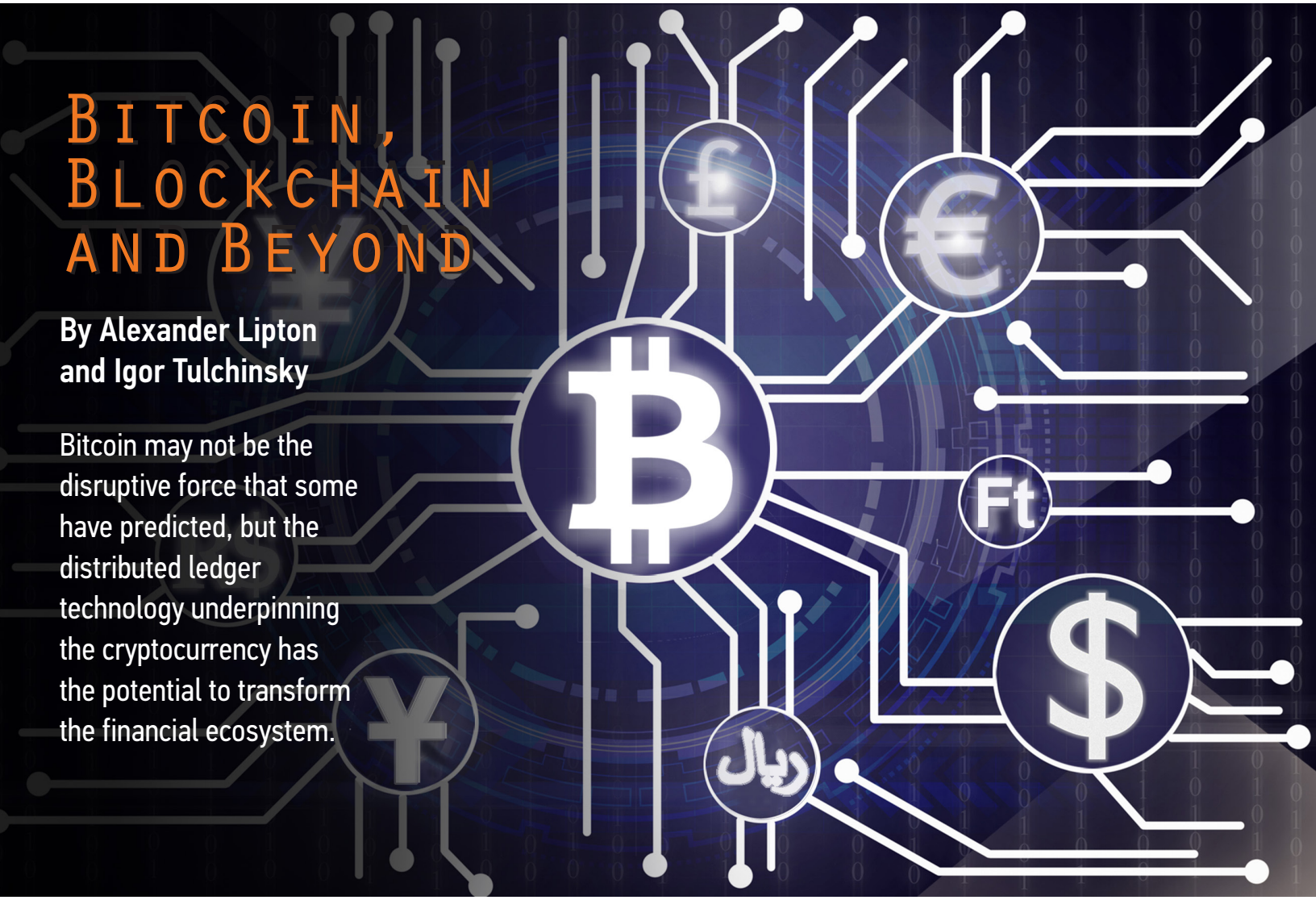
04.21.17

WorldQuant Perspectives



Bitcoin, Blockchain and Beyond

By Alexander Lipton and Igor Tulchinsky

Bitcoin may not be the disruptive force that some have predicted, but the distributed ledger technology underpinning the cryptocurrency has the potential to transform the financial ecosystem.

WORLDQUANT

WorldQuant, LLC
1700 East Putnam Ave.
Third Floor
Old Greenwich, CT 06870
www.weareworldquant.com

FOR DECADES LITTLE ATTENTION WAS PAID TO THE INFRASTRUCTURE underpinning the inner workings of the financial ecosystem — including payments, trading, clearing and settlement — despite its great importance. This infrastructure is currently well past its expiration date.

Fortunately, the situation has started to change, in some instances quite dramatically. The reasons are twofold: First, the global financial crisis put enormous stress on the infrastructure and almost pushed it to the breaking point. Second, remarkable technological breakthroughs — mostly related to distributed ledgers and related concepts — drew the attention of key decision makers, technical experts and the general public to the glaring need for updating the system, while at the same time indicating how such a transformation could be accomplished, at least in theory.

Although the idea of public distributed ledgers isn't new, it burst onto the recent scene in 2009 with the introduction of the cryptocurrency Bitcoin, whose founders' identities are concealed under the pseudonym of Satoshi Nakamoto. Bitcoin has captured the imagination of the public by proposing the first cryptographic electronic currency issued without central authority and having no intrinsic value. The key components of the Bitcoin infrastructure are the private–public key cryptographic signatures, the immutability of its blockchain distributed ledger and the prevention of double spending through Bitcoin mining based on proof of work.

Distributed ledger technology can be applied to many different areas. While digital currencies like Bitcoin come to mind first, more-complex issues — including trust and identity related to the know-your-customer and anti–money laundering aspects of finance — are no less important.

> "Bitcoin has captured the imagination of the public by proposing the first cryptographic electronic currency issued without central authority and having no intrinsic value."

Most building blocks of the Bitcoin ecosystem have been known for some time. Public-key cryptography, including the Diffie–Hellman key exchange protocol and RSA encryption, has been around since the 1970s; distributed ledgers since the 1990s; and the proof-of-work concept since the early 2000s. When the owner of a particular public key broadcasts its intent to send a certain Bitcoin quantity to another public key, miners verify the transaction via the competitive proof-of-work mechanism to ensure there is no double spend. A Bitcoin itself is just a long chain of transactions that can be traced all the way back to the time when it was minted, either as part of the genesis block (the first block in the blockchain) or through mining (by successfully solving a computational puzzle). The size of mining rewards is halved at regular intervals, so that the total number of Bitcoins in circulation asymptotically converges to 21 million. To date, about 16 million Bitcoins have been minted, of which 3 million to 5 million may have been irretrievably lost.

What Is a Distributed Ledger?

Currently, most financial information is kept in centralized ledgers maintained by private banks, asset managers, custodians and other parties. In a centralized ledger, storage devices all connect to a common processor and the writing access is tightly controlled. By contrast, in a distributed ledger all storage devices are independent and many participants have writing privileges. In principle, it is possible to store some financial information in a distributed ledger, provided that it is immutable and resilient.

There are several types of distributed ledgers, varying from the simplest extensions of traditional centralized ledgers to permissioned private distributed ledgers represented by Digital Asset Holdings and consortium R3 CEV to permissioned public ledgers such as Ethereum and Ripple, and finally to the most complex nonpermissioned public ledgers, like the one used by Bitcoin. The usage of a specific ledger depends on the problem at hand. In legacy banking, which requires no joint ledger writing access, a centralized ledger does the job. If participants do need joint writing access but know each other in advance, have aligned interests and can be trusted — as is the case in clearing and settlement — a permissioned private distributed ledger can be employed.

While extremely impressive in its technical conception and execution, the Bitcoin ecosystem is clearly unsuitable for the

purposes of high finance, not least because it cannot solve the all-important know-your-customer and anti–money laundering problems. Bitcoin's narrow nature and low transaction-per-second capacity are also troublesome. Accordingly, for the past five years or so, numerous efforts have begun to adapt Bitcoin's most important feature — namely, distributed ledger — to solve some of the more vexing infrastructure problems. Below we briefly touch upon some of them.

Incremental Improvements

Current financial infrastructure is organized in the form of private centralized ledgers maintained by individual banks and various support players, such as asset managers and custodians, with final reconciliation achieved through the ledgers maintained by central banks. Although the system has served finance faithfully for centuries, it is plagued with numerous problems related to both domestic and, especially, foreign transactions. This is true not only for cash transactions but also for those involving securities.

It is very tempting to apply the distributed ledger concept to simplify and democratize the world of finance. While the frontal attack on the entire infrastructure is probably bound to fail due to the enormous complexity of the task, a number of areas can be dealt with at present. These include, but are not limited to, the triad of trading, clearing and settlement; trade finance; and real estate transactions.

The Trading Triad: At the moment, the number of parties required to trade shares is very large and, in addition to the buyer and seller, involves brokers, central securities depositories, clearing counterparties, custodians and exchanges, to mention but a few. Moreover, while trading on exchanges is very fast and might occur in milliseconds, the subsequent process of clearing and settlement typically takes two to three days, requires numerous reconciliations and is prone to frequent failures.

> "It is conceivable to dramatically reduce the number of parties involved in the process of trading securities, while at the same time increasing the speed, robustness and regulatory compliance of the process as a whole."

In principle, by introducing shares directly into a private permissioned distributed ledger, it is conceivable to dramatically reduce the number of parties involved in the process of trading securities, while at the same time increasing the speed, robustness and regulatory compliance of the process as a whole. We think that abolishing clearing and achieving instantaneous settlement, though theoretically possible, will not be accomplished in practice because it would eliminate many advantages of the existing process, such as anonymity, netting and the ability to borrow, as well as jeopardize the all-important delivery-versus-payment setup. Still, in the future the clearing and settlement process will be shortened and made significantly cheaper than it is now.

International Payments: The other area where distributed ledger technology can be applied with high probability of success is international payments. Given the complexity of current cross-border transactions, having a universal medium of exchange residing outside national boundaries is clearly advantageous, provided that conversion from national currencies into this medium and back can be accomplished with a high degree of reliability and low costs. In this regard, Ethereum and Ripple are promising initiatives.

Real Estate Transactions: Yet another area where distributed ledgers can — and will — improve the status quo is real estate. Given that property titles already represent a chain describing change of ownership and in most instances are public, it is natural to move them to a distributed ledger. A number of companies, including Swedish blockchain start-up ChromaWay and telecom service provider Telia, are actively engaged in this transformation. However, a word of caution is in order: Regardless of whether titles reside in an immutable distributed ledger, it is necessary to have a clear initial (genesis) title for every property, without which the entire chain cannot be reliably built.

Decisive Improvements

While important applications described in the previous section are technical in nature, they lack the revolutionary spirit. One area where a distributed ledger can potentially bring a dramatic

departure from the past is digital currency issued by central banks. The idea is not only to abandon physical cash in favor of its electronic equivalent, but also to replace a large chunk of government debt with central bank digital currency (CBDC) as well.

The techniques underpinning this transformation would liberally use the distributed ledger framework, combined with third-party verification provided by designated miners. The impact of CBDC on society at large is hard to overestimate. In theory, it gives an opportunity to everyone to have an account directly with a central bank, obviating the need for fractional banking and improving the stability of the financial system dramatically. However, the money-creating ability of the banking sector will be significantly curtailed and transferred to central banks.

If this transformation were to come to fruition, commercial banks would become narrow rather than fractional and concentrate on transactions and issues of know-your-customer and anti–money laundering. Money lending would be performed by mutual funds rather than banks. The feasibility and desirability of such a dramatic departure from the status quo is currently hotly debated by central bankers, commercial bankers and academics. To our mind, developments in this direction are inevitable but their magnitude is uncertain.

Another area where distributed ledgers can play a socially transformative role is solving the problem of the unbanked population, especially in developing countries. By combining distributed ledger technology with big data analysis related to mobile phone usage and the like, companies and other entities can bring the benefits of banking to many people currently excluded from the banking system. In this regard, the celebrated M-Pesa money transfer and financing service is a significant step in the right direction. M-Pesa was originally launched by Vodafone in Kenya and Tanzania in 2007 and has since expanded to Afghanistan, Albania, India, Romania and South Africa. Given the importance of the problem of the unbanked, similar efforts on several fronts are to be expected.

> “By combining distributed ledger technology with big data analysis, companies and other entities can bring the benefits of banking to many people currently excluded from the banking system.”

Using distributed ledgers is an attractive and technologically sound alternative to the way financial transactions are conducted currently and has important applications in both mundane and fundamental areas of finance. In one form or another, distributed ledgers will result in a more efficient, resilient and democratic financial infrastructure than what we struggle with now. But a word of warning is appropriate. Initially, many disjointed efforts in the same direction are good for winning models to emerge. However, eventually these efforts have to coalesce into a single standard to ensure the stability and efficiency of the financial ecosystem as a whole.

Alexander Lipton is CEO of StrongHold Bank Labs and a Fellow at MIT Connection Science. Igor Tulchinsky is founder, chairman and CEO of WorldQuant, LLC.