Beyond Bitcoin: The Rise of Blockchain World

Roman Beck, IT University of Copenhagen

The brave new world of blockchain potentially transforms the financial structures we have come to know and feel ambivalent about. What does a decentralized, secure system mean for our society?

Bitcoin—a cryptocurrency built on blockchain technology—was the first currency not controlled by a single entity.[1] Initially known to a few nerds and criminals,[2] bitcoin is now involved in hundreds of thousands of transactions daily. Bitcoin has achieved values of more than US$15,000 per coin (at the end of 2017), and this rising value has attracted attention. For some, bitcoin is digital fool's gold. For others, its underlying blockchain technology heralds the dawn of a new digital era. Both views could be right.

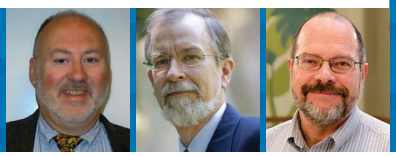
The fortunes of cryptocurrencies don't define blockchain. Indeed, the biggest effects of blockchain might lie beyond bitcoin, cryptocurrencies, or even the economy. Of course, the technical questions about blockchain have not all been answered. We still struggle to overcome the high levels of processing intensity and energy use. These questions will no doubt be confronted over time. If the technology fails, the future of blockchain will be different. In this article, I'll assume technical challenges will be solved, and although I'll cover some technical issues, these aren't the main focus of this paper.

In a 2015 article, "The Trust Machine," it was argued that the biggest effects of blockchain are on trust.[1] The article referred to public trust in economic institutions, that is, that such organizations and intermediaries will act as expected. When they don't, trust deteriorates. Trust in economic institutions hasn't recovered from the recession of 2008.[3] Technology can exacerbate distrust: online trades with distant counterparties can make it hard to settle disputes face to face. Trusted intermediaries can be hard to find, and that's where blockchain can play a part. Permanent record-keeping that can be sequentially updated but not erased creates visible footprints of all activities conducted on the chain. This reduces the uncertainty of alternative facts or truths, thus creating the "trust machine" *The Economist* describes. As trust changes, so too does governance.[4]

Vitalik Buterin of the Ethereum blockchain platform calls blockchain "a magic computer" to which anyone can upload self-executing programs.[5] All states of every

0018-9162/18/$33.00 © 2018 IEEE

EDITORS
HAL BERGHEL University of Nevada, Las Vegas; hlb@computer.org
ROBERT N. CHARETTE ITABHI Corp.; rncharette@ieee.org
JOHN L. KING University of Michigan; jlking@umich.edu



program are publicly visible, with cryptographic guarantees that programs will execute as specified by the blockchain protocol. (Buterin later abandons the term *magic* in favor of *Turing-complete*.) Blockchain might, as the subtitle of this article suggests, usher in a new world. Some refer to blockchain as the most promising new technology since the Internet.[4] The gods of powerful institutions (for example, central banks), are challenged by blockchain. Whether this technology will force these gods into the twilight is unclear, but it's big enough and powerful enough to bring major changes.

WHAT IS BLOCKCHAIN?

Blockchain, as it is used today, is a tamper-resistant database of transactions consistent across a large number of nodes. The blockchain is cryptographically secured against retrospective manipulations, and it uses a consensus mechanism to keep the database consistent whenever new transactions need to be validated. Data storage on the blockchain is secured by cryptographic hashes in which data being hashed return a fingerprint that verifies the authenticity of the data. Alteration of the original data causes the hash of the altered data to no longer match the original fingerprint. Transactions on the blockchain are grouped and stored in blocks. The combined hash of these transactions is also stored, and each subsequent block saves the combined hash of the previous block. This creates a chain of cryptographically secured and linked blocks containing the information—the blockchain.

Any attempt to change information necessitates rehashing, not only the block relevant to the transaction, but all subsequent blocks. This is possible theoretically, but it's impractical since the blocks grow continuously as other nodes add blocks to the blockchain.[6] Technical details are summarized in a paper by Ethereum's Gavin Wood.[7] The Ethereum blockchain goes beyond bitcoin to allow user-created smart contracts executed on a generic, programmable blockchain under decentralized control, using a built-in Turing-complete programming language. This allows smart contracts and customized (even arbitrary) rules for ownership, transaction formats, and state transition functions. These smart contracts enable the distributed user community to resolve some issues without depending on trusted centralized authorities.

> Blockchain, as it is used today, is a tamper-resistant database of transactions consistent across a large number of nodes.

Blocks, hashing, trees, and miners

The foundation of blockchain is the security of code and data in the blocks. Bitcoin uses a "Merkle tree" to store data from new transactions with pointers to original block locations for unchanged data. Transactions are repeatedly paired, merged, hashed and rehashed until only one hash—the Merkle root—remains. Each subsequent block saves the Merkle root of the previous block. Ethereum blocks contain the entire state of the Ethereum system stored in a "Patricia tree," an evolved Merkle tree. Chained hashing keeps blocks well formed and difficult to tamper with. This helps keep the blockchain secure and almost unbreakable. A blockchain isn't run from a single server, but on a network of computers that hold all data and changes to the data in the blockchain. These computers are called "miners," essential to a blockchain that uses a proof-of-work mechanism to achieve consensus.[4] Proof-of-work is the most common consensus mechanism, used by both bitcoin and Ethereum and dating back to 1992.[8]

Proof-of-work mathematically ensures validity as long as no single entity holds enough computing power to add an illegitimate block to the blockchain. Each miner competes with other miners to earn the reward of being able to add a block to the blockchain. This is accomplished by the miner doing computationally intense work. Bitcoin requires the miner to find a string that, when concatenated with a hash of the previous block header and then re-hashed, returns a particular string. Anyone trying to "spoof" the blockchain (for example, to change data on old transactions) must recalculate the proof of work for all subsequent blocks. Convincing the system to use a bogus chain would require continuously adding blocks to the chain faster than a legitimate chain would evolve. Ethereum is developing an alternative consensus scheme that uses proof of stake that doesn't require the computational resources of proof of work, largely in response to processing intensity and energy use as noted earlier.

Each miner that joins the blockchain increases the level of decentralization, and also strengthens the consensus mechanisms. Transactions on decentralized blockchains are transparent and visible to users, in contrast to centralized systems where the users typically don't enjoy such transparency or trust in the provider.[9] Miners who have been able to solve the

cryptographic puzzle are rewarded, so miners continuously try to create the next blocks that can be added to the chain. No central authority decides this. Miners that try to add different blocks than those agreed on through the consensus mechanism are disregarded by the rest of the system. This forces uniformity in the blockchain. It's nearly impossible to cheat the blockchain without circumventing the consensus scheme that dictates nodal agreement that a miner has a right to be a block in a given blockchain.

Smart contracts

Security and transparency helps the blockchain provide a single version of what is the case and how that case was achieved—what some call "the truth." In this, bitcoin and Ethereum are similar. Ethereum goes beyond by permitting smart contracts, a piece of code that enables the Ethereum Virtual Machine (EVM) to execute on the blockchain. The EVM is similar to other virtual machines, compiling instructions from a programming language into low level code for the computer on which it runs. The EVM is a large decentralized computer containing millions of objects called "accounts." Accounts can maintain internal databases, execute code, and talk to other accounts. A smart contract is itself an account. The EVM allows for externally owned accounts (EOAs) controlled by a private key through a user, allowing an account to send ether and messages from the EOA.

A smart contract can't be altered once the code is set, although storage of the smart contract can be altered. The piece of code acts as an agreement, available for anyone to use. Smart contracts are made possible by the Turing-complete programming languages compiled into EVM bytecode. Smart contracts have addresses and execute code based on the data they receive. Smart contracts can call other smart contracts through messages. To avoid malicious behavior, infinite loops or distributed denial of service attacks, execution and creation of smart contracts uses Ethereum's internal cryptocurrency. The amount needed for a contract is determined by the computations and storage entries of bytecode that the EVM compiles the smart contract into. Specific computation costs are calculated by the complexity of the computation, with basic computations (addition, subtraction, and multiplication) costing less and more complications costing more. Miners are paid for use of their computational power. As of 2015, the computing power available on blockchains was small, about equivalent to a 1999 smartphone.[10] However, with powerful smart contracts this could change quickly.

Access to a blockchain is for transaction validation or transaction entry. Transaction validation depends on whether the blockchain is permissionless (all nodes can validate transactions) or permissioned (only preregistered can validate transactions). Transaction entry is available to all nodes in public blockchains. Only preregistered nodes can submit new transactions in private blockchains. Public blockchains can be either permissioned or permissionless.[11]

Blockchain's core ideas are well established: fidelity and transparency. Fidelity is the truthful rendering of the state of things. People trust those things are as represented. The technical structure of the blockchain is that blocks containing requisite information are secured cryptographically, and consensus mechanisms ensure that blocks along the chain agree with the creation of and/or change in the information to be held. Transparency is the ability of anyone to examine the entire record of changes to determine when, how and why changes were made. The architecture of blockchain is such that any effort to "hide" information on the chain is obvious, causing other users of the chain to ask questions about why it's happening. The technology doesn't guarantee that a blockchain cannot be corrupted, but it makes corruption difficult enough to generate trust.

BLOCKCHAIN AND TRUST

Trust is complicated and difficult to define precisely. It has numerous meanings and many different forms. Yet trust is the underlying fabric of human interactions, of central importance to interpersonal and interorganizational relationships. Blockchain affects trust. People sometimes refer to blockchain as a technology that overcomes the need for trust in human interactions. It's unclear that overcoming the need for trust is possible; rather, it's more productive to assess blockchain's effect on the antecedents of trust, including confidence, integrity, reliability, responsibility, and predictability. If we can be confident that collaborations will be executed as intended, and that there's only one version constituting truth, integrity is guaranteed. When contracts are executed as coded, blockchain is seen to be reliable. Roles and responsibilities are determined in advance, and outcomes are predictable. When these trust antecedents are handled effectively by blockchain, certainty can replace uncertainty. This is a major hope for blockchain; time will tell if it can be realized.

Decentralized and autonomous

Much is made of blockchain's decentralization and autonomy. However, nothing in blockchain requires decentralization or autonomy. Decentralization and autonomy are enabled by blockchain, but a choice can be made based on the needs of the application. Authorities, such as central banks, can adopt and apply blockchain technology; but blockchain provides an alternative that might have implications for control, authority, power, and so on. Beyond this, it might be possible to implement previously unavailable solutions when requirements for centralized authority are lifted. As formerly impractical solutions become practical, blockchain's impacts might go beyond "least expected" to "not expected at all."

It's useful to look at R.H. Coase's work;[12] he questioned why, in a market-oriented economy, economic activity

isn't limited to individuals interacting on markets? Why are there firms? Coase was an economist, but his ideas reach beyond economics. Firms emerged to handle "transactions" (searching, negotiating, monitoring, enforcing, coordinating) required by markets. In his model, when transaction costs are high, the firm emerges as more efficient than the market. The choice is between market and firm, but Coase recognized that a third "hybrid" form can emerge around collaborations, alliances, or joint ventures. These hybrids didn't conform to the products and services of the 1930s, and Coase didn't elaborate on them.

Friction costs

In principle, blockchain allows for such hybrids, enabled by its decentralized mechanisms to make claims, attest to things, or enforce rights (such as property rights). Blockchain enables trust that a transaction will be completed even if there are slight variances in protocol, because it's possible to see that the ends are achieved. It can reduce friction that comprises all kinds of direct and indirect costs and efforts due to the lack of trust and bring certainty via transaction logic instantiated as code. Contracts and other forms of agreements can be electronically executed without trust-associated friction costs. Blockchain can be used for transparent and secure transactions between and among individuals, individuals and organizations, and organizations.

Blockchain might alleviate our dependency on central, hierarchical organizing and planning—previously the only way to reliably handle financial transactions—and thus allow for decentralized enforcement of transactions, in a manner similar to the way the Internet enabled changes in social relationships, commerce, and so on. The constraints that now lead to centralized solutions might evaporate if the transaction logic can be orchestrated and enforced without that central authority. Blockchain can generate real-time information flows of transactions to allow new approaches of digital auditing to ensure agreements are honored. This paradigm shift suggests that such systems organize transactions reliably—possibly without human interaction—following a protocol. It's akin to unstaffed, autonomously navigating vessels safely moving passengers from A to B using a protocol capable of minimizing exceptions (malicious and accidental) and getting humans out of the loop. In principle, blockchain could be an Internet of Things backbone, enabling tamper-proof coordination of activities, for example between delivery drones and their delivery stations.

Whether any given application is controlled in a centralized or decentralized manner becomes a matter of choice; it doesn't default to the centralized approach because that's the only way to do it. It's less important for requiring a particular solution than for enabling multiple solutions, thereby increasing the options of those who pay for, design, use, or otherwise interact with blockchain applications.

BLOCKCHAIN WORLD

The emerging blockchain world is the combination of traditional ways of doing things and those that are enabled by blockchain. Third parties might still ensure trustworthiness, but they don't have to do so, nor do those who seek assurance have to depend on third parties. A transaction might be conducted as agreed upon solely because blockchain enables those interested to monitor the status of the transaction, know what's going on, and remind others of their obligations. Or a party could turn to another system (such as the criminal justice system) for enforcement. Blockchain could support many codified agreements handled by traditional means, including stock trades, monitoring contract, managing land records, security of foodstuffs, preserving provenance, and maintaining the chain of custody. In this way, the technology will become part of the infrastructure of daily life, affecting commerce, social interaction, law, education, entertainment, nutrition, livelihood, housing, and so on.

Just because blockchain world is part of a larger infrastructure doesn't mean its effects are trivial. The Internet has had a profound effect on our culture, economy, and systems, and blockchain will be complementary to the kinds of changes that have already transpired, providing the means for decentralized governance in addition to centralized governance. By enabling so-called decentralized autonomous organizations (DAOs), blockchain empowers participants to implement agreements and transactions, without being their own legal entity. DAOs make transactions transparent to DAO members, which in turn makes fraudulent behavior difficult to hide.

The emerging blockchain world is the combination of traditional ways of doing things and those that are enabled by blockchain.

In principle, a DAO can run autonomously as a decentralized, transparent, and secure system for operation and governance among independent participants. Blockchains needn't be controlled by any of the participants as it is serving as a trusted third party to provide the role of proxy and enforcement of rules. To use Coase's insight, a DAO might reduce transaction costs while providing setup, maintenance, regulation, and supervision like traditional third parties. The results

wouldn't be trust-free, but would shift from trust in a counterparty or a third party to the blockchain system itself and the rules coded therein.

One might say the DAO is a shift from a socio-technical system to a techno-social system. Socio-technical systems handle control of transactions through social systems. Techno-social systems handle control of transactions through technical systems that can be autonomous.[13] How this would work exactly is as yet unclear in many ways, but through blockchain technology we have the chance to experiment with secure, decentralized systems, which could enable new social models that go well beyond the economy.

Realizing these blockchain-enabled models will require workers possessing process and management knowledge, as well as information technology skills including programming, design, and an ability to see the big picture. Blockchain world promises much, though many of the details are still being determined.

REFERENCES

1. "The Trust Machine: The Technology behind Bitcoin Could Transform How the Economy Works," The Economist, 31 Oct. 2015; www.economist.com/news/leaders/21677198-technology-behind-bitcoincould-transform-how-economy-works-trust-machine.
2. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008; bitcoin.org/bitcoin.pdf.
3. "2016 Edelman Trust Barometer," annual report, Edelman, 2016; www.edelman.com/insights/intellectual-property/2016-edelman-trust-barometer.
4. W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, Wiley, 2016.
5. V. Buterin, "Ethereum," white paper, 2013; github.com/ethereum/wiki/wiki/White-Paper.
6. S. Underwood, "Blockchain beyond Bitcoin," *Comm. ACM*, 2016, vol. 59, no. 11, pp. 15–17.
7. G. Wood, "Ethereum Yellow Paper," website, 2014; http://gavwood.com/paper.pdf.
8. C. Dwork and M. Naor, "Pricing via Processing or Combatting Junk Mail," *Proc. Ann. Int'l Cryptology Conf.*, 1992, pp. 139–147. Springer, Berlin, Heidelberg.
9. P. De Filippi, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies," *J. Peer Production*, 2016; peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies.
10. V. Buterin, "Ethereum Development Tutorial," 2015; github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial
11. G.W. Peters and E. Panayi, "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," *Banking beyond Banks and Money*, P. Tasca, T. Aste, L. Pelizzon, and N. Perony eds., 2016, Springer, Cham, pp. 239–278.
12. R.H. Coase, "The Nature of the Firm," *Economica*, vol. 4, no. 16, 1937, pp. 386–405.
13. J.M. Quintana Diaz, "The Merger of Cryptography and Finance--Do Cryptographic Economic Systems Lead to the Future of Money and Payments?," 2014; available at SSRN: ssrn.com/abstract=2536876.

ROMAN BECK is at IT University of Copenhagen. Contact him at romb@itu.dk.