Deloitte.

Bitcoin and Analytics

Assessing the opportunities and vulnerabilities of the cryptocurrency marketplace

Contents

Overview

The long-standing desire for two parties to transact online directly—without a third-party intermediary—has accelerated the popularity of Bitcoin and other cryptocurrencies.

The online equivalent of hand-to-hand cash transactions, the cryptocurrency phenomenon—driven primarily by its to-date most popular option, Bitcoin—has struck a chord with growing legions of speculators, consumers, merchants, government regulators, and, naturally, lawbreakers.

As the news of recent Bitcoin-centric scandals has revealed, the latter category of less ethical players has rightfully heightened stakeholder scrutiny and wariness of Bitcoin and its digital brethren. But its growing popularity as a legitimate currency exchange option means Bitcoin holds opportunities as well as risk. Companies are seeking to further capitalize on the Bitcoin trend—even if many remain unsure of the precise implications on their business or industry.

Pros and cons

The first alternative cryptocurrency to successfully emerge, Bitcoin entered the marketplace in 2009. Initially embraced by computer scientists, hackers, and gamers searching for a currency and payment system designed for the Internet era, Bitcoin has since become the domain of speculative investors and venture capital enthusiasts. As a result, Bitcoin's value in terms of US dollars has increased, along with the abundance and diversity of use cases.

One foundational aspect of Bitcoin is the pseudonymity of its users, due to each Bitcoin wallet being associated with one or more "addresses" composed of numbers and characters. This allows participants to conduct business in a nearly anonymous—or pseudonymous—environment. Conversely, the transactions themselves are recorded in the public domain via a public ledger system called the block chain, making it possible to view transaction histories more transparently than traditional market systems.

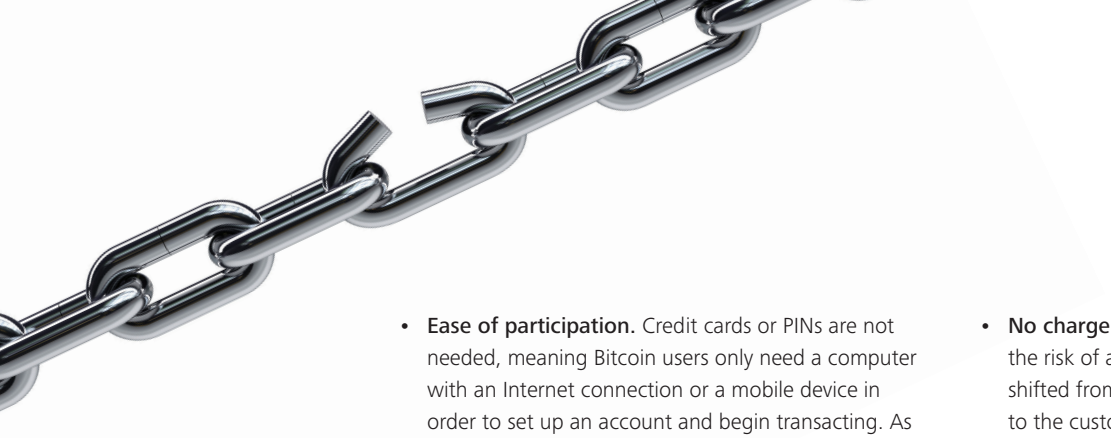
In just a few short years, Bitcoin has matured, including an evergrowing ecosystem of service providers—trading platforms, exchanges, payment processors, e-wallets, and more—designed to help facilitate trades and transactions. Since it is not a nation state currency subject to monetary policy vagaries, Bitcoin and other cryptocurrencies are not subject to traditional currency valuation changes. These currencies have a predetermined and known monetary policy, although its investment value is buffeted by the ebbs and flows that affect all financial markets (as well as the perceived stability and security of the currency itself). Tax advantages may also emerge with the Internal Revenue Service's recent ruling of cryptocurrencies as property rather than cash.

The cryptocurrency industry is evolving, and Bitcoin's advantages have become quite apparent, especially its:

- **Low—or no—transaction fees**. Because transactions occur via the block chain over a distributed peer-to-peer network, a third party is not required for verification and authorization. Currently, Bitcoin has low fees when compared with traditional payment platforms, which render an interchange charge consisting of a flat fee of 10–20 cents combined with a percentage fee of 1%-3%[1]. However, this may change in the future based on incentives offered to Bitcoin users in order to sustain the network and encourage growth. Indeed, some Bitcoin merchants charge no transaction fees, having adopted a flat monthly fee model.
- **Speed**. Similarly, the decentralized nature of Bitcoin means it bypasses banks and other financial institutions, so that payments and transfers can be completed quickly. This is particularly attractive for international transactions. For instance, where a wire transfer could take up to three business days to settle, a typical Bitcoin transfer could be cemented within the consensus block chain in less than an hour[2].
- **Double-payment protection**. Since each transaction in a healthy and well-functioning Bitcoin ecosystem is recorded via the public block chain, the "spending" of the same Bitcoins more than once is next to impossible. (Of course, this assertion cannot be made in a poorly designed Bitcoin system infiltrated by nefarious players.) This double-payment protection would resolve a traditional currency problem where a clearing middleman is essential.
- **No chargebacks for merchants.** The finality of a Bitcoin transaction once it has been committed to the block chain implies that, as with a cash transaction, there is no potential for chargeback of transactions. This is a risk assumed by merchants accepting credit card transactions, and no chargeback means removal of that risk.

[1] http://usa.visa.com/download/merchants/Visa-Interchange-Reimbursement-Fees-April-2014.pdf

[2] Bitcoin Wiki https://en.bitcoin.it/wiki/FAQ#Do_you_have_to_wait_until_my_transactions_are_confirmed_in_order_to_buy_or_sell_things_with_Bitcoin.3F, (Accessed October 2nd, 2014)



- **Ease of participation.** Credit cards or PINs are not needed, meaning Bitcoin users only need a computer with an Internet connection or a mobile device in order to set up an account and begin transacting. As long as the recipient email addresses are known, the transaction can occur.
- **Decreased risk of personal data theft.** In an era where personal data theft at the point of sale is increasingly prevalent, transactions by Bitcoin reduce the risk exposure of the customer. Loss of names and credit card numbers can entail a significant identity theft risk for consumers. However, with Bitcoin, the only risks of exposure are the public key address of the transacting account and the Bitcoin total of the account in question.

Nevertheless, the nascent status of Bitcoin also means it is suffering from growing pains, as instances of fraudulent or other illegal activity have risen in tandem with the technology's popularity. For example, in October 2013, the FBI shut down Silk Road, an alleged black market for drug trafficking, after hackers managed to steal nearly $3 million in Bitcoins. More recently, Mt. Gox—one of the first and largest Bitcoin exchanges—declared bankruptcy after allegedly losing control of $500 million in Bitcoins.

Indeed, some of the Bitcoin benefits that have made it so appealing are also the source of worrisome disadvantages, such as:

- **Regulatory concerns.** The novelty of cryptocurrencies in general has resulted in legal and regulatory ambiguity, with outright opposition from certain countries (one is Bangladesh, which has warned that anyone using Bitcoins could be jailed for money laundering). In the United States, this ambiguity has resulted in a lack of regulatory acknowledgement and insurance from federally insured banks. This disadvantage is gradually receding as more jurisdictions provide guidance around cryptocurrencies; for instance, New York recently became the first state to propose regulations on virtual currencies.
- **Anonymity can beget illegal activity.** As Silk Road revealed, the near anonymity of Bitcoin users makes it a particularly attractive destination for money laundering and transactions involving illicit goods, drugs, and activities.
- **Loss of access is permanent.** Since Bitcoin accounts are cryptographically secured, access to monies contained in an account almost certainly cannot be restored if the "keys" to an account are lost or stolen, and subsequently deleted from the owner.
- **No chargeback** or reversal of transactions means that the risk of a fraudulent or erroneous transaction has shifted from the financial system or merchant back to the customer. This may have an adverse impact on consumer protection.
- **Volatility.** Driven by much publicized hacks into Bitcoin, the value of the coins can be quite volatile, altering the risk reward scenario for Bitcoin speculators.
- **Decentralization.** The decentralization of Bitcoin does come at a cost. With a centralized clearinghouse guaranteeing the validity of a transaction comes the ability to roll back a monetary transaction in a coordinated way. However, no such ability is possible with Bitcoin.
  - Because no centralized clearinghouse validates a transaction, transactions are validated by consensus among the users of the block chain, which is typically achieved after 30 minutes. Before that time, there is potential for transactions to be attached to chains that are not final.
  - In the most innocuous situation, if an incorrect payment is made from the transmitting party to the receiving party, the only way to effect an adjustment is for the receiving party to make an adjusting payment back to the transmitting party. This would become final once the adjusting transaction is committed into the main block chain.
  - At its worst, if a malicious third party manages to steal the keys to a user's wallet, the thief can fully impersonate the original owner of the account and has the same access to the monies in the wallet that the original owner has. Once the Bitcoins are transferred out of the account and that transaction has been committed to the block chain, those monies are lost forever to the original owner. In this sense, Bitcoin is like cash.
  - While final clearing of Bitcoin transactions is faster than international wire transactions, which might take several days, the decentralization and bandwidth limits of Bitcoin tend to limit Bitcoin to around seven transactions per second, far less than current credit card transactional systems.

The differentiation of Bitcoins from the traditional payment mechanisms of yesteryear, substituting their reliance on centralized clearing mechanisms for a decentralized clearing algorithm, as well as the assortment of changes described above, promise to make Bitcoin a disruptive financial technology in the world.

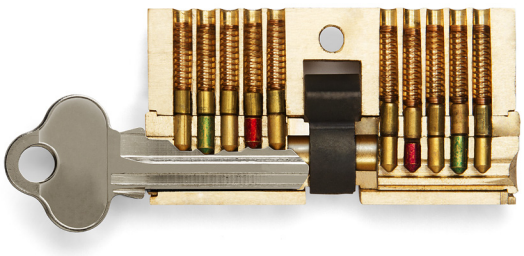
Assessing Bitcoin value with Analytics

Traditional financial industry players—from banks to credit card payment processors—are also sensing that Bitcoin is a disruptive technology that may inalterably change their world order. So, too, are retailers and other product/service providers who are trying to determine if Bitcoin is a payment option they should embrace on behalf of consumers seeking cryptocurrency benefits.

These benefits can extend beyond the notion of currency. From every Bitcoin transaction, valuable data emerges.[3] While anonymity is a hallmark of cryptocurrencies, every transaction is at its basic element a contract, with conditions and limitations, and anonymous or not, that data has value. From the timing, nature of spending, conditions, and limitations of these contracts between sender and receiver, trends will emerge that have the potential to feed new business models and transform long-standing processes. Analytics solutions can extract and interpret data to provide valuable insights about—and beyond—the transaction. Opportunities for Bitcoin transaction analysis are emerging within the following categories:

Block chain ingestion

Because the block chain is a public ledger of all transactions, analytics solutions can access and analyze vast amounts of data residing there. Doing so can unearth valuable information that can reveal specific insights on the audience for Bitcoin payments and transfers. For instance, credit card companies may be interested in delving into Bitcoin transactional data to determine the extent of the technology as a competitive threat. As a result, these companies can more effectively optimize pricing or target marketing campaigns to counter Bitcoin's actions and consider how the block chain may evolve. Although the block chain is transaction focused, in the future it may be possible to glean more information from it; this could be a move beyond historical and chronological information, and reflect more complex relationships among participants.



Transaction tracing

Many Bitcoin owners and exchanges have inquired about getting private insurance for their often sizeable Bitcoin portfolios. Should insurance companies offer it? And at what price? What business models might emerge around insuring such cryptocurrencies? If insurers have the capability of proving whether or not Bitcoin transactions have been stolen via the loss or theft of account keys, they can adjudicate claims more accurately and expeditiously.

Identity resolution

Naturally, the anonymity of the sellers and buyers using Bitcoin can lead to nefarious activity, including money laundering and other illegal transactions. Since the transactions are publicly documented, a number of Web scraping tools can be used by law enforcement officials or other entities seeking either to unmask Bitcoin users[4] or statistically verify trends related to transactions.

To date, at least two academic research efforts have been conducted to not only derive the identities of users but to determine transaction usage and circulation patterns. Each involved downloading the full history of the Bitcoin scheme into a transaction graph, and then thoroughly analyzing it. This research revealed that transactions involving a large number of Bitcoins involved creating chains of smaller, consecutive transactions that used fork-merge patterns and self-loops in an obvious attempt to conceal their ultimate destinations.

Additionally, persistent "detectives" can often ascertain more specific information—even Bitcoin wallet addresses—by using analytics tools to mine online message boards and other social media sites where Bitcoin topics are discussed. One caveat—conclusions reached are highly subjective or directional in nature, since specific information remains extremely difficult to ascertain.

Finally, financial institutions with customers who hold assets in Bitcoin or other cryptocurrencies can and would need to use analytics tools and techniques to ensure compliance with Bank Secrecy Act and other anti-money laundering (AML) regulations. Particularly, the publicly available nature of the block chain makes it both possible and necessary to use these techniques to perform deep transaction reviews of customers, although somewhat contradictorily, the pseudonymity in the block chain addresses makes it difficult to ascertain transactional counterparties.

[3] While this paper is focused on Bitcoin as the most prevalent cryptocurrency in circulation, many of these observations and analytic techniques are generalizable to other types of cryptocurrencies that rely on a distributed block chain)

[4] Fleder, Michael, Kester, Michael S., and Pillai, Sudeep. "Bitcoin Transaction Graph Analysis." http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf (2014)

International transfers

Bitcoin has a number of international political implications, as the relative anonymity of cryptocurrency transfers can enable rogue states or nations facing sanctions to circumvent those deterrents. Thus, a number of national and global governing bodies have become interested in tracking Bitcoin and other transactions that facilitate money movement outside of mainstream networks.

On a more positive note, the speed of Bitcoin transactions can make it an appealing option for legitimate international transactions that would otherwise face considerable delays while the parties navigate the tricky (yet perhaps more secure) conventional monetary exchange platforms.

Predictive capabilities

While the Bitcoin analyses conducted to date have revealed an often labyrinthine pathway of transactions, business and government entities are heartened by the promise of advanced data analytics tools in predicting future transactions or patterns. This area is likely to expand if Bitcoin's growth and popularity continue and it becomes more of a mainstream monetary exchange, with much of the predictive work likely to involve Bitcoin-centric dialogue that is occurring more frequently via social networks. Since Bitcoins can be viewed as assets, then as with other asset classes, it may be possible to use transaction volumes and history to attempt to predict value and securitize portfolios of Bitcoins.

Positioning for disruption

Throughout history, direct hand-to-hand exchange of currency has been the most popular method of transacting business. Bitcoin and other cryptocurrencies are the digital equivalent of these currency exchanges, and come with a phalanx of advantages, challenges, and still-unknown implications that seem likely to entice or frighten numerous stakeholders.

Traditional remittance and money transfer businesses may be at risk of significant market disruption if cryptocurrencies continue to grow in popularity. Services conducting money transfers through Bitcoin can adjust their pricing and marketing to benefit from Bitcoin's advantages vis-à-vis traditional money transfer services. Moreover, new remittance solutions based on cryptocurrencies are possible and can be focused on major markets. Financial institutions can identify those merchants willing to accept Bitcoins and other cryptocurrencies and potentially market customized financial services and products around cryptocurrencies to these merchants. Cryptocurrencies are not limited to transactions as simply monetary instruments; their positioning as assets may allow them to be used in larger swap or derivative transactions as an underlying asset.

Unlike wampum and other currency forms of yesteryear, Bitcoin has arrived as a direct result of technological advancements that—for the first time—make "hand-to-hand" exchanges fully traceable or detectable. This offers numerous opportunities for further use, as well as data analysis.

While there is much we are still learning, we do know that Bitcoin's technology could be used to understand consumer transactions and someday manage personal identifiable information or execute contracts. That is just the tip of the iceberg. Few would argue against Bitcoin's disruptive force. It has the potential to alter the landscape of commerce in significant ways.

Businesses that implement analytical processes and technologies now may be better positioned to mine the real gold from cryptocurrencies over the long term.

Contacts

Prakash Santhana
Director
Deloitte Transactions and Business Analytics LLP
psanthana@deloitte.com

Alex Rozman
Senior Manager
Deloitte Transactions and Business Analytics Services LLP
arozman@deloitte.com

Devaka Viraj Yasaratne
Senior Manager
Deloitte Transactions and Business Analytics LLP
dyasaratne@deloitte.com

Cliff Lou
Manager
Deloitte Transactions and Business Analytics LLP
clou@deloitte.com

Darien Tillinghast
Manager
Deloitte & Touche LLP
dtillinghast@deloitte.com