The Blockchain: Beyond Bitcoin

A data innovation case study by **copia**

Blockchain technology is the distributed database that underlies digital cryptocurrencies such as Bitcoin. Various consensus algorithms can create distributed ledger systems to achieve a verifiable public record of transactions, replacing trust in people or institutions with a trust in mathematics. All of these technologies provide an extremely useful solution for keeping a reliable record of digital information — a practical answer to the theoretical conundrum known as the Byzantine Generals Problem. Keeping track of digital tokens in order to prevent double-spending is the most obvious application, but blockchain technologies allow for any kind of transaction without a requirement for a trusted third party, intermediaries or centralized authority. Hundreds of digital currencies based on blockchain technologies are valued in the billions of dollars with over 100,000 merchants accepting bitcoins, but the applications extend beyond digital cash.

IMPACT

Bitcoin as a currency is only the first application for blockchain technologies, the proof of the concept that shows valuable information can be reliably stored in a digital system scattered all over the world. The blockchain acts as a registrar of deeds, recording and verifying the ownership of assets. The innovation is the technological shift away from human-based verification to algorithmic trust that reduces the costs of transactions and boosts economic efficiency and wealth.

As hundreds of billions of devices connect to the internet, a secure communications platform to ensure trusted software updates and the absence of malware could rely on blockchain technologies. The "internet of things" (IoT) will need a low-cost network that can autonomously maintain itself without the need for human intervention. Just as the telephone system became more efficient and affordable when human switchboard operators were replaced by automation, employing blockchain technology to secure machine-to-machine communications will make smart appliances more widespread and convenient, enabling sharing economies and other efficient markets.

Smart contracts are poised to become innovative legal and financial instruments, offering services that can't be done as efficiently without the automated execution of terms. Escrow services for any-sized transaction become more attractive — for buying small items on Craigslist or other online marketplaces — instead of being used only for large expenses such as cars and homes. Smart insurance contracts would automatically distribute assets upon a person's death, reducing possible disputes over wills and inheritances. There are already car loans that disable a car if a payment is missed, and smart property would aim to reduce theft or unauthorized uses. Business transactions can be programmed to distribute equity or voting rights, and companies will be able to more easily raise funds from a large crowd of investors with minimal fees to enable the transaction. The rise of Decentralized Autonomous Organizations (DAOs) will allow for the creation of entities that wouldn't normally exist, such as organizations funded with micropayments or set up with extremely complex ownership and management structures.

POLICY IMPLICATIONS

Using bitcoin as money is outlawed in three countries: Russia, Vietnam, and Iceland. This doesn't necessarily prevent users from storing the digital information or running programs using bitcoin code, but for these nations, these laws effectively slow the widespread adoption of cryptocurrencies and associated services with a chilling effect. In the US, the Financial Crimes Enforce-

ment Network (FinCEN) allows services that exchange traditional currencies with bitcoin to operate as Money Services Businesses (MSBs), but such businesses would be required to register and be regulated under the Bank Secrecy Act. Obtaining licenses to operate and ensuring that legal obligations are met will undoubtedly take significant time and development efforts, and the guidelines could expand to cover more types of transactions in the future — adding uncertainty for businesses that previously considered themselves unregulated.

The state of New York is drafting its own rules for BitLicense regulations, and other states are expected to follow suit. However, even just operating within the US right now, often requires understanding (and trying to comply with) banking regulations in all 50 states.

Individuals don't need to be too concerned about licenses or registering to use blockchain technologies for uses unrelated to currencies, as exemptions for software developers using blockchain protocols for non-financial purposes are expected to be widely accepted. However, this is new territory for regulation, and it's possible that the underlying algorithms for blockchain technology could be subject to international trade embargoes or other restrictions. Potentially, blockchain platforms for messaging and communications could be subject to laws regulating encryption technologies.

As the blockchain can be more widely used, it starts to create a variety of other policy challenges as well. Regulations are built on the expectation of a world in

> Using bitcoin as money is outlawed in three countries: Russia, Vietnam, and Iceland.

which money is generally heavily regulated by government entities, rather than algorithms and cryptography. Similarly things like enforcing contracts and insurance have their own legal/judicial and regulatory infrastructure that are based on humans adjudicating issues. When things are handled algorithmically instead, it could have a major impact on both that infrastructure and how such contracts are made and enforced.

There are also concerns about law enforcement. Certainly a significant number of "dark market" transactions for illegal products are happening with cryptocurrencies today, leading to concerns about how law enforcement can track down lawbreakers.

Beyond currency and contracts, the blockchain's ability to reliably record information has many exploring how it could be used to revolutionize voting systems as well, potentially building much more secure, reliable and trustable voting systems that are nearly impossible to corrupt. On top of that, some envision a world in which blockchains enable truly distributed online services, that have no central point of attack, or central point of failure.

This could create significant regulatory questions, including how to categorize services that simply aren't based anywhere — unlike today, where, at the very least, key servers must exist somewhere. This creates challenging questions about which regulatory regimes apply — and a variety of other questions regarding freedom of expression, defamation, copyright and more.