Challenges and New Business Opportunities for Bitcoin

Abstract

Virtual currencies like Bitcoin have emerged to enable digital, decentralized, anonymous, and worldwide payment transactions. While gaining more visibility in the media, virtual currencies are still in its infancy compared to the evolution of physical currency, and have several significant challenges for widespread adoption by consumers or businesses. This report showcases some of the near-term business opportunities around addressing these challenges, and predicts long-term winners and losers if virtual currencies overcome the challenges.

Date: October 17, 2014

Authors
Dan Belov / Distinguished Engineer, Google
Surendra Rajam / Director of Engineering, Samsung
Quinn Summers / Director of Product Management
Qinfang Sun / Director of Engineering, Qualcomm
Seokmin Yun / Sr. Director, Engineering, Lam Research

This paper was created in an open classroom environment as part of the Engineering Leadership Professional Program (ELPP) developed and led by Prof. Ikhlaq Sidhu at UC Berkeley. There should be no proprietary information contained in this paper. No information contained in this paper is intended to affect or influence public relations with any firm affiliated with any of the authors. The views represented are those of the authors alone and do not reflect those of the University of California Berkeley.
Section I: Introduction

What is Bitcoin?
A currency is a medium that people can use for selling or buying, such as gold (commodity currency) or dollar (fiat currency). Dollar is an example of a fiat currency and every fiat currency has a centralized government to control the inflation and deflation.

Bitcoin is a digital virtual currency. Bitcoins are not physical coins but generated only through computerized methods. Unlike wire transfers, checks or other transactions, bitcoin transactions complete within ten minutes regardless of where or who the end users are.

A large number of internet insiders have been researching to establish digital virtual currencies. A number of different types of virtual currencies have been proposed and created. Bitcoin is the most successful and well-known virtual currency so far.

History of Bitcoin
The Bitcoin protocol and reference software was created by Satoshi Nakamoto, who is believed to be a pseudonym of a person or group of people behind the technology. In 2008, Nakamoto published a paper on The Cryptography Mailing list at metzdowd.com describing the Bitcoin digital currency. In 2009, he released the first Bitcoin software that launched the network and the first units of the bitcoins. In 2010, a user "laszlo" made the first real-world transaction with Bitcoin. He offered to pay 10,000 BTC for 2 pizzas on the internet forum and the transaction was completed. The value of Bitcoin has risen sharply since 2010 and 1BTC recorded $1000 in 2014. Considering the Bitcoin value of 1 BTC = $1000, the pizza was called a “$5M pizza”.¹

The Bitcoin protocol was backed by mathematical models and cryptography techniques. It was operated and maintained by peer to peer network. Bitcoin could be “mined” by solving an encryption problem. The difficulty of the mathematical code was controlled by the Bitcointalk forums to control the number of “coins”.

Characteristics of Bitcoin
As a digital currency, Bitcoin is decentralized, anonymous, and worldwide. See illustration in Figure 1.

¹ http://en.wikipedia.org/wiki/bitcoin
Digital: Bitcoins are not physical coins but generated only through computerized methods. Unlike wire transfers, checks or other transactions, bitcoin transactions complete within ten minutes regardless of where or who the end users are.

Decentralized: Bitcoin transactions occur on a peer-to-peer network. It is an invented currency that is not controlled by any central bank or government.

Anonymous: Bitcoins flow from one address to another without identifying specific owners.

World wide: Bitcoins are borderless currency and can be used anywhere the peer-to-peer network can be accessed.

Figure 1: Characteristics of Bitcoin

Examples of digital virtual currencies

<table>
<thead>
<tr>
<th>Currency</th>
<th>Year established</th>
<th>Founder(s)</th>
<th>Website</th>
<th>Market capitalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>2009</td>
<td>Satoshi Nakamoto (pseudonym)</td>
<td>None official</td>
<td>~$9.2 billion (USD)</td>
</tr>
<tr>
<td>Ripple</td>
<td></td>
<td>Chris Larsen &amp; Jed McCaleb</td>
<td>ripple.com</td>
<td>~$2.6 billion (USD)</td>
</tr>
<tr>
<td>Litecoin</td>
<td>2011</td>
<td>Charles Lee</td>
<td>litecoin.org</td>
<td>~$600 million (USD)</td>
</tr>
<tr>
<td>Peercoin</td>
<td>2012</td>
<td>Sunny King (pseudonym)</td>
<td>peercoin.net</td>
<td>~$100 million (USD)</td>
</tr>
<tr>
<td>Namecoin</td>
<td>2011</td>
<td></td>
<td>dot-bit.org</td>
<td>~$40 million (USD)</td>
</tr>
</tbody>
</table>

Hypothesis

We believe there are business opportunities around addressing challenges of Bitcoin, regardless of its long term success.

---

2 [http://www.slideshare.net/few](http://www.slideshare.net/few)
Section II: Existing Market

The following map shows which countries are friendly to bitcoins:

![World acceptance to Bitcoin](http://www.BitLegal.net)

There has been significant buzz around Bitcoin in the year 2013 and lots of new companies are jumping in to be a part of this revolution. Here are some of the companies representing what looks like an increasingly mature ecosystem—that could chart the topography of a totally new monetary landscape:

**Bitcoin Ecosystem:**

<table>
<thead>
<tr>
<th>TYPE</th>
<th>FUNCTION</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wallets</strong></td>
<td>Store, send, and receive bitcoins</td>
<td>Coinbase, ZipZap</td>
</tr>
<tr>
<td><strong>Exchanges</strong></td>
<td>Trade bitcoins for local currency</td>
<td>Coinsetter, Kraken, Coinabul</td>
</tr>
<tr>
<td><strong>Payment Processors</strong></td>
<td>Accept and process payments</td>
<td>BitInstant, BitPay,</td>
</tr>
<tr>
<td><strong>HW &amp; Equipment</strong></td>
<td>Bitcoin infrastructure</td>
<td>Butterfly labs, Robocoin</td>
</tr>
<tr>
<td><strong>Investment</strong></td>
<td>Fund companies</td>
<td>Andreesen Horowitz, Google ventures</td>
</tr>
<tr>
<td><strong>Transacting</strong></td>
<td>Accept/support bitcoins</td>
<td>Zynga, Tesla</td>
</tr>
</tbody>
</table>

---

4 [http://www.BitLegal.net](http://www.BitLegal.net)
## Challenges and New Business Opportunities for Bitcoin

### Bitcoin Network:*

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total BTC</strong></td>
<td><strong>12,622,925 BTC</strong></td>
</tr>
</tbody>
</table>
| **Market Cap**          | **5,709,096,519 USD**  
|                         | **or 4,018,129,486 EUR**  
|                         | **or 17,672,095,000 PLN**  
|                         | **or 3,679,582,638 GBP**  |
| **Transactions last 24h** | **66,315**  
| **Transactions avg. per hour** | **2763.13** |
| **Bitcoins sent last 24h** | **453,961.33 BTC** |
| **Bitcoins sent avg. per hour** | **18,915.06 BTC** |

### Top predictions for Bitcoin in 2014:*7
- More than $100 M of venture capital will flow into Bitcoin startups
- US, China and other global forces will not be at the forefront of Bitcoin adoption
- Bitcoin community will solve problems including that of 'anonymity'
- The use of Bitcoin will evolve beyond 'store of value' or 'transactions'
- The price of Bitcoin is likely to range between $4000-5000 by the end of 2014

### Section III: Technology

Following are key components of the bitcoin protocol and transaction flow:*8,9

- **Bitcoin Address:**
  - Cryptographic hash (i.e. short unique form) of a public key of the owner. Owner of the address uses public key cryptography (public key + private key) to verify his ownership of the Bitcoin address. Stealing the private key makes it possible to control the bitcoin address and irrevocably steal all the funds associated with it.

- **Bitcoin Transaction:**
  - A program that describes sources, recipients, amounts and conditions of transfer of bitcoins. Can be as simple as Bob transferring Alice 1BTC or as complex as future contracts that require thousands of parties (represented by an address) to all contribute a signature on a piece of data (e.g. signing a bill by voting).

- **Block Chain:**
  - Public ledger of an ordered chain of validated blocks of transactions between Bitcoin Addresses. The longest valid chain is the source of truth. There is only a list of transactions and no list of account values.

- **Proof of Work:**

*8 [https://en.bitcoin.it/wiki/Main_Page](https://en.bitcoin.it/wiki/Main_Page)
– Cryptographic method of easily verifying that a certain amount of work (computations) has been done. The work in Bitcoin network is targeted to be around 10 minutes worth and the difficulty is adjusted every two weeks to keep the required amount of work at that level.

• Mining:
– The process of getting a reward for finding the right proof of work hash to validate a block of transactions. The reward was 50 Bitcoins in 2009, halving every 4 years.

• Mining Pool:
– A collective of miners who all share in the reward. For a low power miner it might take years to be able to validate a block (think lottery). Being part of a pool allows for a smoother and lower regular reward system instead.

• Transaction Fee:
– The Bitcoin protocol allows some amount of money to be created (not deducted!) to pay for validating a block of transactions. Currently at 25BTC.

• Wallet:
– Collection of public and private keys and thus their associated Bitcoin Addresses.

Figure 3 shows a detailed flow chart of bitcoin transaction.

---

Figure 3: Bitcoin transaction flow

10 http://visual.ly/bitcoin-infographic
Section IV: Evolution of Physical Currency: Opportunities for Bitcoin

Physical currencies appeared thousands of years ago and have evolved throughout human history. New capability and services were invented along the way to solve problems and provide more convenience to meet the need of modern financial activities. From the evolution of physical currency, a lot can be learned and predicted for what is needed for bitcoin to be widely adopted and succeed as a transaction method or virtual currency.

Compared to physical currency, virtual currency such as Bitcoin is still in early development and lacks of important components to make it reliable and trustworthy (see Figure 4). There are abundant business opportunities to fill in the gap, such as

- Legal counseling to assist Bitcoin service providers to comply with new and emerging regulations worldwide
- Insurance, security and escrow
- Bitcoin-based ‘credit card’ to make transaction more convenient.

![Figure 4: Evolution of physical currency and business opportunities for Bitcoin.](https://example.com)

In particular, fraud prevention is critical for wide adoption of Bitcoin. Recent events in the bitcoin business have raised awareness and doubts from general public about the lack of security and regulation on bitcoin exchanges and miner pools.

In January 2014, Ghash.io, one of the top two bitcoin mining pools (the other is BTC Guild), surged its mining power from 32% to 42% in 24 hours, raising immediate concern from the miner community of reaching the 51% market share, which will enable the pool to manipulate transactions and forge frauds. Luckily, the event was not a malicious take-over, but a natural result of market selection, due to the 0% pool fee and excellent customer support provided by Ghash.io. Ghash.io

---

quickly weighs in about its intention and responsibility to protect the health and integrity of the bitcoin community. But the question of how well bitcoin is prepared for real malicious take-over is still open.12

In February 2014, Mt.Gox, the world’s third largest bitcoin exchange, suffered a melt-down and filed bankruptcy after about $500 million or 850,000 bitcoins are stolen. 88% of those are deposited by users of the site, and 12% are owned by Mt. Gox. Mt.Gox CEO Mark Karpeles blames the weakness of bitcoin protocol, but experts on the bitcoin foundation believe the issue is in Mt. Gox’s highly customized wallet software and support procedure, i.e. a design issue that allows the attackers to take the hashes of recent trades and claim them as their own before they are committed to the bitcoin block chain. This again highlights the security risk of purchasing and storing bitcoin with unregulated bitcoin exchanges.13

In March 2014, Flexcoin, another bitcoin exchange described itself as world’s first bitcoin bank, was hacked and robbed of all 896 of its bitcoins stored online in hot wallets, valued at $600,000. Bitcoins stored offline in cold wallets are intact. Flexcoin shut down its site and will return intact bitcoins to its customers.14

Business opportunity for fraud prevention includes the following:

1. Certifying body for testing and approving security of software developed and/or used by bitcoin exchanges.

Bitcoin protocol is available to developers as open source code and APIs, and bitcoin providers develop their own customized wallet software and support procedures. Even though the bitcoin protocol is considered safe, security loopholes in the customer software can expose vulnerability and invite fraud attacks. Bitcoin community needs to form security alliance to define regulation and test procedures to ensure robustness of customer software. New business can be created to establish and develop test procedure, and charge fees to certify bitcoin service providers. The security rating provided by such certifiers will be published for consumers when they consider signing up with any bitcoin service provider.

2. Insurance Corporation for providing insurance for bitcoin deposits, similar to FDIC for US dollars.

FDIC (Federal Deposit Insurance Corporation) is an independent agency of the federal government. Its five-person board is appointed by the president and confirmed by the Senate. FDIC was founded in 1933 in response to massive bank failures in the 1920s and early 1930s. It employs more than 7000 people, insures $9 trillion deposits, and supervises more than 4500 banks. FDIC charges fee for banks to enroll in the service, monitor and supervise the participants for financial wellness and compliance, insures each depositor $250,000 per bank account, and pays depositors for loss when banks fail.15

Given that bitcoin is a virtual currency, and not endorsed or owned by any government, it is more likely that bitcoin deposit insurance will be provided by private insurance corporations, such as Farmers, Allstate, and GEICO. Due to the volatility of the bitcoin exchange rate, the insurance will be based on the number of bitcoins rather than its value in real currency. That is, the insurance is against fraud and loss of bitcoins rather than change in its value (similarly, FDIC insures face value of deposits not inflation or stocks/securities). Bitcoin wallet and exchange providers, such as Coinbase, BitPay, and Mt.Gox, who provides bitcoin exchange and deposit services, will be the customer of bit coin insurance services. The insurance rate will be determined based on the security rating of the business in order to balance risk and revenue.

3. Network security service for monitoring and reporting Bitcoin mining pool health

Sudden change in the mining pool can signal malicious attack, such as surge in mining power of one particular pool, or loss of mining power elsewhere which results in a remaining mining pool to take dominance momentarily. The status and

13 http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228
14 http://www.reuters.com/article/2014/03/04/us-bitcoin-flexcoin-idUSBREA2329B20140304
15 http://www.fdic.gov/
wellness of the mining pools must be monitored continuously to identify anomaly and alarm consumers and merchants about risk of carrying out transaction at the moment. The new business opportunity here is to provide such real time monitoring and report service to bitcoin exchanges and merchant service providers for a fee, to allow users to protect their accounts, and service providers to protect their customers by freezing or delaying transactions.

Section V: Legal Aspects of Bitcoin

Bitcoins and other cryptographic currencies are not recognized as legal tender in US. That is, one cannot cancel a debt to the US federal government by providing bitcoins. Cryptographic currencies are however recognized as a currency and are currently regulated under a number of US laws created by the Bank Secrecy Act and the Racketeer Influenced and Corrupt Organization act.

The Currency and Foreign Transactions Reporting Act of 1970, also known as the Bank Secrecy Act, requires banks and other financial institutions in the US to assist US government agencies detect and prevent money laundering. The US Department of the Treasury gave the Financial Crimes Enforcement Network (FinCEN) the authority to enforce the act, and act as the Financial Intelligence Unit of the United States. As part of its charter, FinCEN look for emerging trends and new methods in money laundering. On March 18th, FinCEN published guidance on virtual currencies like Bitcoin. This guidance clearly defines bitcoin exchanges as a money transmitter business:

"A person that creates units of this convertible virtual currency and uses it to purchase real or virtual goods and services is a user of the convertible virtual currency and not subject to regulation as a money transmitter. By contrast, a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter."

U.S. Code Title 31, Subtitle IV, Chapter 53, Subchapter 2, section 5330 defines Money Transmitting businesses as any other than the United States Postal Service which provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers’ checks, and other similar instruments or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.

U.S. Treasury Department under Title 31, Subtitle IV, Chapter 53, Subchapter II, section 5330, requires money transmitters to register with FinCEN, and name a compliance officer in their company who is responsible for detecting, preventing and reporting money laundering activities from happening.

In a recent case of money laundering with Bitcoin, the CEO of a Bitcoin exchange named Bitinstant was charged with not complying with the above laws. Specifically, he was registered with FinCEN as Bitinstant’s compliance officer, but did not report what he suspected to be money laundering activities by one of his largest customers, Robert Faiella. Robert Faiella was performing over a million of dollars worth of bitcoin transactions primarily from customers of the Silk Road, an on-line exchange for illegal drugs which accepted bitcoins as currency until they were closed down by the FBI on October 1st, 2013.

Challenges and New Business Opportunities for Bitcoin

---

16 http://www.fincen.gov/statutes_regs/bsa/
18 http://www.law.cornell.edu/uscode/text/31/5330
Some Bitcoin exchanges market that they fully comply with US money transmitter laws. For example, Bitcoin exchange Coin Cafe states on their website "Coin Cafe is fully compliant. We are a registered business, respect money transmission laws, are registered with FinCEN, and are completely accountable to our customers." 21

As a part of complying with FinCEN, money transmitters must also make sure that people or businesses who performing transactions are not on the U.S Department of the Treasury, Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons list, or "SDN list." This list consists of names and aliases of people who the US government has sanctions against and prohibits or restricts monetary transactions with. As of March 20th, this list is 593 pages long.

Countries like Japan have similar monetary transaction laws to combat money laundering. Mt. Gox, a bitcoin exchange was asked to close its accounts at Mizuho bank because the bank was concerned with meeting their reporting requirements with the amount of money transfers that Mt. Gox was doing 23.

Outside of the regulations on money transmitters and money service businesses, a recent court case rules that virtual currencies are a type of currency, and as such, is subject to all US laws regarding financial transactions. The court case in question was SECURITIES AND EXCHANGE COMMISSION V. TRENDON T. SHAVERS and BITCOIN SAVINGS AND TRUST, where the defendant was arguing that the US Federal Government and SEC did not have jurisdiction over the case because Bitcoins were not money. The case itself was about fraud, as Trendon T. Shavers was suspected of running a Ponzi scheme with bitcoins. 24

On January 23rd, 2014, Jack Lew, Treasury Secretary, did an interview on CNBC in which he was asked about Bitcoin. He responded, "From the government’s perspective, we have to make sure [bitcoin] does not become avenue to funding illegal activities or to funding activities that have malign purposes like terrorist activities, it is an anonymous form of transaction and it offers place for people to hide. We've made it clear through enforcement actions that we will look at these forms of transactions and we will enforce all of the rules we have on illegal money activity."

From a business opportunity perspective, Bitcoin exchanges could potentially automate regulatory compliance activities, such as automatically searching a list of recipients to see if they are on the SND list and reducing their operating costs. As long as people are converting fiat currencies like the US dollar into Bitcoins, and then using the Bitcoins to purchase something else, the Bitcoin exchanges themselves have a record of where the real money came from. Specifically, all Bitcoin exchanges only accept money transfers, wire transfers, cash in person or cashiers checks before they will release Bitcoins to a purchaser. This is to prevent the Bitcoin exchange from losing money on delivering Bitcoins when the purchaser has written a bad check, or authorized and then revoked a credit card transaction.

Section VI: Conclusions

Bitcoin is an emerging digital currency and payment system that can potentially revolutionize financial transactions in the future. Compared to physical currencies that have evolved to maturity, bitcoin is still in early development, has many challenges, and is missing some key components in the ecosystem. The security and reliability of bitcoin service providers is a prerequisite for wide adoption and success of bitcoin as an alternative payment system. There are abundant business opportunities to address the challenges.

21 https://www.getcoincafe.com/faq.php
When the challenges are addressed, which of the existing bitcoin businesses will win or lose will depend largely on how the players leverage the unique value of bitcoin to compete with traditional payment methods.

- One of the most attractive values of bitcoin is its low transaction fee compared with credit cards, or traditional money transfer (wiring). However this advantage may diminish or disappear once service providers deploy security and insurance measures that will increase the operational cost. Only those businesses that use bitcoin to replace existing transactions with very high fee will have a larger chance of success, such as cross border transactions.

- The reliability of bit coin transaction increases with the depth of the block chain or the length of the transaction time. This is inherent to the bitcoin protocol. Typical transaction time today is 10 minutes; 30-40 minutes of wait is recommended for significant transactions that requires higher reliability. This may be reduced in the future when higher speed processors, either general purpose or specially designed for bit coin mining, emerge. But for the foreseeable future where bitcoin transaction time remains to be much longer than that of credit card, transaction time will be an impediment for wide adoption at point of sales where users wait in line behind cashier’s counter, or for online purchase of software where users expect to start downloading immediately. On the other hand, online purchase of hardware where shipping is the long pole, is less sensitive to transaction time and thus better positioned for bitcoin success. Cross border money wiring which takes days to complete now, will also enjoy the relatively faster speed of bitcoin, in addition to the relatively lower fee discussed above.

In summary, bitcoin has larger chance of success in business segments that seek to replace payment methods with very long transaction time (days) and high fees ($10’s) today. The potential winner and loser from the success of Bitcoin are shown in Figure 5.

<table>
<thead>
<tr>
<th>Bitcoin feature</th>
<th>Winner</th>
<th>Loser</th>
</tr>
</thead>
<tbody>
<tr>
<td>New technology</td>
<td>Bitcoin exchanges, Bitcoin wallets, specialized mining HW providers</td>
<td></td>
</tr>
<tr>
<td>New services</td>
<td>Bitcoin Security, assurance, legal counseling, escrow</td>
<td>Credit card processors</td>
</tr>
<tr>
<td>Lower transaction fee, shorter transfer time</td>
<td>Merchants, consumer</td>
<td>Banks, Paypal, Master/Visa/AmExp, wiring services</td>
</tr>
</tbody>
</table>

*Figure 5: Winner and loser prediction*
National rankings consistently place UC Berkeley’s undergraduate and graduate programs among the world’s best. Berkeley is home to top scholars in every discipline, accomplished writers and musicians, star athletes, and stellar scientists—all drawn to this public university by its rich opportunities for groundbreaking research, innovative thinking and creativity, and service to society.