bitcoin transaction, which indeed is a monetary transaction, is as simple as sending an email, is tamper-proof, is publicly auditable and non-reversible. Each transaction is firstly broadcasted to the Bitcoin network and then validated by anonymous independent 'peers' according to a specific consensus protocol which determines whether and when the given transaction must be added to the ledger. This consensus mechanism represents the major breakthrough of Bitcoin as it automatically determines a trustworthy chronological order of the "truth" (a monetary transaction history) among anonymous users without the need of a third-party neutral intermediary or a central counterparty.

C. The Blockchain

In Bitcoin transactions are broadcasted to the bitcoin network and their validity is verified independently by network participants. Valid transaction are recorded locally by a special kind of network participants called 'miners' that must verify the validity of the transactions and put them in a list forming a 'block' that is cryptographically 'sealed' (see Fig.2). In Bitcoin blocks are sealed every approximately 10 minutes and contain in average 1,700 transactions for a

value around $ 1 million. The cryptographic 'sealing' is an hash number generated from the content of the block, the previous block hash and a random part. Hashing is a very simple operation that associates any digital information to a number. The algorithm is devised to generated an almost unique number with fixed number of digits associated with the input in a deterministic way. The function is injective with any two very similar inputs (e.g. two long pieces of text differing by only one character) corresponding to completely different output numbers in a way that the input cannot be reconstructed back from the output. Bitcoin mining uses Secure Hash Algorithm hashing protocol producing numbers of 256 bit size (SHA256).

D. Proof of Work

In bitcoin hashing is used for 'Proof of Work' (PoW), a mechanism that links consensus with computing power making duplication of participants influential to consensus outcomes. The Proof of Work is what the so-called 'miners' are performing. In brief, mining is a competition among users to approve transactions. A userÕs chance of winning the competition is proportional to the computing power he controls. Accordingly with original Satoshi's motto: 'one CPU one vote'. Miners are rewarded for contributing to the verification and block construction process. Indeed, each mined block contains a *coinbase* transaction (currently of the amount of 12.5 Bitcoins) that is allocated to the winning user. This mechanism is the only way to generate new bitcoins.

E. Mining

This compensation, that at current exchange rate can be quantified in excess of $12,000, has generated a specialized kind of 'peer', the miners, that perform only Proof of Work for profit. Nowadays, most of mining is concentrated in large "mining farms" mostly located in regions with low electricity cost. Alterantively miners are gathered in "mining pools" that share profits in proportion to hashing power contribution. Mining is performed almost exclusively with hardware developed explicitly for bitcoin hashing. These state-of-the-art ASIC machines compute several tera hashes per second consuming some fraction of Watt per giga-hash. Figure 3 shows the historic mining activity in terms of Tera Hash per second produced in the world for Bitcoin verification purposes.

F. Transactions

To better grasp the mechanism used by Bitcoin to register transactions we should consider three key elements: the private key (k), the public key (K) and the *Bitcoin address*. Ownership of Bitcoins is established through the possession of k that is automatically generated and stored in a file called wallet. k is used to encrypt transactions and, like the PIN code of a credit card, it must be kept secret to the public, otherwise revealing it would give control over the Bitcoins secured by k. K is generated by k and it is used in pair with k to allow recipients to decrypt transactions. The Bitcoin address is generated by K through the use of one-way cryptographic hashing and it is used to identify a user in the Bitcoin network. Any Bitcoin user identity is hidden behind their addresses that work as pseudonyms. Adresses are normally used only for one transaction. When a transaction takes place, the change of Bitcoin ownership is registered in the Blockchain by debiting the Bitcoin amount to the Bitcoin address used by the sender and by crediting the same amount to the Bitcoin address used by the recipient.

Imagine that Alice (A) wants to give Bob (B) one Bitcoin. Since Bitcoin uses the concept of *money-as-information*, the transferring of one Bitcoin from A to B, is a string of bits where A writes the message"I, A, am giving B one Bitcoin with serial number 123456". To this message, A attaches a code that will act as a signature: A takes the hash of the message and encrypts the message with k. Therefore, the signature depends on the content of the message and on k and it is generated via a signing algorithm. Finally, A will send to B the message together with the signature and K. Similarly to sending an email, the sender need to know the email address of the recipient, also in this case A need to know the Bitcoin address of B. Through the presentation of the message, the signature and K, B (but also everyone else in the Bitcoin network) can verify and accept the transaction as valid, confirming that A owns indeed one Bitcoin at the time of the transfer. B hashes the original message and with the use of K decrypts the originally signed data. If the two hashes are identical the signature is valid and message authentication, non-repudiation and integrity will be granted.

A key passage is the transaction validation process. Indeed, to verify the transaction from A, B does a sanity check that the Bitcoin with serial number 123456 belongs indeed to A. If it is the case, B will broadcast the signed string of bits to the entire network and other nodes in the network will collectively verify whether A holds one Bitcoin with serial number 123456. Now imagine that David (D) is one user (a miner) in the network receiving the message "I,

A, am giving B one BTC with serial number 123456". It is worth mentioning that serial number 123456 contains references to specific previous transactions received in the address of A (transaction inputs) for an equivalent amount of Bitcoins sufficient to cover one Bitcoin that now A wants to send to B. Therefore D can verify if the inputs allow A to transfer exactly one Bitcoin to B. As D holds a replica of the Blockchain and has access to all the public keys, D can easily verify whether the transactions in the block are valid. Once verification is done, D appends the transaction, together with other messages recently received that must be digested into a block. Together, all these verified transactions form a block. Now D needs to compute new hash values based on the combination of the previous hash values contained in the message, the new transaction block and a *nonce*, such that the new hash value will start with a given number of zeros $\leq$ *target*. If D finds the suitable nonce, he will broadcast the message "*Yes, A owns one Bitcoin with serial number 123456 and it can be transferred to B*" together with the other transactions in the transaction block and the nonce such that the network can check-test the validity.

III. NOVELTY OF BLOCKCHAIN TECHNOLOGIES: A BRIEF HISTORY

It has been written that Blockchain is a disruptive technological innovation, a 'trust Machine' that might had even set the beginning of human recorded history and that will revolutionize our society [2]. What is the innovation then? As matter of fact, there is no true technical innovation in Bitcoin and Blockchain, all ingredients were already developed well before the 'disruptive' bitcoin paper by Satoshi Nakamoto in 2008.

From an historic perspective (see [8]) this technology has his roots in the ideas of Merkle elaborated at the end of the 70' when he proposed the use of concatenated hash in a tree structure for digital signature, the so called 'Merkle tree' [9]. Hashing was invented sometime earlier in the 50' [10] and it has been widely used in cryptography for information security, digital signatures and message integrity verification. About ten years after Merkle the idea of a chain of hashes was prosed by Leslie Lamport for secure login [11]. Then after other ten years in 1990, just at the dawn of the World Wide Web (Tim Berners-Lee 1989 [12]), the first crypto currency for electronic payments, the e-Cash, was proposed by Chaum [13]. Further evolutions and refinements over the idea of a chain of hashes were introduced in the 1994 paper by Neil Haller on hash chain for Unix login (S/KEY) application [14]. Ideas that made immediately their way into proposals for electronic payment systems with hash chains [15, 16] and electronic cash [17]. In 2002 Adam Back proposed the hashcash [18] an electronic currency based on Blockchain an proof of work which has most of the elements of bitcoin and it is indeed cited by Satoshi Nakamoto as reference work. Interestingly, the literature remained rather quiete for the following six years until, at the end of 2008, Satoshi Nakamoto come out with his 'disruptive' paper on bitcoin. The reasons for its adoption are most likely to be attributed to the historic period, the banking crisis and the developing of alternative business (and criminal) models, more than the technological innovation.

We can say with some confidence that the main innovation in bitcoin is bitcoin itself that managed to exist and operate in an autonomous way for the last 9 years with a considerable capitalization and a sizable transaction volume without being seriously challenged by any attack. The proof of concept that peer-to-peer systems can operate without intermediation of trusted central authorities is the main novelty of Bitcoin and it can indeed revolutionize our way to do business and our society.

IV. OVERVIEW ON ALTERNATIVE BLOCKCHAIN SYSTEMS

This section provides a general overview of the major Blockchain technologies by classifying them into four main categories according to their application: 1) Internet-based medium of exchange (digital currencies); 2) Applications that link digital tokens to real assets (asset registry technologies); 3) Platforms for the development and execution of complete applications (application stacks); and 4) Semi-decentralized consensus mechanisms and permissioned Blockchains (asset-centric technologies).

A. Application Stacks

Application stacks are "non-currency" Blockchain-based platforms that are used for the development and execution of complete applications on top of decentralized networks. To better grasp the role that application stacks play in the Blockchain innovation path, it is firstly important to understand what complete applications are. We confine them in: Autonomous agents, Smart contracts, Decentralised applications, Decentralised Organisations and Decentralised Autonomous Organisations.

- **Autonomous agents (AA).** These are independent software programs that exist with limited human intervention, if not at all. This beside the initial effort that might be necessary to build the hardware and writhe the

software that the agent runs on. One example of an AA is a computer virus. The virus survives by replicating itself from machine to machine without deliberate human action. Another more benign example of AA is a self-replicating cloud computing service that runs an automated offer a full range of cloud computing services (e.g. virtual desktops, development platforms) on one virtual private server, and then once its profits increase it rents other servers and install its own software on them, adding them to its network. AAs are very complex to create because they need to be endowed of some artificial intelligence necessary for them to take the "optimal" decision according to their evolutionary algorithms in an environment that is not just complicated and rapidly changing, but also hostile and business unethical.

- **Smart contracts (SC).** A smart contract is the simplest form of decentralized application. It is a set of "rules by code" which facilitates the automatic agreement among two or more parties (in fix number), the identification of the legal socio-economic function of the act, its object, its form and its final conclusion. The entire process is automated and the terms of the SC are recorded in a computer language as a set of instructions. SCs are entirely digital and written using programming code languages such as C++, Go, Python, Java. The code defines the rules and consequences in the same way that a traditional legal document would, stating the obligations, benefits and penalties which may be due to either party in various different circumstances. The code is then encrypted and sent out to other computers (counterparties) via Blockchain. If this is done via public permissionless Blockchain such as Bitcoin, the contract is sent out similar to the way that a network update of a Bitcoin transaction would occur. This can also be done in a permissioned or hybrid distributed ledger platform such as the R3 distributed ledger [19]. Execution (unique or continued) and enforcement of the agreement are also automated.This is the so called self-execution and self-enforcement. In this type of contract, party manipulation is averted because control over the execution of the SC is no longer possible because execution is no longer in the hands of a single party. The main goal of a SCs is to enable two (or more) anonymous parties to trade and do business with each other, usually over the internet, without the need for a middleman. The SC facilitates the parties to upload digitized assets on the Blockchain and automatically redistribute them and eventually their revenues and losses among the parties according to specific conditions based on the occurrence of certain events that are predefined at the time the contract is initiated.

- **Decentralised applications (Dapps).** A decentralized application differ from a smart contract because: 1) a Dapp has an unbounded number of participants on all sides of the market; 2) a Dapp needs not be necessarily financial. Because of this second requirement, Dapps are easier to code as there are not complex financial models and legal layouts to be written. There are several examples of Dapps but they can generally be classified into two categories:

  - *Fully autonomous Dapps.* In this case, it does not matter the identity of the nodes because every participant is essentially anonymous and the system is made up of a series of instant atomic interactions. BitTorrent and BitMessage are examples of this.
  - *Reputation-based Dapps.* In this case, the reputation metric assigns to nodes a degree of importance. The reputation is untransferable and does not have monetary value. Madesafe is an example.

  However, a clear distinction between the two categories is impossible. For example, BitTorrent-like systems have nodes maintaining "reputation statistics" of other nodes for anti-DDoS purposes.

- **Decentralised Organisations (DO).** The DO, as any traditional organisation, is governed under specific divisional, functional structures according to which decisions are taken (at different levels along the hierarchy) based on predetermined set of rules, routines and codes of conduct. The DO simply brings a centralised organisation process and decentralise it. Instead of a hierarchical structure managed by a set of humans interacting in person, a DO involves a set of humans interacting with each other according to a protocol specified in code, and enforced on the Blockchain. For example the DO uses on Blockchain voting systems, accounting and production system, shareholders registry, etc. As in any cooperative model, the DO enables its members to participate in the management of the DO and equally share its collectively managed resources. As cooperatives generally do, also the DOs can flatten and democratize, or even invert, the traditional hierarchical pyramid of management. But differently from the traditional cooperative model where the humans are the ones making the decisions, in the DOs the decision-making process is in some fashion handled by itself: i.e., a pre-defined enforceable tamper-proof set of rules coded into SCs.

- **Decentralised Autonomous Organisations (DAOs).** The DAO is an organisation that, under a predefined set of rules, runs a business or social activity (either online or off-line) completely autonomously in a open-source software which is: decentralised (distributed across the computers of the stakeholders), transparent, secure and auditable. The DAO is a pool of smart contracts and/or AAs linked together and endowed with an

initial capital. The decision making processes are independently handled by the DAO, under a predefined set of rules, without need of human intervention. The difference between the DO and the DAO relies on the fact that the information is managed and process into the DO by the humans which control the information flow. In other terms, the DO decision process is bias toward the type of information through which decisions are made. Instead, the DAO holds full control of the information process and no majority can influence the decision process, i.e., collusion attacks are considered as a bug. The Bitcoin can be consider a first experiment of a DAO with producers (miners), investors (buyers of Bitcoin) and customers (merchants and users of Bitcoins). In this case, the Bitcoin DAO's product would be the social welfare of the Bitcoin network participants.

Blockchain application stacks represent a revolution because they will replace most of our business logics with new models still to come, will introduce new economic paradigms and will change our society at large. Imagine for example, a DAO which is able to autonomously select and invest in different start-ups, to govern their business development and then to sell its stakes on them to other funds and redistribute the profits to its shareholders. Indeed, a first practical implementation of such DAO has already been attempt. The DAO called "The DAO" was instantiated on the Ethereum Blockchain, and had no conventional management structure or board of directors. The DAO was intended to operate as a hub capable to autonomously disperse funds (Ether, the Ethereum value token) to real business projects voted on by an open community of donors and members. The DAO did not hold the money of donors and members; instead, they held DAO tokens that gave them rights to vote on potential projects. Anyone could have pull out their funds until the time they first vote. The DAO was crowdfunded via a token sale in May 2016. It set the record for the largest crowdfunding campaign in history with ca. 160 million USD (denominated in ether) from more than 11,000 investors but also it set the record as the faster to collapse: after few months from its launch, an investor tunnelled ca. 50 million USD out of The DAO. The DAO collapsed following an incident in which an attacker was able to exploit a functionality in The DAOÕs code and repeatedly launched a Òrecursive call exploitÓ requesting funds from The DAO. Indeed, The DAO was not hacked. It simply executed its code, and by doing so, it went bankrupt. It was a bad business model. The DAO was only a failure from the standpoint of its investors. From a technical standpoint, the DAO worked seamlessly. This example explains at the same time the big potentialities of the applications running on the top of Blockchains but also their big challenges and risks, [20]. Current application stacks that allow for implementation of decentralized automation are NXT, Ethereum, and Eris, which distinguish themselves based on their core functions.

V. BLOCKCHAIN EFFICIENCY AND PHYSICAL LIMITS

Blockchain systems have several appealing features, their power reside in the interoperability, in the absence of any vulnerable single point of failure and in the community-based verification process. However, when it comes to efficiency and control, centralized systems are often easier to manage, easier to scale and faster to operate. Let us here briefly account for the advantages and disadvantages of distributed Blockchain systems.

At the basis of Blockchain technology is the PoW, a community verification and cryptographic sealing mechanism that joins blocks together. This mechanism has been proven to be very resilient to attempt to tamper the Blockchain and it is probably the main and most important part of this technology. The PoW processes information which is feed by the community of user and the community itself is also verifying the authenticity and validity of the information. To tamper the system one must control a large portion of the user community and this is very difficult, and costly, to achieve. In Bitcoin the PoW is made computationally intensive and truth is decided by the majority of computational power. However, in bitcoin this mechanism had the negative effect to produce a community of special peers, the miners, that are not users which participate to the system but only contribute to the PoW for profit. This specialisation and concentration causes several issues because such a 'distributed' 'peer-to-peer' community is de-facto controlled by a few groups of miners.

Bitcoin is consuming very large amount of electricity to perform PoW and keep the system secure. Currently in bitcoin a successful hash is generated in average after $2\ 10^{21}$ (two billion trillions) hash attempts which corresponds to an average electricity consumption per block of 1,000 GW at an estimated cost of around $10,000. This is a massive quantity of energy, however, it was pointed out in [21] that the cost of PoW must be equivalent to the amount one can potentially profit from an attach that attempt to alter transaction history. Given that a block contains around $1M in transactions and that an attacker should control a chain of around 10 blocks to falsify transaction history for long enough to collect the profits, a fair cost for the proof of work should be indeed at least $10,000 that would make an attack costing at least $100,000 which is 10% of what potentially could be stolen. This cost makes bitcoin an expensive system to transfer money consuming about 1% of the transferred value in electricity. However, in bitcoin, community

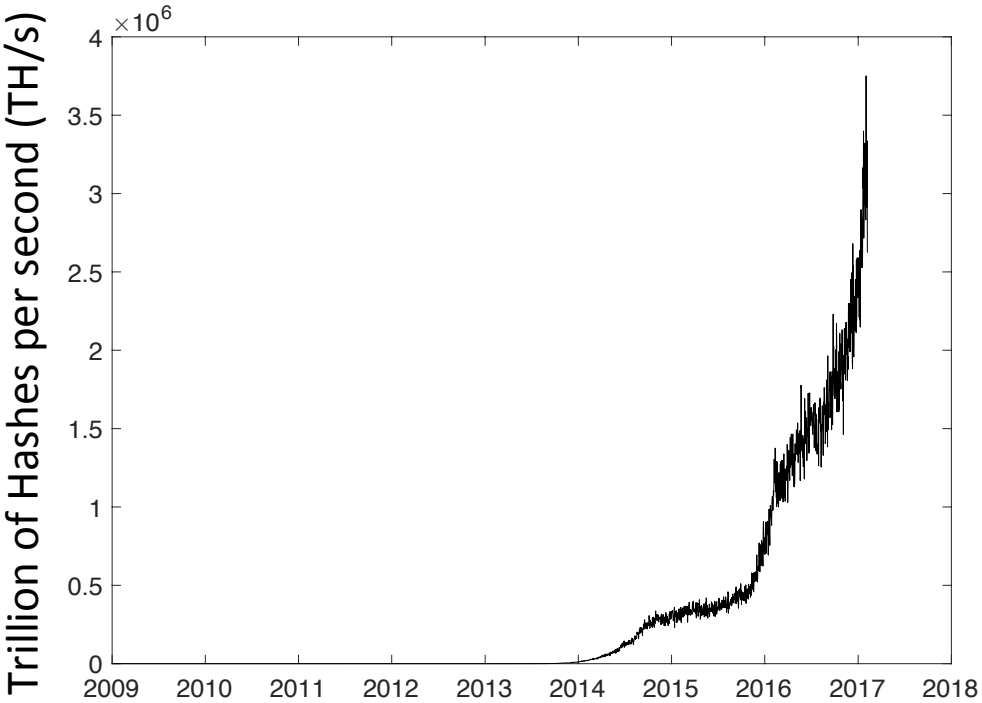

FIG. 3: Bitcoin Blockchain mining requires the production of a large number of hashing attempts. Currently the network is generating around 4 million trillion ($4\ 10^{18}$) of hashes per second. Electricity consumption can be estimated around 0.1 to 1 W/GH corresponding to around 1GW of electricity consumed every second. Data from https://Blockchain.info/.

verification must be costly because participants are anonymous and their 'vote' must be verified in proportion to used computational power. A worrying note must be added at this point. Bitcoin PoW was considered 'fair' by assuming current block values at about \$1M and it is reasonable to expect that the system itself will dynamically adapt the PoW cost to the transferred value. However, if coloured coins introduce transactions associated with other external assets that are not represented in value as bitcoin transfer, then the system becomes biased with blocks containing larger real value than the nominal content. in this case costly attacks can become profitable.

Blockchains can be constructed through several other mechanisms that do not require computational intensive PoW. However, these other mechanisms must relax also some other properties such as anonymity or equalitarian distributed verification. Reduction in the PoW cost can be obtained by increasing the number of blocks to wait before a transaction is considered accepted, by reducing the value of the transactions in each block or by reducing anonymity in the validation by consensus process. For instance in a permissioned Blockchain systems, where only identifiable and authorized users contribute to the verification process, the PoW could be virtually eliminated by using direct voting, paraphrasing Satoshi, 'one-user one vote'. However, such a system would introduce other vulnerabilities, for instance in the process of verification of authorized voters and the ratification that each vote is counted only once.

There are physical limits as well. Current electronic payments systems such as PayPal or VISA are handling several thousands transaction per seconds and exchanges such as NASDAQ can reach over one million transactions per second. A distributed system that requires community validation across the globe is limited by the speed of light, which is fast, but still takes over 1/10 of a second to travel around the globe. A community validation system scattered geographically cannot be faster than 0.1 seconds. Of course, such a system could still handle large volumes of transactions but this would require large blocks or mechanisms where more than one block is validated simultaneously. There are plenty of alternative models that we can image: local validations, hierarchical validations, sampling validations, simultaneous validations, etc. These, and many others, are valuable and achievable paths to improve system efficiency and scalability but they all require changes with strong implications over centralization, security, egalitarian structure, anonymity issues.

There are even more severe, governance limits. Every time changes to the protocol are introduced there are big tensions within the Bitcoin community because they can impact revenues and business models. Bitcoin is a distributed

system, but it has a highly centralized governance. It might be argued that the power of governance is limited in these systems because the technology can operate independently and outside the original network and rules. This is, for instance, what happened to Ethereum's DAO when in June 2016, someone profiting of an unforeseen code path managed to move a 50 million USD into a clone of the DAO held by only the attacker itself. After a week the Ethereum community decided for an hard fork reversing the transaction and in doing so creating 'Ethereum Calssic' a new chain where the $50M transaction was reverted. Now there are two simultaneous Ethereum where in both transactions are traded. And in the meantime other hard forking had occurred. This question to the roots the fundamental concept of immutability of the Blockchain and also demonstrate that governance in distributed systems is a very complex matter where minorities can autonomously separate form the system while keeping technology and assets but trading on parallel forks.

Technology is not neutral and technical changes have practical implications affecting power balances and business models.

Another point of weakness of distributed system is the tendency towards concentration and monopolistic regimes. We have witnessed such aggregation and creation of semi-monopolistic regimes in all new technology sectors that start distributed and egalitarian and then evolve into a highly concentrated structure. This tendency is particularly strong and fast for ICT and web services sproviders. Indeed, one of the main aspect associated with the emergence of new technology is that the required infrastructure it is costly to setup. This makes convenient to scale operations up and concentrate the provision of services in the hand of few providers only. It would be arguable to avoid excessive concentration in the Blockchain domain maintaining distributed systems truly decentralized and truly peer-to-peer both for what concerns their operation and their management and control. This is an open challenge that, we hope, the academic, business and regulator communities would take onboard facilitating the organic growth of this sector.

VI. FUTURE PERSPECTIVES

We are at the verge of a radical change that is likely to affect a large portion of our industry and society. Blockchain technologies create the opportunity to generate the necessary level of trust between unknown and anonymous counterparts to allow them to trade without the need of intermediaries. This disintermediation opens the possibility to directly exchange value between peer over the web. Peer-to-peer systems are little known and if now we begin to see the positive potentials of these systems, we are also starting to be concerned bout the new treats they can introduce. Is a peer-to-peer disintermediated market more reliable than a traditional one? Would operators and consumers be more or less protected in such a market? Would a peer-to-peer market be more or less stable during periods of stress? How much collective irrational phenomena such as sentiment/confidence swings will affect the capability of these markets to operate? How can we govern and regulate these systems to avoid abuses and protect users? These are all questions that require further understanding and investigation.

Acknowledgments

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[2] T Economist. The trust machine. The Economist, 2015.
[3] https://www.everledger.io/, 2017.
[4] https://www.fca.org.uk/publication/corporate/business-plan-2016-17.pdf, 2016.
[5] The Economist Newspaper Limited, editor. The trust machine. The Economist, 2015.
[6] Calebe de Roure and Paolo Tasca. Bitcoin and the ppp puzzle, 2014.
[7] Paolo Tasca. Digital currencies: Principles, trends, opportunities, and risks, 2015.
[8] Eduard de Jong. A short history of the blockchain, 2015.
[9] Ralph C Merkle. A digital signature based on a conventional encryption function. In Conference on the Theory and Application of Cryptographic Techniques, pages 369–378. Springer, 1987.
[10] Herbert Hellerman. Digital computer system principles. 1967.
[11] Leslie Lamport. Password authentication with insecure communication. Communications of the ACM, 24(11):770–772, 1981.
[12] http://webfoundation.org/about/vision/history-of-the-web/.
[13] David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In Proceedings on Advances in cryptology, pages 319–327. Springer-Verlag New York, Inc., 1990.

[14] Neil Haller. The s/key one-time password system, 1995.
[15] Torben P Pedersen. Electronic payments of small amounts. In International Workshop on Security Protocols, pages 59–68. Springer, 1996.
[16] Ronald L Rivest and Adi Shamir. Payword and micromint: Two simple micropayment schemes. In International Workshop on Security Protocols, pages 69–87. Springer, 1996.
[17] J.E.K. De Jong and C.J. Stanford. System with and method of cryptographically protecting communications, March 31 1999. EP Patent App. EP19,960,920,052.
[18] Adam Back et al. Hashcash-a denial of service counter-measure, 2002.
[19] R3 cev, http://www.r3cev.com/, 2017.
[20] R Price. Digital currency ethereum is cratering because of a $50 million hack. Business Insider, 2016.
[21] Tomaso Aste. The fair cost of bitcoin proof of work, 2016.