Finn Brunton goes inside the Bitcoin blockchain to explore the weirdly meticulous collective archive, and how it might someday govern us.

KEEPING THE BOOKS

"First, the Company was forced to assume all public power. (The unification was necessary because of the vastness and complexity of the new operations.)"
—Jorge Luis Borges, "The Lottery in Babylon"

MANY OF BORGES'S STORIES FOLLOW A SIMILAR ARC: some seemingly small, innocuous thing—an encyclopedia, a lottery, the act of dreaming or trying to write a novel—expands in scope and scale until it becomes indistinguishable from its context, like his famous 1:1-scale map that completely covers its territory. In "The Lottery in Babylon," the administration of a lottery grows to incorporate misfortunes as well as winnings of all kinds, and extends to every citizen, until the operation of the lottery effectively becomes the state (and, latterly, something more like fate itself). Part of Borges's sly joke in this story is that the seemingly cruel and arbitrary actions of the Company in charge of the lottery are actually *preferable*, as a mode of governance, to those by which people are still elevated and ruined largely by chance: a chance skewed, rendered impure, by wealth and power. There's a deeply seductive appeal to governance by an inhuman system: however byzantine the nested layers of the lottery become, there's a random draw at the center of it that can't be bribed, intimidated, or begged for mercy. What makes this system "inhuman," given that there are few activities more human than staking an outcome on the turn of a card, and that every step of the rewards and punishments expresses our all-too-human convictions? Can you call a lottery a government? How could you defer authority to a system you *know* has nothing at the center, nothing but pure chance? We shake our heads together in puzzlement.

Welcome to Bitcoin.

Or, rather, welcome to the "blockchain," the system that underlies Bitcoin. Like Borges's lottery (that most wasteful of civic activities) that becomes the state, Bitcoin is a largely experimental, novel form of currency—an idea somewhere between "visionary ambition" and "kooky absurdity"—whose underlying mechanism, the blockchain, is being transformed into the technological substrate for a new, abstract kind of governance. The blockchain is a payment system with no money; a single, canonical record that is copied everywhere and maintained by everyone; a quasi-system of government whose ultimate authority rests on a series of deliberately useless, arbitrary computational problems. This state isn't built completely around a lottery, but rather around a *ledger*.

We start with physical cash to understand how this ledger, the blockchain, works, because they share a common problem, one that's far more challenging to address with digital cash: making unique objects that are easy to produce and difficult or impossible to reproduce. When I hold currency—let's put a U.S. $20 bill on the table now—I have an object with a very particular set of constraints. It must be almost exactly like every other U.S. $20 issued by the Treasury so it can function as legitimate money. But it must also be unique: if there is a single other bill *exactly* like it, one of them is a counterfeit. The bill must be very easy and cheap for the Mint (and a small set of textile and printing organizations) to produce, and yet nearly impossible for any other group to reproduce. There is no other bill like this one before us (serial number JB9557548B, 2009 series, Timothy Geithner's signature, a little ballpoint pen squiggle over the portico of the White House), but there are 6.4 billion others that are very, very close.

Meanwhile, the history of computing and telecommunications is primarily the work of transmitting perfect copies over imperfect channels, whether those copies are in the RAM and the hard disk of a single computer, or on a screen and a server on different continents. It is not enough to say that digital objects can be copied (with the connotation of a degraded, knockoff version): they can be *duplicated*, by design, thanks to decades of brilliant research devoted to reliably producing and verifying bit-for-bit duplicates of files.

Unique objects, yet perfect duplicates. You can already hear the grinding friction between the words "digital cash." The "cash" part is crucial; individuals can transact cash directly without having to pass through a "trusted third party"—a credit card payment or an online payment from our bank account. The besetting problem of digital cash research and development throughout the last two decades has been to produce a digital object that could be easily generated, transmitted, recognized, and exchanged—but not duplicated—without relying on a third party like a central bank, a clearinghouse, or the state. We should be able to transact this "cash" without creating new money objects or new copies of existing money objects. The Bitcoin blockchain's answer to this seemingly intractable problem of digital objects acting as money: don't have objects.

There's no string of characters that constitutes a bitcoin, no file or set of bits or bitcoin "thing." All that exists are *addresses* in the ledger, which represent bitcoin *ownership*; bitcoins don't exist apart from their attachment to an address. Think of it as an archive that has rich and meticulous documentation of provenance and chains of custody without any actual documents or artifacts. It resolves the complex legal and technical distinctions between data and metadata, text and paratext, by having *only* metadata. These transactional records and ownership logs constitute the existence of "bitcoins."

All the exchanges of ownership between Bitcoin

PREVIOUS PAGE:
20 July 1917, Secretary of War Newton D. Baker, blindfolded, drew the first draft number in the lottery to be called up: Number 258. "US LOTTERY, 1917" U.S. NATIONAL ARCHIVES' LOCAL IDENTIFIER:165-WW-420(P379) FROM: AMERICAN UNOFFICIAL COLLECTION OF WORLD WAR I PHOTOGRAPHS, COMPILED 1917 - 1918 (RECORD GROUP 165)

addresses are broadcast on the network; these transactions are settled, or confirmed, every 10 minutes. *Settlement* means that everyone running the Bitcoin protocol software—all the peers on the peer-to-peer network—takes the latest transactions on the system and races to solve a cryptographic problem that will link the "block" of new transactions with the previous blocks, which in turn are linked into the chain. The problem is difficult enough that most of the community would have to work together to post false transactions, double-spend money, or otherwise mess with the system. The winner of the solution race gets some new bitcoins, in the form of new records of ownership that didn't exist before. In other words, what makes new money in this system—what the money is, in a literal sense, made of—is the record of the existence and circulation of the money thus far. (The solutions to the problems are meaningless, exceedingly improbable results of slowly escalating difficulty to keep the rate of settlement and the production of new money constant.)

This is, therefore, an "append-only public ledger." It is a record of events—transactions between addresses—that everyone maintains (public) and to which new events can be added but not removed or altered (append-only). As of this writing, the ledger held 77,219,785 transactions. At first, the ledger was stored mostly on personal computers and custom-built servers in backyard sheds and basements; now it is kept in massive installations in cold regions of the world with inexpensive electricity and high-bandwidth Internet connections. It's nearly 20 gigabytes in size, and not just from transactions.

THE LOTTERY EXPANDS, WRITES BORGES, from merely contributing to the vicissitudes of human life to apportioning power: "I have been proconsul," says his narrator, and "I have been a slave. I have known omnipotence, ignominy, imprisonment." Very quickly, blockchain users and developers realized that an append-only public ledger—a system, collectively maintained, that only confirms that an event took place at one time, never to be changed, edited, or denied—could serve as a kind of archive, and then as the bare-bones foundation of a contractual order that could create companies, even minimal governments. The collective maintenance meant that, seen in a certain light, the blockchain was a robust, distributed archival backup system. If you could incorporate something into your transaction, it would be swiftly stored on hard drives all over the world; thus, the blockchain now includes 2.5 megabytes of diplomatic cables from WikiLeaks, a thousand digits of pi, texts from the *Bhagavad Gita* and the Pope, ASCII art and Valentine's Day messages, and encoded images and mysterious encrypted files.

This archival property of the ledger—complete with timestamps and planet-scale redundancy—also made it ideal for the sorts of activities previously relegated to notaries, such as witnessing contracts. More than ideal, in fact, because the blockchain could be used as the basis of automated contracts that could publicly document their own fulfillment, and could even accrue and arrange payment out of the blockchain itself. Carefully designed blockchain contracts could become the basis for "decentralized autonomous organizations" (DAOs), institutions that operate largely without human guidance and share out rewards to human "employees" for their contributions. DAOs connected together, requesting work and distributing resources, have been proposed as a system of experimental, minimal government written in scripting language, the libertarian dream realized of society assembled out of contractual relationships. The conditional is important here; some of these advances *could* happen, and several organizations are rapidly building on the blockchain—whether Bitcoin's or their own, comparable version—to make them viable, most notably the "smart contract" platform Ethereum.

Before they get into the mire of practice, before the messy dissolution of the first blockchain-based marriage (marriage vows are a favorite hypothetical test case for smart contract architectures), or the tangles of offshore "autonomous" operations dodging taxes, storing files, and making payments in currency units like satoshis, szabos, dogecoins, and litecoins, we can see the conceptual implications of the blockchain with greater clarity. The blockchain's simple, abstract promise is to trust neither in people nor the state, but in a set of cryptographic properties. Given those properties, a system of records can be perfectly and publicly maintained. Borges imagined a society that mitigates the injustice of the human condition by submitting *everything* to rigorous, inhuman chance, to the total lottery. The social imaginary in the blockchain is still stranger: that money, contracts, even law and government, can be built on nothing but meticulous, automated, collective maintenance of the archive. ■

FINN BRUNTON *(finnb.net) is an assistant professor in Media, Culture, and Communication at NYU.*

The blockchain now includes 2.5 megabytes of diplomatic cables from WikiLeaks, a thousand digits of pi, texts from the *Bhagavad Gita* and the Pope, ASCII art and Valentine's Day messages ...