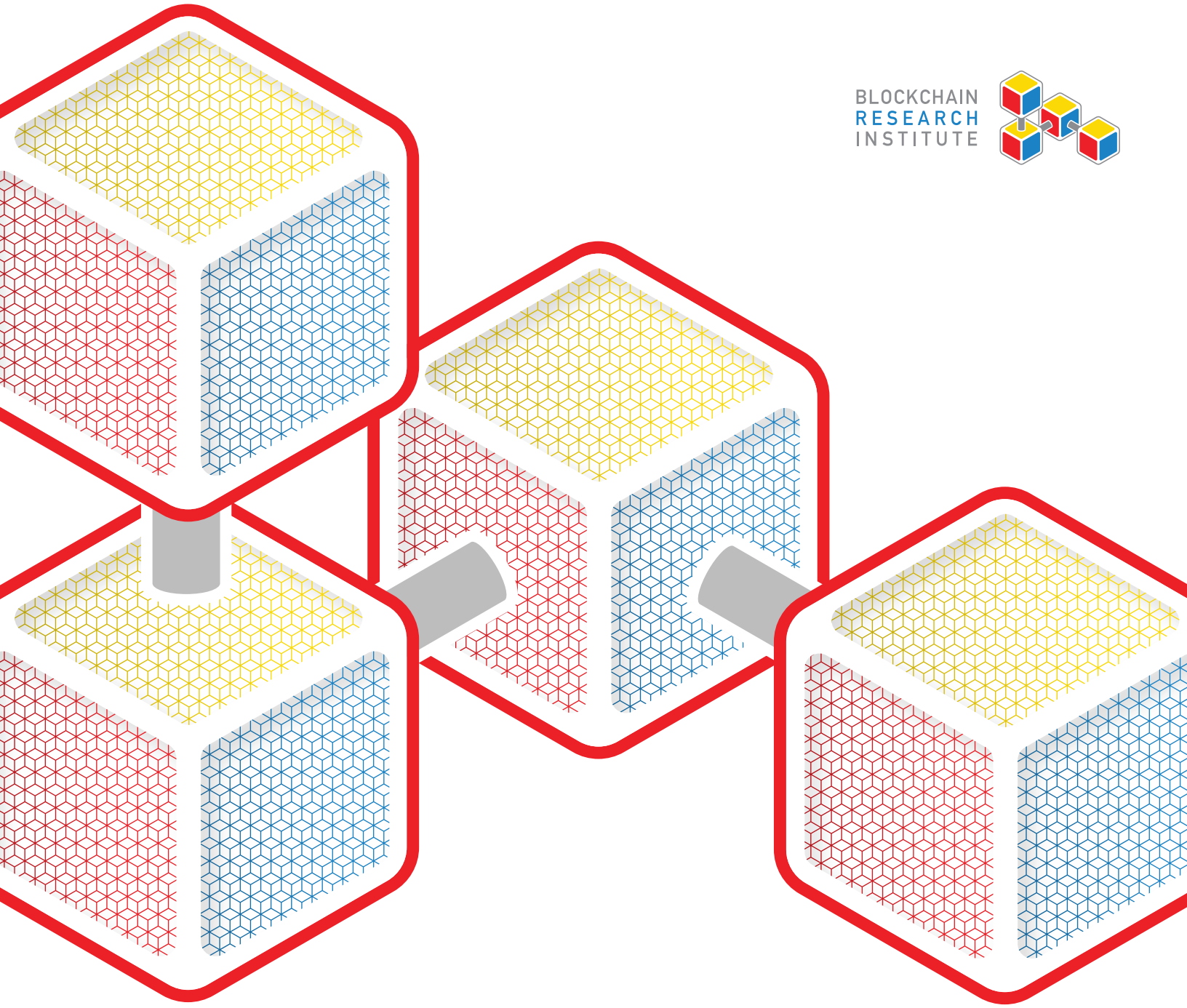
BLOCKCHAIN RESEARCH INSTITUTE



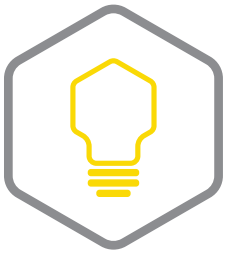
MANAGING BLOCKCHAIN TRANSPARENCY

Strategies for a Private/Open World

Andreas Park
University of Toronto

November 2017

A BLOCKCHAIN RESEARCH INSTITUTE BIG IDEA WHITEPAPER



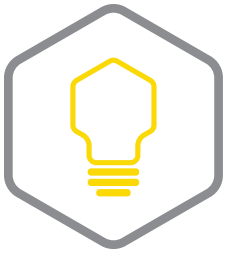
Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, "the digital economy," with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

In 2017, Don and Alex Tapscott launched the Blockchain Research Institute to help realize the new promise of the digital economy. We research the strategic implications of blockchain technology and produce practical insights to contribute global blockchain knowledge and help our members navigate this revolution.

Our findings, conclusions, and recommendations are initially proprietary to our members and ultimately released to the public in support of our mission. To find out more, please visit www.blockchainresearchinstitute.org.

Contents



Foreword

For many years, I have echoed the words of US Supreme Court Justice Louis D. Brandeis, "Sunlight is said to be the best of disinfectants." In my view, transparency is critical to the robust functioning of markets, corporations, and governments. Consider the murkiness of Enron's balance sheet and the opacity of the US subprime mortgage market: the former contributed to the largest corporate failure ever at the time, the closure of a storied accounting firm with 85,000 jobs lost, and the convictions of several C-suite executives, and the latter factored into the 2008 market crash. Trillions of dollars of underfunded derivatives—and some experts peg that amount much higher—threaten to trigger an economic crash that would make 2008 look like a tremor.

That's why I think transparency is one of the most important benefits of blockchain. Distributed ledger technology makes such obfuscation more difficult, if not impossible; and this project deftly explains why. For starters, two people cannot claim ownership of the same asset—the ledger will not allow it. That reminds me of the next part of Justice Brandeis' quote: "Electric light [is] the most efficient policeman."[1]

In our global search for the best faculty for our research program, we did not have to look far for our transparency expert, Andreas Park, a finance professor at the Rotman School of Management. He studies equity markets and advises regulatory bodies on the economic impact of technology within the financial industries. Andreas cogently explains that transparency is a design choice and argues for public disclosure even on permissioned blockchains. His is a compelling argument, and one well worth considering for those weighing their public/private blockchain design options.

DON TAPSCOTT
Co-Founder and Executive Chairman
Blockchain Research Institute

Idea in brief

» The advent of blockchain technology forces us to reconsider the upside and downside of public revelation of transactions and contracts. The implementation, application, and possible regulation of distributed ledgers involve choices that will critically affect information disclosure and economic interactions.

» Blockchain technology can facilitate the monitoring of a firm's investment decisions by storing contracts and transactions in a manner that is comparatively inexpensive and inherently visible to anyone who has access to the Internet.

» It does not matter whether the blockchain is public and permissionless, such as the Bitcoin or Ethereum blockchains, or private and permissioned, such as Ripple or Hyperledger implementations: in principle, transactions are traceable with attribution of actions to identifiers. Therefore, the technology has a native high level of transparency.

» Users can still protect their privacy in both private and public blockchains: some methods are procedural and involve the smart usage of the protocol, whereas others are technological and use mathematics.

Introduction

On October 19, 2001, Enron Corp.'s multi-year success story ended without anyone's living happily ever after: the firm announced $638 million in quarterly losses and a $1.2 billion reduction in shareholder equity. Fast forward a few months, following a US Securities and Exchange Commission and US Department of Justice investigation, the world learned that Enron management had fudged the books and hid massive debt obligations in complex accounting constructs. Enron executives received 24-year prison sentences, which was little consolation to tens of thousands of Enron and Arthur Andersen employees who lost their jobs and pensions and to shareholders who saw $65 billion of equity disappear. Several more accounting scandals later, US Congress passed the Sarbanes-Oxley Act, which tightened disclosure, accounting, and accountability standards.

Taking a step back, let's ask ourselves: what is the root problem that regulators and legislators have been trying to solve? Lenders want to know whether a borrower is likely to pay back a loan, and equity investors want to know whether they are likely to receive a return on their investment, particularly whether the current market price of a public company indeed reflects the intrinsic value of a share. Yet, time and time again, managers of banks, corporations, accounting firms, and government agencies have been caught in lies.

Asymmetric information, when one side of a deal has better information than the other and can use it to the latter's detriment, is toxic for the functioning of markets.

Asymmetric information, when one side of a deal has better information than the other and can use it to the latter's detriment, is toxic for the functioning of markets. For this reason, an elaborate and often burdensome system of regulations exists to reduce this asymmetry by mandating regular and accurate disclosures. Accounting rules give managers leeway to reallocate funds and revenues inside the company. Moreover, accounting reports are published intermittently, and there is ample evidence that managers engage in numerous economically pointless yet costly activities such as earnings "smoothing." Finally, the external certification of the books is expensive.

Supplying intermittent reports was appropriate, time-consuming, and costly in the pre-digital world: management needed to aggregate information from various units and pay a third party to check and verify it before mailing it to shareholders. Today, firms have electronic accounting systems: executives get financial information in real time but haven chosen not to share such raw and unaudited data streams with investors.

In principle, blockchain technology allows firms to disclose verified financial transactions publicly, directly, and in real time. It also allows them to disclose an extensive set of contracts. These published deals would be in the form of code which would eliminate ambiguity about a firm's financial condition and commitments. Although fraudulent activities are still possible, many of the deals that led, for instance, to the demise of Enron would no longer be possible.[2] Assets couldn't appear to be owned by two parties at once, hiding liabilities would be impossible, and would-be Enrons couldn't attract such positive media attention and additional funding as Enron did.

The benefits of shared knowledge

Ownership of an asset is attributed to an address, which is a set of letters and numerals that we can think of as an identifier.

A critical component of asset ownership and of a contract is attribution: who holds the asset, and who has established and is party to the contract? A blockchain stores this information by recording asset origination and transactions, and thus changes of ownership within a distributed (as opposed to central) ledger. This complete record of transactions and contracts establishes the current owner of an asset. Ownership is attributed to an address, which is simply a set of letters and numerals and can be thought of as an identifier.

By recording transactions on a blockchain, a network with multiple parties has shared knowledge of past and current ownership of

assets. An intrinsic part of the technology is thus that there is some degree of transparency regarding past actions and present ownership. Indeed, by default, the transaction attribution is entirely transparent to anyone with access to the network. In principle, the addresses or IDs are anonymous.

Disclosure is inherent. In principle, those with access to the blockchain's information can have the same information about a firm as the firm's managers. This feature may reduce the costs of generating accounting statements and performing audits.

Had Enron's management been required to disclose the firm's addresses publicly, then investors and oversight bodies could have traced the movement of assets and liabilities. The beauty of blockchain-based transactions is that disclosure is inherent. In principle, those with access to the blockchain's information can have the same information about a firm as the firm's managers. This feature may reduce the costs of generating accounting statements and performing audits.[3] There are further cost savings: asymmetric information is a risk, for which financiers require compensation. By reducing information asymmetry, firms reduce risk and lower their cost of capital; they have more money for investment and research, and they can use these funds to build better products and increase employment. Blockchain technology can therefore be a catalyst for incremental economic growth.

How much is too much transparency?

For all its virtues, transparency affects the economic interactions of market participants, and it can have downsides. For instance, an investment dealer is asked by a client to absorb a large position because the client has a liquidity need. The investment dealer now has a risk on its book that it doesn't want. In a relatively liquid market, this problem may be small because the dealer will likely be able to trade out of the position quickly. But, in a fairly liquid market, the client probably wouldn't have approached the dealer in the first place. In an illiquid market, with few prospective counterparties, the dealer has to worry about a squeeze: a well-capitalized bandit trader may be able to move the market against the dealer and force the dealer to liquidate the position at a fire sale price. The dealer does not want the public to see its risky position.

Should we care about the dealer? I believe we must. The risk of a position squeeze is real, dealers want to be compensated, and thus either the cost of trading illiquid assets goes up or markets for illiquid assets collapse altogether.

Put differently, there are legitimate reasons to settle transactions on a highly transparent blockchain and legitimate concerns about such transparency. Indeed, when confronted with the concept of a public blockchain that records all transactions publicly, financial industry executives were put off—not on their watch!

The alternative is a permissioned, private blockchain, organized and controlled by a known and trusted consortium of entities such as banks. The assumption is that the level of visibility of such a private distributed ledger or blockchain is a design choice. But matters are not that simple: even a private blockchain, possibly organized by a consortium of banks, still involves the record-keeping of everyone's

transactions in each node of the distributed network. In other words, even in a private blockchain, our competitors can see our activities.

Is that the end of the discussion? No. If banks have concerns about lack of privacy, then they should not be using the Internet either. Instead, I believe that the discussion around transparency should focus on the desired, socially optimal level of transparency. This level is a critical design choice for firms that wish to establish a private blockchain. Moreover, regulators and lawmakers need to carefully think about what disclosure they require of corporate users of public blockchains.

Our discussion of transparency should focus on the desired, socially optimal level, which is a critical design choice for firms that wish to establish a private blockchain.

In this paper, I outline how the recording of information on a blockchain differs from that in the current world of asset transfers, and who gets to see what information. Changes in transparency have economic consequences and may create winners and losers. I will therefore describe the business cases against and for transparency. Finally, I discuss the technological solutions that exist to reduce the built-in full transparency of blockchains.

Native transparency in blockchain technology

Ownership transfers: Central registries versus distributed ledgers

To illustrate the possible transparency issues, let's look at the workings of blockchain technology and how they relate to the transparency of actions and holdings.

All non-physical, non-registered asset transfers require a mechanism to change the record of ownership. At present, centralized ledgers keep most such records, and only highly trusted parties can access and modify these records. Cash is kept in bank accounts, and a bank account is a central registry. The record of ownership of a house is kept in a property registry. Securities such as stocks, too, are kept in central securities depositories such as the Depository Trust and Clearing Corporation (DTCC) in the United States or the Canadian Depository for Securities (CDS) in Canada.[4] Finally, records of most bilateral contracts are commonly kept by the parties involved, and transactions that the terms of the contract trigger thus involve a complicated account-reconciliation process. Consumer loan agreements are usually additionally registered with the credit bureau such as Equifax or TransUnion.[5]

Blockchain technology is a consensus protocol to change records in distributed ledgers, and its setup defines who can make changes to the ledger and under what circumstances. At its core, a blockchain is an append-only protocol that stores "transactions," where in principle

a transaction can be a trade but also text-based information such as a piece of programming code.

The key feature of a blockchain is that by recording transactions, it ensures a consensus on the current owner of an asset. Figures 1, 2, and 3 below look at token transfers on the Ethereum blockchain. This information comes from the public website Etherscan.io, which pulls data from the Ethereum blockchain. (Blockchain.info is a similar web-based service for the Bitcoin blockchain.)

A key feature of a blockchain is that, by recording transactions, it ensures a consensus on the current owner of an asset.

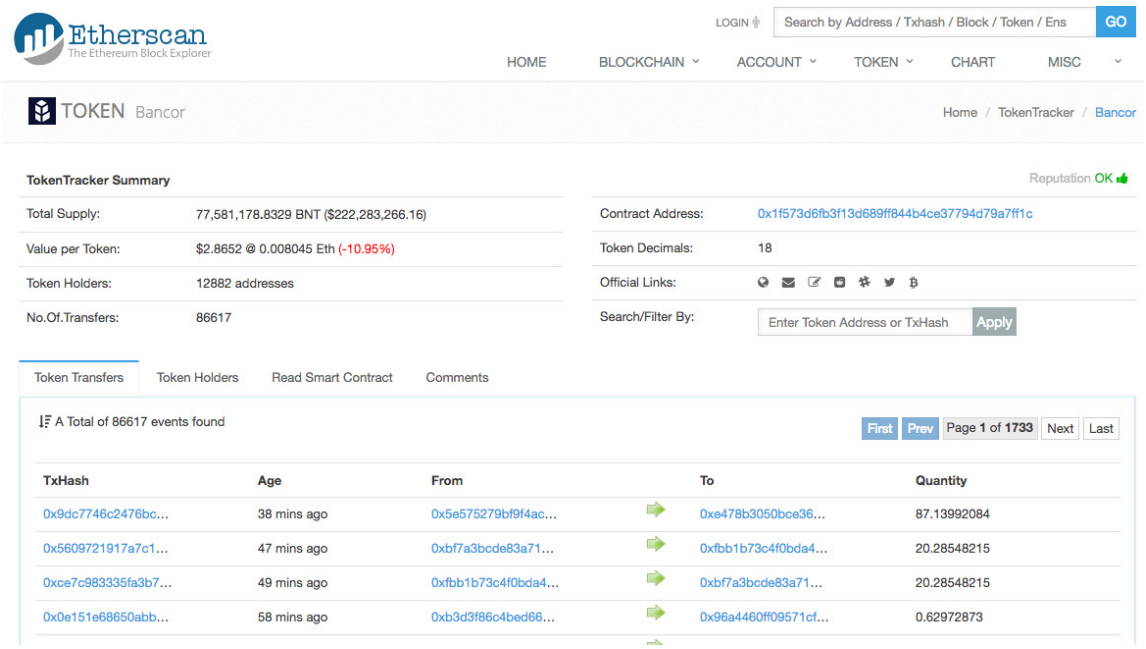
Ownership transfers: Public versus private blockchains

Let's consider the differences in data storage. To date, most firms still store enterprise data in a central database. This setup is simple and easy to understand. Also, since all information is stored and changed at a central location, one party cannot sell the same asset or spend the same dollar twice. Think about a bank account: Bob cannot send the same dollar to both Sue and Alice, and Bob cannot use the same asset as collateral in two transactions. The centralization of data storage prevents this *double spend* problem.

There are, however, many concerns with central databases, foremost among them, security: if the database fails because of, say, a major

Figure 1: Transactions by token

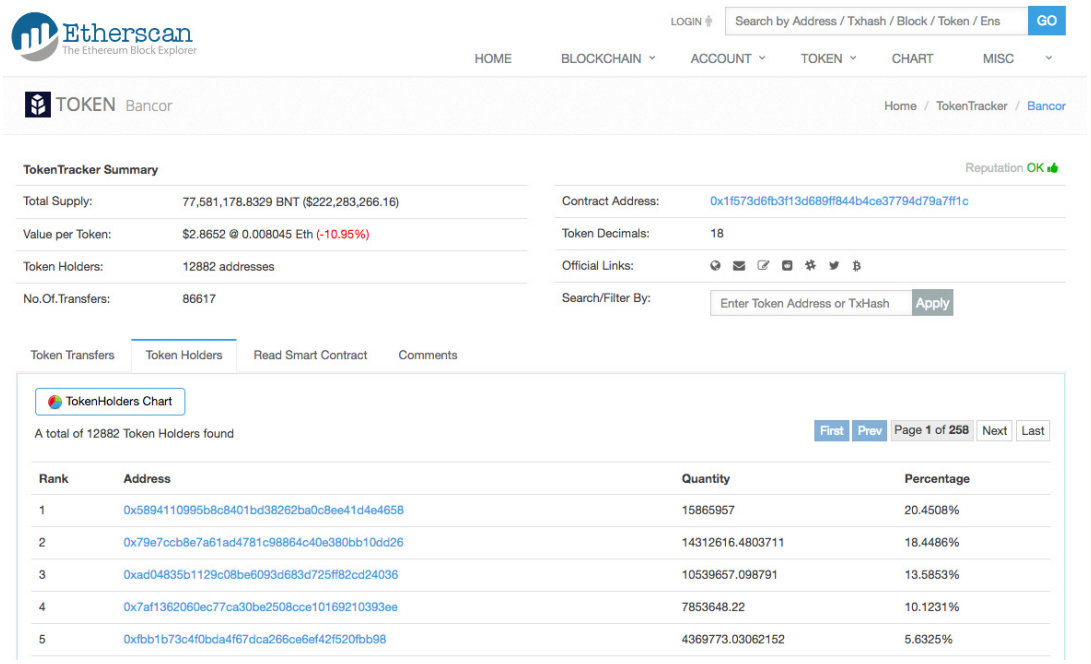
On Etherscan, anyone can see records of transactions on the Ethereum blockchain involving the digital tokens (or assets, in this case) of a company named Bancor.



Source: etherscan.io, accessed 2 Sept. 2017.

Figure 2: Top holdings of token

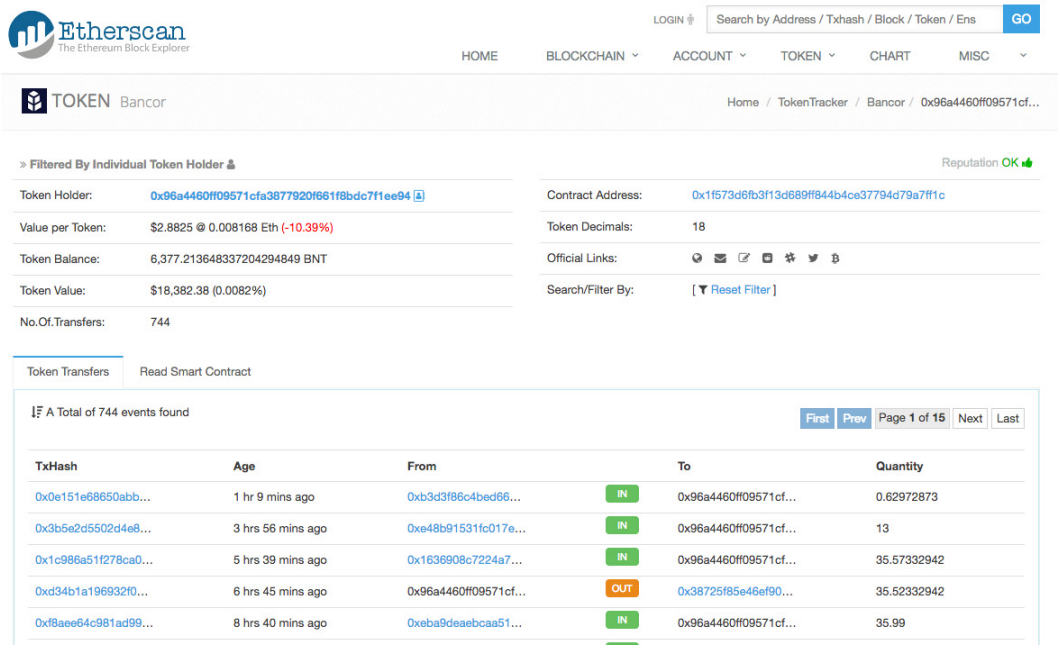
Here we see the top five holders (by public Ethereum address or ID) of Bancor tokens.



Source: etherscan.io, accessed 2 Sept. 2017.

Figure 3: Transactions by ID

We can also see the most recent transactions of Bancor tokens for the top owner (i.e., for a particular Ethereum address).



Source: etherscan.io, accessed 2 Sept. 2017.

hardware failure, all data might be lost. For that reason, keepers of central databases always make backups—and a backup model is one step closer to a distributed database. Namely, the keepers need to update their backups continuously to avoid data loss and thus need a backup protocol to ensure that data in the backup is accurate.

A distributed database shares features with a central-backup system in that it keeps all information at several locations. The key difference is that in a distributed database, there is no single primary location from which all changes originate. Instead, each site can make changes to the data.

There is no single point of failure, all data are available locally, and the system can be set up so that the different locations need not trust one another, yet all sites continuously agree on the content of the database.

There are numerous advantages to this setting: there is no single point of failure, all data are available locally, and the system can be set up so that the different locations need not trust one another, yet all sites continuously agree on the content of the database. According to Richard Gendal Brown from R3, "[a] system[...] that [is] operated by multiple parties, none of whom fully trust each other, that nevertheless come[s] into and remain[s] in consensus as to the nature and evolution of a set of shared facts."[6]

However, a side effect of a distributed database is that *all* information is stored at *all* locations. So, for instance, if a set of banks organizes the distributed ledger (wherein each bank is a network node), then every bank holds the information of all other banks' accounts. Such an arrangement raises red flags for executives, and so we need to understand what the information reveals (because storing information is not synonymous with accessing it).

There are two main types of distributed ledgers: public and private.

A public ledger is permissionless: anyone can become a network node and anyone can, in principle, enter records in the ledger. The most prominent examples are the Bitcoin and Ethereum blockchains. Indeed, the process of becoming a network node is part of using the blockchain: as a first step to use the Ethereum blockchain, one downloads a so-called wallet software; an example is the "Mist wallet." These wallets monitor the Ethereum blockchain to find transactions that have been sent to the wallet. As part of the process, one downloads the information from the Ethereum blockchain and becomes a node.

A public ledger is permissionless: anyone can become a network node and anyone can, in principle, enter records in the ledger. The most prominent are Bitcoin and Ethereum.

A private distributed ledger, in contrast, is built by either an individual firm or by a consortium of firms and differs from public distributed ledgers in several key ways. First, a private network can be permissioned and can thus restrict who can use it to record transactions and can view the flow of information and assets across it. For financial institutions, this feature is important as it allows them to comply with know-your-customer (KYC) legislation, which is a usually a prerequisite for compliance with anti-money laundering (AML) rules. Moreover, in principle, these networks don't need a trustless protocol. A downside is that a consortium solution raises the specter of collusion and rent extraction typical of a trust; for instance, network members may restrict entry, fix prices, and collude

on fees. From a competition policy perspective, it may thus be desirable to mandate a trustless protocol to remove a barrier for new entrants wishing to join a consortium network.

A private distributed ledger is built by an individual firm or consortium, can be permissioned, and can thus restrict who can use it or view the flow of information and assets across it. Moreover, in principle, it doesn't need a trustless protocol.

Figure 4: Signing and verifying transactions with public and private keys

The sender uses the transaction text and applies his private key to generate a signature. He then sends the transaction text plus the signature to the network. The network uses the public key and the text to verify the signature.

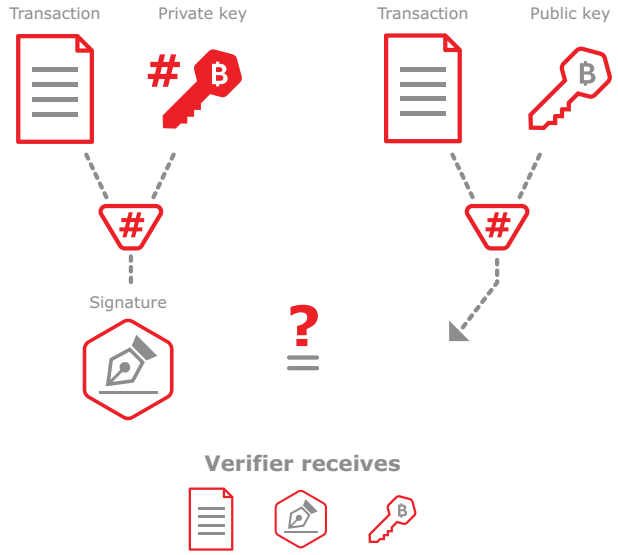


Figure 4 illustrates the workings of the verification of a blockchain transaction.[7] The key idea is that a user's blockchain address has (implicitly) two components, a public one and a private one. Everyone can see every transaction linked to the public portion of an address; the private component is used to sign the transaction. Furthermore, the public key is a crucial component in the verification that the user indeed authorized the transaction. The appendix explains how to obtain an address and transfer funds to this address.[8]

In a nutshell: How a blockchain transfer works

Step 0: Two parties agree on a transfer of specific funds or other assets.

Step 1: The buyer (identified by an address) of an item sends a message to the blockchain network asking to initiate the transfer to a seller (an address).

Step 2: The network checks whether the buyer has funds specified and whether the buyer can verify that he or she is authorized to initiate the transfer; this verification requires

signing the transaction with the private key/the private component of the address.

Step 3: Transactions are bundled into blocks and added to the chain based on the blockchain's protocol.

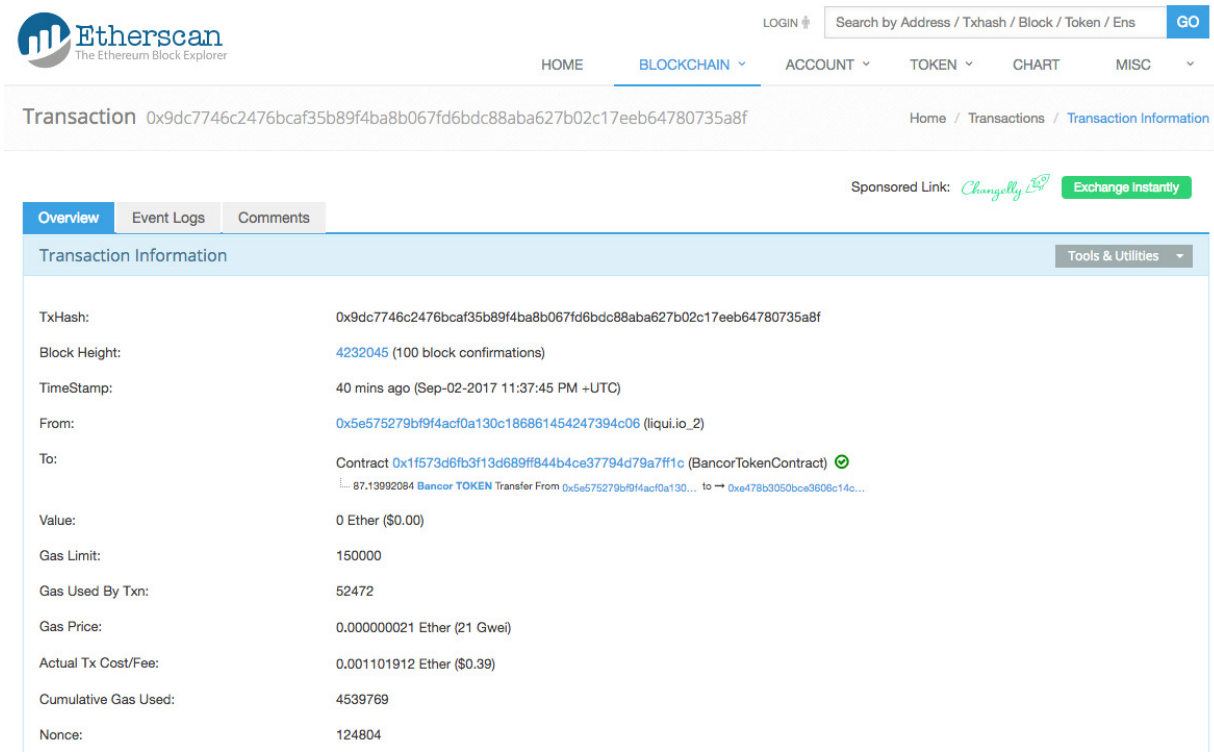
Step 4: Once a block has been added to the chain, the transaction has settled. Implicitly, the buyer's account has been decreased and the seller's account increased by the transferred amount.

Figure 5 displays an example of a randomly selected transaction with its associated identifers. Using information from the blockchain, EtherScan tracks each address' holdings, as shown in Figure 6.

The take away of this discussion is that a blockchain records all transactions with IDs of buyers and sellers, that this information is kept at each node, and that this info is thus shared across a wide network. Critically, one must not mistake a *private* distributed ledger with a blockchain protocol for a solution that guarantees *privacy*. On the contrary—the protocol above and the attribution of ownership to IDs in principle works the same way in a private blockchain. The main difference is that a private blockchain can control whether anyone other than the network members sees the transaction records.

Figure 5: Transaction records on Ethereum blockchain

Here we see the details—timestamp, sender, recipient, value, fee ($.39)—of a record of a token transfer transaction from the Ethereum blockchain.



Source: etherscan.io, accessed 2 Sept. 2017.

Transparency as a risk and an asset

The corporate bond market has become almost entirely over the counter. Even with significant advances in trading technology, this multimillion-dollar market is still surprisingly low-tech, as most trades are arranged in phone conversations or via Bloomberg chat.

In many situations, transparency is a double-edged sword, and some of the parties that may benefit the most from it are also the most fevered opponents. In the introduction to this paper, I have already highlighted intermediaries as strong opponents, for instance because absorbing client inventories exposes intermediaries to risk. Transparency of past transactions and holdings may also help them identify possible counterparties.[9]

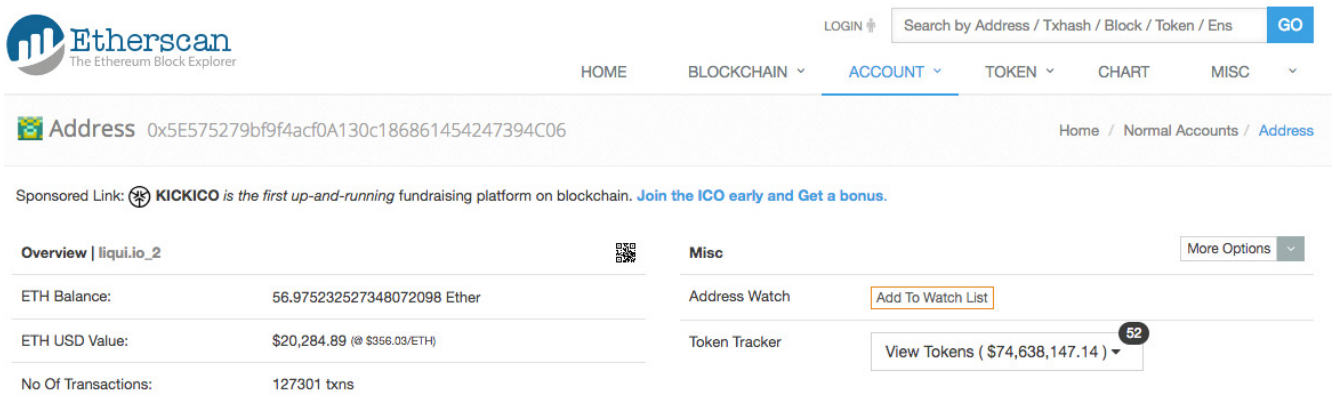
Transparency as a strategic risk

The market for corporate bonds illustrates the complexity of this issue. At the beginning of the last century, corporate bonds were regularly traded on stock exchanges such as the New York Stock Exchange. But over time, this market moved almost entirely to over-the-counter arrangements; even though there have been significant advances in trading technology, this multimillion-dollar market is still surprisingly low-tech, as most trades are arranged in phone conversations or via Bloomberg chat.

The industry also strongly resists attempts to increase transparency, even in terms of post-trade information. For instance, the introduction of the US National Association of Securities Dealers' (NASD) Trade Reporting and Compliance Engine (TRACE) in 2002 and similar efforts by the Investment Industry Regulatory Organization of Canada (IIROC) were met with much resistance. O'Hara, Wang, and Zhou provide one possible explanation: active traders, presumably regular customers, get better prices, and dominant dealers tend to offer worse prices.[10] These findings suggest that dealers have margins to protect. Non-competitve margins, however, ultimately come at the issuers' expense because investors will price-in liquidity costs.

Figure 6: Holdings of an identifier

Here we see the holdings of ether associated with a particular identifier.



Source: etherscan.io, accessed 2 Sept. 2017.

At the same time, start-up fintech firms such as Algomi, which offer systematic, algorithmic matching of corporate bond trading positions, report that some of their biggest clients are intermediaries. In other words, dealers recognize the usefulness of liquidity-enhancing technology. Similarly, there is ample evidence that market prices after the introduction of TRACE became significantly more precise. More accurate, efficient prices benefit intermediaries as a whole because poor pricing increases a risk.

Dealers recognize the usefulness of liquidity-enhancing technology.

Sell-side intermediaries are, however, not the only parties that worry about too much transparency. A host of research shows that institutional investors, in particular, are very concerned that competitors might imitate their trading strategies. For instance, mutual funds are required to publicly disclose their holdings regularly in 13-F forms; and Christoffersen, Danesh, and Musto document that actively managed mutual funds commonly delay publishing this information for as long as possible.[11] In other words, these funds try to obfuscate their activities for as long as possible, presumably because they worry about losing their competitive advantage. Furthermore, on a more short-term basis, institutional traders spend much effort hiding their trading activities: instead of trading a large quantity in one go, they use complex computer algorithms that "shred" their large orders into tiny pieces. They do this to avoid being detected by the market at large because, as van Kervel and Menkveld report, the longer they spend working their orders over a day, the more likely other smart algorithmic traders detect these orders and move the price against them.[12]

Over the last 20 years, many firms left the public equity markets: the number of publicly listed firms in the States has dropped by over 40 percent since its height in the late 1990s, and some of the exiting firms are household names such as Dell or Safeway. Other highly successful and famous firms such as Uber avoid the public markets deliberately.[13] There are numerous reasons for this trend, but mandated public disclosure for publicly listed firms is an often cited one.[14] CEOs have to publicly disclose their salaries, and financial disclosure may expose firms to the risk of revealing competitive or strategic business information.

Mandated public disclosure for publicly listed firms is an often cited reason for leaving the public equity markets, and the number of publicly listed firms in the States has drop by over 40 percent in the last 20 years.

In addition to situations when some parties desire privacy, there are situations where privacy is a necessity. A good example is blockchain based voting. The underlying idea of using a blockchain for voting is to issue digital, single-use tokens to eligible voters. With a controlled and auditable supply and distribution of tokens, it would be difficult to manipulate a vote. However, at the same time in democratic, political elections, votes must be private, and thus privacy is essential. In other situations, a public vote may be desirable: for instance, in votes during general shareholder assemblies, as recently introduced by the TMX Group, shareholders may want to know if their proxy votes have been used as promised.

Existing blockchain technology can address many of the issues of transparency highlighted here. The arguments presented here are not against the usage of blockchain solutions.

Transparency as a strategic asset

The advent of the Internet and of electronic documents and data vastly increased the information that investors, consumers, trading partners, and regulators can obtain about firms, governments, non-governmental organizations, and people. Over time, many of these entities have learned to embrace transparency and to use it in their favor.

Transparency should be a core principle of responsible management practice, and researchers have found ample evidence that organizations that embrace transparency benefit greatly.

Blockchain technology enables firms to benefit from transparency both directly and indirectly.

Indirect effects: Reputation and perceived integrity

There is a long standing literature in management science that studies the *indirect* effects of transparency.[15] This literature posits that transparency should be a core principle of responsible management practice, and researchers have found ample evidence that organizations that embrace transparency benefit greatly. These benefits are, in my view, indirect, because much of the reported benefits that derive from a firm's openness improve relationships over time. For instance, in many business dealings, one party gains knowledge about the other, and for a successful relationship, parties need to trust one another that one side of a deal will not exploit this knowledge. A common approach of firms to increase trust is to publish the adopted ethical codes of conduct, which makes it easier for employees to know what is expected and create credibility in business dealings. Furthermore, sharing relevant information with partners and supply-chain members in a timely manner improves trust, and can generally lift a firm's brand.

As Tapscott outlines, there are five elements for firm success with increased transparency and public scrutiny. Firms need to

1. Create true value that withstands the scrutiny that transparency brings about.
2. Understand customers and build relationship capital.
3. Protect customers' privacy.
4. Behave with integrity since lapses are caught quickly in a transparent world.
5. Be candid as shortcomings can be seen quickly.[16]

Greater transparency in some markets could increase investor-to-investor interactions (and thus decrease costly intermediation).

Many of these principles apply in a world where financial transactions and contracts are visible on a blockchain. Indeed, Parris et al. define transparency as "the extent to which a stakeholder perceives an organization provides learning opportunities about itself."[17] Transactions and *smart contracts* (pieces of programming code) visible on a blockchain deliver "hard" information (and thus learning opportunities) in that the information is verifiable and immutable.

An extreme case of transparency is the *decentralized autononmous organization* (DAO).[18] Set up as a venture fund, all DAO investments and its entire governance are transparent by design, because the underlying code is open-source and visible to all. The basic idea of DAO governance is that owners of DAO tokens would vote on whether or not to fund proposed projects. This autonomous, non-human operational model of a DAO is not practical for all firms, but it is a fascinating, stark contrast to "normal" corporate decision making where executives have great discretion over the usage of funds and where shareholders rarely have a direct say and often have only limited or indirect knowledge about their CEOs' decisions.[19]

Transactions and smart contracts (pieces of programming code) visible on a blockchain deliver "hard" information (and thus learning opportunities) in that the information is verifiable and immutable.

As an example for how the "hard" information stored in a blockchain can help an entity, consider a historically corrupt country. How can the government of this country improve its standing? In the end, it is difficult to prove that one is not corrupt. Blockchain technology can be an answer. In the current world, it is often impossible to credibly and efficiently reveal all of a government's relevant transactions and business dealings—but when all transactions and contracts are recorded on a blockchain, nothing remains hidden. And as the money and contract terms can be traced, this government can credibly document that its actions are not furthering corruption.

Direct benefits: Disintermediation, improved governance

There are also direct benefits from transparency: transactions that are recorded on a blockchain are usually of a financial nature, and recording transactions and thus holdings on a blockchain can have *direct* procedural advantages in market interactions. Many financial assets, such as corporate bonds, are very illiquid, meaning that it is difficult for a willing trader to find a counterparty; recent regulatory changes such as the Volcker Rule have exacerbated the situation.[20] One problem is that under the current market structure, where most trades are arranged offline through dealers, it is difficult to know who traded a product in the recent past (and thus might have a continued interest) or who might hold the securities (and might thus be a candidate to trade with). Arguably, greater transparency in this market could increase investor-to-investor interactions (and thus decrease costly intermediation). Malinova and Park show theoretically that a setup with features of a public blockchain (even when market participants take steps to hide their behavior) improves allocative efficiency relative to the traditional, opaque setup where all information about past trading and current holdings remains in silos of information at dealers.[21]

Greater transparency in some markets could increase investor-to-investor interactions (and thus decrease costly intermediation).

Another example is the market for initial public offerings. During its last boom during the dot-com bubble at the end of the 1990s, this market was fraught with problems. One critical issue was the distribution and access rules to the offerings. Traditionally, the lead underwriting investment bank controls who gets shares in an offering. For popular initial public offerings (IPOs), there were numerous conflicts of interest: for instance, a widely reported concern was that underwriting investment banks have an interest to please their best customers by giving them underpriced shares.[22]

Another widely reported issue was the process of *laddering*, whereby investors received shares in offers only if they committed to purchase further shares at higher prices.[23] In the current world of investment banking, underwriters cannot easily convince issuers and investors that conflicts of interest play no role in their advice and decision making. Contrast this with the currently hot (for better or worse) market of *initial coin offerings* (ICOs), many of which, for all practical purposes, look like securities offerings.[24] The allocation mechanism in this market is entirely transparent because it is intrinsic to the piece of publicly visible code that determines how tokens are distributed.[25]

The allocation mechanism in the initial coin offering market is entirely transparent because it is intrinsic to the piece of publicly visible code that determines how tokens are distributed.

In a celebrated paper, David Yermack highlights numerous potential benefits for corporate governance that blockchain technology can bring about.[26] Yermack argued, for instance, that transparent ownership attribution in a blockchain can help address the so-called *empty voting* phenomenon, where an entity gets to vote on economically meaningful decisions without having an economic stake in the firm.[27] The usual assumption is that economic interest in a firm and voting rights are coupled with the ownership of a share. However, derivatives contracts make it possible that a party obtains a large number of voting rights without having an economic stake in the firm.[28] With ownership attribution via a blockchain, it would be transparent at any point in time who owns a stock and who has an economically justified right to vote.

Insider trades, another topic of much contention both in the financial industry and in academia, are a further obvious use case. Insiders are already required to announce their trades and holdings, but there are often significant delays between the transactions and their reporting.[29] Therefore, if all trades were recorded on a blockchain, then—by revealing their public IDs—insiders could credibly and immediately show their trades. All their trades would be visible, which would eliminate costly reporting requirements and could increase public trust.[30] The public would be in the position to understand insider holdings and insider trading better, and firm executives would create trust with their shareholders. This argument applies particularly in jurisdictions where insider trading violations are less strictly enforced than in North America. Finally, transparency of insider trades should reduce the propensity of insiders to engage in illicit trading. As transparency reduces the flexibility of insider traders, it becomes more profitable for outsiders to generate information about firms.

If insiders recorded all their trades on a blockchain, then—by revealing their public IDs—insiders could credibly and immediately show their trades. All their trades would be visible, which would eliminate costly reporting requirements and increase public trust.

Yermack highlights that the immutability of public blockchains improves (corporate) governance. In the current system, land records can be forged, corporate income statements can be manipulated, and option grants can be backdated. When all these data are recorded on a public blockchain, performing such manipulations becomes prohibitively difficult and expensive.

In finance, transparency of contracts and holdings extends beyond the resolution of adverse selection and moral hazard at the heart of corporate governance and has potentially far reaching consequences

for risk management. One major development in the wake of the 2008 financial crisis was that particular types of derivatives contracts, such as swaps, were forced to be cleared with a newly-developed *central counterparty* (CP). The basic idea is that when A wants to sell to B, then A sells to the CP, and the CP sells to B. Why is this necessary? Imagine that A has also bought from C, but that C goes bust. A would then not be able to deliver to B and may go bust, too. Thus when dealing with A, B faces two counterparty risks: (a) the risk of A's going bust independently and (b) the risk that C goes bust and takes A down with it.

The root cause for the necessity of a central counterparty is that there is insufficient information about the aggregate risk, and that creates moral hazard.

Consider the derivative dealings of AIG prior to the financial crisis in the market for credit default swaps, where it became apparent that AIG had taken large unhedged positions. AIG's default would have triggered defaults of its counterparties, causing a chain reaction all through the financial system. When all trades are cleared by a CP, risk is concentrated at the CP. Although this system can generate a mutually beneficial level of risk sharing, there are problems: because it is a too-big-to-fail entity, the CP needs to be tightly monitored, well-capitalized, and possibly heavily regulated. Moreover, currently, only a small number of contracts qualify for CP clearing. The root cause for the necessity of a CP is that there is insufficient information about the aggregate risk, and that creates moral hazard. As we've known since the path-breaking work of American economist George Akerlof, asymmetric information can lead to the breakdown of a market.

We could argue that the transparency possible with blockchain technology enables a market-based solution: when all financial obligations are visible, we will be able to trace counterparty risk beyond bilateral interactions. Unhedged positions would be visible. Moreover, we would be able to write smart contracts with protective covenants such that counterparties are forced, through the code, to establish hedges in a timely manner, or prevented from engaging in unhedged contracts.

When all financial obligations are visible, we will be able to trace counterparty risk beyond bilateral interactions. Unhedged positions would be visible.

Finally, smart contracts themselves can fundamentally improve economic interactions. As a first step, a smart contract can facilitate the delivery of collateral by automatically transferring the title in the case of a default. Such automation vastly improves the enforcement of collateral, increases its value, reduces risk, and potentially frees up capital.

We use contracts to prove to others (e.g., shareholders) that a transfer of goods will occur (or has been legitimized). We can use smart contracts without blockchains and in non-transparent environments; but in transparent blockchains, parties may be able to sell rights to future payments. In other words, firms may be able to sell cash flows directly from contracts, and they may be able to ensure cash flow risks directly. Furthermore, as Cong, He, and Zheng show, smart contracts can mitigate information asymmetry, leading to enhanced entry and competition and then higher social welfare and consumer surplus.[31]

Smart contracts can mitigate information asymmetry, leading to enhanced entry and competition and then higher social welfare and consumer surplus.

Altogether, there is a solid business case in favor of the transparency of transactions and contracts that blockchain technology affords, and these advantages go much beyond addressing the concerns that arise from front-page scandals. As it is, the privacy of corporate entities is already limited, especially compared to that of individuals. It is not unreasonable to presume that regulation can simply require blockchain-based disclosure of interactions—and if indeed blockchains become the standard for financial transactions, then this type of disclosure is procedurally inexpensive.

Finally, the validity of the arguments that I present here are confirmed in a recent study by IBM of C-suite executives.[32] The vast majority of executives that have already actively adopted blockchain technology report that the technology will create more trust, for instance, through traceable audit trails of transactions, that reputations can be built by offering transparency about past actions.

Solving the problem: Technological approaches to privacy in blockchains

The primary purpose of a blockchain is to ensure the authenticity of the records—by default, distributed ledgers are not set up to guarantee privacy for their users. Indeed, there is ample evidence that transactions in public blockchains are not private,[33] and that individuals' actions can potentially be traced.

As a prerequisite, it is important to separate the concerns that different parties may have. Judging by the tone of the discussions in popular Internet forums, many proponents of cryptocurrencies and particularly bitcoin worry whether their dealings can be traced or detected, for instance by a government entity. Considering that bitcoin was a popular method of payment for illegal drug purchases on sites such as the Silk Road or for ransomware payments, this is not surprising.

In contrast, most enterprise users are used to the government auditing their actions, and they worry less about government knowledge per se. Indeed, they may actually welcome a system that makes traceability easier. Instead, enterprise users are mostly concerned whether their actions are traceable by their competitors, diminishing their intellectual property (IP).

Procedural workarounds: Usage of multiple IDs

So are actions on blockchains always fully traceable and attributable? The answer is no. There are several simple, low tech, procedural workarounds that allow users to obfuscate their behavior.

Let me explain the ideas with a concrete example. A mutual fund wants to make a large investment in a recently issued firm whose

securities are blockchain-based tokens. The mutual fund would convert fiat currency, such as the Canadian dollar, into a blockchain-based currency such as ether. This transfer would occur at a blockchain-based exchange. The exchange would know who bought the ether (because they have to follow KYC regulations). After the transfer is made, the fund would use the newly purchased ether and buy the crypto security. As I outline in the appendix, usually, this transfer is performed in an exchange wallet that combines the actions of numerous market participants. For final settlement, the fund would then transfer the securities to a non-exchange wallet. But the fund does not have to use a known wallet or reveal the wallet ID to the public. Instead, the fund can create a dedicated new wallet. Or the fund can create an arbitrary number of new wallets and split the holding among these. If done carefully, it would be impossible for an outsider to piece together this big purchase. This solution can also be formally programmed using so-called *hierarchical deterministic* (HD) wallets, which algorithmically generate a new public key for every piece of a larger trade.

Hierarchial deterministic wallets have also been proposed as a solution to privacy in private distributed ledgers.

HD wallets have also been proposed as a solution to privacy in private distributed ledgers. Suppose that a private network is run by a consortium of large banks and brokers. Each of them would create one (or many) HD wallets, and record individual customers' holdings within their own systems. This arrangement is similar to the current settlement of stock trades. Namely, currently, the settlement of stock traders occurs at a central depository, such as the US DTCC or CDS in Canada, and the settlement is at the broker level. The main difference is that HD wallet settlement is on a distributed ledger, and not in a central database. With the distributed ledger there is no informational advantage over the central depository solution, even for someone with access to the ledger (in particular not for Canada where trades usually carry a broker attribution).

Another solution to generate privacy that is related to HD wallets is a merge and re-split operation: under this protocol, several entities anonymously submit new addresses to a smart contract; the contract collects the same number of units of cryptosecurities from the parties (e.g., 100 bitcoins each), and then the contract redistributes the amounts to the new addresses.[34] From the outside, we could not further follow a trail of money. Needless to say, in a public blockchain without outside control, what I am describing is money laundering, for all practical purposes. In permissioned blockchains, however, the IDs would be known, and a regulator or tax authority would be able to track individuals. The primary purpose of this endeavor would then be to obfuscate one's behavior to outside observers.

In a public blockchain without outside control, what I am describing (in the paragraph to the right) is money laundering, for all practical purposes.

High-tech solution: Zero knowledge proofs

In addition to the aforementioned low-tech solutions, modern cryptography offers several high-tech and elegant ways to obtain privacy. The common privacy-related concern regarding a transaction is that the owner of a piece of information wants to provide cryptographic proof that she is a valid owner of that information

without having to reveal that information to the validator (i.e., the network).

Modern cryptography offers several high-tech and elegant ways to obtain privacy.

For example, zero knowledge is critical in blockchain-based voting. For such a vote, one receives a voting token. When casting the vote, the token holder needs to verify that she is the legitimate owner of the token; but with secret suffrage, the validator must not see who the owner is because that knowledge might allow the validator to trace the actual vote back to the voter. After all, in public blockchains, each network member keeps a record of all information.

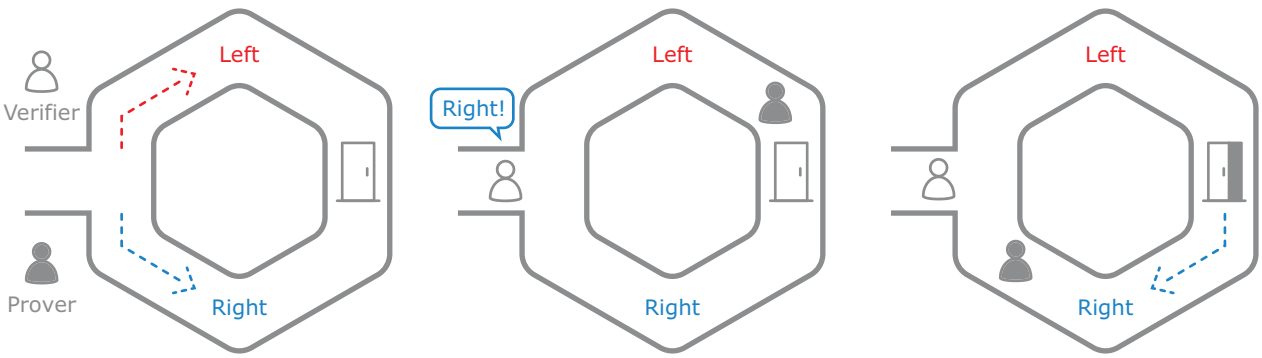
Probably the most sophisticated method yet to solve this problem involves so-called *zero knowledge proofs*. Figure 7 shows how this verification works.[35]

Here's a standard example of a zero knowledge proof. Suppose Bob is colorblind but doesn't know it. Alice wants to prove to Bob that there is a difference between green and red. Bob takes two snooker balls, one is red, the other green, but they are otherwise identical. To Bob, they seem completely identical, and he is skeptical that they are actually distinguishable. Alice wants to prove to him that they are in fact differently-colored. At the same time, Alice doesn't want Bob to learn which is red and which is green.

Here is the proof system: Bob takes two balls so that he is holding one in each hand. Alice can see the balls but doesn't tell him which is which. Bob then puts both hands behind his back. Next, he either switches the balls between his hands, or leaves them be, with equal chance. He then brings them out from behind his back. Alice now

Figure 7: Illustration of zero knowledge proofs

A prover wants to show that she has the key to a secret door in a cave. Irrespective of whether she goes left or right, she can always use the key and return from either direction. The verifier, not having seen which direction the prover went, demands she returns through the right tunnel. The prover, with the key to the door, opens the door and returns from the right tunnel. Of course, she could have been lucky; someone without the key could have taken the right tunnel in the first place. But they repeat the experiment many times, and the prover's appearing from the correct tunnel by chance diminishes every single time.



has to "guess" whether or not Bob switched the balls. Of course, Alice can say with certainty whether or not Bob switched them by simply looking at the colors. If they were the same color and hence indistinguishable, she will guess the correct color with 50 percent probability. Of course, one try is thus not enough, but if Bob and Alice repeat this "proof" many times, the chance vanishes that Alice got it right all the time just by luck. Bob should therefore become convinced that the balls are indeed differently colored. Furthermore, the proof is "zero-knowledge" because Bob never learns which ball is green and which one is red; indeed, he gains no knowledge about how to distinguish the balls.[36]

At this writing, the developers of the public blockchain Ethereum are incorporating the option to use a generalized version of zero knowledge proofs as part of the Ethereum blockchain. The concept that they employ is zero-knowledge succinct non-interactive argument of knowledge or, more succinctly, *Zk-Snark*. Related to the example above, a Zk-Snark is a zero knowledge proof protocol whereby someone can reveal only the necessary information to the verifier and no more. ZCash is one example of a cryptocurrency based on zero knowledge proofs.

When would a company want such an option? Imagine that a firm stores smart contracts on a blockchain. A lender wants to assess the creditworthiness of the firm and asks to reveal what payments the firm can expect based on existing contracts. The firm may not wish to reveal all the details of the contracts (such as counterparties) to the lender. Zero knowledge proofs are the solution: The firm can prove that it is the recipient of upcoming payments without revealing all the details.

Another blockchain-based cryptocurrency that offers privacy is Monero. It is based on a different concept, the so-called *linkable ring signatures*. The idea is that the system mixes the true ID with a random collection of other IDs for each transaction. In signing a transaction, the user reveals that s/he is the rightful owner without revealing which one. Linkability ensures that double-spending cannot occur. There are several other technological and procedural solutions that can deliver privacy but discussing all of them is beyond the scope of this white paper.

Zero knowledge proofs are the solution: the firm can prove that it is the recipient of upcoming payments without revealing all the details.

In summary, there are multiple solutions to ensure privacy: Some technological (such as zero-knowledge proofs), some procedural (usage of multiple IDs).

Implementation in public versus private blockchains

The procedural solutions to obtain privacy that I describe above are intrinsic to public blockchains. The direct downside of the usage of many addresses is that it creates tangible costs: Although the creation of IDs is free, each transaction involves a fee, and invoking privacy in this manner comes at a cost. Other than the costs, nothing prevents entities from using an arbitrary number of IDs and from hiding their identity.

More critical for private blockchains is that users understand the ID setup and that they understand the network governance and the information available to network members.

While privacy is a right for private citizens, many jurisdictions such as Canada and the States already limit privacy for firms and executives. For instance, firm insiders have to disclose trades in their company's stocks, and mutual funds and some hedge funds are required to disclose their holdings. For firms that use public blockchains, a regulator or lawmaker could impose disclosure requirements. For instance, regulated hedge funds or firms that have issued security-like digital tokens on a blockchain may be required to reveal the addresses that they use from time to time. Doing so is arguably a more elegant solution than the current, administratively burdensome disclosure. Furthermore, as I have argued above, firms and executives may disclose the used addresses proactively to take advantage of the strategic value of transparency.

The usage of high-tech solutions to attain privacy, such as Zk-Snarks, is not contradicting firms using blockchain transparency as a strategic asset. For instance, smart contracts, which are one of the most appealing features of blockchain technology, could involve one party, A, making a delivery to another party, B, while using firm A's IP for tasks that are necessary to make the delivery. Firm A would not want firm B to see its IP, nor does it want the broader public to see the IP. The solution here is to use Zk-Snarks to verify that the tasks have indeed been accomplished. Firms that want to be transparent (e.g., about relevant accounting features) would not have to reveal contract details, but instead they will still be able to announce the final delivery, or they could verifiably display the key parameters of an agreement.

In private or permissioned blockchains, the procedural workarounds from public blockchains apply, too. However, in private blockchains, there are further options. Whether a user can create multiple IDs is a design choice. The economic incentives for the verification and settlement of transactions are also a design choice, as are the costs for using multiple IDs. Private blockchains can also include features that mask user IDs or that limit visibility of subsets of transactions to a selection of parties.

The economic incentives for the verification and settlement of transactions are a design choice, as are the costs for using multiple IDs.

More critical for private blockchains is that users understand the ID setup and that they understand the network governance and the information available to network members. For instance, is the setup identical to that of a public blockchain except that all users have gone through a KYC procedure? Or are there limitations to ID usage? Do all network members use IDs similarly? Do customers of networks have equal access or do some institutions give some customers more information than others?

If indeed leading financial institutions were to introduce private blockchains to facilitate their interactions, then the handling of the information and the identifiers would require much thought (and likely a lengthy legislative and regulatory process). For instance, the main benefit of a blockchain technology is that it enables peer-to-peer interactions, which will lead to further disintermediation. Institutional investors that rely on bank-consortium operated private blockchain need to understand what information they or any other party can derive from the blockchain.

A related concern arises for corporate users, that of baseline information. A business partner may make a subset of information visible. For instance, a party may share information to build a reputation as a good business partner. However, if disclosure is selective rather than full, then users cannot construct a baseline for a meaningful comparison.

The regulation would need to ensure the mitigation of information asymmetries between members and non-members and the resulting conflicts of interest.

As this discussion highlights, there are many possible information asymmetries that can arise with private blockchains. Since the existing financial institutions are already heavily regulated, any private blockchain they build would likely also need to be regulated. The regulation would need to ensure the mitigation of information asymmetries between members and non-members and the resulting conflicts of interest.

In the history of finance, it has been difficult to change transparency regimes, and such moves have often been met with much resistance.[37] Personally, I believe that the regulation of private or consortium blockchains will quickly become extremely problematic, because it would need to cover multiple strong-willed jurisdictions.

In my view, there are two salient outcomes: The first is that the private, permissioned blockchains are identical to the public ones except that the access to the network is controlled by network members, but all other informational and transparency features are the same as in public blockchains.

The second outcome is that the financial institutions manage to design a distributed ledger that precisely mimics the current world. Indeed, the R3 consortium, formed by most of the world's largest financial institutions, promotes its own version of a distributed ledger, the Corda system. R3 describes this system as an open, distributed ledger that preserves privacy in the sense that a firm that is part of the ledger can see only the information that pertains to it.[38] The best description of Corda, in my view, is that it is a system of bilaterally agreed and verified transactions with conflict resolution provided by (algorithmic) notaries. This system looks like a digitized version of the current world of contracts using some of the features that have been developed and deployed in public blockchains (e.g., smart contracts). Since blockchain technology is often compared to the Internet, the appropriate analogy here is that Corda looks like the AOL of the 21st century.

Corda is a system of bilaterally agreed and verified transactions with conflict resolution provided by (algorithmic) notaries.

Finally, public blockchains such as Bitcoin or Ethereum are very secure: The proof-of-work (and possibly proof-of-stake) protocols require an attacker to control more than 51 percent of the respective networks' computing power. At present, obtaining these resources comes at an astronomical cost; therefore, tampering with records is economically infeasible on these blockchains. Private blockchains would become large, lucrative targets for hackers; and depending on the protocol, a single compromised network member could contaminate the entire ledger. The security of private blockchains is a real and significant concern, albeit one beyond the scope of this paper.[39]

Conclusions and recommendations

When corporate executives first learned about the concept of a blockchain, they quickly realized that the native transparency fundamentally went against the grain of their current procedures—in particular for financial institutions. At first blush, private blockchains then seemed to be the obvious choice—the term, *private,* suggests that they could maintain the traditional level of total privacy for financial transactions. The truth is more complicated.

Bitcoin or Ethereum are very secure—tampering with records is economically infeasible on these blockchains.

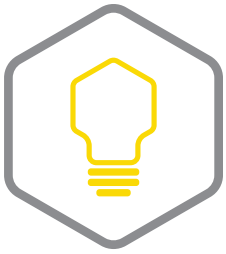
Transparency is native to most blockchains, including private ones. We would be wrong to think that a private blockchain is synonymous with privacy or to equate a public blockchain with lack of privacy. Instead, there are technological solutions that allow users to keep their transactions masked. Therefore, transparency and privacy are choices, even in public blockchains.

With that in mind, blockchain users must understand that they send signals when they opt for privacy instead of transparency. Insisting on privacy may come with a reputation loss. As firms consider incorporating blockchain technology into their business operations, they ought to consider the positive potential of high transparency for their business. Transparency increases trust and can help build positive reputations—with business partners, customers, and investors. It can be conceptually complex to add disclosure features to existing systems—but with blockchain technology, being transparent is straightforward, and disclosure can come at no operational cost.

Transparency and privacy are choices, even in public blockchains.

Over the next years, we will likely see implementations of private blockchains that offer *masking* functionality of identifiers. The intrinsic security concerns and the signaling effect notwithstanding, executives who go down this path face important questions regarding the governance of information in private blockchains: Who knows what? Who masks and unmasks identifiers? Who controls and monitors the ensuing protocols? It is crucial not to set up a private blockchain in a manner that creates asymmetric information, adverse selection, and moral hazard, lest we see a whole set of innovation-stymieing regulations.

My hope is that executives embrace the positive network effects of transparency. It is challenging to amend existing disclosure practices, and historically we have seen meaningful changes only in the wake of scandals. The advent of this new technology is a unique opportunity to reconsider and to embrace transparency and to take advantage of the economic benefits of an open world.



About the author

Andreas Park is an associate professor of finance at the University of Toronto, where he has been a faculty member since 2003. He is a member of the department of management at the University of Toronto Mississauga, and he is cross-appointed at the Rotman School of Management and the Institute of Management and Innovation. Andreas works on numerous theoretical and empirical research projects on the economic impact of technological transformations such as high frequency and dark trading in Canadian equity markets and the impact of the market design of trading when securities are on the blockchain.

His work has been published in such top economics and finance journals as *Econometrica*, the *Journal of Finance*, the *Journal of Financial Economics,* and the *Journal of Financial and Quantitative Analysis*. He has received and has been an affiliate of research grants from the Economic and Social Research Council in the United Kingdom, the Social Sciences and Humanities Higher Research Council in Canada, and the Global Risk Insitute. Andreas has served as co-director of the Master of Financial Economics program at the University of Toronto, he is the associate chair of the department of management at UTM. He teaches courses on financial technology, market microstructure, trading, investments, asset pricing, and corporate finance.

He currently serves a two-year term on the Ontario Security Commission's Market Structure Advisory Committee. He is a pro-bono consultant for the Investment Regulatory Organization of Canada, and he is a principal researcher at the Rotman School of Management's Financial Innovation Hub.

Disclosures

The author has no financial stake or other material interest in any of the companies cited. He has not invested in, advised, or received research funding from said companies as of this writing and its publication.

Appendix: How to access the Ethereum blockchain

The advent of this new technology is a unique opportunity to reconsider and to embrace transparency and to take advantage of the economic benefits of an open world.

Items on the Ethereum Blockchain are associated with public addresses, which are combinations of numbers and letters. For instance, my public address is 0xb1f0ab5ba4DBABAACba71baB7d6bF79D64EE397c.

To receive a payment, we need to have such an address. Creating one is straightforward by using, for example, the website MyEtherWallet.com. To create an address, we enter an arbitrary string as a password. The website then creates a public ID and a private ID from this information, and it creates a file that contains the relevant information. For the term, "showmethemoney!" I received the information shown in Figure 8. Note: this information is for illustration only. It is not advice. *No one should use this particular information*.

I can now receive payments to this address; by itself, however, the address is not useful. Namely, to make payments, one needs to obtain a wallet. A standard one is Mist, available here https://github.com/ethereum/mist/releases.

How can we obtain ether, the native currency of the Ethereum network? There are at least three ways:

1. We become *miners*, meaning that we use our computer to participate in the verification activities of the Ethereum blockchain. If we succeed in creating blocks of transactions then we obtain newly minted ether as a built-in reward. However, successful mining requires specialized computing equipment—a standard central processing unit is much too slow.

Figure 8: Generation of a wallet using the term, "showmethemoney!"

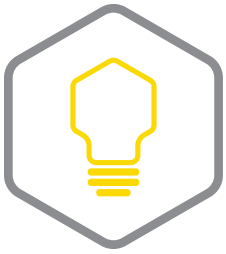
2. A third party sends ether to our address, for instance, in return for a real-world item of value (say, a baby stroller that we sell on Craigslist).

3. We convert fiat currency (e.g., Canadian dollar, US dollar) into ether and send it to this address.

On that last point, as of this writing, converting fiat currency into digital money is a multi-step process. First, we need to create an account at a cryptocurrency exchange such as Coinbase, Kraken, Poloniex, or QuadrigaCX. These exchanges perform KYC, meaning that we need to verify our identity by providing a credit card number and a scan of our passport or driver's license. Once the exchange has verified our identity, the exchange creates an account, which we can fund by sending money to the exchange in our name using, say, a credit card or a wire transfer. Needless to say, this process involves non-negligible fees.

Once funded, we can then buy ether or other digital assets at these cryptocurrency exchanges. Coinbase, for instance, instantaneously converts fiat currency into ether. However, the conversion transaction has not settled on the blockchain yet—the money is still technically at the exchange. So *if the exchange gets hacked or goes bankrupt, our money is lost*. To be a true owner of ether, we need to transfer funds away from the exchange and send it to an address such as the one listed above.

If the exchange gets hacked or goes bankrupt, our money is lost.



About the Blockchain Research Institute

Co-founded in 2017 by Don and Alex Tapscott, the Blockchain Research Institute is a knowledge network organized to help realize the new promise of the digital economy. It builds on their yearlong investigation of distributed ledger technology, which culminated in the publication of their critically acclaimed book, *Blockchain Revolution* (Portfolio|Penguin).

Our syndicated research program, which is funded by major corporations and government agencies, aims to fill a large gap in the global understanding of blockchain technology and its strategic implications for business, government, and society.

Our global team of blockchain experts is dedicated to exploring, understanding, documenting, and informing leaders of the market opportunities and implementation challenges of this nascent technology.

Research areas include financial services, manufacturing, retail, energy and resources, technology, media, telecommunications, healthcare, and government as well as the management of organizations, the transformation of the corporation, and the regulation of innovation. We also explore blockchain's potential role in the Internet of Things, robotics and autonomous machines, artificial intelligence, and other emerging technologies.

Our findings are initially proprietary to our members and are ultimately released under a Creative Commons license to help achieve our mission. To find out more, please visit www.blockchainresearchinstitute.org.

Leadership team

Don Tapscott – Co-Founder and Executive Chairman
Alex Tapscott – Co-Founder
Joan Bigham – Managing Director
Kirsten Sandberg – Editor-in-Chief
Jane Ricciardelli – Chief Marketing Officer
Hilary Carter – Director of Research
Jenna Pilgrim – Director of Business Development
Maryantonett Flumian – Director of Client Experiences
Luke Bradley – Director of Communications

Notes

1. "Justice Louis D. Brandeis," *Louis D. Brandeis Legacy Fund for Social Justice*, Brandeis University, 2017. www.brandeis.edu/legacyfund/bio.html, accessed 4 Nov. 2017.
2. For example, Enron had founded numerous "Special Purpose Entities" (SPE), companies that are (legally) founded for limited time horizons to allow the management of a particular risk. Usually, these SPEs are funded by separate equity investors. Enron had used its own equity, thereby fully exposing Enron shareholders to the risk that the SPE allegedly hedged. This activity would be visible if the SPE transactions were recorded on a blockchain.
3. Michael Minnis, "The Value of Financial Statement Verification in Debt Financing: Evidence from Private U.S. Firms," *Journal of Accounting Research* 49, no. 2 (May 2011). onlinelibrary.wiley.com/doi/10.1111/j.1475-679X.2011.00411.x/epdf, accessed 30 Oct. 2017. According to Minnis, small and medium sized firms that have their books audited by a certified public accountant increase their chances significantly of obtaining a loan and receive on average a 69 basis points lower interest rate. An audit costs between $15,000 and $25,000. An audit of blockchain-based entries would be entirely automated at nominal costs.
4. There are some interesting wrinkles in the ownership and recording of ownership of stocks. Formally, all US stocks are owned by the DTCC, and shareholders merely hold a claim on the original certificates. In Canada, CDS records ownership and transfers, but these transfers are recorded only at the broker level. This procedure has important implications for issuers. For example, suppose CIBC customers buy 100,000 shares of Barrick Gold and sell 80,000. Then CDS records only the net transfer of 20,000. When Barrick needs to contact its owner for, say, the annual shareholder meeting, it needs to contact another third party, Broadridge, to collect the information on the current holders. Being a monopolist, Broadridge's service comes at considerable cost.
5. In contrast to these examples of centralized ledgers, a distributed ledger stores all information at all locations.
6. Richard Gendal Brown, "A Simple Explanation of Enterprise Blockchains for Cryptocurrency Experts," *Richard Gendal Brown*, www.wordpress.com, 7 July 2017. gendal.me/2017/07/07/a-simple-explanation-of-enterprise-blockchains-for-cryptocurrency-experts/, accessed 30 Oct. 2017.
7. Here is a simple mathematical description. The public key PUK is essentially a hash of the private key PRK, where a hash is a conversion of arbitrary length text into a fixed-length combination of letters and numbers. For all practical purposes, this hash cannot be inverted, and so no one can derive PRK from PUK. Mathematically, we write H(PRK)=PUK. Next, combining the text of the transaction (MSG) with the hash of the private key and then hashing both delivers the signature SIG, H(MSG+H(PRK))=SIG. So how does verification work? Well, the verifier has SIG, MSG, and PUK, so all she has to do is check if H(MSG+PUK)=SIG.
8. Creating an address on a public blockchain is straightforward: (1) go to the website MyEtherWallet.com and (2) enter an arbitrary string and a password. The website then creates a public ID and a private ID from this information.
9. Some of the regulations introduced after the 2008 financial crisis have severely limited the ability of financial institutions to absorb client orders. Specifically, the Volcker Rule limits banks' proprietary trading to market-making activities only. In illiquid markets, in particular, drawing the line between taking a position as part of a market making activity and taking it to speculate on price changes can be difficult. Dealers may therefore appreciate technological advances that allow them to shorten the time they expect to hold an inventory.

10. Maureen O'Hara, Yihui Wang, and Xing (Alex) Zhou, "The Execution Quality of Corporate Bonds," Fordham University Schools of Business Research Paper No. 2680480 (1 June 2016). ssrn.com/abstract=2680480, accessed 30 Oct. 2017. See also Gjergji Cici, Scott Gibson, Yalin Gündüz, and John J. Merrick, "Market Transparency and the Marking Precision of Bond Mutual Fund Managers, "Bundesbank Discussion Paper, no. 9 (2014). ssrn.com/abstract=2796963, accessed 30 Oct. 2017.
11. Susan Kerr Christoffersen, Erfan Danesh, and David K. Musto, "Why Do Institutions Delay Reporting Their Shareholdings? Evidence from Form 13F," Rotman School of Management Working Paper No. 2661535, University of Toronto, Ontario, 15 Aug. 2015. papers.ssrn.com/sol3/papers.cfm?abstract_id=2661535, accessed 30 Oct. 2017.
12. Vincent van Kerveland and Albert J. Menkveld, "High-Frequency Trading around Large Institutional Orders," WFA Paper, 29 Jan. 2016. ssrn.com/abstract=2619686, accessed 30 Oct. 2017.
13. Geoff Colvin,"Take this Market and Shove it," *Fortune*, 17 May 2016. fortune.com/going-private/, accessed 30 Oct. 2017.
14. Nancy L. Sanborn, Phillip R. Mills, and Saswat Bohidar, "Going Private Transactions: Overview," Practical Law Company, 2010. www.davispolk.com/files/uploads/davis.polk.going.private.pdf, accessed 30 Oct. 2017. They assert that "the Exchange Act and the Sarbanes-Oxley Act, […] require[s], among other things, periodic disclosure of what may be competitive or strategic business information and impose inflexible corporate governance requirements." Indeed, much literature studies whether the Sarbanes-Oxley Act caused the increased prevalence of going-private deals; see Ellen Engel, Rachel M. Hayes, and Xue Wang, "The Sarbanes–Oxley Act and Firms' Going-Private Decisions," *Journal of Accounting and Economics* 44, no. 1–2 (2007): 116-145.
15. Denise L. Parris et al., "Exploring Transparency: A New Framework for Responsible Business Management," *Management Decision* 54, no. 1 (2016): 222-247. ABI/INFORM Collection, ProQuest Central (1759323162), accessed 30 Oct. 2017.
16. Don Tapscott, "Transparency as a Business Imperative," Association Management 57, no. 4 (April 2005): 17-18. connection.ebscohost.com/c/articles/16701312/transparency-as-business-imperative, accessed 30 Oct. 2017.
17. Denise L. Parris et al., "Exploring Transparency."
18. The first DAO was launched with a crowdfunding campaign in fall 2015. At the time, it was the largest crowdfunded project. See David Z. Morris, "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, and Counting," *Fortune*, 15 May 2016. fortune.com/2016/05/15/leaderless-blockchain-vc-fund/, accessed 16 May 2016.
19. From a game-theoretic perspective, it is not clear at all whether DAO voting structures lead to desirable outcomes. Following Kenneth Arrow's insights from his work on his Impossibility Theorem, a large body of literature on game theory explores the implication of voting on alternatives. The main insight is that there are numerous pitfalls in designing a voting system, and that care is needed to get it right.
20. Jack Bao, Maureen O'Hara, and Xing (Alex) Zhou, "The Volcker Rule and Market-Making in Times of Stress," *Journal of Financial Economics* (8 Dec. 2016). ssrn.com/abstract=2836714, accessed 30 Oct. 2017.
21. Katya Malinova and Andreas Park, "Market Design with Blockchain Technology," 26 July 2017. ssrn.com/abstract=2785626, accessed 30 Oct. 2017.

22. Ritter and Zhang (2007), for instance, provide some evidence for this type of nepotism during the height of the dot-com bubble; see Jay R. Ritter and Donghang Zhang, "Affiliated mutual funds and the allocation of initial public offerings," *Journal of Financial Economics* 86, no. 2 (Nov. 2007): 337-368. dx.doi.org/10.1016/j.jfineco.2006.08.005, accessed 30 Oct. 2017. Also see Tim Jenkinson and Alexander P. Ljungqvist, *Going Public: The Theory and Evidence on How Companies Raise Equity Finance, 2nd ed.* (New York: Oxford University Press, 2001).

23. Qing Hao, "Laddering in initial public offerings," *Journal of Financial Economics* 85, no. 1 (2007): 102-122. www.sciencedirect.com/science/article/pii/S0304405X07000347, accessed 30 Oct. 2017.

24. There is a gray zone as to what exactly a token is. The so-called US Howey Test determines whether a transaction is a security: Is there an investment of money? An expectation of profit? Is the investment in a common enterprise? Does profit come from the efforts of the promoter? Many tokens are set up as "usage" coins, but my reading is that (a) there is a tacit promise of value and thus price appreciation of the coin and (b) these coins are meant as compensation for firm insiders. The first point generates capital gains profits, the second implies a financial reward and hints at option value. In practice, tokens are traded like stocks on cryptosecurity exchanges. Indeed, the SEC stated that DAO tokens were securities (www.sec.gov/news/press-release/2017-131). Similarly, in its investor advisory section, the SEC highlights that tokens are often securities and should be treated as such (investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings).

25. Discussing the mechanism of an initial coin offering (ICO) goes beyond the scope of this piece. The basic idea, however, is this: most ICOs to date involve the issuance of tokens using the Ethereum blockchain. For this blockchain, a token is a smart contract written in Ethereum smart contract language Solidity. This contract or code governs the issuance protocol. Commonly, the contract specifies a particular time (measured in block numbers) during which it accepts payment, and it specifies who receives the tokens once payment has been received (e.g., pro-rate, first come first serve, etc). The contract's code is publicly visible. For more information, see blockgeeks.com/guides/ico-basics/.

26. David Yermack, "Corporate Governance and Blockchains," *Review of Finance* 21, no. 1 (1 March 2017): 7–31. doi.org/10.1093/rof/rfw074, accessed 30 Oct. 2017.

27. Susan E.K. Christoffersen et al., "Vote Trading and Information Aggregation," *Journal of Finance* 62 (2007): 2897–2927. doi.org/10.1111/j.1540-6261.2007.01296.x, accessed 30 Oct. 2017.

28. An example is the 2012 dispute between Telus and the US hedge fund Mason Capital. Mason had taken a long position in Telus' voting stock and it had offset this position with a short position in Telus non-voting stock. As a consequence, Mason had a voting interest but no economic interest.

29. In Canada, insider filings are submitted to the System for Electronic Disclosure by Insiders (SEDI), and insiders must disclose transactions within five calendar days. In the United States, insiders must file Form 4 by the 10th of the month following the transaction. In addition to insider trading, there is also a long history of illegal insider trading, the type that usually makes it to the news. A recent study by Patrick Augustin, Menachem Brenner, and Marti G. Subrahmanyam found that 25 percent of M&A deals show heightened levels of informed trading in options. When insiders would be required to reveal their blockchain IDs, such trades would be visible. See Patrick Augustin, Menachem Brenner, and Marti G. Subrahmanyam, "Informed Options Trading Prior to M&A Announcements: Insider Trading?" 26 Oct. 2015. papers.ssrn.com/sol3/papers.cfm?abstract_id=2441606, accessed 30 Oct. 2017.

30. There is one caveat to this argument: currently, trades occur at specialized exchanges. To trade there, one transfers holdings to an exchange wallet. Formally, this wallet then owns the shares and trades on the exchange that can occur within this wallet. Moreover, an exchange wallet is not necessarily exclusive for a person but instead may mix ownership of several entities. A person only truly and irrevocably owns a digital item when it is transferred out of the exchange wallet to a "normal" wallet and settled on the blockchain; see also the Appendix.

31. Lin William Cong and Zhiguo He, "Blockchain Disruption and Smart Contracts," SSRN, 14 June 2017. ssrn.com/abstract=2985764, accessed 5 Nov. 2017.

32. IBM Institute for Business Value, "Forward Together: Three Ways Blockchain Explorers Chart a New Direction," Global C-suite Study 19th ed., May 2017. public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03835usen/GBE03835USEN.PDF, accessed 30 Oct. 2017.

33. In a 2013 article, *Forbes* describes in detail how their illicit endeavors with the infamous Silk Road were largely traceable. At the time, they relied on a method developed by Sarah Meiklejohn from UC San Diego; at around the same time, Ivan Pustogarov developed techniques to deanonymize transactions on the Bitcoin blockchain (see crypto.stanford.edu/seclab/sem-14-15/pustogarov.html).

34. The solution here is related to the so-called "CoinJoin" approach; see Vitalik Buterin, "Ethereum: Platform review; Opportunities and Challenges for Private and Consortium Blockchains," Ethereum Foundation, 2 June 2016. static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57506f387da24ff6bdecb3c1/1464889147417/Ethereum_Paper.pdf, accessed 30 Oct. 2017.

35. "What is zkSNARKs: Spooky Moon Math," Blockgeeks, n.d. blockgeeks.com/guides/what-is-zksnarks/, accessed 30 Oct. 2017.

36. The underlying logic of zero knowledge proofs is usually spelled out in mathematical terms, and the reader need not worry that, for instance, text based information of statements are incompatible with the concept. Indeed, in the practical-mathematical application strings are converted using so-called hash-functions, which allow a concise mathematical representation of relations. Furthermore, as I depict the situation, there would be a constant back and forth between prover and validator–which is not practical. There are, of course, cryptographic protocols in place that are non-interactive.

37. Examples are corporate bond markets where information about past trades and quotes information are sparse, and dealers showed strong resistence to the collection and publication of such information. For instance, the implementation of the Trade Reporting and Compliance Engine (TRACE) was met with much resistance. In Canada, corporate bond trading data has only been published since 2016, and this information covers only a subset of trades. In the United States, data on trades in treasuries have only been included this July in TRACE–even though the system has been around since 2002.

38. My personal view is that, conceptually, Corda is, in fact, not a distributed ledger at all. For instance, a ledger records transactions, whereas Corda records current balances.

39. Wei-Tek Tsai, Xiaoying Bai, and Lian Yu, "Design Issues in Permissioned Blockchains for Trusted Computing," 2017 IEEE Symposium on Service-Oriented System Engineering, 6-9 April 2017. ieeexplore.ieee.org/document/7943306/?reload=true, accessed 30 Oct. 2017.

blockchainresearchinstitute.org