

Blockchain Technologies: The Foreseeable Impact on Society and Industry

Tomaso Aste and Paolo Tasca, University College London and UCL Centre for Blockchain Technologies

Tiziana Di Matteo, King's College London, University College London, and UCL Centre for Blockchain Technologies

The authors describe blockchain's fundamental concepts, provide perspectives on its challenges and opportunities, and track its origins from the Bitcoin digital cash system to recent applications.

Blockchain is a technology that uses community validation to keep synchronized the content of ledgers replicated across multiple users. Although blockchain derives its origins from technologies introduced decades ago, it has gained popularity with Bitcoin. In 2008, an anonymous individual, or group, under the pseudonym of Satoshi Nakamoto posted a white paper introducing Bitcoin, a blockchain digital currency application.¹ Bitcoin is the first example of widespread digital currency that provides a solution to the problem of trust in a decentralized self-sovereign monetary system. Bitcoin's blockchain is a decentralized peer-validated time-stamped ledger that chronologically registers all valid transactions. The ledger is publicly auditable by all network participants (peers), which can be either individuals or autonomous agents operating without human intervention.²

Transactions are broadcast to the Bitcoin network, and their validity is verified independently by peers. Valid transactions are collected into blocks that are

cryptographically sealed. Special peers, called *miners* or (more generally) *voters*, compete to interlock the new block on top of the last block to form a chronological sequence—a chain of blocks. Competition is based on the relative computational power of each miner with respect to the total computational power of all the miners active in the network.

Blockchain has opened a range of new possibilities for businesses in which value can be directly transferred between participants over the Internet in the same easy way as paying cash and in the same convenient way as using instant messaging without intermediaries or centralized points of control.

Blockchain is generally included in the larger family of distributed-ledger technologies, which encompass all methods for decentralized record keeping of transactional and data sharing across multiple servers, countries, or institutions. Not all distributed ledgers employ a chain of blocks, but for simplicity, here we use the term “blockchain technologies” to indicate the general class

of distributed ledgers based on community consensus.

DRIVERS OF THE BLOCKCHAIN REVOLUTION

Apart from its original 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.³ To better grasp the potentialities of blockchain, we can view it through two lenses. Through the first lens, it can be seen as an information and communications technology (ICT) to record the ownership of on-platform and off-platform assets and the rights and obligations arising from agreements. Indeed, any data type can be recorded on a blockchain—from ownership of assets to contractual obligations to creative art copyrights or credit exposures or digital identity. Through the second lens, blockchain can be seen as an institutional technology to decentralize the governance structures used to coordinate people and economic decision making.⁴ Although we take the ICT perspective, the blockchain revolution's key drivers can be described in terms of both the ICT and institutional perspectives. The main drivers include decentralized and transparent consensus, security and immutability, and automation.

Decentralized and transparent consensus

In blockchain, consensus is a method for validating the chronological order in which requests, transactions (deploy and invoke), and information have been executed, modified, or created. The correct order is critical because it can establish ownership and therefore rights and obligations. A blockchain

network has no centralized hub or authority that determines transaction order, approves transactions, or sets rules for how nodes interact with one another. Instead, many validating peer nodes implement the network-consensus protocol, and all nodes have access to the information according to their access-permission level. The records are thus transparent and traceable. The consensus protocol 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 in which records are made irreversible and nonrepudiable thanks to one-way cryptographic hash functions. Immutability eliminates the need for reconciliations because it provides a unique reconciled version of the truth—the transaction history between peers. An immutable historic record validated by community consensus generates trust in the system. It becomes exceedingly difficult for an individual or any group to tamper with such a record, unless these individuals control the majority of the miners (voters). Indeed, *The Economist* has even labeled blockchain “the trust machine.”³

Automation

Blockchain allows a group of independent parties to work with universal data sources, automatically reconciling among 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-constrain* the performance of the contracts (smart legal contracts or smart contract codes⁵). This allows the creation of decentralized applications and decentralized autonomous organizations (DAOs) that can operate without central governance.

Metadata

Blockchain scripting languages have the potential to store metadata on the blockchain. Metacoins are second-layer systems that exploit the portability of the underlying coin used only as “fuel”—that is, as an enabler for action on the other layer. Any transaction in the second layer is directly linked to a transaction in the underlying network. With blockchain, financial institutions can build new networks that digitize existing asset classes (such as securities and currencies) so that they can be moved efficiently and securely. For example, colored coins (en.Bitcoin.it/wiki/colored_coins) are applications for digitally representing and managing real-world assets (stocks, bonds, precious metals, and commodities) on top of the Bitcoin blockchain. These applications aim to color Bitcoins, turning them into general tokens that represent real assets or services. A certain amount of a real asset's digital representation can be encoded into a Bitcoin address. The value of the colored coins is independent from the Bitcoin's face value; it depends instead on the value of the underlying real asset or service and on the issuer's creditworthiness. In this context, creditworthiness represents the willingness and capability of the

issuer to redeem the colored coins in exchange for the corresponding real asset or service.

To issue colored coins, colored addresses need to be generated and must be held in colored wallets managed by a color-aware clients like Coinprism (coinprism.com) or Coloredcoins (coloredcoins.org), via Colu (colu.co) or CoinSpark (coinspark.org). 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 (counterparty.io) works by time-stamping and storing extra data in regular Bitcoin transactions.

EFFECT ON SERVICES, BUSINESS, AND REGULATION

Both the private and public sectors have great expectations for blockchain technologies because they provide the bedrock for developing peer-to-peer platforms for exchanging information, assets, and digitized goods without intermediaries. Blockchain has the potential to radically change many economic sectors and to enhance the enforcement of governance and regulatory controls in a completely innovative way. In the context of the current fourth industrial revolution, which is characterized by the fusion of diverse technologies that blurs the borders between physical and cyber space, blockchain is part of a broader toolbox: together with other emerging technologies, notably machine learning, artificial intelligence (AI), autonomous vehicles, and fog computing, blockchain can disrupt many business sectors and society at large. It would be restrictive and certainly not exhaustive to mention

business applications. A more enlightening perspective is an analysis of the ways in which these technologies will bring efficiencies and cost-effective solutions across markets.

Operational efficiency

Immutable and distributed record keeping validated by community consensus will promote operational efficiency in many domains. Indeed, current information management systems rely on databases in which information is kept in silos. Companies hold individual digital books of records that frequently require manual reconciliation. 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 interfirm reconciliation. It introduces the possibility of establishing proof-of-existence and proof-of-nonexistence over events. It provides a unique historical single version of the truth that has community consensus, lowering disputes over audit trials.

Currently, several pilot projects and running applications exploit these fundamental characteristics of blockchain technologies. For example, several businesses use immutable time-stamping to certify the authenticity of documents and other assets, even diamonds (everledger.io). Blockchain can be used to time-stamp anything and provide a digital or digitalized asset's proof-of-existence at a given moment. This can be a game changer in sectors such as creative arts in which digital identical duplication makes artifact value hard to protect. Instead, blockchain provides a way to make the artifact unique and uniquely located in time (and space). Blockchain

provides the instrument for creating digital value that can be transferred, exchanged, and traded with protection from illegal uncontrolled duplication and counterfeiting.

Rebalancing information symmetry

Information symmetry can be improved through transparent record keeping. At present, trades and negotiations are influenced by asymmetric information among economic agents, which gives rise to problems such as moral hazards and adverse selections. Those problems have been historically solved by the introduction of central authorities that function as a single point of control in good times, but also as a potential point of failure in bad times. Lack of traceability and transparent accounting and accountability increase the need for 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 the move from post-transaction monitoring to on-demand and immediate monitoring and improves the capability of regulators to fulfill their mandate of ensuring the markets' legality, security, and stability by enabling access to auditable data that is verified, time-stamped, and immutable. The reliability and reputation of clients and service providers can be verified and monitored by analyzing the historic record in the blockchain. Rules can be encoded within the system, enabling automated review through audit software. In this way, blockchain generates a transparent, interoperable

environment in which rules can be implemented, enforced, and adapted. As such, its adoption in the services sector could benefit both industry and regulators. This convergence of industry and government interests is unique, provides great opportunities for both business players and regulators,⁶ and reduces regulatory compliance costs significantly.

Decentralized corporations and governance

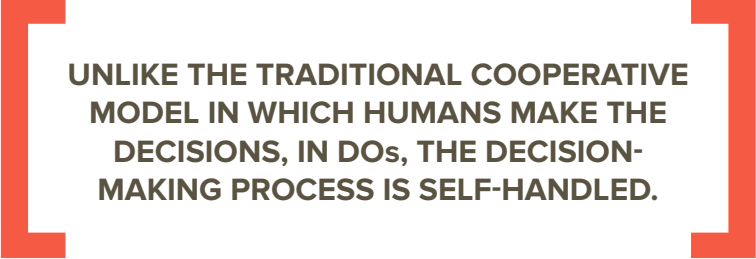
Our society is centralized and institutional hierarchies exist to govern the activities of our socioeconomic communities. Blockchain enables new business models, innovative organization forms, and novel work and production processes in which access is over ownership, and sharing is over property. Blockchain shifts the boundary between hierarchical organizations and nonterritorial, spontaneously ordered, self-organizing economies. Decentralized organizations (DOs) and DAOs will enable new models of nonhierarchical governance, in which decision making is spread across the network's nodes instead of being concentrated at its center. DOs and DAOs will be able to run a business autonomously under an incorruptible set of business rules coded into smart contracts.

As is true of any traditional organization, the DO is governed under specific divisional functional structures in which decisions are made at different hierarchical levels on the basis of a predetermined set of rules, routines, and codes of conduct. The DO simply decentralizes a centralized organizational process while also making it automatically executable. Instead of a hierarchical structure managed through personal interaction, a DO

manages human interaction through a protocol specified in code and enforced on the blockchain. For example, a DO might use a blockchain voting system, a blockchain accounting and production system, or a blockchain shareholders registry.

Decentralized organization. The DO follows a cooperative model in that its members participate in its management and equally share its collectively managed resources. As cooperatives generally do, DOs can flatten and

with an initial capital. The DAO handles decision-making processes independently under a predefined rule set without human intervention. Unlike the DO, the DAO fully controls the information process, and no majority can influence the decision process; for example, collusion attacks are considered to be a bug. In contrast, in the DO, humans control the information flow and thus the decision-making process is biased toward the type of information through which decisions are made.



UNLIKE THE TRADITIONAL COOPERATIVE MODEL IN WHICH HUMANS MAKE THE DECISIONS, IN DOs, THE DECISION-MAKING PROCESS IS SELF-HANDLED.

democratize, or even invert, the traditional hierarchical management pyramid. But unlike the traditional cooperative model in which humans make the decisions, in DOs, the decision-making process is self-handled in some fashion, such as through a predefined enforceable tamper-proof set of rules coded into smart contracts.⁷

Decentralized autonomous organization. Under a predefined rule set, the DAO runs a business or social activity either online or offline completely autonomously through open source software that is decentralized (distributed across the stakeholders' computers), transparent, secure, and auditable. The DAO is a pool of smart contracts and/or autonomous agents linked together and endowed

Bitcoin can be thought of as the first DAO experiment with producers (miners), investors (Bitcoin buyers), customers (Bitcoin merchants and users), and product (the social welfare of the Bitcoin network participants).

Blockchain application stacks based on DAOs represent a revolution because they replace most of our business logic with new models still to come, introducing new economic paradigms that could change our society. Imagine, for example, a DAO that can autonomously select and invest in different start-ups, govern their business development, and then sell its stakes on them to other funds and redistribute the profits to its shareholders. Indeed, a first practical implementation of such a DAO—called The DAO—has already been attempted. The DAO was

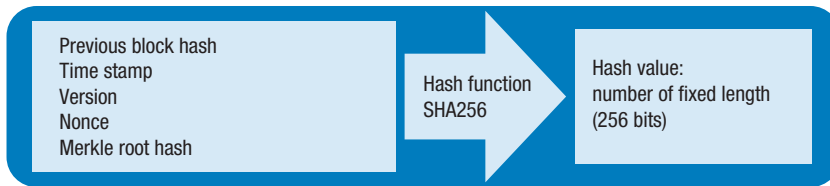


FIGURE 1. Bitcoin mining. The Bitcoin mining operation generates a hash 256-bit number from the block content, the previous hash, and other elements. The operation is computationally demanding because a hash smaller than a given number must be generated by adding a random nonce—an arbitrary number that can be used only once—to the block.

instantiated on the Ethereum blockchain (ethereum.com) and had no conventional management structure or board of directors. It was intended to operate as a hub for autonomously dispersing Ether, the Ethereum value token, to real business projects voted on by an open community of donors and members. The DAO did not hold money; rather, it held tokens that gave its donors and members rights to vote on potential projects. Anyone could pull out their funds until their 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. However, it also set the record for the fastest collapse: a few months from The DAO's launch, an investor tunneled out about \$50 million by exploiting a functionality in The DAO's code, repeatedly launching a recursive call requesting funds from The DAO.⁸ In other words, The DAO was not hacked; it simply executed its code and, by doing so, went bankrupt. It was a bad business model.

However, The DAO was a failure only from the viewpoint of its investors. From a technical perspective it had worked seamlessly. The DAO is an example of how applications running on top of blockchains have much potential but also pose challenges and risks. Current application stacks that allow for decentralized automation implementation and distinguish themselves by their core functions include NXT (nxt.org), Ethereum, and Eris (monax.io).

BITCOIN

Blockchain technologies are compelling for several business cases well beyond their original purpose of digital cash. However, Bitcoin is not only the first example of using blockchain and community validation, but, with a market capitalization of more than \$40 billion as of May 2017, it also remains the largest-scale application. Other blockchain systems have been proposed, but most of these are built on the original Bitcoin design.

Origins

In the first few years after its introduction in 2008,¹ Bitcoin was limited mostly to underground cryptoanarchist communities. These groups employed cryptography to enable individuals to make consensual economic arrangements that transcended national boundaries and centralized authorities. Unfortunately, those activities were often associated with the *counter* economy which generally includes all the underground actions of civil and social disobedience outside normative and legal frameworks. In fact, Bitcoin was de facto the *only* currency used in the deep web—the hidden Internet where illegal services and goods can be traded without any police or criminal agency interference and access is only through the Onion Router (Tor) anonymous communication system (torproject.org). According to the FBI, the online black market Silk Road (the eBay of drugs), which ran in the deep web between 2011 and 2013 and generated a revenue of almost \$3 billion (at the current exchange rate), was Bitcoin's first killer app.⁹

Adoption

Lately, practitioners, academics, and the general public have started to show interest in Bitcoin, thanks to increasing media attention sparked by the Bitcoin-USD exchange rate, which spiked to about \$1,200 in late 2013 from an exchange at tiny fractions of a dollar in 2009. Meanwhile, various individuals began using Bitcoin as a medium of exchange and in small businesses. As of May 2017, Bitcoin had reached hundreds of thousands of transactions per day.⁴

People frequently ask, "Is Bitcoin money?" The answer is yes, but it is smarter than cash; Bitcoin is money as information. Namely, every Bitcoin transaction is a monetary transaction that is as simple as sending an email; it is tamper-proof and publicly auditable and irreversible. Each transaction is first broadcast to the Bitcoin network and then validated by anonymous independent peers according to a specific consensus protocol that determines whether and when the given transaction must be added to the ledger. The consensus mechanism represents a major breakthrough, as it automatically determines an agreed-on trustworthy chronological order of the truth among anonymous users without the need for a third-party neutral intermediary or a central counterparty.

The blockchain

Transactions are broadcast to the Bitcoin network, and their validity is verified independently by network participants. Valid transactions are recorded locally by miners, who must verify the validity of the transactions and put them in a list that becomes a cryptographically sealed block. The block is then locked on the previous block

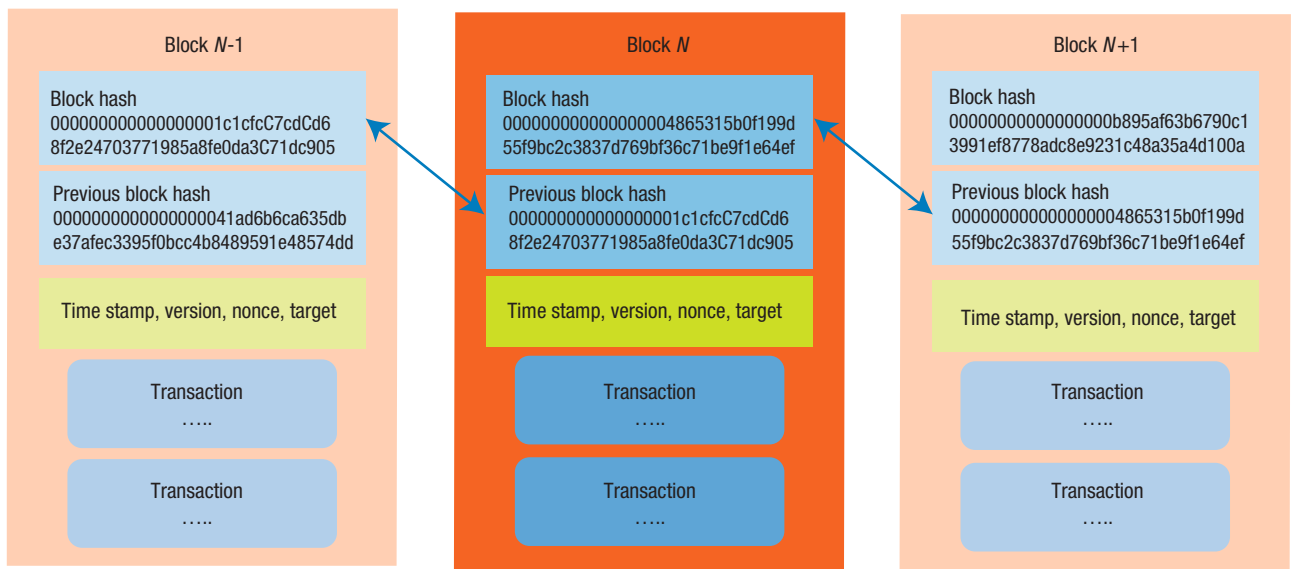


FIGURE 2. Bitcoin blockchain. The blockchain consists of text blocks containing records of transactions that are linked through consecutive hash numbers generated from the content of the previous block plus a random part.

through hashing, as shown in Figure 1. Blocks are sealed approximately every 10 minutes and contain an average 1,700 transactions accounting to about \$1 million.

Cryptographic sealing involves generating a hash number from the current block's content, the previous block's hash, and a random part. Hashing is a simple operation that transforms and synthesizes any digital information into a single number (digest). The algorithm is devised to generate an (almost) unique number with a fixed size that is deterministically associated with the input. The function is injective: after hashing, any two very similar inputs (for example, two long pieces of text that differ by only one character) will correspond to completely different digests in a way that makes it impossible to reconstruct the original two inputs. Bitcoin mining uses the Secure Hash Algorithm hashing protocol to produce 256-bit numbers (SHA256), as shown in Figure 2.

Proof of work and mining

Hashing is used for *proof of work* (PoW): a mechanism that links consensus with computing power, making the consensus mechanism expensive. The

PoW is the basis for mining—a competition among users to validate transactions. A user's chance of winning is proportional to the computing power he or she controls, following Nakamoto's motto "one CPU, one vote." Users are rewarded for contributing to block verification/validation and construction. Each mined block contains a *coinbase* transaction (as of May 2017, 12.5 Bitcoins), which is allocated to the winning user. This mechanism is the only way to generate new Bitcoins in the system.

This rich compensation for winning has generated miners who perform the PoW only for profit. Nowadays, most mining is concentrated in large mining farms located primarily in China and in regions with low electricity costs. Miners can also be in mining pools that share profits in proportion to hashing power contribution. Mining is performed almost exclusively with hardware developed explicitly for Bitcoin/altcoin hashing. These state-of-the-art ASIC machines compute several terahashes per second (TH/s) consuming some fraction of watts per gigahash (W/GH). Figure 3 shows the historic mining activity for Bitcoin verification worldwide.

Transactions

The mechanism for registering Bitcoin transactions has three key elements: private key (k), public key (K), and Bitcoin address.² Bitcoin ownership is established through the possession of k , which is automatically generated and stored in a wallet file. k is used to encrypt transactions and, similar to a credit card's PIN, must be kept secret so that no one else has control over the Bitcoins secured by k . K is generated by k and paired with k so that recipients can decrypt transactions. Finally, the Bitcoin address is generated by K through one-way cryptographic hashing and is used to identify a Bitcoin network participant. The address is essentially a pseudonym for the participant and, to increase anonymity, is typically changed in any new transaction.

When a transaction takes place, the blockchain registers the change of Bitcoin ownership by debiting the Bitcoin amount to the sender's Bitcoin address and crediting the same amount to the recipient's Bitcoin address. To illustrate these elements, consider the transaction in which Alice (A) wants to give Bob (B) one Bitcoin.

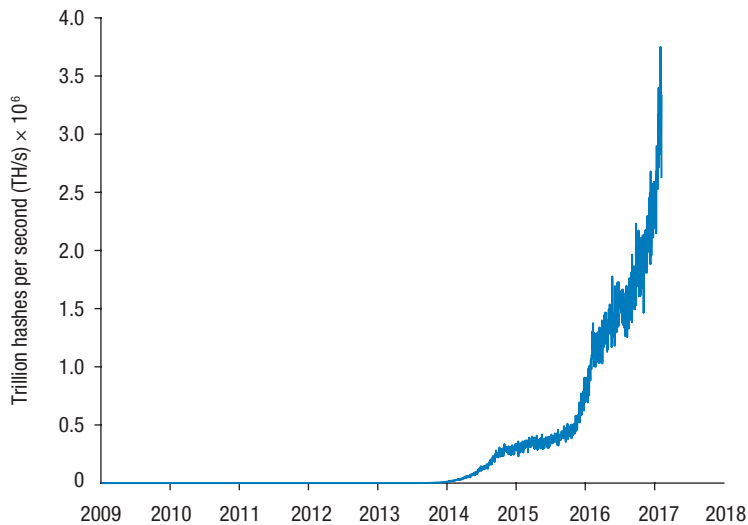


FIGURE 3. Mining in the Bitcoin blockchain. The mining operation requires the production of a large number of hashing attempts. As of May 2017, the network was generating around 4 quintillion (4×10^{18}) hashes per second. Estimated electrical consumption is 0.1 to 1.0 watts per gigahash (W/Gh) corresponding to around 1 gigawatt (GW) of electricity consumed per second. The figure is based on data from blockchain.info.

Sender's role. Because the Bitcoin system uses the money-as-information idea, the transaction is a string of bits in which 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 . The signature then depends on the message content and on k and is generated through a signing algorithm. Finally, A will send to B the message together with the signature and K . Similar to sending an email, the sender must know the recipient's address, in this case, B's Bitcoin address.

Recipient's role. With the message, signature, and K , B can verify and accept the transaction as valid, confirming that A does indeed own one Bitcoin with serial number 123456 at the time of the transfer. All other network participants can then collectively verify this ownership. B hashes the original message and uses K to decrypt the originally signed data. If the two hashes are identical, the signature is valid and message authentication, non-repudiation, and integrity are granted.

Collective validation. To verify the transaction from A, B does a sanity check that the Bitcoin with serial number 123456 belongs to A. If it does, B will broadcast the signed string of bits to the entire network and other network participants will then collectively verify whether A holds one Bitcoin with serial number 123456. For example, suppose that David (D) is a network miner who receives A's message: "I, A, am giving B one Bitcoin with serial number 123456." Serial number 123456 also contains references to specific previous transactions received at A's address (transaction inputs) for an equivalent number of Bitcoins to cover the one Bitcoin that A wants to send to B. D can then verify if the inputs allow A to transfer exactly one Bitcoin to B. Because 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. Finally, D appends the transaction into a block together with other recent transactions.

Hashing. D now needs to compute new hash values that are 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; en.Bitcoin.it/wiki/nonce), such that the new hash value will start with a number of zeros larger or equal to a given target number. Because it is infeasible to predict which bit combination will yield the right hash, many nonce values are tried, and the hash is recomputed for each value until a hash containing the required number of initial zeros is found. If the nonce exhausts all combinations and does not find the right one, then the block time is changed. If D finds the suitable nonce/block-time that produces a valid hash, 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 block and the nonce such that the network can check-test the validity.

WHY BLOCKCHAIN IS INNOVATIVE

It has been written that blockchain is a major technological innovation, a trust machine that might have even set the beginning of human recorded history and that will revolutionize our society.³ What is meant by "innovative" then? In fact, there is no true technical innovation in Bitcoin and blockchain; all ingredients had already been developed well before the "disruptive" Bitcoin paper by Nakamoto in 2009.¹

From a historic perspective,¹⁰ this technology has its roots in the ideas that Ralph C. Merkle elaborated at the end of the 1970s when he proposed the *Merkle tree*—the use of concatenated hashes in a tree structure for digital signatures.¹¹ Hashing had been in use since the 1950s¹² and was widely applied in cryptography for

information security, digital signatures, and message-integrity verification. About a decade after the Merkle idea, Leslie Lamport proposed using a hash chain for secure login.¹³ In 1990, at the dawn of the web,¹⁴ e-Cash, the first cryptocurrency for electronic payments, was described.¹⁵ Further evolutions and refinements of the hash chain concept were introduced in the 1994 paper by Neil Haller on the S/KEY application, a hash chain for Unix login.¹⁶ These ideas immediately made their way into proposals for electronic payment systems with hash chains¹⁷⁻¹⁸ and into electronic cash.¹⁹ In 2002, Adam Back proposed hashcash,²⁰ an electronic currency based on blockchain and a PoW that has most of Bitcoin's elements and was indeed cited by Satoshi Nakamoto as Bitcoin's reference work. Interestingly, the literature remained rather quiet for the next six years until Nakamoto came out with the "disruptive" paper on Bitcoin.

We can say with some confidence that Bitcoin's main novelty is its proof of concept that peer-to-peer systems can operate without the intermediation of trusted central authorities. The proof is that Bitcoin has managed to exist and operate autonomously for the past nine years with a considerable capitalization and a sizable transaction volume without being seriously challenged by any attack. The reasons for its widespread adoption are most likely attributable to the historic period in which it began, the banking crisis, and the development of alternative business (and criminal) models to technological innovation. Regardless of its origins, Bitcoin and blockchain technologies have started to revolutionize our way of doing business and our way of life.

EFFICIENCY AND PHYSICAL LIMITS

Blockchain systems have several appealing features: their power resides in their interoperability, the absence of a vulnerable single failure point, and consensus-based verification. However, in terms of efficiency and control, centralized systems are often easier to manage, easier to scale, and faster to operate. Miners can be a source of problems because they are a specialized user community motivated by profit. Replication and broadcasting of all transactions is computationally and network intensive. Operations are slowed by the need for verified consensus. Limited governance and concentration in select market sectors are also issues.

Specialization

As a consensus mechanism, the PoW is a critical part of the Bitcoin blockchain and has proven highly robust to tampering. It processes information fed by users, and the user community collectively verifies the information's authenticity and validity. Tampering with the system would require controlling a large part of that community, which is difficult and costly to achieve.²¹ However, truth is decided by the miners, those with the most computational power. Miners are frequently not network users but rather participate only to contribute to the PoW for profit. As a result, control of the peer-to-peer community is given de facto to a few miner groups. From 2013 to 2015, the cumulative market share of the largest 10 pools relative to the total market hovered at about 70 to 80 percent.⁴ This market concentration has continued: in May 2017, mining pools were producing 45 percent of the Bitcoin hashrate (blockchain.info).

Power cost

As a consensus mechanism, PoW is necessarily computationally intensive and thus consumes large amounts of electricity because participants are anonymous and their vote must be verified in proportion to the computational power used.

At the beginning of 2017, a successful hash was generated on average after 2×10^{21} (two billion trillion) hash attempts, with an electricity consumption per block of about 1,000 GW. PoW cost is calculated as the equivalent of the potential profit from an attack that attempts to alter transaction history.²¹ Each block in the Bitcoin blockchain typically represents a transferred value of \$1 million, and an attacker must control at least 10 blockchains to falsify the transaction history for long enough to collect a profit.²¹ Bitcoin consumes 1 percent of the transferred value in electricity, or \$10,000 per block. A double-spending attack with some chance of success would cost around \$100,000—a large amount to put at risk for an attack that will double-spend no more than \$1 million. Adding to this concern is the complication of introducing coloring. It is reasonable to expect that Bitcoin will dynamically adapt PoW cost to the transferred value. However, if colored coins introduce transactions associated with external assets that are not represented as value in a Bitcoin transfer, the system could become biased toward blocks with larger real value. In that case, costly attacks could become profitable.

Blockchains can be constructed through mechanisms that do not require expensive consensus mechanisms, but at the cost of relaxing one or more other properties, such as anonymity or equality in distributed

verification. Cost-reduction approaches include increasing the number of blocks to wait before a transaction is considered accepted, reducing the value of the transactions in each block, or minimizing anonymity in consensus validation. For example, in a blockchain system with permissions, in which only identifiable and authorized users contribute to verification, the PoW could be virtually eliminated by using direct voting. However, such a system would introduce other vulnerabilities, such as in the verification of voters and the control over double-counting votes. Several other consensus protocols have been proposed, including proof of stake (PoS), proof of importance (PoI), proof of activity (PoA), proof of burn (PoB), proof of deposit (PoD), proof of capacity (PoC), and federated Byzantine agreement (FBA).²² All these protocols solve some of the problems of Bitcoin's PoW but they also introduce new issues.

Slower operation

Blockchain systems have physical limits as well. Current electronic payment systems, such as PayPal or Visa, handle several thousand transactions per second, and exchanges such as Nasdaq reach over one million transactions per second. Financial markets are currently trading at nanosecond speed, but a distributed system that requires community validation worldwide is limited by the speed of light, which takes over 0.1 s to traverse the globe. Consequently, a geographically scattered community that needs to reach consensus to validate transactions and that operates sequentially cannot operate faster than 0.1 s per block. A system that could handle large transaction volumes would require large blocks or mechanisms in which

multiple blocks are validated simultaneously. Alternative validation models might include local, hierarchical, and sampling validations. All these are possible paths to improve system efficiency and scalability, but they would require changing current models, which has strong implications for centralization, security, egalitarian structure, and anonymity.

Limited governance

Governance is even more problematic than physical limitations. Protocols, rewards, and incentives affect system efficiency.²³ During the last few years we have witnessed that every proposed protocol change creates tension in the Bitcoin community because it could affect business models and threaten investments' returns. Bitcoin is a distributed system, but it has a highly centralized governance. Arguably, the power of governance is limited because the technology could operate independently, outside the original network and rules. Ethereum's The DAO is an example. After someone, profiting from an unforeseen code path, managed to move \$50 million into a clone of The DAO held by the attacker, a week later, the Ethereum community imposed a hard fork, reversing the transaction and in doing so created the Ethereum Classic chain. The community now had two coexisting Ethereum chains: one with the \$50 million transaction and one without.

This example brings into question blockchain's fundamental immutability and demonstrates that governance in distributed systems is a thorny matter in which minorities can autonomously separate from the system while keeping technology and assets trading on parallel forks. The lesson is that technology is not neutral,

and technical changes have practical implications for power balances and business models.

Sector concentration

Another blockchain weakness is its tendency to concentrate in sectors and its inclination to create semimonopolistic regimes. We have witnessed this happening in new technology sectors that started as distributed and egalitarian and then evolved into highly concentrated structures. This trend is particularly strong and fast for ICT and service providers. One of the main aspects associated with emerging technology is the cost of setting up the required infrastructure. The high cost makes it convenient to scale operations and place service provision in the hands of only a few providers. An open challenge is to avoid excessive concentration in the blockchain domain and maintain distributed systems that are truly decentralized and peer to peer. We hope that academic, business, and regulatory communities will take on this challenge, which will facilitate the organic growth of this sector.


We are on 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 intermediaries. Tokenization of the economy through digital currencies supported by blockchain technologies is the next foreseeable revolution. Several trillion dollars will be involved in this new economy that promises to reduce costs and increase the speed and security of transactions through

ABOUT THE AUTHORS

TOMASO ASTE is a professor of complexity science in the Computer Science Department at University College London (UCL), founder and director of the UCL Centre for Blockchain Technologies (UCL CBT), head of UCL's Financial Computing and Analytics Group, program director of UCL's MSc in financial risk management, and vice director of the UCL Centre for Doctoral Training in Financial Computing & Analytics. His research interests include financial systems modeling and complex data analytics, predictive analytics using network theoretic and statistical physics tools, and the application of blockchain technologies to domains beyond digital currencies. Aste received a PhD in material sciences and engineering from Politecnico di Milano. He is a member of the board of the London School of Economics and Political Science (LSE) Systemic Risk Centre. Contact him at t.aste@ucl.ac.uk.

PAOLO TASCA is a digital economist specializing in peer-to-peer (P2P) financial systems, an advisor on blockchain technologies for international organizations including the EU Parliament and the United Nations, and UCL CBT's founder and executive director. Contact him at p.tasca@ucl.ac.uk.

TIZIANA DI MATTEO is a professor of econophysics in the Mathematics Department at King's College London and an honorary professor at UCL's external faculty of complexity science hub in Vienna. Her research interests include complex networks and data science. Di Matteo received a PhD in physics from the University of Salerno. She is co-editor-in-chief of the *Journal of Network Theory in Finance* and editor of the *European Physical Journal B*. Contact her at tiziana.di_matteo@kcl.ac.uk.

disintermediation. This disintermediation opens the possibility of direct value exchange between peers over the web. Peer-to-peer systems are little known and, if we begin to see the positive potentials of these systems, we also begin to be concerned about the new threats they can introduce.²⁴ 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 will collective irrational phenomena such as sentiment and confidence swings affect the capability of these markets to operate? How can we govern and regulate these systems to avoid abuses and protect users? All these questions require further understanding and investigation. 

ACKNOWLEDGMENTS

We acknowledge support from Economic and Political Science Research Council (EPSRC) grant EP/P031730/1.

REFERENCES

1. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008; bitcoin.org/bitcoin.pdf.
2. A.M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, 2014.
3. "The Trust Machine," *The Economist*, 31 Oct. 2015; economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.
4. P. Tasca, "Digital Currencies: Principles, Trends, Opportunities, and Risks," 2015; papers.ssrn.com/sol3/Papers.cfm?abstract_id=2657598.
5. C.D. Clack, V.A. Bakshi, and L. Braine, "Smart Contract Templates: Foundations, Design Landscape, and Research Directions," 2016, arXiv preprint; arXiv:1608.00771.
6. Financial Conduct Authority, "Business Plan 2016/17," 2016; fca.org.uk/publication/corporate/business-plan-2016-17.pdf.
7. C.J. Dew, "Post-Capitalism: Rise of the Collaborative Commons—The Revolution Will Not Be Centralized," 18 Mar. 2015; medium.com/basic-income/post-capitalism-rise-of-the-collaborative-commons-62b0160a7048.
8. R. Price, "Digital Currency Ethereum Is Cratering because of a \$50 Million Hack," *Business Insider*, 16 Jun. 2016; www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6.
9. C. de Roure and P. Tasca, "Bitcoin and the PPP Puzzle," SSRN, 2014; doi [.org/10.2139/ssrn.2461588](https://doi.org/10.2139/ssrn.2461588).
10. V. van de Nieuwenhof, "Eduard de Jong: A Short History of the Blockchain," Inst. of Network Cultures, Dec. 2016; networkcultures.org/moneylab/2015/12/15/eduard-de-jong-a-short-history-of-the-blockchain.
11. R.C. Merkle, "A Digital Signature based on a Conventional Encryption Function," *Proc. Conf. Theory and Application of Cryptographic Techniques*, Springer, 1987, pp. 369–378.
12. H. Hellerman, *Digital Computer System Principles*, McGraw-Hill Education, 1967.
13. L. Lamport, "Password Authentication with Insecure Communication," *Comm. ACM*, vol. 24, no. 11, 1981, pp. 770–772.
14. "History of the Web: Sir Tim Berners-Lee," Worldwide Web Foundation, 2016; webfoundation.org/about/vision/history-of-the-web.

15. D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," *Proc. Advances in Cryptology*, Springer Verlag, 1990, pp. 319–327.
16. N.M. Haller, "The S/Key One-Time Password System," *Proc. Internet Society Symp. Network and Distributed System Security (NDSS 94)*, 1994, pp. 151–157.
17. T.P. Pedersen, "Electronic Payments of Small Amounts," *Proc. Int'l Workshop Security Protocols*, Springer, 1996, pp. 59–68.
18. R.L. Rivest and A. Shamir, "Password and Micromint: Two Simple Micropayment Schemes," *Proc. Int'l Workshop Security Protocols*, Springer, 1996, pp. 69–87.
19. J.E.K. De Jong and C.J. Stanford, "System with and Method of Cryptographically Protecting Communications," 31 March 1999; EP Patent App. EP19,960,920,052.
20. A. Back et al., "Hashcash—A Denial of Service Countermeasure," 2002; hashcash.org/papers/hashcash.pdf.
21. T. Aste, "The Fair Cost of Bitcoin Proof of Work," Univ. College London; 27 June 2016; SSRN 2801048.
22. G. Briscoe and T. Aste, "Blockchains: Distributed Consensus Protocols, Transparency and Business Models," Univ. College London; submitted to *J. Digital Economy*, 2017.
23. G. Pappalardo et al., "Blockchain Inefficiency in the Bitcoin Peers Network," 2017, arXiv preprint; arXiv:1704.01414.
24. P. Tasca, et al., eds., *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty First Century*, Springer, 2016.

myCS Read your subscriptions through the myCS publications portal at <http://mycs.computer.org>



IEEE Security & Privacy magazine provides articles with both a practical and research bent by the top thinkers in the field.

- stay current on the latest security tools and theories and gain invaluable practical and research knowledge,
- learn more about the latest techniques and cutting-edge technology, and
- discover case studies, tutorials, columns, and in-depth interviews and podcasts for the information security industry.



computer.org/security