This is a section of doi:10.7551/mitpress/14712.001.0001

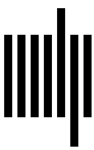
Cryptographic City

Decoding the Smart Metropolis

By: Richard Coyne

Citation:

Cryptographic City: Decoding the Smart Metropolis
By: Richard Coyne
DOI: 10.7551/mitpress/14712.001.0001
ISBN (electronic): 9780262374811
Publisher: The MIT Press
Published: 2023



The MIT Press

7 Writing the Block

The city as financial hub entitles urbanists and architects to claim a professional stake in the world of money and finance. In Britain, the *city* is that part of London occupied by the Royal Exchange, the Bank of England, the Stock Exchange, and the headquarters of major companies making up London's financial center, which is still one of the world's major financial hubs. The *city* is therefore synonymous with major financial infrastructure and financial technologies, so-called *fintech*.

Money is the city's lifeblood, vice, and symptom. The cryptographic city is a site of economic interactions. I will demonstrate in this chapter the importance of cryptography in securing monetary transactions as a major element of fintech. That introduces the concept of the *blockchain*, a disruptive technology that claims much promise in the smart city. An explanation of blockchain methods helps illustrate a range of city concepts about encryption, validation, secret communications, and transactions. Whatever the extent of its adoption, the blockchain tests ideas about distribution, sharing, and democratization in the city. The blockchain and the emerging field of *tokenomics* challenge how people think about cities. They also provide an entry point for consolidating the wider role of cryptography across many aspects of city evolution, design, and governance.

Street Life

Lewis Mumford argued that cities have their origins in family and community relationships that are nonmonetary,[1] but the contemporary city depends on financial transactions. Citizens choose among numerous methods for transferring money to pay for goods and services, or to gift

money to a charity, friend, or family member. Debit, credit, and cash cards deliver the necessities, habits, and addictions of the modern consumer, aided by cardless surrogates such as mobile payment and digital wallet services (e.g., Apple Pay, Google Pay, M-Pesa). These payment systems rely in turn on multiple layers of encryption to hide transaction information as it courses through networks, thus evading snoops, hackers, leakage, and accidental disclosure. Encryption is almost as vital as money in the digital age. As we have seen, most personal and business communications are encrypted, as are hard drives and files stored in the cloud. Digital encryption hides the content of a message or file by converting it to something that's unreadable by anyone except the designated receiver equipped with translation software and a private decryption key. Encryption and decryption are ubiquitous in digital communications and information processing.

As long as we are digitally connected, secure digital transactions are much more convenient than storing and passing around cash, as in handling coins and notes. For digital transactions we do, however, have to rely on centralized record systems for securely logging the credits and debits of every one of our transactions. With cash you know what you've spent as you see the cache of notes diminish in your wallet. In the case of digital transactions, the records of each transaction are kept by your bank, or a digital wallet service. You also rely on their encryption processes. Such transaction service providers are of course regulated and answerable to governments. So, most of us for much of the time have little trouble trusting our bank. But any taxpayer who has been audited by their government tax department knows that our transaction histories are visible to officials and their systems. You might also be concerned that companies that handle your money can analyze your transactions to profile your spending habits. That data about your habits may also be sold to third parties.[2]

It is only recently that citizens in some countries have become used to walking into shops with no cash in their purses and pockets. But buyers and sellers used to rely on cash transactions, formalized via various methods of recording and receipting. Cash has the advantage that no one but the buyer and seller need know what you are doing with it during the transaction. Cash transactions are person-to-person, sometimes referred to as *peer-to-peer* (P2P) transactions, as discussed in the context of the Tor browser, a computer term implying transactions among social equals, or

at least individuals in proximity to one another. In a cash society, you can ask your employer, customer, or bank to pay you in banknotes and coins. Then you exchange the cash for goods from someone else, or indeed give some of your cash away. Needless to say, human societies have been served well by cash transactions. Cash-only transactions hark back to less formal social transactions and are closer to familial social exchanges, bartering, and societies that foreground the exchange of gifts.[3]

Contrary to this story about the benefits of cash, many people now regard cash transactions with some suspicion. Cash-only societies provide opportunities for unregulated and therefore unreliable commerce. The aptly named *Journal of Money Laundering Control* contains numerous articles outlining the pros and cons of various means of exchange, including the prospects, benefits, and risks of cash and cashless societies.[4] Unreceipted cash transactions provide a way of avoiding record keeping, avoiding tax, paying for stolen goods, and paying bribes. That is the dark side of the cash economy. It will become apparent as we progress that digital transactions offer variations on these challenges.

For the time being I'll pursue the line of argument that identifies cash as providing positive benefit to individuals and economies. Urban scholars point to the important relationships between informal (cash-driven) and formal (regulated) aspects of urban living, particularly in developing megacities populated by entrepreneurial street sellers, snack vendors, pedicab drivers, and domestic services unable or unwilling to enter into arrangements with banks and the state.

In her influential book *The Death and Life of Great American Cities* in which she extolled the virtues of variety in the way cities form and are planned, geographer Jane Jacobs wrote, "Deliberate street arrangements for vendors can be full of life, attraction and interest, and because of bargains are excellent stimulators of cross-use. Moreover, they can be delightful-looking."[5] The image of the city as vibrant and dynamic invokes the romance of these kinds of person-to-person exchanges, including—I would add—the physicality of cash practices, the immediacy of unmediated exchange of money for goods, and the accompanying habits of browsing, persuading, bargaining, carrying and displaying your purchases, and being seen as active participants in the transactional life of the city. Though many of us can now engage in these routines without handling notes and coins, cash is emblematic of vigorous city living.

Cash Benefits

Cryptocurrencies are an attempt to reestablish the autonomy, flexibility, and confidential nature of person-to-person monetary transactions. As I have shown, encryption is ubiquitous in online activity anyway, but cryptocurrencies involve a special class of online transaction mechanism. Others have followed, but the first major, successfully engineered cryptocurrency was Bitcoin that emerged in 2009 around the time of the banking crisis. At that time trust in banks was at a low ebb. According to the seminal paper that launched Bitcoin, a cryptocurrency is "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[6] Normally you would trust your bank or other transaction service provider to keep accurate and secure records of your digital transactions. In the case of cryptocurrencies, the trust is relegated to a series of smart algorithms distributed across a digital network.

A cryptocurrency such as Bitcoin is digital money that purportedly carries some of the benefits of cash. You can buy things with it, give it away, invest it, and stash it without involving a bank. But unlike cash, there is no physical paper or coinage. Students in one of our classes design banknotes as a graphic exercise, using graphic software. But they can't use those notes as currency. Were we to design our own banknote or make a PDF of a scanned real banknote and email it to a friend, we would soon find that it carried no value; in fact, you would still have your own copy of the file, which means it could be reproduced and sent to someone else. Like real paper money, digital money has to be scarce. When you give some of it away, then you should no longer have what you had. As a further illustration of the need for scarcity, my local fitness center used to send me a PDF of a free visitor pass when I answered an online customer satisfaction survey. That free visitor pass served as currency of a kind. I would approach the reception counter with a friend and a printed copy of the coupon, and they would let the friend enter for free. They stopped sending out free passes when it became obvious that customers could print any number of copies of their free pass and use it more than once. It wasn't scarce, so it quickly lost its value as a means of rewarding and regulating customer activity.

Simulated, digital versions of paper money are redundant anyway. Our money with the bank or digital transaction platform is just a series of texts and numbers in a database. As you receive or spend money the balance goes up or down, and we trust the bank to keep an accurate and secure record. As I have suggested, digital money is for people who don't want banks or transaction services to manage, monitor, and profit unduly from their transactions. People want the benefits of cash but without the physical paper or coinage. It ought to be possible to process digital money as records of transactions on a digital database.

A Shared Ledger

When desktop computers were still a novelty, I supplemented my PhD study by designing and maintaining an accounting system for the residential college where I lived. It was a Victor 9000/Sirius desktop computer running dBASE II. With no real instinct for accounting, the first conceptual hurdle to overcome was figuring out how to create a database for each resident's transactions, that is, the expenses they incurred and their payments. That wasn't necessary of course. A system to record transactions with the residents could be stored as one big database rather than as a separate database for each resident. Transactions would include amounts billed for accommodation, extra meals, sports fees, payments, and refunds. As long as each transaction record clearly identified a unique ID for each resident, the date, what the transaction was for, and the amount of money, then the computer could generate monthly reports that only showed the transactions for that individual. That way, the residents could be sent specific billing information each month. As they paid their bill then the accountant would enter that payment as yet another transaction, a credit, in the ledger. Each time we printed an account statement for a resident a balance would appear at the bottom of the page showing what was owed, or in credit. It was simple enough to devise an algorithm to quickly total all the transactions for any resident to deliver their current balance.

This is basic accounting, an update on double-entry bookkeeping, one of the progenitors of Enlightenment rationality as I outlined in chapter 2. I mentioned accounting systems here to help explain what is meant by a ledger, and how it can accommodate an arbitrary number of users and their

transactions. The database of all transactions was the ledger, which mirrored the ruled pages in the college accountant's paper-based bookkeeping system, which my system would eventually replace. There need only be one single ledger, even though it records the transactions of hundreds or thousands of customers, clients, or residents.

My system was stored on one computer in one place, managed by the accountant and me. The accountant needed access to every transaction. In fact, she or her assistant, entered the transactions herself as the invoices and cheques came in. Between us we played the role of a bank as record keeper. The challenge for a cryptocurrency is to maintain such a ledger. But any customer needs access to their own transaction records at their own computer or smartphone. That personal, user-level access is common enough now with digital money flows, online banking, cash cards, and so on. The next challenge for a cryptocurrency is to keep people from tampering with the ledger, eliminating their own debts or entering false payments. Banks of course are specialists in such security. The college accountant and I kept our little system and its database securely locked in an office, and we were the only ones with the room key and computer password to edit the transaction records.

The idea of cryptocurrencies is to avoid such a centralized storage facility, and the main challenge of cryptocurrencies is to obviate the risk of tampering. In the case of decentralized cryptocurrencies, the solution to the security problem is paradoxical. To keep the ledger secure, a cryptocurrency system creates and maintains multiple copies of the ledger and distributes the copies to a large number of computers in a network. That's the ledger of all transactions, not just ones belonging to any particular customer. To continue the analogy with our in-house accounting system, that would be like distributing electronic copies of the ledger file to a trusted collection of college residents and requiring them or their computers to update the ledger each time a new transaction comes into the main office. They would have to keep comparing their versions of the entire ledger to see that nothing has been altered among the previous transactions. That is an implausible and time-consuming challenge for human beings but can be easily automated now with networked computers.

In the case of cryptocurrencies, software compares distributed copies of the ledger to one another in case someone tries to double-spend an amount of money or modify the record. In fact, nothing gets recorded in the ledger

unless computers on the network agree it should be there, and the distributed versions of the ledger are compared to each other to make sure nothing has been changed. This is a task for dedicated computer processors on the distributed cryptocurrency network whose job it is to validate transactions. In the case of Bitcoin there can be around ten thousand or more active nodes on the network, labeled as "fully-validating nodes."[7] The state of the distributed system fluctuates as computers equipped to undertake the validating procedure come online or go offline.

Once the cryptocurrency software is distributed for this process, then it should take care of the ledger. The software that runs the cryptocurrency ledger is maintained collaboratively as an open-source project. Regular users wanting to make transactions most likely encounter the currency through third-party platforms that provide digital wallet services such as Luno, Bitpay, BRD. These platforms operate as intermediaries providing access to the cryptocurrency ledger, but none of them monitor or maintain the ledger or monitor what the transactions are for. In fact, the encryption protocols are designed so that neither a human being nor a computer algorithm could read or deduce who made the transaction, who was the recipient, or what it was for. Users of digital wallets gain access to their own account of transactions via a unique private encryption key (a kind of passcode). If they lose the key, then they lose access to their transaction records. No one can redeem that information for them. The value of the account is lost.

In my simple in-house college example, I think there were three reasons the accountant was happy for me to develop a bespoke accounting system rather than buy one from a commercial supplier. First, such commercial systems existed, but the printouts looked like impersonal computer printouts as opposed to the personalized letters the residents were used to. Second, my system was designed to mirror as closely as possible the college accountant's paper-based bookkeeping system. Third, I also designed my system to mirror her ability to correct the ledger if she or her assistant made a mistake. I thought that if the accountant were to over- or under-charge someone, or mistype a payment, then she would enter another transaction (e.g., a refund) that corrects the mistake. The new transaction is labeled as an adjustment. But that would appear on the account sent to the resident as an adjustment arguably creating an unprofessional impression. So, I did what any sensible accounting system would *not* allow—I provided a user-friendly interface that let the accountant enter the record system and adjust

the ledger to correct it. In the wrong hands, there was little to stop someone with access to hack the ledger or insert false payments. Everyone involved in this case, however, happened to be extremely trustworthy: nothing went awry, and in any case external auditors would be performing annual checks.

But a distributed ledger cannot allow alterations to transactions whether to correct a mispayment or to extort. How does a cryptocurrency system disallow alterations to the ledger, especially as it is so widely distributed? What happens if the different versions of the ledger don't match up? Here, analogies with conventional systems for keeping accounts fail. The best I can think of is the banal practice of writing transactions into a paper ledger in ink rather than pencil. Then they can't be erased or altered, or if they were then the alteration would be obvious to an auditor looking at the ledger.

Securing Transactions

For a cryptocurrency, the way to secure each transaction in the ledger is to provide some method of locking it down so that it cannot be accessed or changed. Transaction records are secured by a form of cryptographic coding known as *hashing* introduced in chapter 4 as the translation of data into a short piece of random-looking code. The way I developed an appreciation of the method was to spend time on a website that has an empty field into which you type or paste an item of text. The website then returns the corresponding hash string. The site run by xorbin.com implements the SHA256 function, the name given to one of several standard secure hash functions.[8]

A hash string is a kind of signature of the transaction, a 64-character-long string of arbitrary-looking alphanumeric characters. That hash string can be created for any body of text, of whatever length. For example, you could run a standard hash algorithm to create a hash of the text of one of Shakespeare's sonnets or the entire set of ordinances for a city. That sixty-four-character hash string will look nothing like the text from which it is derived, and it is impossible to reconstruct the sonnet or the ordinance from the hash string. But if even one character in the original document is changed, or a comma is out of place, then the hash string of that version will look different, and any pattern-matching software could easily detect that the file has been altered. If you email the text of the document and its hash string to someone, they should then be able to reproduce the same hash string from the body of text you sent. If the hash string is different,

that means the document has been altered. Comparing hash strings is a way of checking if a document has been tampered with or corrupted in transit. The process is automated of course. The algorithm that does the comparison can't detect what has been changed in the file, but it could certainly signal that the file needs to be rejected. The same technique is applied to transactions in a ledger.

At this stage it is worth noting that the algorithms in the cryptocurrency system check and secure transactions in real time. For efficiency the transactions are processed as groups of transactions. The Bitcoin digital money system processes and secures around five hundred transactions at a time as they come into the system and irrespective of who made those transactions or where they were made. This collection of validated transactions is called a "block," from which the terminology *blockchain* derives.[9] The shared and ordered ledger and its verification apparatus is called the *blockchain*. The agreement to accept a block of transactions is reached by algorithms running at the node computers in charge of validating blocks of transactions.

The method of agreement is another conceptual sticking point to most people new to the working methods of cryptocurrencies. I alluded to the method in chapter 6. I will elaborate here pending further explanation in chapter 11.

The algorithms at the node computers, meaning the fully validating nodes, try to outcompete one another in solving an arbitrary numerical puzzle that requires brute-force computation to solve. The node that finds the solution to the puzzle first receives some digital money as a reward, and the answer to the puzzle is planted into the block of transactions as a record that the most recent transactions are verified. Individuals and companies that dedicate processing time to securing the blocks are called "validators." For most cryptocurrency systems they are also referred to as "miners" as they automatically generate digital money as a reward for their role in keeping the currency secure. They effectively generate money for themselves, which in turn increases the supply of Bitcoins. Their digital reward is simply a transaction recorded on the ledger credited to the miner. The miners keep what they generate, though they incur the considerable cost of the hardware and electricity to run their processors solving the numerical puzzle.

Anyone so motivated can become a Bitcoin miner. You don't need approval or a license. Sites such as www.bitcoinmining.com provide instructions on how to become a miner.[10] In the early years of Bitcoin mining

individuals with powerful desktop computers could download the software and configure their home computer to contribute automatically to the contest to validate blocks of transactions. As the competition between miners has increased, so has the demand for more efficient processing. Now, there are specialized microprocessors that you plug into a home computer arrangement. For individual miners, the usual practice is to connect to a mining pool. That is a consortium of computer owners who share processing power and distribute any profits from Bitcoin mining among themselves. By most reckonings, home-made Bitcoin operations will now barely make enough to cover the cost of the electricity consumed by always-on Bitcoin mining hardware.[11] Stories about crypto-mining circulate amongst enterprising students. Ethereum (ETH) is a cryptocurrency related to Bitcoin. One of our student informants reported about a friend: "A software engineer working in London at the time, was mining Ethereum (ETH) back in 2017, making enough money to offset his increased electricity bills and save the excess ETH." The mining challenge has since migrated to companies with the resources to run large-scale specialized processing farms in places where electricity is cheapest. This constraint has lured cryptocurrency mining to countries such as China. As of 2021, China ran 65 percent of all Bitcoin mining operations, though its activity in the area has varied with the rise and fall in energy costs and responses to government policies.[12]

I'll put aside details of the validation process for the time being. Most of the transaction information in the Bitcoin ledger is in plain sight and can be read on a computer screen on web pages, for example, at blockchain.com/explorer. You can see the amounts of money being transacted in each block on the ledger, but information about who is spending or receiving the money and what it is for are encrypted as a series of arbitrary-looking hash strings. The visibility of this ledger is of value to researchers assessing the performance of the Bitcoin ledger's operations. Though it is in plain sight, the confidentiality of individual transactions is maintained by the cryptographic protocols. No humans are involved in the process of verifying transactions. That is done by algorithms. I'll explain more about the arcane procedures of the blockchain as I progress, but for the time being it's worth drawing attention to the implications of cryptocurrencies for the cryptographic city. That is the subject of chapter 8.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Coyne, Richard, author.
Title: Cryptographic city : decoding the smart metropolis / Richard Coyne.
Description: Cambridge, Massachusetts ; London, England : The MIT Press, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2022021507 (print) | LCCN 2022021508 (ebook) | ISBN 9780262545679 (paperback) | ISBN 9780262374811 (pdf) | ISBN 9780262374828 (epub)
Subjects: LCSH: Smart cities. | Internet of things. | Urban development—Data processing. | Public administration—Security measures. | Data encryption (Computer science)
Classification: LCC TD159.4 .C69 2023 (print) | LCC TD159.4 (ebook) | DDC 004.67/8—dc23/eng/20221011
LC record available at https://lccn.loc.gov/2022021507
LC ebook record available at https://lccn.loc.gov/2022021508

10 9 8 7 6 5 4 3 2 1