Blockchain-ing the Money Machine

How the technology that powers bitcoin can reshape the financial services landscape

STATE OF THE BANKS

The financial services industry is today arguably the world's most powerful industry. The global financial system is responsible for moving trillions of dollars every day, serving billions of people, and supporting a world economy worth more than $100 trillion. A closer inspection of this omnipresent money machine, however, reveals the haphazard ways in which it has evolved. Most notably, the machine is plagued by a helter-skelter patchwork of new technology welded onto old infrastructure. Take, for instance, the somewhat strange co-existence of internet banking and paper check issuance at banks that run on mainframe computing infrastructure from the 1970s. Or the fact that, when a customer uses Apple Pay to buy a drink at Starbucks, the money goes through some five different intermediaries before finally reaching the coffee chain's bank account – the transaction clears in seconds, but takes days to settle.

Such bizarre ways of working are widespread in the industry. Stock and bond trades clear almost instantly but take two to three days to settle. A foreign laborer in Singapore earning daily wages could wire his money home and, in the process, have to tolerate absurd transaction costs and a long wait, as if it were physical notes making their way across the world. Worse still, such daily wage laborers – part of the almost one billion people around the world living on less than two dollars a day - are seen as unattractive for banks to take on.

The crux of these problems lies with the fact that the gears of the financial services industry are powerful centralized intermediaries that consolidate capital and enforce monopoly economics. This makes the industry exclusive and centralized, leaving billions unbanked and the industry vulnerable to Equifax-like data breaches.

So how can we make today's money machine efficient, secure and truly global in scope?

IN CRYPTOGRAPHY WE TRUST

In the wake of the global financial crisis was unveiled the world's first cryptocurrency, bitcoin, by an anonymous person (or persons) under the pseudonym Satoshi Nakamoto. The fundamental message in Nakamoto's white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' resonated with the belief that the mass adoption of virtual currencies would ultimately obliterate the institutions – intermediaries such as banks and other 'trusted' third parties – that, one could argue, were responsible for the crisis. The white paper proposed a breakthrough approach to owning, exchanging and accounting for value.

So what is bitcoin? It is a digital currency with a security system run by a massive network of total strangers. The technology that underpins bitcoin represents one of the greatest innovations of our time – a true revolution in distributed computing that eliminates the need for trust. **This technology, called the blockchain, is an open and immutable digital ledger that stores the history of financial transactions in a decentralized and distributed manner.** Because blockchain can be adapted to store any kind of digital information conceivable, systems like bitcoin could be the future of all secure digital transactions, and thus overhaul how today's money machine works.

HOW DO BITCOIN AND THE BLOCKCHAIN REALLY WORK?

The blockchain is a decentralized, distributed and secure digital ledger of all past transactions ever made using a digital currency or token such as bitcoin. Owners of bitcoins have a digital signature represented by a two-part key. The private key, kept safe from view, proves ownership, while the public key is stored on the blockchain, which is accessible to anyone with a computer and an internet connection. Individual blocks of the blockchain – components of the ledger – contain multiple transactions, each of which stores a reference to an earlier record in the chain.

Using bitcoin to pay for something triggers a request to update the ledger. This request is sent to a specific class of participants on the distributed network, called miners. Miners are responsible for detecting transaction requests from users, aggregating them into a block, and ultimately ensuring the irreversibility of new transactions. Specifically, they run the new block and all previous blocks through a set of energy-intensive mathematical calculations called hash functions. Here, all miners compete to solve a complex cryptographic puzzle; the more computing power a miner uses, the more likely they are to solve the puzzle first. The first miner to solve a block tags it onto the end of the blockchain and broadcasts it to all other miners, who then check to verify the accuracy of the hash function. Once verified through a 50 percent consensus mechanism, the ledger is updated and the miner that solved the block is rewarded with newly minted bitcoins (25 bitcoins or about $150,000 per block today). New blocks are created on average every 10 minutes. Also, the supply of the currency is limited so that there will only ever be 21 million bitcoins.

Solving the cryptographic puzzles on the blockchain is so complex that every new block makes the previous blocks and the whole blockchain more secure. Hacking the blockchain would require tremendous computing power and speed. In order to alter just one past transaction, an attacker would have to change the information in that block and every block that comes after it before the blockchain is updated. With countless miners working on the chain simultaneously, corrupting the ledger would require massive amounts of computing power – more than half of the power being committed to the bitcoin network at any given time. This immutability feature makes the blockchain a database that everyone can see and add to, but nobody can destroy. Additionally, because computers belonging to many different entities enforce these rules, no single party is in charge and there is no need for a central entity such as a bank.

THE WORLD COMPUTER

Bitcoin is far from the only application that uses blockchain technology. In 2013, a 19-year-old cryptocurrency researcher and programmer, Vitalik Buterin, developed Ethereum. Ethereum is a decentralized platform on which one can build and deploy virtually any kind of decentralized application. The breakthrough with Ethereum is that it allows one to build smart contracts – digital triggers that self-execute and manage enforcement, performance and payouts. Applications deployed on Ethereum, called decentralized applications or ĐApps, run exactly as programmed without the threat of downtime, censorship, or third-party interference, thereby enabling secure and transparent governance for communities and businesses.

The Ethereum protocol, which is powered by a digital currency called Ether, makes the process of creating blockchain applications easier than ever before. Instead of having to build new blockchains for every application from scratch, Ethereum enables the development of any application imaginable on one single platform. For this reason, the Ethereum protocol is often referred to as the 'world computer'. ĐApps have the potential to profoundly disrupt a wide range of industries – from financial services, healthcare and ride-hailing to social media and music.

THE GREAT UPHEAVAL

With its decentralized and distributed features, blockchain technology has clear potential to bring about a profound paradigm shift, busting the monopoly of large powerful intermediaries and offering end-users the chance to shape how they want to manage their money. One of its greatest advantages is the consensus mechanism that eliminates the need for trust. This has implications for today's banks and insurance firms. ĐApps have already demonstrated the power of blockchains to make banking truly digital and distributed, secure and tamper-proof, inexpensive and inclusive, and able to run intelligently with significantly fewer intermediaries.

We now have the power to transform not only the payments world, as bitcoin has shown, but also other parts of the machine such as insurance, risk management, securities trading, capital raising, accounting, and auditing. There are essentially five core functions of the money machine that are ripe for blockchain-based disruption. These are as follows.

1. **Authenticating identity**: The banking industry is, at its core, a trust broker. These intermediaries ultimately decide who gets to access banking services via establishing trust and verifying identity. The blockchain eliminates the need for trust altogether by relying on cryptographic technology, and enables peers to establish identity that is verifiable and cryptographically secure. Blockstack, a blockchain startup, uses a blockchain to track usernames and encryption keys – the basis of a new identity system that relies on decentralized information not tied to any single social network or other website. Using a similar system, banks can collaborate to authenticate identity, lower their compliance costs of individually having to perform Anti-Money Laundering (AML) and Know Your Customer (KYC) checks, and more easily provide services to a segment that was previously ignored.

2. **Moving and exchanging value**: The financial services industry is responsible for moving money around the world, ensuring no double-spending. The blockchain does exactly this for anything of value, but at a much lower cost, regardless of geographical borders. Given that several intermediaries can be eliminated, the blockchain can cut settlement times on all transactions from days and sometimes weeks to mere minutes. Further, in countries with low financial inclusion, building a blockchain payment rail and connecting it to mobile phones can enable billions of currently unbanked individuals to send funds across borders quickly and cheaply, and participate in the world economy. Coins, a mobile-first, blockchain-based platform in the Philippines, does precisely this; it has partnered with financial services firms and retail outlets to create a distribution network of more than 22,000 cash disbursement and collection locations. Over half a million users use Coins for remittances, bill payments and mobile airtime top-ups.

3. **Managing risk**: Risk management is intended to protect against uncertainty, but a common complaint is a lack of transparency of how risk is measured, especially in the developing world. Blockchain-based insurance systems have the power to run more transparently, simplify cumbersome claims processes and lower premiums. A distributed ledger can enable the insurer and any third parties to instantly and seamlessly access and update relevant information such as claim forms, police reports and third-party review reports. BITPARK, a blockchain-based startup, strives to provide an insurance service that is both transparent and user-directed by offering a peer-to-peer insurance model. Built on smart contract technology, the service offers customers fulfillment of contractual obligations, an approval and compensation system managed between users, a user-based evaluation system, and more.

4. **Funding, investing and lending**: Raising capital has traditionally required intermediaries such as investment bankers and venture capitalists. Initial Coin Offerings (ICOs) – new crowd-funded ways to raise capital on the blockchain – are fast replacing venture capitalists. ICOs have raised a combined $3 billion to date, with more than $800 million of that raised in September 2017 alone. In addition, on the blockchain, anyone will be able to issue, trade and settle traditional debt instruments, allowing consumers to seamlessly access loans from peers. The blockchain automates many functions of investing such as making dividend and coupon payments but in an efficient and secure way through the use of smart contracts.

5. **Accounting for value**: Accounting is a multi-billion dollar industry, but there are questions over whether it can survive the velocity and complexity of modern finance. The blockchain ledger is an already audited trail. Blockchain-based accounting methods will make auditing and financial reporting transparent and able to occur in real time, thereby dramatically

improving the way regulators can scrutinize financial actions in large corporations. Since the data stored in distributed ledgers is continually updated, it offers finance teams the possibility of real-time reporting to both management and external auditors. This could free up auditors to offer more value-added services to their clients.

IS ANY OF THIS POSSIBLE TODAY?

We have a banking system that is in dire need of overhaul, and what seems to be the perfect, foolproof approach for disrupting the machine. So what is stopping us from going full steam ahead? Several factors, such as enormous electricity usage (if bitcoin were a country, it would rank 69th in the world for annual electricity usage), limited scalability, and the lack of a well-defined and universally accepted regulatory framework all pose challenges to the blockchain technology going mainstream.

Of these, limited scalability is a particularly hard problem to solve. To put things in perspective, PayPal clears 200 transactions per second, Visa manages 1,700 transactions per second, and the Shanghai Stock Exchange clears significantly more than 10,000 transactions per second. The most promising blockchains of today are orders of magnitude away – the bitcoin blockchain is realistically limited to seven small or three complex transactions per second. Ethereum fares marginally better at between seven and twenty per second.

The scalability limitation is a side effect of decentralization; the consensus mechanism necessitates that every fully participating computer in the network process and validate every transaction and maintain a copy of the ledger. As a blockchain grows in size, the requirements for speed, bandwidth and computing power required by the network will increase exponentially. This could reach a point where it becomes unfeasible for every node in the network to play the same role, leading to the risk of centralization.

SLOWLY BUT SURELY

The blockchain technology is still in its infancy. To truly overhaul the money machine, the crypto-technology world would need to first figure out a way to scale while keeping power consumption in check. Regulators would need to develop strong legal frameworks and agree on how inherently decentralized protocols should be governed. In addition, the financial services industry would have to agree on standards, develop easy-to-use programming modules, and clarify regulatory uncertainties.

As innovation in the space progresses at breakneck speed, governments and various factions of the crypto-technology and financial services industries are currently working to solve these complex problems. In the meantime, the industry and both its users and non-users should prepare for an inevitable revolution in the way they manage anything of value.

REFERENCES

[1] *Blockchain Revolution* by Don Tapscott and Alex Tapscott

[2] https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

[3] https://www.weforum.org/agenda/2017/06/3-ways-blockchain-can-accelerate-financial-inclusion

[4] https://www.cbinsights.com/research/report/blockchain-trends-opportunities/

[5] https://digiconomist.net/bitcoin-energy-consumption