Demystifying Bitcoin

Threat or opportunity?

Eric Collard
Partner
Governance, Risk & Compliance
Deloitte

Gwenaël Gavray
Director
Business Transformation
Deloitte

Despite an explosion in media coverage, virtual currencies such as Bitcoin are misunderstood. Many articles describe exchange meltdowns, price volatility, and government crackdowns. This focus on Bitcoin as a volatile and even renegade currency may be distracting businesses from its potential long-term significance as a disruptive new money technology.

Introduction

Bitcoin is more than just a new way to make purchases. It is a protocol for exchanging value over the Internet without an intermediary. Much has been written about Bitcoin's payment applications, however Bitcoin could soon disrupt other systems that rely on intermediaries, including property transfer and identity management.

As the Bitcoin ecosystem—relying on the blockchain technology—evolves and use cases emerge, the public and private sectors will face new challenges, opportunities, and responsibilities. Companies may build upon this technology to create innovative products and services. In the future, Bitcoin and blockchains may revolutionize the way we conduct business. The sooner the public and private sectors understand the potential of this new technology, the better prepared they will be to mitigate its challenges and realize the benefits of bitcoin and other similar virtual currencies.

Why did Bitcoin emerge?

Throughout history, many items have been used to store value and as a medium of exchange, such as clay tablets, coins, and now paper money. As our understanding of money as a store of value, medium of exchange, and unit of account has matured, so have the methods and modes for exchanging it. There have always been functions of the technology available. We moved from precious metal coins to paper money before inventing checks and then credit cards. Yet credit cards weren't created for the Internet era. They have simply been adapted to meet the needs of consumers operating in a networked and digital world. With the consumer-accessible Internet now 20 years old, the question is not why a currency specifically designed for the Internet has emerged, but what took it so long.

Bitcoin is one of the first currencies born on the Internet to be used in the real economy. Other virtual currencies have since been created from the same open-source code as bitcoin, and more are popping up every day. Some of these currencies aim to improve upon Bitcoin's technical or operational difficulties, such as transaction speed and security. However, Bitcoin has so far sustained its first-mover advantage. It is the most popular and has the highest value in circulation. As at 1 August 2015, there are 14.45 million bitcoins in circulation with a total market capitalization of US$4.1 billion.

How does Bitcoin work?

Bitcoin is a protocol for exchanging value over the Internet without an intermediary. It is based on a public ledger system, known as the blockchain that uses cryptography to validate transactions. Bitcoin users gain access to their balance through a password known as a private key. Transactions are validated by a network of users called miners, who donate their computer power in exchange for the chance to gain additional bitcoins. They receive newly created bitcoins for this, which is the only source of additional bitcoins. There is no monetary authority that creates bitcoins. There is a fixed supply of 21 million bitcoins that will be gradually released over time at a publicly known rate; the rate of supply diminishes over time in a predictable way. As a store of value, this means that bitcoins are inherently deflationary. It also means that there is no government or central entity to make discretionary decisions about how much currency to create or to attempt to defend it through monetary policy actions.

In order to process a bitcoin-denominated transaction, Bitcoin verifies two facts:

1. When user A transfers a bitcoin to user B, user A has a bitcoin to spend (prevention of counterfeiting)
2. When user A transfers a bitcoin to user B, user A is not trying to transfer the same bitcoin to another user, user C, simultaneously (prevention of double spending)

As Bitcoin matures, an ecosystem of companies is emerging to support consumers and retailers in storing, exchanging, and accepting bitcoins for goods and services:

- Banks and wallets store bitcoins for users either online or on storage devices not connected to the Internet, known as "cold storage"
- Exchanges provide access to the Bitcoin protocol by exchanging traditional currencies for bitcoins and vice versa
- Payment processers support merchants in accepting bitcoins for goods and services

What are the qualities of Bitcoin as a technology system?

Bitcoin has three qualities that differentiate it from other currencies and payment systems.
First, Bitcoin is peer-to-peer (P2P), transferring value directly over the Internet through a decentralized network without an intermediary. Current payment systems, like credit cards and PayPal, require an intermediary to validate transactions; Bitcoin does not. As a result, Bitcoin has been referred to as "Internet cash," as it can be exchanged from person to person much like paper currency today.

Second, Bitcoin is open, yet securely authenticated. Traditional payment systems rely on the privacy of transaction information to maintain security. For example, the compromise of a credit card transaction can result in the release of valuable information that can be used to conduct future transactions. In comparison, Bitcoin relies on cryptography. As every transaction is validated with cryptography by the network of miners, Bitcoin functions because of its openness, not despite it.

Third, Bitcoin is self-propelling. Bitcoin uses its own product, bitcoins, to reward or "pay" miners who are providing the computing power that serves as the engine of the transaction verification system. As a result, the system does not require the same type of overheads that traditional payment systems might. These three aspects are part of what drives Bitcoin's success, enabling a nearly frictionless global payment system. However, these same factors have also created challenges.

What are the main challenges of Bitcoin?

In order to achieve wider adoption as a currency, Bitcoin needs to address significant questions around volatility, regulatory uncertainty, exchange security, ease of use, and transaction volume.

Bitcoin speculators have driven significant price volatility, reducing Bitcoin's utility as a medium of exchange. People may be reluctant to use Bitcoin when the price can change by 30 percent overnight. The global regulatory environment around Bitcoin remains uncertain. Any news of new government scrutiny or rumors of a policy change can significantly affect Bitcoin prices, reducing its stability as a currency.

Security problems, punctuated by highly publicized exchange meltdowns, may prevent mainstream usage of bitcoins as a currency. To mature, exchange security needs to be as strong as at traditional banks. Mainstream consumers are unlikely to use Bitcoin until wallet services develop more user-friendly and secure storage techniques.

Validating transactions requires significant electricity, bandwidth, and data storage. The resources required to support Bitcoin's relatively small volume of transactions are already being pushed to their limits. Currently, Bitcoin averages about 120,000 transactions per day, while Visa handles more than 2.1 billion card transactions. In order to support mainstream transaction volumes, the Bitcoin system for validating transactions will likely have to change how it uses electricity, bandwidth, and data storage.

Opportunities with Bitcoin and blockchain

Bitcoin is more than a new currency. Bitcoin and other virtual currencies are creating a new architecture for exchanging information over the Internet that is P2P, open yet secure, and nearly frictionless. Currently, when an individual transfers funds, he or she must work with a third party often charging fees. Bitcoin allows for a direct payment to anyone, anywhere in the world, at any time. This may allow companies to charge lower fees than they do today.

Now imagine how other systems that rely on intermediaries, such as property transfer and identity management, could be disrupted by a similarly open P2P system.

Bitcoin is a protocol for exchanging value over the Internet without an intermediary. It is based on a public ledger system, known as the blockchain that uses cryptography to validate transactions

Bitcoin allows for a direct payment to anyone, anywhere in the world, at any time. This may allow companies to charge lower fees than they do today

Transfer of property

The Bitcoin protocol could simplify complex asset transfers, revolutionizing the services that support this industry. Currently, the transfer of large assets requires significant time and resources. For example, in order to purchase a car from an individual seller, one has to use services to learn about the car's accident and inspection history. The blockchain, Bitcoin's public ledger, could change this. Bitcoins can be qualified in such a way that they represent real-world assets. Bitcoin entrepreneurs at companies like Colored Coin are already working on ways to use small portions of bitcoin to denote physical property. A fraction of a bitcoin would publicly identify who currently owns that property and could include a record of both past ownership and other history about the property. When purchasing a car, one would be able to verify all accidents and inspections over the blockchain and transfer the title on-site.

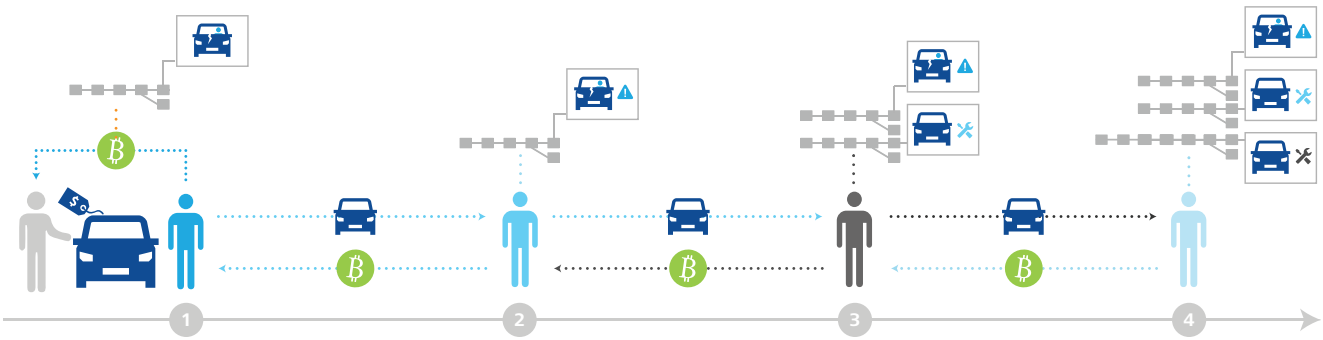
Similarly, real estate and financial instrument transactions could all be executed over blockchain protocol. This could soon create efficiencies and reduce friction by allowing individuals to directly transfer property without the use of a broker, lawyer, or notary to sign off on the transfer.

Identity management

Blockchain could also transform identity management. Much of identity management, including passports, still operates on a paper-based system. These documents are frequently forged and stolen. But what if there was a way to create a unique, verifiable key that was impossible to forge? A cryptographic network based on blockchain could be used to verify individuals' identities and monitor movement across borders. When a person travels through a checkpoint at a border crossing, instead of showing and scanning a paper passport, he or she could present his or her Bitcoin key. A government entity could verify the key and register the entry into the blockchain.

This could also be used for other forms of identity management like social security numbers, tax identification numbers, or driver's licenses.

Transfer of property



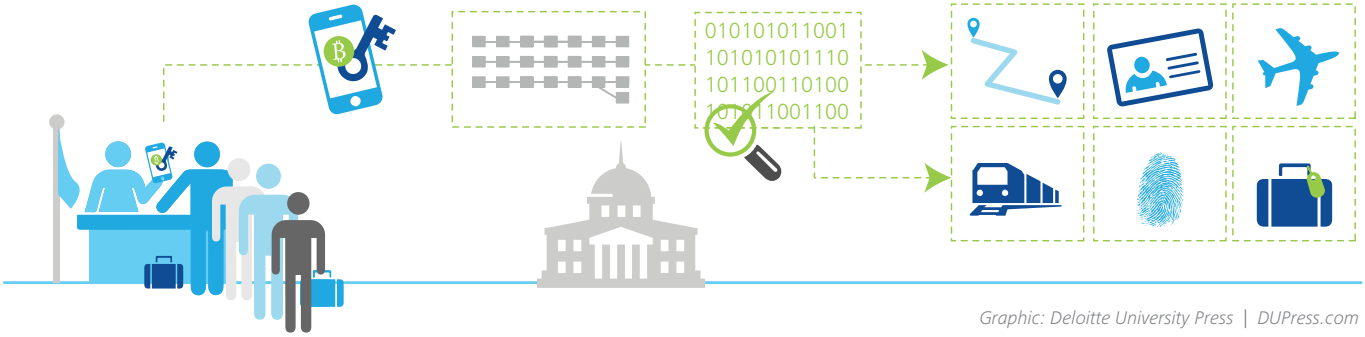
Person A
purchases a car from a dealer. That car is represented in the block chain by a bitcoin, allowing the purchaser to view the car's history in the public ledger.

Person B
purchases the car from Person A and learns the car was in an accident by reviewing the car's history in the block chain.

Person C
purchases the car from Person B and learns the car was serviced regularly and there was an accident by reviewing the car's history in the block chain.

Person D
purchases the car from Person C and reviews the car's history in the block chain to learn about the accident, service history, and recent work that was done on the car to pass an emissions test.

Identity management



Graphic: Deloitte University Press | DUPress.com

Deloitte's observations regarding blockchains

To date, many of Deloitte's clients worldwide are still in the exploratory phase of the technology, with most still attempting to determine the differences between Bitcoin and other blockchains.

Some, however, are moving to apply this technology to specific pain points, either to add additional revenue streams or cut costs. Some of Deloitte's banking clients are primarily interested in using the blockchain for the trade, transfer, and settlement of transactions. Elsewhere, retail clients are interested in the use of the blockchain for rewards program management. The challenge is to find use cases where more revenue can be generated with a different client experience or reduced costs.

As far as Deloitte is concerned, for internal use, various areas of interest have been identified. For example, Deloitte US is currently developing a solution using the blockchain to accelerate the audit process. A company would post every transaction in a blockchain. To audit this company, Deloitte would look at that blockchain and all the transactions, as the blockchain is immutable and time-stamped.

On the consulting side, the potential for Deloitte is around the ability to source consulting services through a P2P crowdsourcing platform. For example, instead of asking Deloitte for help on a given strategy, clients could request a service on the blockchain, and the blockchain would match the client with the right individuals to do that.

Identifying opportunities

Payments are obviously being influenced by Bitcoin and the blockchain, but enterprise clients are currently interested in the broader applications of the technology. Bitcoin should be considered a technology for all transactions, including those that are not necessarily financial.

Bitcoin is a technology that is interesting for companies wanting to manage any type of transaction: it could be a transaction between two persons transferring bitcoin or asking a driver to pick them up at an airport. Over time, blockchain may become a foundational layer for asset transfer, smart contracts, and voting, but different blockchains may be created that specialize in each of these use cases. These evolutions will nevertheless have to be carefully pushed forward taking into consideration the regulations on data protection.

Conclusion

- Bitcoin is more than a new virtual currency. It is an ecosystem relying on the blockchain technology that has applications beyond payments
- Applications of bitcoins & blockchain technologies have a high disruption potential beyond the financial industry, especially in activities relying on intermediaries
- Many factors will influence Bitcoin's evolution, including regulation, technological innovation, and economic conditions
- Predicting the future of Bitcoin and blockchain today resembles what it must have been like to try to comprehend the significance of the Internet in the 1990s. But if Bitcoin's short history is an indicator, the future of this technology will be an exciting ride!

Sources:
www.blockchain.info
http://www.coindesk.com/deloitte-blockchain-auditing-consulting/
Deloitte University Press – Bitcoin. Fact. Fiction. Future.


CHALLENGE
Technology
Virtual
MOBILE
BITCOIN
TRANSACTION
MOBILE
OPPORTUNITY
MOBILE
MOBILE
BITCOIN
ECO-
SYSTEM
Currency
CHALLENGE
THREAT
BITCOIN