# Beyond Bitcoin: How Technology Could Help Fix Our Broken Financial System

Alexander Lipton, Alex "Sandy" Pentland ⋮ 18-22 minutes ⋮ 1/1/2018

On a spring day more than 5,000 years ago in the Mesopotamian city of Ur, a foreign merchant sold his wares in exchange for a large bundle of silver. He didn't want to carry the bundle home because he knew he'd be back in Ur again to buy grain at the end of harvest season. Instead the merchant walked to the local temple, where valuables were often stored, and asked the priest to hold onto the silver for him.

Shortly after, the priest's nephew showed up to ask for a loan. The young man wanted to buy seed to grow his own crops, a wish that tugged at his uncle's heartstrings. So the priest loaned him some of the silver, reasoning that if his nephew failed to repay him by the time the merchant needed the silver back, he could fill in the missing amount with his personal funds or borrow it from friends. By using a long-term contract with the foreign merchant to support a short-term loan to his nephew, the priest doubled the number of commercial transactions by using the same money twice. In other words, he invented fractional banking.

Based on archaeological evidence, we know that some scenario like this one occurred in Mesopotamia, and it profoundly changed the financial environment in two ways. First, it increased the overall productivity of the economy, because the nephew could now afford seed. Second, it introduced risk: the nephew might not be able to pay the money back in time.

A few millennia later the emergence of government-backed central banks in 17th-century Europe connected this “double spending” with taxation. The king would borrow money from merchants to fight wars or build roads, and he would use it to pay arms manufacturers, purveyors and troops. That money began circulating, generating economic activity and profits, and at each step the amount of money was doubled—or more. The king typically repaid the loans with taxes imposed on profits, launching a prototype monetary circuit that marks the beginning of the banking system we use today.

Distilled to its simplest form, the modern circuit works along these lines: First, firms borrow money from private banks like JPMorgan Chase or HSBC to pay workers' salaries and other expenses. This is the step where money is created. Second, consumers purchase goods produced by firms or deposit the money as savings in banks. Finally, those firms use the money they receive to repay banks, and the cycle is complete. At this stage, the originally lent money is destroyed,

but the interest stays in the system forever. That's how private banks can jump-start economies by creating money “out of thin air.” Their power to do so is regulated in part by central banks, which impose limits on the amount of capital and liquidity private banks must always have to back lending activities.

If only it were so simple. Unfortunately, the monetary circuit introduces some fundamental problems into society. For one thing, it inevitably creates a handful of billionaires who control a high concentration of total wealth. It is also distressingly common to see leveraged money creation without sufficient understanding of (or care for) the risks. Which is how we get financial crashes, such as the one in 2008: when bankers and politicians spurred an insatiable demand for mortgages, it was met by a significant increase in the amount of money created—along with an even more significant increase in risk.

It may seem obvious to blame the monetary circuit itself for these problems. But it's not the root of the issue. Leveraged money creation works well as long as we can understand and control its inherent risks while suppressing undesirable wealth concentration. Today, however, a tangled web of factors, such as a booming population, global trade and powerful computers, makes the system far too complicated to manage and regulate, let alone understand.

What's more troubling is that the prevailing framework we use to guide macroeconomic activity is based on outdated paradigms. Models that are typically used to govern money creation and interest rates, for example, still treat private banks as simple intermediaries, ignoring the fact that they are big, active, money-creating elements unto themselves. That banks have their own motivations and profit-making strategies injects major opacity into the system. It's no wonder that the 2008 mortgage crisis was difficult to see coming.

Today's supercomplex monetary circuit needs to be modeled in unprecedented detail for us to actually understand it. Technological limitations have long prevented such a gargantuan task. But big data and the emergence of digital currencies and digital contracts are finally changing that. Rather than using historical averages to estimate what might happen in any economic system, it is finally becoming possible to completely simulate every individual trade and transaction and analyze all potential outcomes. The prospect of this feat is shaking up the functionality and ideology of global finance, and its implications could make economic security much better—or much worse.

# The Rise of Digital Currencies

New technologies that make it feasible to reinvent our financial system have exploded on the scene in only the past decade. Most everyone has heard of Bitcoin, but that's only one piece of an up-and-coming financial-technology industry characterized by buzz and speculation. What is important to know is that

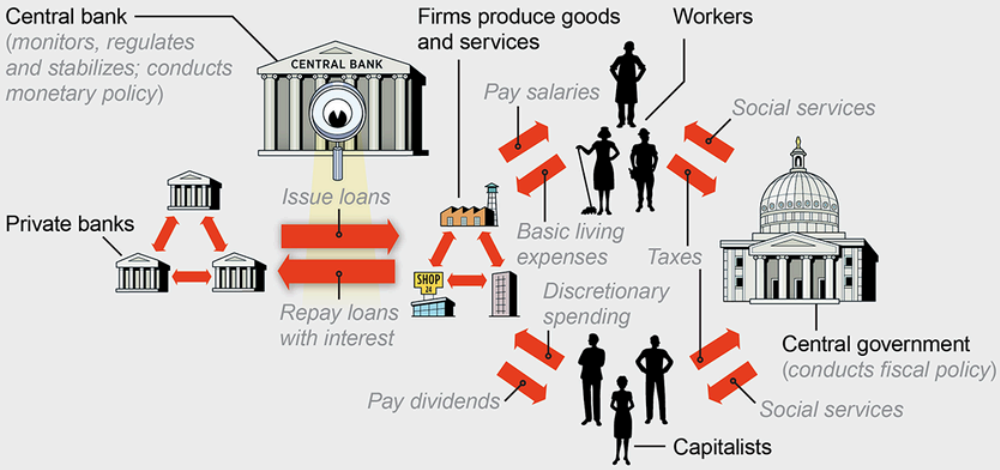
the core invention is a “distributed ledger,” a database shared and managed by multiple participants. Think of it as a communal, digital bookkeeping system. It represents the foundational technology that has made cryptocurrencies—simply, digitally encrypted currencies—such as Bitcoin possible. Its underlying data structure, called a blockchain, is held in a series of sequentially encrypted blocks. To make those blocks reliable and secure, they are consensually updated by a variety of “proving” mechanisms that involve both humans and computers.

Conceptually speaking, blockchains and distributed ledgers are not new—blockchains, for instance, naturally occur whenever power, land or property changes hands. What *is* new is the marriage of the two concepts in a tamper-resistant computer system that can be applied to a wide range of practical problems. New technologies for blockchain-based distributed ledgers are making it possible to create digital currencies that are far more efficient than the U.S. dollar and more efficient than even Bitcoin.

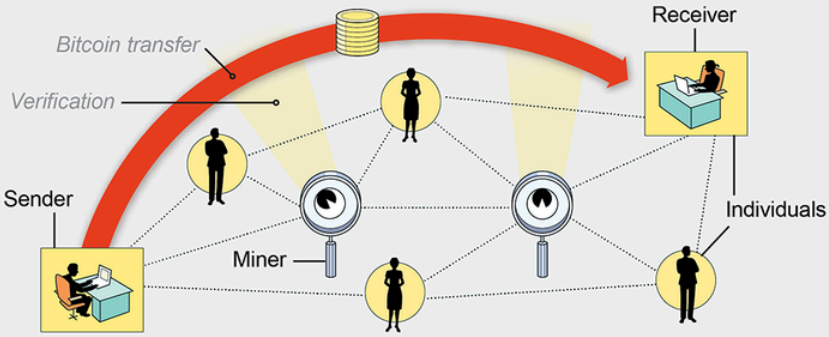
# Three Types of Financial Systems, Visualized

The current monetary circuit has become too complicated to understand. Emerging "blockchain technologies," such as the one driving Bitcoin, decentralize (and defog) the system. New networks are in development.

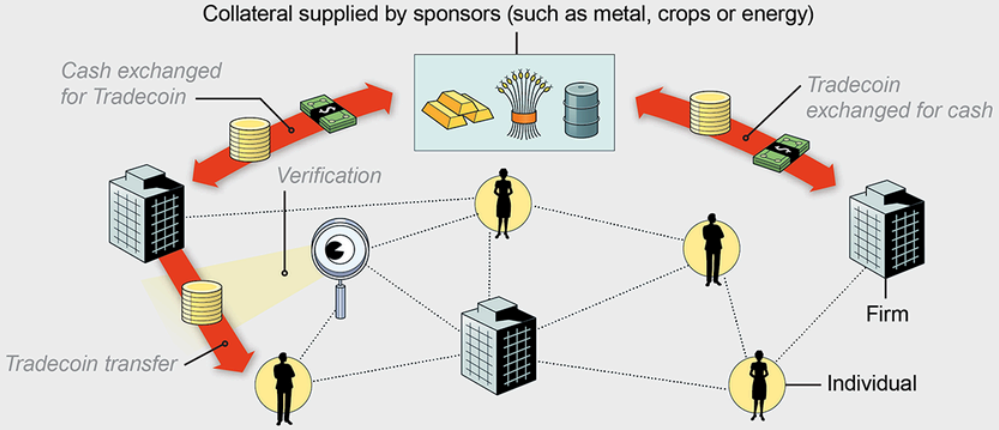
**Fractional Banking (current monetary circuit)**
Banks create money "out of thin air" when they issue loans to firms. Firms pay salaries and dividends to households. Households buy goods and services from firms. When loans are repaid, the "created" money is destroyed, but interest stays in the system for good.




**Peer-to-Peer Bitcoin Network**
Transactions are made directly between users, without the help of designated intermediaries. They are publicly broadcast and recorded in a blockchain. Consensus is maintained by random validators. Bitcoin has no value, so its price is inherently unstable.




**Peer-to-Peer Tradecoin Network**
As with Bitcoin, transactions would be made directly between users and are publicly recorded in a blockchain. But consensus is maintained by designated validators. Tradecoin's value is backed by real assets supplied by sponsors, so its price is relatively stable.



Credit: Peter and Maria Hoey

These tools could enable us to monitor and analyze transactions at such a granular level that we can finally understand the monetary circuit. With a whole new level of clarity, we could learn to recognize and act on early-warning signals that arise from within the trillions of transactions recorded in the ledger, thus increasing system stability and safety. This kind of open-book, real-time monitoring is also safer for the community as a whole. In the 2008 crash, for example, there was not enough bureaucratic capacity to deal with the individual losses of tens of millions of citizens. As a consequence, regulators focused mostly on triaging the much smaller number of big banks, leaving ordinary people to suffer the most.

As this rapidly evolving technology gets tapped for an expanding range of applications, confusion abounds. Because Bitcoin is currently the most well-known (some might say notorious) form of digital currency, it is worth backing up to explore its origins and its weaknesses and how it is different from more promising forms that are now being pursued. Bitcoin was designed as a peer-to-peer digital payment system that operates without central authority. Anyone can join, which is both a strength and a weakness. Users make financial transactions with one another directly, without the help of intermediaries. These transactions are recorded in a publicly distributed blockchain ledger, for all participants to (theoretically) see. Since Bitcoin's inception in 2009, its price has gone up several orders of magnitude, making it the darling of speculators.

Bitcoin's promises are grand. Its proponents—mostly techno-savvy idealists and libertarians but also some criminal types—expect it to become a global currency that eventually supplants national currencies, which, in their minds, can be easily manipulated. Some enthusiasts even believe that Bitcoin is the digital version of gold, perhaps forgetting that gold gains stability both from its physical attributes and from billions of stakeholders and that in the digital world, good technologies are routinely overtaken by better ones.

Bitcoin is actually not the first digital currency, and it's very likely not the last major one either. It also has serious logistical constraints. For example, the number of transactions that can be handled per second is approximately seven, compared with the 2,000 on average handled by Visa. It's an energy suck, too: mining—the process by which nodes of the cryptocurrency network compete to securely add new transactions to the blockchain—depends on a huge amount of electricity. In high energy-cost countries, miners go bust if they cannot afford the utility bills for the computing power. While exact numbers are not known, it is believed that Bitcoin consumes as much electricity as eBay, Facebook and Google combined. The system was also set up to distribute authority among many miners, but by banding together into gigantic pools, a small number of

groups have become powerful enough to control the Bitcoin system. So much for peer-to-peer!

Bitcoin's use is limited, too. The term “money” can be defined by its three types of use: for transactions, for store of value, and as a unit of account. Because Bitcoin's price versus the U.S. dollar (and other government-designated legal tender) is extremely unstable, it is difficult to use on a day-to-day basis. Bitcoin and Ether, another major digital currency, are not backed by real-world assets or even by government promises; consequently, they are purely speculative. In colloquial terms, that means they are not “real” money: what has no value can have any price. Some Bitcoin enthusiasts frame its valueless nature as a virtue and claim that in the future all money is going to be Bitcoin-like. This is highly unlikely for both technical and political reasons.

As the first successful decentralized digital currency, though, Bitcoin is an impressive breakthrough. The underlying technology and the philosophy of an unregulated, peer-to-peer financial system are innovative, and Bitcoin poses practical solutions to big problems. Of course, it's only one application of blockchain-based distributed ledgers. Blockchain, after all, is a technology, not a singular ideology: it should not be conflated with the driving philosophy behind Bitcoin or with the motivations of any of its current and future applications. Just as it has the potential to solve some of the existing problems of our financial system, it can be used to entrench them instead. And when you consider that a key element of power is the control of money—both existing money and future money creation—we can already peek into the Pandora's Box of moral hazards that this technology has opened.

Take the central banks of the major reserve currencies such as the U.S. Federal Reserve and the Bank of England. Trust is often associated with size—the bigger, the more trustworthy—but these players have proved such thinking to be a grave mistake. They have repeatedly chosen to make the “little guys” poorer by diluting their financial obligations through inflation, suppressing interest rates and other policies. Recently they have been testing negative interest rates and contemplating ways to get rid of cash.

What is more alarming is that some central banks are discussing the possibility of making *all* of their currency digital and recording purchases directly on a ledger. This could bypass input from private banks and give the government absolute control over the economy. It would also mean that the government has a record of everything you buy—including the stuff you currently purchase with cash to intentionally avoid a paper trail. This is increasingly looking like a possible scheme, and countries such as China, the U.K., Singapore and Sweden have announced plans for studying and potentially implementing such a strategy. The critical takeaway here is that although the technology itself is decentralized by design, it can be used to create centrally controlled systems.

# Toward a More Stable Financial System

It is clear that the invention of blockchain and distributed ledgers won't eradicate problems like financial crashes and unhealthy inflation—at least not in the short term. But it does enable the creation of legitimate alternatives to the big, powerful players. Technology now makes it possible to form specialized global currency systems that previously would not have had sufficient scale, trust or political stability to compete. That is why a natural next step is for the little guys—such as emerging economies or large numbers of individual citizens—to band together to form alternatives to central banks.

With that possibility in mind, our lab at the Massachusetts Institute of Technology is working on creating a digital currency suitable for large-scale transactional purposes. Called Tradecoin, it will be indelibly logged on a blockchain and anchored at all times to a basket of real-world assets such as crops, energy or minerals. Doing so will help stabilize its value and make it easier for the public to trust it. The core idea is that a broadly useful currency needs both human trust and efficient trade systems.

Credit: Borja Bonaque

A digital Tradecoin built on a distributed ledger can allow alliances of small nations, businesses, commercial traders, credit unions or even farmers to put together enough assets to back a large, liquid currency that would potentially be

as trustworthy and at least as efficient as the national currencies used by the World Bank and the International Monetary Fund. This would give the Tradecoin alliance members some protection from the selfish policies of the big players. The cryptographic structure makes it much easier, safer and cheaper for them to engage in international trade. If the alliance members are geographically and politically diverse, they could have greater immunity from the risk of default than if they were backed by a single large entity. Indeed, this is exactly how the Bank of England got started in 1694: as an alliance of merchants.

By design, the principles behind currencies such as Tradecoin are fundamentally different from cryptocurrencies like Bitcoin, which are not backed by real-world assets and do not involve alliances. Tradecoin can also avoid the energy-intensive process of mining by using a preapproved network of diverse and trusted “validators.” Participants can choose a set of validator nodes who are sufficiently diverse so that no one can bribe 51 percent of the validators all at once. The result is a fast, fully scalable, reliable and environmentally friendly financial instrument. It combines the most recent technologies with the very old idea of a gold coin having intrinsic value, giving it the necessary trust to be used far away from its place of origin.

Currencies such as Tradecoin can be even safer than today's currencies because they can be designed to make the details of the monetary circuit visible for supervision. Oversight by human stakeholders is still necessary, much as ICANN oversees the Internet system or regulators such as the Federal Reserve Board oversee the banking system in the U.S. They allow for easy distributed accounting, which means we can more reliably model and predict risks. Right now this kind of transparency is impossible because the details of financial transactions and contracts are tightly restricted. But if such a system had been in place in 2008, it could have monitored the extreme concentration of some traders in mortgage-backed credit-default obligations and “simulated” in detail the consequences of changes in home values. Instead of hidden packages of bad mortgage deals, there could have been bright red flags.

We are taking on these transparency challenges. For instance, we are building “trust network” software systems for European Union nations and major U.S. financial companies to use as pilot programs. They will allow recording and “playback” of transactions and contracts among different parties without exposing proprietary data or violating privacy. This software is also the core system for Tradecoin. We are exploring how to pilot two Tradecoin currencies: one that is intended for international commerce and backed by an alliance of small nations and another that is backed by farmers for use in commodity markets. We are now recruiting alliance members to test the idea.

It is exciting that for the first time ever, there is the possibility of worldwide digital currencies that are largely immune to selfish policies of the rich central banks that control much of the money. Indeed, a flurry of new alternatives is likely to

emerge, and a few might ultimately rise to compete with the biggest reserve currencies. That we can now create monetary systems that are truly understandable means we can potentially build the tools for minimizing risk, avoiding crashes, and maintaining individual freedom from intrusive governments and overly powerful corporations. And because they will be backed by (and convertible into) traditional assets, they have a real baseline value. That means they are less likely to be targeted for speculative attacks and will be strongly resistant to both political manipulation and inflation caused by the problems of single nations.

Taken together, next-generation cryptocurrencies such as Tradecoin could dramatically reduce frictions in global trade, even amid the chaos of the current political and economic climate. As a result, major currencies such as the dollar might become less dominant, or else the U.S. financial system might become better behaved. The hope is that these distributed systems, backed by broad alliances of diverse players, can bring more transparency, accountability and equity to the world.

# A Brief History of Money

**7th century B.C.:** Lydians and Greeks create standard coinage.

**14th century:** Merchant banks such as the Medicis expand involvement in multistate finance, trade and manufacturing.

**17th century:** By loaning out the value of deposited money, bankers increase economic productivity while creating new sources of risk that regularly result in local crashes and even widespread depressions. Central banks emerge, linking banking with taxation.

**18th century:** The gold standard evolves from previous tactics in which circulating money was loosely controlled by a reserve of precious metals. This lowers risk.

**20th century:** The gold standard is replaced by the Basel Accords, which say that holding easily sold assets is just as good as holding gold.