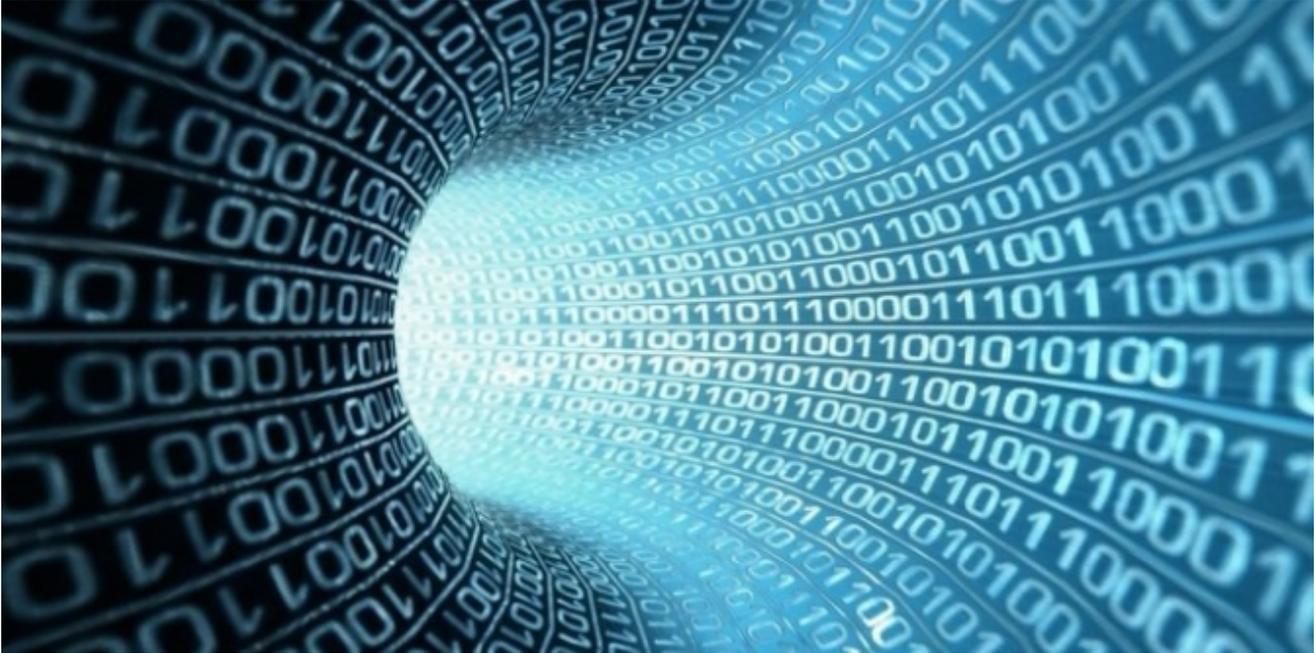


Blockchains may replace the institutions that safeguard commercial activities

 blogs.lse.ac.uk/businessreview/2016/03/31/blockchains-may-replace-the-institutions-that-safeguard-commercial-activities/

3/31/2016



My book *Blockchain: Blueprint for a New Economy* highlights the possibility that blockchains are a modernising information technology that extends well beyond digital cryptocurrencies, smart contracts, and automated Dapps and DACs (distributed autonomous applications and corporations). Blockchains could engender a new Internet era that now includes payment and secure value transfer. This means that many current institutional activities might be digitised and automated, and more fundamentally that there could be a redesign of economic, legal, and political systems. Beyond institutional redesign, more broadly blockchain architectures could allow a much larger and truly global scale of activity than has been possible previously with hierarchical models, for example million-member genome banks. This book introduces digital cryptocurrencies, blockchains, smart contracts, and decentralisation as important technological developments that could shape a completely new tier of human endeavour and have a substantial impact in the contemporary world.

What is blockchain technology? A new means of secure value transfer

Blockchains are a software protocol, the distributed cryptographic ledger system that underlies cryptocurrencies like Bitcoin. In one sense, they are nothing more than a modernising information technology. In another sense, they are novel and disruptive. Whereas the first Internet era facilitated the transfer of information, blockchains as a possible second Internet era allow the secure exchange of value across networks. The implication of the ease of transferring value across digital networks is that current methods of value exchange (such as the banking system) could become obsolete. Blockchains might offer an improvement over the extensive institutional apparatus that is currently in place globally for any kind of activity that requires trust. The key point is that their secure value transfer features could allow the information technology revolution to finally reach the last major sectors of the economy: finance, economics, governance, and law, which have been updated but not completely re-architected.

What are smart contracts and smart property?

There are different kinds of blockchain applications. Most widely deployed at present are digital payment systems and cryptocurrencies such as Bitcoin. Other application areas include smart property and smart contracts, where one implication is that in the future, nearly all agreements, contractual relationships, and governance might be enacted through code-based *smart contracts*, and property might be registered and transacted via blockchains as *smart property*.

Smart property is the idea of registering assets on the blockchain for tracking and exchange, for all manner of both physical and intangible assets. Each asset registered to a blockchain has its own unique key, which could be used to track its geo-location 24-7, record ownership lineage, and execute buy-sell transfers. In the case of hard assets, blockchains might serve as an asset registry, and facilitate a variety of inventory, tracking, and exchange functions. Smart property also applies to intangibles and documents, where important functionality is notary, attestation, and provenance (origins-tracking) services. Here, contracts, agreements, wills, and intellectual property (IP) can be registered to blockchains for record-keeping, assurity, and transaction. A key feature of blockchain-based intangibles registration is hashing. Hashing is a way to register the state of any digital file with a timestamp, while keeping the contents private. Later it can be confirmed easily whether file contents (still private) have changed. Thus blockchains might be used to coordinate smart property registries of both hard assets (physical property) and intangible assets (patents, trademarks, votes, contracts, ideas, health data, etc.).

Smart contracts are just like any regular contract, an agreement existing between two or more parties with terms and consideration, in this case registered to the blockchain for validation and possibly some sort of automated execution. Cryptolaw is the intersection of law and technology, where traditional legal contracts and code-based contracts overlap. The salient difference is that code-based contracts will execute inexorably even if conditions have changed, as opposed to human-based contracts which are always open to discretionary compliance. Code-based contracts could come to have a greater economic presence, for example orchestrating entire industries such as mortgage servicing. Whereas cryptocurrencies like Bitcoin accommodate the spot market for immediate digital currency transfer, the broader financial market requires more complicated functionality which could be supported by smart contracts. Many financial agreements have contingency-based parameters that are dependent upon future events, and these could be instantiated in blockchain-based smart contracts tied to lookup oracles for seamless future execution as events unfold. The larger market space for smart contracts is ongoing financial obligations and transactions executed over time such as bonds, loans, mortgages, securities portfolios, mutual funds, pensions, and derivatives.

What are public and private ledgers?

Blockchain technology is being deployed in two modes at present, public and private ledgers. Private (permissioned) ledgers are a more circumscribed controlled use of the technology being implemented by some financial institutions where user identity is known and confirmed. Public ledgers are permissionless censorship-resistant pseudonymous ledgers where user name (wallet address) is not fully traceable back to the real-life person executing the transaction. Private blockchains are a *better horse*, and public blockchains are a *car* (novel and uncharted waters). Private ledgers are analogous to telco provider, AOL, and CompuServe's 'walled gardens' – early roll-outs of Internet service in a controlled user experience. Walled-garden private ledgers would be expected in the early phase of implementation as offering parties gradually test blockchains, possibly acting on fear, if missing the underlying point of blockchains as a new model for universal decentralized reach. Over time, there could be a migration away from private permissioned ledgers.

Conclusion

Blockchains are an important new technology that digitises, automates, and allows secure value transfer. While long-term potential could be significant, it is still very early in the development and maturity of the technology. There are many technical and other problems to be resolved for mainstream adoption, particularly scalability. However, it is also important to realise that blockchains are fundamentally a new *kind* of technology that could be extremely transformative. The argument can be seen at three different levels. Bitcoin might not be the final cryptocurrency.

Blockchains might not be the final means of engendering algorithmic trust and updating truth states in distributed computing networks. But it is harder to deny decentralisation as a model for large-scale human endeavor, especially with the hugely successful demonstration case of the Internet. Blockchain technology could bring about a significant reconfiguration of the economic, legal, political, and scientific apparatus as we advance to further stages of modernity and the automation economy.

◆◆◆

Notes:

- This post is based on the book [Blockchain: Blueprint for a New Economy](#), O'Reilly Media, (2015)
- The post gives the views of its author, not the position of LSE Business Review or the London School of Economics.
- Featured image credit: [luckey_sun CC-BY-SA-2.0](#)

Melanie Swan is a Blockchain Theorist in Philosophy and Economic Theory at the New School for Social Research in New York NY. She is the [founder](#) of several startups including the Institute for Blockchain Studies, DIYgenomics, GroupPurchase, and the MS Futures Group. Ms. Swan's educational background includes an MBA in Finance from the Wharton School of the University of Pennsylvania, an MA in Contemporary Continental Philosophy from Kingston University London and Université Paris 8, and a BA in French and Economics from Georgetown University. She is a faculty member at Singularity University and the University of the Commons, an Affiliate Scholar at the Institute for Ethics and Emerging Technologies, and a contributor to the Edge's Annual Essay Question.



- Copyright © 2015 London School of Economics