SEVEN POSSIBLE KILLER APPS FOR BLOCKCHAIN & DIGITAL TOKENS

There are many applications that could benefit from decreased transaction costs, a neutral shared database, and the superior security of a shared ledger. Here are a few.

DECEMBER 1, 2016

By Philip Evans

with Lionel Aré, Patrick Forth, Nicolas Harlé, and Massimo Portincaso

The disruptive potential of tokens and blockchains initially surfaced with payments thanks to the controversy over and curiosity about their application in Bitcoin. But these two technologies could have much broader application. As explained in the companion article "Thinking Outside the Blocks," blockchains and digital tokens establish digital continuity. The technologies can undergird any number of applications that bring together many different parties that often have no reason to trust one another. They can eliminate duplicative and error-prone transactions, and they can help create digital identity.

Assuming (and it is a big assumption) that the tradeoffs among security, functionality, and scale will be largely resolved within five years, a range of radically new blockchain applications are possible. Here are seven potential killer apps.

1. **TRANSACTING ON THE INTERNET OF THINGS.** Most current IoT applications connect devices with a common owner, so they only need to exchange information or instructions. When devices have different owners, however, they must transact. Today, when device owners lack a shared intermediary and the sums involved are minuscule, transacting is not economically worthwhile. But with a blockchain, especially one that enables smart contracts, transactions between devices become possible on a direct, peer-to-peer basis. A car can purchase parking simply by driving onto a space: a transponder in the car connects to a $25 meshed device embedded in the asphalt. (Streetline is already deploying such transponders.) The German company Slock.it has developed a cheap Ethereum computer prototype that mediates between smart devices in the home and the Ethereum blockchain. In one application, the computer negotiates a room rental as a smart contract and instructs the smart lock on the front door to open when the renter arrives. The blockchain holds the deposit in escrow

and releases funds on fulfillment of the contract. This disintermediates not only PayPal and the banking system but also Airbnb.

2. **TRANSFORMING THE ECONOMICS OF DIGITAL CONTENT.** Today, internet content is funded by either subscription or advertising. But with cheap, blockchain-based transactions, it would be possible to meter media consumption by the page or the minute. Especially if consumers' privacy concerns intensify, blockchain could drive a fundamental shift in the revenue models of the online media industry. An extension of this idea is using a blockchain to register and protect intellectual property. In October 2015, Imogen Heap, the British singer and songwriter, released her song "Tiny Human" on the Ethereum blockchain as a smart contract. It allowed fans to download, stream, remix, and sync the song, distributing royalties directly to the creators—and entirely bypassing the complex and costly web of music intermediaries.

3. **MAKING SUPPLY CHAINS CHEAP AND TRANSPARENT.** The $40 trillion global supply chain is another inefficient transaction network characterized by slow and error-prone transactions among parties with imperfect mutual trust. Some banks are already registering letters of credit on a blockchain so that importers, exporters, and their respective financiers can share common data and release funds without delay or error. By extension, the item itself—like a bitcoin—can carry a continuous identifier that accesses digitally signed data entered on a blockchain by freight forwarders, customs authorities, shippers, wholesalers, retailers, and trusted independent certifiers. This can replace the bill of lading, but it can also certify that a good was handmade in Firenze, manufactured by a Fair Trade Federation member, or is free of genetically modified organisms. Provenance.org, similar to Everledger, provides an Ethereum-based platform that allows companies to register claims about themselves, their products,

and even specific production batches. Paperwork is eliminated and the locus of trust shifted from intermediaries to the originator of the claim.

4. **REFORMING LAND REGISTRIES.** In mature economies such as the US, land registries are riddled with incomplete paperwork requiring manual inspection and expensive title insurance to protect against residual errors. In many emerging economies, registries are radically incomplete or corrupted, depriving poorer citizens of basic property rights. In Honduras, where some 60% of land has no registration, bureaucrats have been known to reassign property to themselves. A land registry lodged on a blockchain would be public and incorruptible. Honduras and the Republic of Georgia have launched such initiatives, but with mixed results so far. The long-term potential, however, is immense: Peruvian economist Hernando de Soto has powerfully argued that establishing clear title to land would give poor people access to credit and the motive to invest.[1]

5. **GUARANTEEING DIGITAL IDENTITIES.** Governments (or some broad coalition of service providers) can play a crucial role by giving their citizens digital identities, thereby enhancing peripheral trust in all peer-to-peer transactions. A digital identity would be data with provable ancestry from the authority, universally verifiable, just like a bitcoin. It is not obvious that such data would need to be stored on a blockchain. Citizens could create public/private-key combinations to release selected personal data to specific recipients. Thus, a young person could prove that he or she is old enough to purchase liquor without revealing other, irrelevant information, as with a driver's license. Over time, legally binding digital signatures, passports, licenses, security passes, key cards, certificates, log-ins, ownership documentation, voter registration, and a panoply of other legal information could be built on that foundation. The most ambitious step in this direction is the AADHAAR national-identity scheme, which has enrolled over a billion

citizens in India. Visionaries see an entire “India stack” built on this foundation, possibly extending into payments for the unbanked.

6. **STREAMLINING HEALTH CARE AND REVOLUTIONIZING RESEARCH.** Health care is characterized by duplicative, incompatible, and inconsistent medical records, while patient data is subject to stringent security and privacy requirements—a perfect application for a permissioned blockchain. But visionaries are looking beyond simple data sharing to “precision medicine”: a continuously learning health care system built on electronic health records, data analytics, and universal disease registries. These new systems will record patient data (and ultimately, complete genomic maps), symptoms, treatments, and above all, outcomes. The central challenge in designing such systems is to reconcile patients’ privacy with researchers’ need for granular and universal data sets. Mere anonymization does not work.[2] Blockchains can be designed in which an individual’s record is scrambled and distributed over multiple nodes, and database queries are distributed across the ledger. Access would be controlled through smart contracts and digital identities. But in the US, because of institutional fragmentation, even such a relatively straightforward innovation as electronic medical records has proved extraordinarily difficult to implement. Scandinavia, not the US, will be the pioneer in these approaches.

7. **MINTING DIGITAL FIAT CURRENCY.** At least a half-dozen central banks are considering this step. The Bank of England, say, would mint “bit£” as digital bearer instruments. Unlike bitcoin, bit£ would have a fixed value and be backed by the full faith and credit of the government. The central bank would purchase government securities with bit£ through an interbank-permissioned blockchain. Commercial banks would then use the bit£ on their balance sheets to settle interbank obligations, massively reducing the counterparty risks that brought the financial system to the brink of collapse

in 2008. Over time, access to bit£ could be extended, ultimately to all citizens. Bit£ would then displace physical cash and much of the traditional payments settlement function of commercial banks. Bitcoin itself would be disrupted by bit£, a universally acceptable, zero-risk competitor. Regulatory and compliance costs would be substantially reduced across the financial system. A recent Bank of England study even concluded that macroeconomic policy would be easier to administer (bit£ could pay a negative interest rate, for example) and that such a regime could permanently raise GDP by as much as 3% by lowering real interest rates, distortionary taxes, and transaction costs.[3]

Notes:

1. Hernando De Soto, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*, Basic Books, 2000.
2. Justin Brickell and Vitaly Shmatikov demonstrated a severe tradeoff between the degree of anonymity and the utility of the resulting information. See "The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing," *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, August 2008.
3. John Barrdear and Michael Kumhof, "The Macroeconomics of Central Bank Issued Digital Currencies," Bank of England Staff Working Paper No. 605, July 2016.

AUTHORS

PHILIP EVANS
Senior Advisor
Boston

LIONEL ARÉ
Senior Partner and Managing Director
Paris

PATRICK FORTH
Senior Partner and Managing Director
Sydney

NICOLAS HARLÉ
Senior Partner and Managing Director
Paris

MASSIMO PORTINCASO
Partner and Managing Director
Berlin