DOI:
10.1109/MC.2017.3571064

Document Version
Peer reviewed version

Blockchain Technologies: foreseeable impact on industry and society

Tomaso Aste[1,2], Paolo Tasca[1,2] and T Di Matteo[1,2,3]
[1] *UCL Centre for Blockchain Technologies,* [2] *Department of Computer Science, UCL, London, UK*
[3] *Department of Mathematics King's College, London, UK*
(Dated: May 6, 2017)

The paper provides basic concepts about Blockchain and offers our perspective on the challenges, the future opportunities and the foreseeable impact of Blockchain and distributed ledger technologies in industry and society. The origins of this technologies are tracked, from the Bitcoin digital cash system to more recent applications. Additional possible usages of Blockchain and distributed ledger technologies in other domains are covered by highlighting potentials but also weaknesses, limitations and risks.

Draft NOT for distribution, to be published on IEEE 2017

I. INTRODUCTION

Blockchain is a technology that uses community validation to keep synchronised the content of ledgers replicated across multiple users. Although Blockchain derives its origins from technologies introduced already decades ago (see Section IV for a discussion), in recent years it gained popularity with Bitcoin. In 2008 an anonymous individual, or a group of individuals, under the pseudonym of Satoshi Nakamoto published a white paper whereby the Blockchain digital currency application called Bitcoin was developed [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 which is distributed and 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 interlocked one on top of the other in a chronological sequence: a chain of blocks. As a matter of principle, participants do not even need to be humans, they can be autonomous agents operating independently from any human intervention. 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. Blockchain is generally included in the larger family of distributed ledger technologies which encompass all methods for decentralised data sharing where replicated and synchronised digital data is spread across multiple sites, countries, or institutions. Let us note that not all distributed ledgers employ a chain of blocks, however, for the sake of simplicity, in the following we will refer to 'blockchain technologies' to indicate, more generally, community consensus based distributed ledgers.

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. [2]. Indeed, to better grasp the potentialities of blockchain one should look at it by using two different lenses. With the first lens, it can be seen as an "ICT technology" to record ownership of on/off platform assets and rights/obligations arising from agreements. 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. With the second lens, blockchain can be seen as an "institutional technology" to decentralise governance structures used for the coordination of people and economic decisions making [3]. Although in this paper we will take the "ICT technology" perspective, let us mention in the following points what, in our opinion, must be considered the key drivers of the blockchain revolution both from an ICT and an institutional perspective:

Decentralized and Transparent Consensus. In blockchain, consensus is a method for validating the chronological order at which requests, transactions (deploy and invoke) and information have been executed, modified or created. The correct ordering is critical because it can establish ownership and therefore rights and obligations. On a blockchain network, there is no centralized hub or authority 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 all nodes have access – limited to the permission level – to the information. The records are thus transparent and traceable. Beside, from the different types of consensus protocols proposed so far, the consensus ensures that a quorum of nodes agrees on the exact order in which new records are appended to the shared ledger.

Security and Immutability. Blockchain is a shared, tamper-proof replicated ledger where records are irreversible thanks to one-way cryptographic hash functions and community consensus. Immutability eliminates the need for reconciliations providing a historical, unique reconciliated version of the truth. A very important direct consequence

of 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 individuals to tamper with such a record, unless these individuals control the majority of "voters". For this reason, Blockchain has been indeed defined by The Economist 'The trust machine' [4].

Automation. Blockchain allows 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 or double records cannot be permanently written in the ledger. Automation includes the deployment of algorithms that can *self-execute*, *self-enforce*, *self-verify* and *self-constraint* the performance of the contracts (smart legal contracts or smart contract codes [5]), Decentralised Application and Decentralized Autonomous Organizations, upon business outcomes.

Metadata. Blockchain scripting languages have the potential to store small amounts of metadata on the blockchain. Meta-coins are second-layer systems that exploit the portability of the underlying coin used only as "fuel". Any transaction in the second layer represents a transaction in the underlying network. Bockchain allows financial institutions to build new networks that digitize existing asset classes (such as securities and currencies), so they can move efficiently and securely. For example, coloured coins are applications for digital representation and management of real world assets (e.g., stocks, bonds, precious metals, commodities) on top of the Bitcoin blockchain [6]. These are applications with the purpose of "coloring" Bitcoins and turning them into general tokens which represent real assets or services. Indeed, a certain amount of a digital representation of a real asset can be encoded into a Bitcoin address. The value of the coloured coins is independent from the face value of the Bitcoin, it depends instead on the value of the underlying real asset/service, and on the credit worthiness of the issuer. In this context, creditworthiness represents the willingness and capability of the issuer to redeem the coloured coins in exchange for the corresponding real asset/service. To issue a coloured coins, "colored" addresses need to be generated and they must be held in "colored" wallets managed by a color-aware clients like Coinprism [7], Coloredcoins [8], via Colu [9] or CoinSpark [10]. Note that the "coloring" process is an abstract concept indicating an asset description, some general instructions symbol and a unique hash attached to the Bitcoin addresses. Similarly, Counterparty [11] works by time-stamping and storing extra data in regular Bitcoin transactions.

II. IMPACT OF BLOCKCHAIN ON SERVICES, BUSINESS AND REGULATION

Great expectations are building up around blockchain technologies both from the private and the public sector. This is because these technologies provide the bedrock for the development of peer-to-peer platforms for the exchange of information, assets and digitized goods without the need of intermediaries. Blockchain has the potential to radically change many economic sectors and to enhance the enforcement of regulatory controls. While keeping in mind that the current fourth industrial revolution is characterized by the fusion of different technologies that blurs the borders between the physical and cyber space, blockchain shall be considered as part of a toolbox: together with other emerging technologies like Artificial Intelligence, autonomous vehicles, cloud computing, to cite a few, blockchain can disrupt many business sectors and our society at large. It would be restrictive and certainly not exhaustive to mention here some business applications. Indeed, it would be more enlightening analyzing the ways through which these technologies will bring efficiency and cost-effective solutions across markets.

A. Operational efficiency through immutable and distributed record-keeping

Current information management systems rely on databases where information is kept separated in silos. Companies hold individual digital book of records which very often require manual reconciliation activities. The lack of a "single version of the truth" and audit trails creates arbitrage concerns. Blockchain challenges the logic of information silos between market participants and eliminates the need for inter-firm reconciliation. It introduces the possibility to establish proof-of-existence and the proof-of-inexistence over events. It provides a unique historical "single version of the truth" which has community consensus, lowering the disputes for audit trials. Currently, there are several pilot projects and running applications that exploit these fundamental characteristics of blockchain technologies. For example, several businesses use the immutable time-stamping to certify the authenticity of documents and other assets, even diamonds [12]. As a matter of fact, Blockchain can be 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 artefacts 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.

B. Information symmetry through transparent record-keeping

At present, trades and negotiations are influenced by asymmetric information between economic agents which give origin to problems like moral hazard and adverse selections. Those problems have been historically solved by the introduction of central authorities with function as a single point of control (in good time) but also as a potential point of failure (in bad times). Lack of traceability and transparent accounting increase regulatory oversight. Blockchain challenges this paradigm by eliminating the imbalance of information among agents. A shared, transparent ledger increases the cooperation between regulators and regulated entities. Thus, Blockchain becomes a shared data repository for them. It allows to move from post-transaction monitoring to on-demand and immediate monitoring and improves the capability of regulators to fulfill their mandate of ensuring the legality, security and stability of the markets. 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 [13]. Finally, it reduces regulatory compliance costs significantly.

C. Decentralised Corporations and Governance

Our society is centralised and institutional hierarchies exist to govern the activities of our socio-economic communities. Blockchain enables new business models, innovative organization forms or new processes of work and production where "access" is over ownership, and "sharing" is over property. Blockchain shifts the boundary between hierarchical organizations and non-territorial, spontaneously ordered, self-organizing economies. Decentralised Organisations (DOs) and Decentralised Autonomous Organisations (DAOs) will enable new models of non- hierarchical governance, where decision making will be spread on the edges of the network instead of being concentrated at the center. DOs and DAOs will be able to run a business under an incorruptible set of business rules.
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 centralized organization process and decentralize 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 its management 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 smart contracts [36].
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: decentralized (distributed across the computers of the stakeholders), transparent, secure and auditable. The DAO is a pool of smart contracts and/or autonomous agents 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 the 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 making 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. Somehow Bitcoin can be conceived as 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 based on DAOs represent a revolution because they replace most of our business logics with new models still to come, introducing new economic paradigms changing our society. 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 attempted.

Such a DAO called **"The DAO"** was instantiated on the Ethereum blockchain [14], 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 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 about $ 160 million (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 about $ 50 million out of The DAO by exploiting a functionality in The DAO's code repeatedly launching a "recursive call exploit" 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, [15]. Current application stacks that allow for implementation of decentralized automation are NXT [16], Ethereum [14] and Eris [17], which distinguish themselves based on their core functions.

III. AN INSIGHT INTO BITCOIN

Blockchain technologies are very appealing for several business cases 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 recall how Bitcoin Blockchain and Bitcoin network work.

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 [18], 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 (at the current exchange rate) becoming the first "killer app" of Bitcoin [19].

B. Adoption

Lately, practitioners, academics and the general public 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 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 over $ 15 billion in market capitalization and the system processes hundreds of thousands of transaction a day [3].

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 an agreed 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.

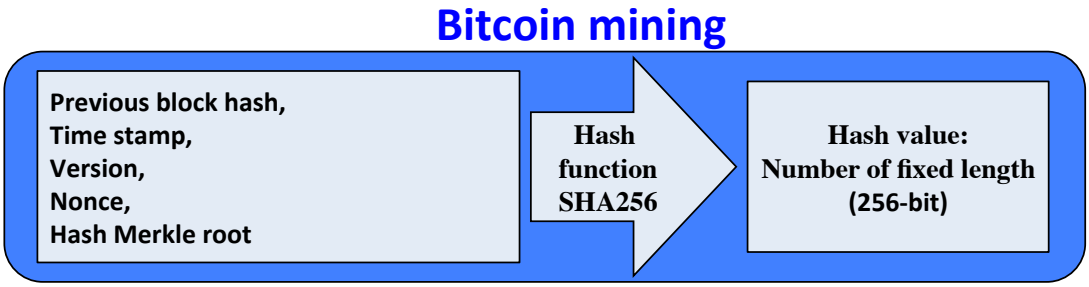

FIG. 1: Bitcoin mining is an operation that generates an hash 256bit number from the block content, the previous hash and other elements. The operation is made computationally demanding by requiring to generate a hash that is smaller than a given number by trying by chance adding a random nonce to the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

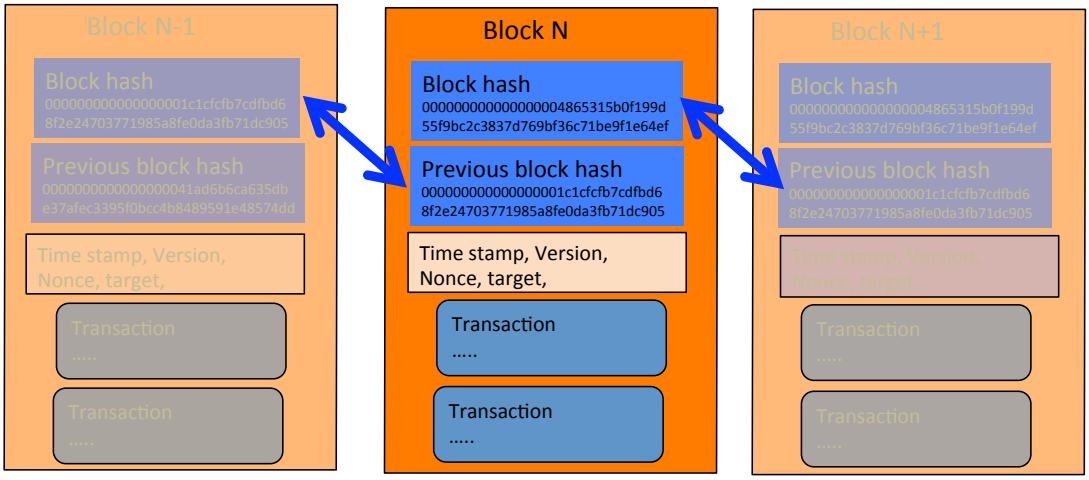

FIG. 2: Bitcoin Blockchain is a chain of text blocks containing records of transactions connected together through consecutive hash numbers generated from the content of the previous block plus a random part.

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' and locked on the previous block through hashing (see Figs.1 and 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 generate an almost unique number with a 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), see Fig.2.

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 PoW is what the so-called 'miners' are

performing. In brief, mining is a competition among users to approve transactions. A user's 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 in the system.

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 PoW for profit. Nowadays, most of mining is concentrated in large "mining farms" mostly located in regions with low electricity costs. 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* [20]. 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. Addresses are normally used for one transaction only. 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 address of the recipient which, in this case, is 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 Bitcoin 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 into 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* (a random 32-bit field), 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. The nonce in a Bitcoin block is a 32-bit (4-byte) field whose value is set so that the hash of the block will contain a run of leading zeros. The rest of the fields must not be changed, as they have a defined meaning (though, when the nonce has exhausted unsuccessfully all combinations, the block-time is changed). Since

it is believed infeasible to predict which combination of bits will result in the right hash, many different nonce values are tried, and the hash is recomputed for each value until a hash containing the required number of zero bits is found [21].

IV. 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 [1].

From an historic perspective (see [22]) this technology has his roots in the ideas of Merkle elaborated at the end of the 70' when he proposed the use of concatenated hashes in a tree structure for digital signature, the so called 'Merkle tree' [23]. Hashing was invented sometime earlier in the 50' [24] and it has been widely used in cryptography for information security, digital signatures and message integrity verification. About ten years after the Merkle idea of a chain of hashes was prosed by Leslie Lamport for secure login [25]. Then, after other ten years in 1990, just at the dawn of the World Wide Web (Tim Berners-Lee 1989 [26]), the first crypto currency for electronic payments, the e-Cash, was proposed by Chaum [27]. 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 [28]. Ideas that made immediately their way into proposals for electronic payment systems with hash chains [29, 30] and electronic cash [31]. In 2002 Adam Back proposed the hashcash [32] an electronic currency based on Blockchain an PoW 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.

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. 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.

V. BLOCKCHAIN EFFICIENCY AND PHYSICAL LIMITS

Blockchain systems have several appealing features, their power resides in the interoperability, in the absence of vulnerable single point of failure and in the community-based verification process through consensus mechanism. 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.

A. Specialization

At the basis of Blockchain technology is the PoW, the community verification and cryptographic sealing mechanism that joins blocks together. This consensus mechanism has been proven to be very resilient to attempts 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, in most of the cases, are not users which participate to the system but they 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. Currently, 45% of Bitcoin hashrate is produced by five mining pools [33].

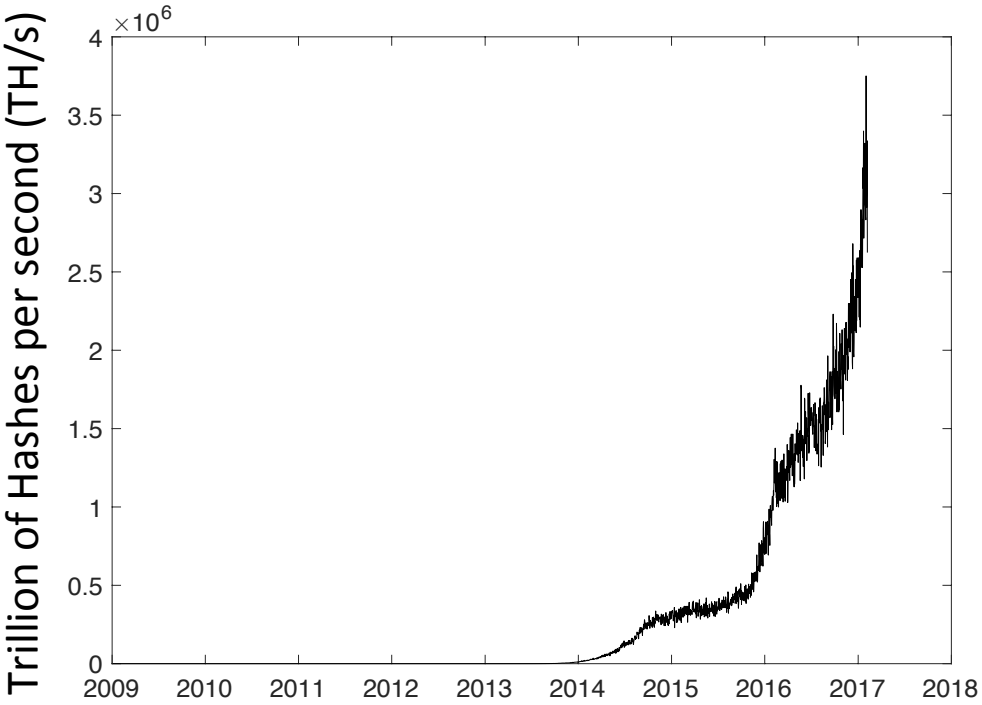

FIG. 3: Bitcoin Blockchain mining requires the production of a large number of hashing attempts. Currently the network is generating around 4 million trillion ($4\ 10^{18}$) of hashes per second. Electricity consumption can be estimated around 0.1 to 1 W/GH corresponding to around 1GW of electricity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

B. Costs

Bitcoin is consuming very large amount of electricity to perform PoW. Currently in Bitcoin a successful hash is generated in average after $2\ 10^{21}$ (two billion trillions) hash attempts which correspond to an average electricity consumption per block of about 1,000 GW at an estimated cost of an order of magnitude around $10,000. This is a massive quantity of energy, however, it was pointed out in [34] that the cost of PoW must be equivalent to the amount one could 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 PoW should be indeed around $10,000. Indeed this makes a double spending attack with some chances of success costing around $100,000. This is a large amount to put at risk with such an attack which has potential to double spend no more than $1M (the total amount typically transferred in a block). This cost makes Bitcoin an expensive system to transfer money consuming about 1% of the transferred value in electricity. However, in Bitcoin, community 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 previously [34] estimated '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 could 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. Alternatively, Proof-of-stake (PoS) approach pseudo-randomly selects next block creators among participants in relation to their 'wealth' reducing in this way the need to burn large resources in PoW [21].

C. Speed

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 reach over one million transactions per second. Finacial markets are currently trading at nano-second speed but 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 to current models with strong implications over centralization, security, egalitarian structure and anonymity issues.

D. Governance

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. Protocols, rewards and incentives are affecting system efficiency [35]. Changes can impact on business models and threaten investment's returns, sparkling huge tensions. 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 into a clone of the DAO held by only the attacker itself (see Section II C). 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 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 demonstrates that governance in distributed systems is a very complex matter where minorities can autonomously separate from 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.

E. Concentration

Another point of weakness of distributed system is the tendency towards concentration and creation of semi-monopolistic regimes. We have witnessed this happening in all new technology sectors that started distributed and egalitarian and then evolved into highly concentrated structures. This tendency is particularly strong and fast for ICT and web services providers. Indeed, one of the main aspects associated with the emergence of new technology is that the required infrastructure 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 peers 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

We acknowledge support from EPSRC grant EP/P031730/1.

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[2] T Economist. The trust machine. The Economist, 2015.
[3] Paolo Tasca. Digital currencies: Principles, trends, opportunities, and risks, 2015.
[4] The Economist Newspaper Limited, editor. The trust machine. The Economist, 2015.
[5] Christopher D Clack, Vikram A Bakshi, and Lee Braine. Smart contract templates: foundations, design landscape and research directions. arXiv preprint arXiv:1608.00771, 2016.
[6] Bitcoin Wiki. Colored Coins. `https://en.bitcoin.it/wiki/Colored_Coins`, 2015. (Date last accessed: 03-Jan-2017).
[7] Coinprism. `https://www.coinprism.com/`, 2015. (Date last accessed: 15-Jan-2017).
[8] Colored Coins. `http://coloredcoins.org/`, 2017. (Date last accessed: 15-March-2017).
[9] Colu. `http://colu.co/`, 2015. (Date last accessed: 03–Feb-2017).
[10] CoinSpark. `http://coinspark.org/`, 2015. (Date last accessed: 03-Jan-2017).
[11] Counterparty. `http://counterparty.io/`, 2015. (Date last accessed: 10-Jan-2017).
[12] `https://www.everledger.io/`, 2017. (Date last accessed: 20-Apr-2017).
[13] `https://www.fca.org.uk/publication/corporate/business-plan-2016-17.pdf`, 2016. (Date last accessed: 20-Apr-2017).
[14] `https://www.ethereum.org/`. (Date last accessed: 20-Apr-2017).
[15] R Price. Digital currency ethereum is cratering because of a $50 million hack. Business Insider, 2016.
[16] `https://nxt.org/`. (Date last accessed: 20-Apr-2017).
[17] Eris. `https://monax.io/`. (Date last accessed: 20-Apr-2017).
[18] `https://www.torproject.org/`. (Date last accessed: 20-Apr-2017).
[19] Calebe de Roure and Paolo Tasca. Bitcoin and the ppp puzzle, 2014.
[20] Andreas M Antonopoulos. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. " O'Reilly Media, Inc.", 2014.
[21] Bitcoin wiki. https://en.bitcoin.it/wiki/Nonce, 2017.
[22] Eduard de Jong. A short history of the blockchain, 2015.
[23] 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.
[24] Herbert Hellerman. Digital computer system principles. 1967.
[25] Leslie Lamport. Password authentication with insecure communication. Communications of the ACM, 24(11):770–772, 1981.
[26] `http://webfoundation.org/about/vision/history-of-the-web/`. (Date last accessed: 20-Apr-2017).
[27] 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.
[28] Neil Haller. The s/key one-time password system, 1995.
[29] Torben P Pedersen. Electronic payments of small amounts. In International Workshop on Security Protocols, pages 59–68. Springer, 1996.
[30] Ronald L Rivest and Adi Shamir. Payword and micromint: Two simple micropayment schemes. In International Workshop on Security Protocols, pages 69–87. Springer, 1996.
[31] 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.
[32] Adam Back et al. Hashcash-a denial of service counter-measure, 2002.
[33] `https://blockchain.info/`. (Date last accessed: 20-Apr-2017).
[34] Tomaso Aste. The fair cost of bitcoin proof of work. SSRN 2801048, 2016.
[35] Giuseppe Pappalardo, T Di Matteo, Guido Caldarelli, and Tomaso Aste. Blockchain inefficiency in the bitcoin peers network. arXiv preprint arXiv:1704.01414, 2017.
[36] Christopher J. Dew. Post-Capitalism: Rise of the Collaborative Commons. The Revolution will not be Centralized. `https://medium.com/basic-income/post-capitalism-rise-of-the-collaborative-commons-62b0160a7048/`. (Date last accessed: 10-Feb-2017).