How the blockchain will become our new signature

the wired world in 2016

Dated: 05 January 16

Published by: Brian Forde Brian Forde is the director of digital currency at the MIT Media Lab, and

Michael Casey Michael Casey is senior adviser at the MIT Media Lab's digital currency initiative

Republished by: David Doran

This article was taken from The WIRED World in 2016 -- our fourth annual trends report, a standalone magazine in which our network of expert writers and influencers predicts what's coming next. Be the first to read WIRED's articles in print before they're posted online, and get your hands on loads of additional content by subscribing online.

http://www.wired.co.uk/news/archive/2016-01/05/blockchain-is-the-new-signature

When a baby boy was born on August 4, 1961, the local newspaper announced his birth, as it did many others. More than a declaration of happy news by his parents, those few lines of information were part of a long-lasting tradition -- using the local daily to register, at a set point in time, the addition of a new person to society. Seemingly inconsequential timestamps like these occur every day and, as it turns out, play a key role in ensuring more fair and just societies.

It's not just limited to births. Kidnappers take photos of hostages holding the front page of a recent newspaper to act as proof that they are still alive. Governments often require entrepreneurs to publish the establishment of their new company in a local newspaper. Beyond newspapers, a postmark confirms to a government that taxpayers filed their taxes on time. A patent helps inventors to prove that they developed an invention first.

But when we depend on private companies to manage this task, we have the potential for exposing ourselves to abuse. Manipulation of the chronological order -- as when banks process a customer's largest cheque first rather than their most recent to increase the likelihood of it bouncing -- creates a less just world.

Similar to the internet's facilitation of instant, global communication, a combination of time-stamped and digitally signed transactions hosted on an accessible ledger could play an important role. They could help governments reduce friction and increase transparency associated with important transactions.

How might this be accomplished? Ironically, Bitcoin, an idea that was once thought to be anti-government, could end up a key platform for governments to achieve these goals.

In autumn 2008, Barack Obama was elected president, global financial markets were crashing and Satoshi Nakamoto issued a white paper called "Bitcoin: A Peer-to-Peer Electronic Cash System". This paper introduced the idea of a blockchain ledger, which the author intended to enable people to transfer money to each other without a bank.

Now entrepreneurs and developers are proposing other uses for this ledger, such as writing executable contracts without lawyers and automatically settling the transfer of stocks and bonds without a clearing house. They're building applications on top of the blockchain that could publicly and immutably record everything from the birth of a child to a transfer of property ownership. Timestamps, ledgers and digital

signatures have been around for many years, but this combination has unlocked the opportunity for many new and consequential innovations.

With more than $800 million (£525m) in venture capital invested in digital currency-related startups over the last few years, the conversation around Bitcoin has shifted from curiosity, confusion and doubt to one in which serious decision-makers are recognising the many ways blockchain ledgers can be used. Bitcoin was initially thought of in narrow terms as an alternative currency to the dollar and other fiat currencies. Experts in other fields are now actively looking at how the blockchain can be used for non-monetary uses.

According to a 2013 report from McKinsey and Company, open data -- freely accessible, machine-readable data provided by governments -- can help unlock more than $1.1 trillion in economic value in the US and $2.6 trillion globally. Startups to the world's largest companies rely on open data to show home buyers crime on real-estate sites, help farmers perform precision farm-cropping or show parents the side effects of medicine for their sick children. However, other than weather and GPS data, it's generally only released once a year and is rarely responsive to citizens' input.

The blockchain could be a critical piece of infrastructure for governments to implement what we call "responsive open data". Unlike today's open data, responsive open data responds to the commands of citizens -- when they want it, where they want it.

By putting business licences, property titles or birth certificates on the blockchain, governments will enable citizens to digitally conduct transactions without lawyers, notaries or queuing at government offices. Once on the blockchain, registered ownership of a car, a home or other assets can be transferred from one person to another without the need for a government recorder or other third party, while still being legal and publicly acknowledged.

"The conversation around Bitcoin has shifted from curiosity, confusion and doubt to one in which serious decision-makers are recognising the many ways blockchain ledgers can be used"

Brian Forde and Michael Casey

This is now possible because the blockchain is a public ledger of all previous transactions to which new transactions are added. As the blockchain grows, it becomes harder and harder to manipulate past transactions since the records of each are built on top of each other. This interdependence in the stacks of transactions gives permanent integrity to the recorded sequence of events and facts. It enables both the vital function of timestamping and, with the addition of digital signatures, the transfer of ownership without a third party like a government, bank or notary to confirm the transaction took place.

We're not the only ones thinking about this. The US state of Vermont is considering using the blockchain to track government records. Honduras is exploring the registration of property titles with the same technology. The pay-off: more confidence in the agencies that govern transactions and a chance to help secure a stronger foundation for just societies.

Like the internet, anyone can post anything to the blockchain, but the credibility and veracity of that information can be determined by whomever's digital signature was used to append that information. If the organisation or person signing the transaction into a blockchain-based record is trustworthy at the outset -- that is, if there are sufficient checks and balances to show that the signature belongs to whom it claims to represent -- the system can then offer a highly authoritative verification of any changes to it.

It's important to note that the integrity of the data must also be assured at the pre-blockchain stage. As the saying goes, garbage in, garbage out. Similarly, it's critical that transactions, contracts and documents are verified on a globally accessible public ledger -- ensuring that the information stored on it cannot be deleted or manipulated by any person, institution or government. Otherwise, in the hands of a bad government or actor, a poorly designed blockchain system could be abused, with drastic consequences.

If these data-integrity standards are adhered to, the blockchain could become a powerful tool for maintaining those records.

Challenges still exist to implementing this technology. Currently, Bitcoin has scalability limitations, requiring updates to its core code that are proving highly contentious among developers. Security concerns also persist. The oft-cited risk that hackers can steal bitcoins, though, hinges more on weaknesses with company security than the underlying core protocol itself. The same goes for the negative impression generated by some high-profile cases of illicit uses of bitcoins. Some criticism is valid, but much of it stems from past problems and lingering negative perceptions. Until sophisticated new protections for digital-wallet software and hardware have been properly stress-tested in the real world and the digital currency gains more mainstream acceptance, many in the general public will mistrust it -- and that makes it harder for governments to embrace.

Similar to the internet's vast, decentralised nature, finding information on the blockchain is difficult and connecting public keys to real-world individuals is challenging. Both merit more research as developers compete to create tools and applications that work to address many of these issues.

Still, in the boardrooms and offices of some of the largest companies, not-for-profit institutions and government agencies, there's growing interest in Bitcoin's underlying technology. Whether it's adopted as is or adapted for special-use cases, the blockchain has enormous potential to disrupt the global economy and, we think, help support more open and fair societies.

"By putting business licences, property titles or birth certificates on the blockchain, governments will enable citizens to digitally conduct transactions without lawyers, notaries or queuing at government offices"

Brian Forde and Michael Casey

In that spirit, the MIT Digital Currency Initiative is working with entrepreneurs, open-source developers, philanthropists, non-government organisations, academic institutions and, of course, governments to conduct fundamental research and develop practical pilots to identify where the blockchain could bring real improvements to society. Building on the work of many software developers, academics and entrepreneurs, below we lay out several examples worthy of exploration. Research and experimentation in these areas could help us get to the future, faster -- something we think companies and citizens should demand from their governments.

BIRTH AND DEATH CERTIFICATES

Much of what we do in life stems from being able to prove we were born on a certain date under a certain name to an identifiable mother. Documentation of our birth and the date on which it occurred confers a right to vote, a right to open a bank account, or a right to obtain a passport and travel. For the purposes of inclusion in the global economy, it's hard to imagine a more important record-keeping task, yet mismanagement is rife. Up to a third of children under the age of five have not been issued a birth certificate. According to UNESCO research, a lack of formal citizenship status and ID is the single greatest risk factor contributing to the trafficking of girls in places like Thailand.

The blockchain could be used by governments or other locally trusted institutions to issue birth certificates and death certificates. When encoded with encryption methods that give people personal control over such data, it will not only make the record-keeping more reliable but could also empower citizens to access critical services. People could point government agencies or service providers to a digital record of their birth, or to a family member's digital death certificate. Taxpayers would also benefit, reducing the problem of governments continuing to pay social welfare or other benefits to deceased people.

BUSINESS LICENCES

Civic-tech entrepreneurs Chris Taggart and Rob McKinnon launched OpenCorporates just over four years ago with the goal of cataloguing every company in the world and entering them into its open database. After thousands of hours spent culling through millions of original records, they have laboriously constructed a useful cache of information covering some 90 million companies. It did a great

service, but in a globalised economy we need a more seamless, automatic way to gain access to all these data.

It doesn't help that these business records lack international standards. Some government agencies publish business-licence information in an easily accessible machine-readable format. Others publish it in a more challenging to access PDF format. Many also require publication in local newspapers to complete the process of registering a company.

Enter the blockchain. Adopting a responsive open-data strategy, governments could leverage the record-keeping reliability of the blockchain to register businesses in a quick and efficient manner. The interoperability of the blockchain means that disparately maintained registries in different jurisdictions could be combined without people like Taggart and McKinnon having to do their laborious work. Not only would entrepreneurs benefit from the efficiency of the technology, but the blockchain's timestamping powers could slash the amount of work civil servants spend tracking down lost documents, reconciling records and generally maintaining the databases.

PROPERTY TITLES

People's homes are most often their biggest asset -- something that can be borrowed against to start a business or secure a safe retirement. In the developing world, property titles take on even more meaning. Peruvian economist Hernando de Soto, for example, has identified trillions of dollars of "dead capital" in the developing world: people living in the world's poorest slums own their homes, but without formal titles they can't easily sell, appraise, insure or borrow against those assets.

"The blockchain can only do so much. It can't get around the deep political failings and corruption that leave certifying authorities unable or unwilling to do the work needed to survey, define and draft titles"

Brian Forde and Michael Casey

Here, too, the timestamped power of the blockchain could help. Using this decentralised ledger to keep track of the many transactions that accumulate over time with a specific land deed could greatly reduce both the costs and headaches associated with managing them. The blockchain's interoperability should also mean that these benefits can be carried across borders so that data from different land registries apply across geographic zones.

The blockchain can only do so much. It can't get around the deep political failings and corruption that leave certifying authorities unable or unwilling to do the work needed to survey, define and draft titles. But if officials can be persuaded to start the process, each phase can be recorded in the blockchain. This could make it possible to verify that appropriate steps were taken in the right sequence. Once the title itself is registered on the blockchain, locals could, for the first time ever, have verifiable ownership of a valuable piece of collateral.

Governments who shift their land title registries to a blockchain-based system could lay the foundation for more fair and transparent land-ownership transactions in the future. Furthermore, these records would be more resilient during times of conflict or state collapse when such legal documents are more likely to be destroyed or tampered with.

NON-GOVERNMENT RECORDS

This model need not apply solely to government record-keepers. A similar opportunity exists for universities to use blockchain record-keeping for college transcripts.

In Pakistan, Kenya and other countries, government leaders have been required to have university degrees to hold office. This has generated headlines from "Leaders warned on use of fake degrees" to "Over 100 MPs in Pakistan may have fake degrees."

Confirming a person's educational credentials can be laborious. To improve this process, universities -- and even secondary schools -- could store transcripts on a universal, decentralised ledger. This could bring greater transparency to the assertions people make about their educational records and make it easier for students to selectively share their scores with educational tech companies for customised tutoring or support.

There are no easy fixes for any of these problems, and we must stress that Bitcoin and blockchain technology are largely untested for the use cases we describe. But as an academic research initiative, we are exploring options and identifying innovations that have the potential for impact. That way, when solutions are finally implemented, they serve society in the best possible way.

What's clear is that the existing system of government and institutional registries could be updated to address the needs and challenges of our digital age. By implementing responsive open data via the blockchain, we now have an opportunity to do that.

Five decades later, that August 1961 announcement in the local daily newspaper, the*Honolulu Advertiser*, served a useful purpose. It allowed Barack Obama to point to a timestamp reinforcing the authenticity of his birth certificate -- and helped ensure he became the 44th President of the United States.

But for the rest of us, digging into the microfiche of old newspapers to verify transactions just doesn't scale. The Bitcoin blockchain and its timestamping and peer-to-peer transaction system could be the answer, providing a path to data reliability and interoperability. With it, we could empower citizens and boost their confidence in the agencies that govern their lives.

In memory of Jake Brewer and the tireless work he did advancing open data throughout his life.

Submitted by: Roger Buhlert – Cardinia Shire Council