BitCoin & Alternative Currencies: Prospects and Legal Questions

Steve Mott
Principal
BetterBuyDesign
Topics for Today

1. What’s all the fuss about?
2. Is this stuff for real?
3. How did we get here?
4. What’s involved (BitCoin as the exemplar)?
5. What are the prospects going forward?
6. Will the legal issues get resolved?
7. What applications might exist for Treasury departments?
8. Appendices
1. What’s All the Fuss About?

• News captures public’s fancy
• Celebrities get involved
• Government steps in
• Word of mouth: YOU can make money….
• Current political environment invites a digital alternative to central bank ‘whims’
BitCoin Saga & the Search for Digital Currency

Related stories
Man bids to sell house for bitcoins
21 March, 2013
US govt clarifies virtual currency regulatory position
19 March, 2013
Bitcoin Tipper lets users tweet virtual currency
15 March, 2013
Technical glitch sparks bitcoin sell-off
12 March, 2013
MT. Gox and CoinLab team up for US Bitcoin push;
Valley Bank onboard
28 February, 2013
US State Representative adopts Bitcoin donation system
04 September, 2012
Users sue Bitcoin exchange over $460k in missing funds
13 August, 2012
Bitcoin value crashes after exchange compromise
20 June, 2011

Check out the fast rise of Bitcoin prices during the past two months in the chart below:
Bitcoin value surpasses $100 — is this another bubble?

April 1, 2013 2:30 PM
Sean Ludwig

The value of a single Bitcoin surpassed $100 today, a huge milestone for the virtual currency. But with its crazy rise in the past few months, it’s time to start seriously wondering if Bitcoin is in a bubble. Bitcoin is a virtual, decentralized currency that no government or central bank controls. As of this report, a single Bitcoin is trading at $104.50 on Mt. Gox, the largest Bitcoin exchange. In January, the currency was trading at $15 a pop.

Likely riding a massive speculation wave, Bitcoin prices exceed $200

April 9, 2013 7:38 AM
Sean Ludwig

It’s been a great past few weeks if you’re a holder (or hoarder) of Bitcoins. The value of a single Bitcoin surpassed $200 today on the Mt. Gox exchange, yet another impressive milestone for the virtual currency.
But What Goes Up, Eventually Comes Down

Bitcoin wallet service Instawallet hacked, shuts down ‘indefinitely’

April 3, 2013 12:11 PM
Sean Ludwig

Bitcoins are a hot commodity now, but are your Bitcoins actually safe? Bitcoin wallet company Instawallet has suspended its service “indefinitely” after being hacked. Bitcoin is a virtual, decentralized currency that no government or central bank controls. Several companies, including Reddit and Expensify, have recently added Bitcoin support, helping the value bubble up. The value of Bitcoin surpassed $100 per coin just two days ago, and early today it reached as high as $145. Now the price reportedly sits below $117.
Instawallet Hack Shows Odd Value Prop

Instawallet provided a way to easily set up a Bitcoin wallet that can be used to store your Bitcoins and associated data. But the company had its database “fraudulently accessed,” so it has decided to close down until it can develop a new architecture that is safe from hacking attacks.

Instawallet writes on its homepage:

INSTAWALLET SERVICE NOTICE

The Instawallet service is suspended indefinitely until we are able to develop an alternative architecture.

Our database was fraudulently accessed, due to the very nature of Instawallet it is impossible to reopen the service as-is.

In the next few days we are going to open the claim process for Instawallet balance holders to claim the funds they had stored before the service interruption.

Important information on claims submission:

For the first 90 days we will accept claims for individual Instawallets. Your wallet’s URL and key will be used to pre-populate a form to file the claim.

After 90 days, if no other claim has been received for the same url, your Instawallet balance under 50 BTC will be refunded. If several claims have been filed for the same url, we will process those claims on a case by case basis, under the presumption that the claim we received first belongs to the legitimate balance holder.
Winklevoss Twins: No ‘bail-ins’ like Cyprus; “It’s Gold 2.0!”

The Winklevoss Bitcoin Trust ETF is a notable attempt to bring access to bitcoin investing to the masses. It is still somewhat difficult to invest in bitcoins.
Peter Thiel: BTC only a 20% chance
U.S. Treasury Pulls the Plug

- Ruling on digital currency issued by U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN)
- Seizure of Mt. Gox exchange’s Dwolla funds and its subsequent decision to require authentication of its users
- Seizure and closure of Liberty Reserve—has been seen by some as the beginning of the end for such wild west monetary systems
On May 14, 2013 the Department of Homeland Security, acting in concert with FinCEN, seized the US assets of Mutum Sigillum and shuttered its business.

Liberty Reserve didn’t register either. Liberty Reserve was a Costa Rican payment processor that did not use bitcoin, but did use its own form of centralized digital currency called “Liberty Reserve Dollars”. One of its services was accepting funds from Customer A, holding those funds, and then distributing them to Customer B at Customer A’s direction using Liberty Reserve Dollars.

Like Mutum Sigillum’s business, this was also a classic example of money transmission. It serviced customers across the globe, including the United States, without collecting any of the information or making any of the reports required under the BSA.

In May, 2013, the US federal government seized the Liberty Reserve website and shut down its business, citing, among other things, its operation as an unlicensed money transmitter. The seizure notice is still on its website.
The New York Department of Financial Services (DFS) has issued subpoenas to a number of bitcoin companies requesting information about the way in which they operate and the consumer safeguards they have in place.

A memo issued by the DFS, written by department head Benjamin Lawsky, suggests it wants to work with bitcoin companies to ensure the virtual currency industry can continue to exist as a “legitimate business enterprise”. “It is in the common interest of both the public and the virtual currency industry to bring virtual currencies out of the darkness and into the light of day through enhanced transparency. It is vital to put in place appropriate safeguards for consumers and law abiding citizens,” the memo states.
## Better than Bucks, But not Gold…?

<table>
<thead>
<tr>
<th>Attribute</th>
<th>U.S. Dollar</th>
<th>Bitcoins</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Durability</td>
<td>Poor: 18-24 mos. lifetime of $100 bill</td>
<td>OK: digits exist on computers and over the Internet</td>
<td>Great: Doesn’t fade, corrode or disappear</td>
</tr>
<tr>
<td>Portability</td>
<td>Great: carried everywhere</td>
<td>OK: still need computer and Internet</td>
<td>Poor: Heavy to carry in volume, but easy to wear</td>
</tr>
<tr>
<td>Divisibility</td>
<td>OK: many denominations (but no good if torn)</td>
<td>Great: One of main attractions</td>
<td>Good: Can be transacted with in many weights</td>
</tr>
<tr>
<td>Intrinsic (value)</td>
<td>Poor: only valuable if government issuer is competent</td>
<td>Poor: digits have to be traded, like stocks</td>
<td>Great: Has borne intrinsic value throughout history</td>
</tr>
</tbody>
</table>

*Source: Tony Davis: Atlanta Gold & Coin Buyers*
Fed Attack & GS Doesn’t Control it
2. Is it for Real?

- There IS a network
- There IS information on how to use it
- It has the attention of the highest authorities
- It is real enough for the biggest state to want to shut it down
- Legally, it has been judged to be a ‘currency’—or, money!
Network Volume is Real and Growing

**Bitcoin Network**

**Economy**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total BTC</td>
<td>11,760,075 BTC</td>
</tr>
<tr>
<td>Market Cap</td>
<td>1,444,137,210 USD</td>
</tr>
<tr>
<td></td>
<td>or 1,146,254,393 EUR</td>
</tr>
<tr>
<td></td>
<td>or 4,504,226,326 PLN</td>
</tr>
<tr>
<td></td>
<td>or 984,565,239 GBP</td>
</tr>
<tr>
<td>Transactions last 24h</td>
<td>54,112</td>
</tr>
<tr>
<td>Transactions avg. per hour</td>
<td>2254.67</td>
</tr>
<tr>
<td>Bitcoins sent last 24h</td>
<td>716,353.02 BTC</td>
</tr>
<tr>
<td>Bitcoins sent avg. per hour</td>
<td>29,848.04 BTC</td>
</tr>
</tbody>
</table>

**Blocks**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>260,402</td>
</tr>
<tr>
<td>Blocks last 24h</td>
<td>174</td>
</tr>
<tr>
<td>Blocks avg. per hour</td>
<td>7.25</td>
</tr>
<tr>
<td>Difficulty</td>
<td>148,819,200</td>
</tr>
<tr>
<td>Next Difficulty in 1678 blocks</td>
<td>158,377,581</td>
</tr>
<tr>
<td>Network Hashrate</td>
<td>1133.71</td>
</tr>
<tr>
<td>Terahashes/s</td>
<td>14398.13</td>
</tr>
</tbody>
</table>

**Network Hashrate**

![Network Hashrate Graph](http://bitcoin.sipa.be/)


**Hashrate Distribution**

- BTC Guild
- BitMinter
- ASICMiner
- Eligius
- Slush
- EclipseMC
- Deepbit
- 50BTC
- Other Known
A Cult Following Exists in Market

Welcome!

Bitcoincharts provides financial and technical data related to the Bitcoin network.

Bitcoin News

- Carrie Kirby - Bitcoin Paychecks
  - 25 Sep 2013
- Video: Vacate Wall Street
  - 17 Sep 2013
- Jeffrey Tucker - Bitcoin's Brilliant Combination
  - 11 Sep 2013
- Index To Candidates For Bitcoin Foundation Board Election (Individual Seat)
  - 6 Sep 2013
- Bitcoin-Qubitcoin version 0.8.4 released
  - 6 Sep 2013
- Jonathan Stucke - Bitcoin in India
  - 6 Sep 2013
- Marco Santori - Bitcoin Law in The U.S., Part I
  - 17 Aug 2013
- Fixes For Android Mobile Bitcoin Wallets Released
  - 15 Aug 2013

LocalBitcoins.com

Buy bitcoins near Colorado Springs, United States

<table>
<thead>
<tr>
<th>Distance</th>
<th>Location</th>
<th>Price/BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3 miles</td>
<td>Colorado Springs, CO, USA</td>
<td>144.65 USD</td>
</tr>
<tr>
<td>10.9 miles</td>
<td>80920, Colorado Springs, United States</td>
<td>138.74 USD</td>
</tr>
</tbody>
</table>

FX Trading with NO LIMITS

ZuluTrade.com/ForexAutoTrade
1500 pips/Mo, ROI 1800%/Yr. Follow the Best Forex Traders.

Request an Invite

<table>
<thead>
<tr>
<th>Market</th>
<th>Price</th>
<th>Avg.</th>
<th>Change</th>
<th>30d Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtgoxUSD</td>
<td>135.8196</td>
<td>136.038</td>
<td>-0.599%</td>
<td>461643</td>
</tr>
<tr>
<td>bitstampUSD</td>
<td>125.7500</td>
<td>124.000</td>
<td>+1.407%</td>
<td>342736</td>
</tr>
<tr>
<td>bitcUSD</td>
<td>122.3020</td>
<td>121.107</td>
<td>+0.987%</td>
<td>102006</td>
</tr>
<tr>
<td>bitcCNY</td>
<td>746.5000</td>
<td>749.213</td>
<td>-0.362%</td>
<td>95194</td>
</tr>
<tr>
<td>mtgoxEUR</td>
<td>100.0000</td>
<td>101.751</td>
<td>-1.721%</td>
<td>73342</td>
</tr>
</tbody>
</table>

View all markets

Currency Converter
Trading is Tracked and Monitored
Markets Function in Real-time

<table>
<thead>
<tr>
<th>Overview</th>
<th>Currencies</th>
<th>All Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All</td>
<td>ARS AUD BGN BRL BTC CAD CHF CLP CNY CZK DKK EUR GBR GUA GBP HKD HUF ILS INR JPY KRW MYR NOK NZD PEN PLN RON RUB SAR SEK SGD DKK THB UAH USD XRP XAU ZAR</td>
</tr>
<tr>
<td></td>
<td>Symbol</td>
<td>Latest Price</td>
</tr>
<tr>
<td>▼</td>
<td>mtgoxUSD</td>
<td>135.815</td>
</tr>
<tr>
<td></td>
<td>USD Mt. Gox</td>
<td>0 min ago</td>
</tr>
<tr>
<td>▲</td>
<td>bitstampUSD</td>
<td>125.75</td>
</tr>
<tr>
<td></td>
<td>USD BHSamp</td>
<td>1 min ago</td>
</tr>
<tr>
<td>▼</td>
<td>btoeUSD</td>
<td>122.302</td>
</tr>
<tr>
<td></td>
<td>USD btoe</td>
<td>0 min ago</td>
</tr>
<tr>
<td>▲</td>
<td>bitcnyCNY</td>
<td>746.5</td>
</tr>
<tr>
<td></td>
<td>CNY bitcny.com</td>
<td>20 hrs, 14 min ago</td>
</tr>
<tr>
<td>▼</td>
<td>mtgoxEUR</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>EUR Mt. Gox</td>
<td>0 min ago</td>
</tr>
<tr>
<td>▲</td>
<td>mtgoxJPY</td>
<td>13290</td>
</tr>
<tr>
<td></td>
<td>JPY Mt. Gox</td>
<td>1 hr, 7 min ago</td>
</tr>
<tr>
<td>▼</td>
<td>btcdeEUR</td>
<td>94</td>
</tr>
<tr>
<td></td>
<td>EUR bitcny</td>
<td>0 min ago</td>
</tr>
<tr>
<td>▲</td>
<td>cbxUSD</td>
<td>124.99</td>
</tr>
<tr>
<td></td>
<td>USD Camp BX</td>
<td>48 hrs ago</td>
</tr>
<tr>
<td>▲</td>
<td>bitcurexPLN</td>
<td>380.7</td>
</tr>
<tr>
<td></td>
<td>PLN bitcurex</td>
<td>just now</td>
</tr>
<tr>
<td>▲</td>
<td>virtexCAD</td>
<td>124.4999</td>
</tr>
<tr>
<td></td>
<td>CAD Canadian Virtual Exchange</td>
<td>1 hr, 51 min ago</td>
</tr>
<tr>
<td>▼</td>
<td>virwoxSLL</td>
<td>30337</td>
</tr>
<tr>
<td></td>
<td>SLL VirWox</td>
<td>0 min ago</td>
</tr>
<tr>
<td>▲</td>
<td>btoeRUR</td>
<td>3688</td>
</tr>
<tr>
<td></td>
<td>RUR btoe</td>
<td>30 hrs ago</td>
</tr>
<tr>
<td>▼</td>
<td>mtgoxAUD</td>
<td>143.9953</td>
</tr>
<tr>
<td></td>
<td>AUD Mt. Gox</td>
<td>0 min ago</td>
</tr>
<tr>
<td>▼</td>
<td>mtgoxGBP</td>
<td>83.721</td>
</tr>
</tbody>
</table>

AFP® Annual Conference
Who is right? Winklevosses for, Peter Thiel against bitcoin

It is quite evident that when influential people talk about bitcoin, the masses listen. Strike up a conversation about virtual currencies with an everyday person in your life, and they will recall information received from major news outlets. Mainstream media likes to put things in a neat package so they’re easily understood.

A beginner's guide to bitcoin

Bitcoin is a digital currency that is being used increasingly all over the world. Find out more about how it works and how you can use it with our straightforward guides.

What is bitcoin?
It's a decentralized digital currency

Why use bitcoin?
It's fast, cheap to use, and secure
FOR IMMEDIATE RELEASE  
March 18, 2013

MEDIA CONTACT: Steve Hudak  
703-905-3770

FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities

Describes Circumstances Where "Money Transmitter" Definition Applies

VIENNA, Va. - To provide clarity and regulatory certainty for businesses and individuals engaged in an expanding field of financial activity, the Financial Crimes Enforcement Network (FinCEN) today issued the following guidance, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. The guidance is in response to questions raised by financial institutions, law enforcement, and regulators concerning the regulatory treatment of persons who use convertible virtual currencies or make a business of exchanging, accepting, and transmitting them. Convertible virtual currencies either have an equivalent value in real currency or act as a substitute for real currency.

FinCEN's rules define certain businesses or individuals as money services businesses (MSBs) depending on the nature of their financial activities. MSBs have registration requirements and a range of anti-money laundering, recordkeeping, and reporting responsibilities under FinCEN's regulations. The guidance considers the use of virtual currencies from the perspective of several categories within FinCEN's definition of MSBs.

Financial institutions with questions about this guidance should contact FinCEN's Regulatory Helpline at (800) 949-2732.

###

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.
May 30, 2013

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

BitCoin Foundation
71 Columbia Street, Suite 300
Seattle, WA 98104

Re: Warning Concerning Unlawful Conduct of Money Transmission Business

Dear Sir/Madam:

It has come to the attention of the Commissioner that BitCoin Foundation may be engaged in the business of money transmission without having obtained the license or proper authorization required by the California Financial Code.

YOU ARE HEREBY WARNED TO CEASE AND DESIST FROM CONDUCTING THE BUSINESS OF MONEY TRANSMISSION IN THIS STATE. FAILURE TO DO SO WILL RESULT IN APPROPRIATE ACTION BEING TAKEN.

Subject to certain exceptions, Financial Code § 2030 provides that no person shall engage in the business of money transmission in California without first obtaining a license from the Commissioner of Financial Institutions.

Any person who violates Financial Code § 2030 is subject to civil money penalties of $1,000 for each violation or $1,000 per day under Financial Code § 2151 and/or criminal prosecution under Financial Code § 2152. Conviction under Financial Code § 2152 could result in a fine and/or imprisonment. The California Attorney General may also institute suit pursuant to Business and Professions Code §§ 17200, 17205 and 17206, which can result in imposition of penalties of up to $2,500 per violation of statutory law (that is, per day or per transaction).

In addition, under § 1960 of Title 18 of the U.S. Code, it is a felony violation of federal law to own, control, or conduct the business of money transmission which is operated without the appropriate State license, or which fails to register with the U.S. Treasury Department, or which transmits funds known to have been derived from criminal activity or intended to be used to promote or support unlawful activity. Violations of § 1960 are punishable by up to 5 years in prison and a $250,000 fine. Additionally, this activity conducted without a license is a felony under California law, pursuant to Financial Code § 2152(b).
Bitcoin Ruled to be Real Money

Judge rules bitcoin ‘is a currency or form of money’
Published on August 7, 2013 at 13:41 BST | By Emily Spaven | News, Regulation

A judge in Texas has ruled that bitcoin is a currency or form of money, which gives the Securities and Exchange Commission (SEC) the go-ahead to sue Ponzi scheme operator Trendon Shavers. A document signed by US magistrate judge Amos L. Mazzant details the SEC’s case against Shavers, founder and operator of Bitcoin Savings and Trust (BTCST), formerly known as First Pirate Savings & Trust.
Shavers enticed people to invest in BTCST with the promise of 1% interest per day. Some investors suffered losses, totalling 263,104 BTC, which equates to around $25 million, based on current exchange rates.
The SEC asserts Shavers defrauded investors and that the BTCST investments are classed as securities, as defined by Federal Securities Laws. Shavers, however, argues the BTCST investments are not securities because bitcoin is not money, nor is it part of anything regulated by the US authorities.
The court document states: “Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money. … For these reasons, the Court finds that it has subject matter jurisdiction over this matter.
Bubble Bursts--again

FBI shuts down online drug market Silk Road

By Jose Pagliery @Jose_Pagliery October 2, 2013: 5:20 PM ET
Mt. Gox accused of violating US money transfer regulations
May 16, 2013 7:14 AM
The seizure of funds of the largest bitcoin exchange, Mt. Gox, was triggered by an alleged failure of the company to comply with U.S. financial regulations, according to a federal court document. The U.S. District Court in Maryland on Tuesday ordered the seizure of Mt. Gox's funds, which were in an account with Dwolla, a payments company that transferred money from U.S. citizens to Mt. Gox for buying and selling the virtual currency bitcoin.

Dwolla kills support for bitcoin
11 October 2013 | Finextra
Payments firm Dwolla is severing its ties with bitcoin exchanges and services, cutting off a major route for moving funds between the virtual currency and its fiat cousins.
3. How Did We Get Here?

- S&H Green Stamps got us started
- Airline miles turbo-charged the market
- Financial services firms turn miles into rewards currency
- First-generation digital currencies came and went in the early 2000s (leaving a sour taste)
In the Beginning: S&H Green Stamps
Air Travel Mileage Programs

Join Western Airlines TravelPass, The First Class Frequent Traveler Program

TravelPass: The First Class Frequent Traveler Program

Current Mileage Levels

Transaction Complete
Loyalty Points: An Old Standby

Points Values in $ Millions

<table>
<thead>
<tr>
<th>Credit Card</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express</td>
<td>$3,300</td>
<td>$3,267</td>
<td>$2,353</td>
</tr>
<tr>
<td>Capital One</td>
<td>$760</td>
<td>$1,000</td>
<td>$1,300</td>
</tr>
<tr>
<td>Discover</td>
<td>$738</td>
<td>$879</td>
<td>$1,000</td>
</tr>
</tbody>
</table>

Source: Mercator Advisory Group (from Company filings)
Digital Currencies: Come and Gone
e-Gold is an electronic currency issued by e-Gold Ltd., a Nevis corporation, 100% backed at all times by gold bullion in allocated storage.

Other e-metals are also issued: e-silver is 100% backed by e-silver, e-platinum is 100% backed by platinum, and e-palladium is 100% backed by palladium. However, the most popular e-metal (by an overwhelming margin) is e-gold.

e-Gold is integrated into an account based payment system that empowers people to use gold as money. Specifically, the e-gold payment system enables people to spend specified weights of gold to other e-gold accounts. Only the ownership changes - the gold in the treasury grade vault stays put.

In other words, e-Gold is an international payment system, which allows it’s customers to make fast, inexpensive and reliable transactions over the Internet.

The World Wide Web needs worldwide money. e-Gold was created in response to this need.
Value Access Plan
June 05, 2013

e-gold Value Access Plan – Claims Interface Now Available

We are pleased to report that the VAP Claims Process was launched June 3, 2013 ("VAP Launch") as scheduled. Starting from VAP Launch, Users have a 120 day window in which to submit a VAP Claim ending on October 1, 2013.

Upon completion of VAP CIP, a User may submit and finalize a VAP Claim as follows:

1. Submit VAP Claim
   User may submit a VAP Claim from the e-gold website by logging into their account, clicking the VAP Claim icon, and following the directions.

2. Finalize VAP Claim
   Upon VAP Claim submission, e-gold will provide User with login credentials needed to finalize their VAP Claim with Rust Consulting Inc, the E-Gold Claims Process Administrator ("Rust"). If VAP Claim is for Linked Accounts, separate login credentials will be provided for each account. User must login to Rust website with each set of login credentials to finalize their VAP Claim for each Linked Account separately.

Prior to finalizing a VAP Claim on the Rust website, User should read Rust’s Claim Filing Information to collect all information required to finalize their VAP Claim in advance. For example, Rust specifies that the payment method used to pay approved VAP Claims is determined by a) the country in which payee bank account is located and b) the amount claimed. Rust provides downloadable forms for User to collect required banking information in advance of finalizing their VAP Claim. If User does not have all required information when they begin the process of finalizing their VAP Claim, User may cancel and start again once they’ve gathered all required information, but their previously entered work...
Even the Bad Guys Like Digital Money

What is e-dinar?

e-dinar is the name of an internet based electronic payment and exchange system that facilitates online transactions 100% backed by physical gold and silver.

The physical gold and silver bullion backing e-dinar and e-dirham units are always equivalent or larger than all electronic e-dinar and e-dirham in circulation. The physical gold and silver bullion is held securely in internationally renowned bullion repositories.

Account holders always have the option to exchange their gold and silver into any major national currency or redeem them and take physical possession of an equivalent amount of gold dinar and...
**Local Currencies Arise**

<table>
<thead>
<tr>
<th>Community Currency</th>
<th>Launch</th>
<th>Exchange Rate</th>
<th>Issuance</th>
<th>Merchant Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay Bucks Traverse City, MI</td>
<td>2006</td>
<td>$1 per 1 Bay Buck</td>
<td>38,586 (start of 2012)</td>
<td>About 100 local merchants</td>
</tr>
<tr>
<td>BerkShares Southern Berkshires Region</td>
<td>2006</td>
<td>$95 per 100 BerkShares</td>
<td>More than 2.7 million</td>
<td>More than 400 businesses</td>
</tr>
<tr>
<td>Cascadia Hour Exchange (CHE) Portland, OR</td>
<td>1993</td>
<td>Varies (exchanged for services)</td>
<td>n.a.</td>
<td>Hundreds of participants</td>
</tr>
<tr>
<td>Equal Dollars Philadelphia, PA</td>
<td>1996</td>
<td>n.a. (earned through community service)</td>
<td>n.a.</td>
<td>More than 100 local businesses</td>
</tr>
<tr>
<td>Ithaca Hours Ithaca, NY</td>
<td>1991</td>
<td>$10 per 1 Ithaca Hour</td>
<td>More than 100</td>
<td>More than 900 participants</td>
</tr>
<tr>
<td>Life Dollars Bellingham and Seattle, WA</td>
<td>2004</td>
<td>Fluctuates based on local hourly living wage; 1 Life Dollar = 1 hour of time</td>
<td>Exchanges have totaled more than $1.1 million</td>
<td>n.a.</td>
</tr>
<tr>
<td>Local Trade Partners Fayetteville, AK</td>
<td>2009</td>
<td>Varies (exchanged for services)</td>
<td>n.a.</td>
<td>600 businesses</td>
</tr>
<tr>
<td>Potomacs Washington, DC</td>
<td>2009</td>
<td>95¢ per 1 Potomac</td>
<td>About 3,000</td>
<td>More than 10 businesses</td>
</tr>
</tbody>
</table>

Source: Jeffrey Greene, Mercator Advisory Group, 2013

Historically, ... for example, five local banks distribute and exchange the currency, which is valued at a 5% discount to U.S. dollars.
From virtual currencies to another form of alternative coin, we bring you the BerkShares, a type of coin that can only be used in the Berkshires, a region in western Massachusetts (USA). According to the BerkShares website, more than 400 businesses located in the Berkshires area accept the currency, while 13 banks serve as exchange stations.
Merchant-Specific: Amazon Coins

Although it’s a company-specific currency, Amazon Coins, were created after the boom of Bitcoin. They can be exchanged for some items sold on Amazon like Kindle Fire apps or games. Since it’s a new thing, you can learn more about it here.
Amazon: Counters Digital Venues

- Launched 5/2013, this currency enables Kindle Fire tablet owners to buy games, apps and in-app items
- Prepaid type of currency could be extended to mainstream purchases
- Counters trend away from virtual currency by digital venues (e.g., Facebook credits retired last month, and Microsoft ending xbox video game points)
- New users got $5 in coins (each coin is worth a penny); purchase of additional coins can generate a 10% discount
- Amazon has patented a virtual currency for mobile transacting...
Bitcoin: It’s Just Math

• Created by a mysterious programmer known as Satoshi Nakamoto
• Only 21 million bitcoins can ever be created by miners
• Divisible down to one hundred millionth of a bitcoin (called a “Satoshi”)
• The mathematical formula is open to inspection
• The software is open source
• Mining requires special computer power (and even special chips)
• It’s catching on now because it’s traded, and miners willing to work for others

Source: CoinDesk
Key Features of Bitcoin: It’s Digital

1. **decentralized.** The network isn’t controlled by one central authority. Every machine that mines bitcoins and processes transactions makes up a part of the network, and the machines work together. That means that, in theory, one central authority can’t tinker with monetary policy and cause a meltdown—or simply decide to take people’s bitcoins away from them, as the Central European Bank decided to do in Cyprus in early 2013. And if some part of the network goes offline for some reason, the money keeps on flowing.

2. **easy to set up.** Conventional banks make you jump through hoops simply to open a bank account. Setting up merchant accounts for payment is another Kafkaesque task, beset by bureaucracy. You can set up a bitcoin address in seconds, no questions asked, and no fees.

3. **anonymous.** Well, kind of. Users can hold multiple bitcoin addresses, and they aren’t linked to names, addresses, or other personally identifying information.

4. **transparent.** Bitcoin stores details of every single transaction that ever happened in the network in a huge version of a general ledger, called the block chain. The block chain tells all. If you have a publicly used bitcoin address, anyone can tell how many bitcoins are stored at that address. They just don’t know that it’s yours.

5. **Transaction fees are miniscule.** Your bank may charge you a £10 fee for international transfers. Bitcoin doesn’t.

6. **fast.** You can send money anywhere, and it will arrive minutes later, after the bitcoin network processes the payment.

7. **non-repudiable.** When your bitcoins are sent, there’s no getting them back unless the recipient sends them to you—they’re spent.

Source: CoinDesk
Ideal for Gambling (and Adult Fare)

- Payment is fast
- Bets can be small, with immediate returns or losses
- Bets can be verified (by tracking payouts in the blockchain or recording cash inputs to random numbers)
- SatoshiDice is the most popular online gambling site: users mail money to one of a set of addresses, and get a payout based on probability of winning
- PeerBet, Just-Dice, BetCoin Dice and Satoshi Circle are other betting sites of note

Source: CoinDesk
Merchant Adoption Still Small

- **Bitcoinshop.us** offers products from air-conditioners through to watches, all priced in bitcoin, for those in U.S. wanting to make a purchase
- **Coindays** offers electronic products such as laptops, cameras, and TVs for sale in bitcoin, and ships internationally
- **All Things Luxury** offers a range of jewelry items, and **Keystone Pet Place** will handle your pet needs with a variety of products
- For more examples of physical merchants, check out **Spendbitcoins.com**
- **Bitcoin.Travel** is a respected site, offering a mappable list of accommodations, apartments, attractions, bars, and beauty salons around the world. **Coinmap** is another, and **UseBitCoins** also offers a list, although this site extends further, covering services and other goods, too
- Notable taverns, such as the **Pembury Tavern** in London, and the **Old Fitzroy** pub in Sydney, Australia, have become beacon sites for bitcoin
- **Foodler**, a site enabling you to browse and order delivery and take-out meals from restaurants across the globe, has 13,000 restaurants in 3,150 cities on its books. You can use bitcoins to pay for ‘Foodler credits’, which can be used at any of the restaurants
- **Bitcoin-Kiez** in Berlin is persuading local establishments in small numbers along the Graefekiez there to support bitcoin.
Bitcoin Marketplaces Emerging

• **Bitmit**, an eBay-style site that features auctionable items, along with the now-familiar ‘buy it now’ option seen on eBay.
• **Coingig** enables people to set up their own bitcoin-based stores online, which are often specialized. It features stores with specialties ranging from survivalist gear, to sunglasses.
• **Bitcoin Market** and **Cryptothrift** are two category-driven sites, albeit sparsely populated.
• **Flibbr** was in pre-testing at the time of writing, but will allow you to search listed products by name.
• Reddit offers a subthread called **Bitmarket**, that allows people to list their goods as Reddit posts.
• Specialist site **BitPremier** will enable you to sell your high-end luxury items with bitcoins, using an escrow service. Items listed at the time of writing included a 2012 motorhome, a 2009 Porsche, and a 3.5 story office building in Bali.

Source: **CoinDesk**
Silk Road: Popular Bitcoin Site for Purchasing Contraband
Transaction Fees? It Depends

• Some bitcoin wallets enable manual settings for fees
• Most miners process transactions for free now
• But any portion of a transaction that isn’t borne by a recipient or returned as change can become a reward for the miner
• Coming version 0.9 will make payments more user-friendly
• Payment processors like BitPay offer advanced features like receipts and order confirmations

Source: CoinDesk
5. Prospects Going Forward?

• Exchanges getting funded, but how many will survive?
• Mainstream funding and conversion will help
• Self-regulation is emerging
• New infrastructure providers are lending stability
# Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitomat</td>
<td>PL</td>
<td>4/11 – 8/11</td>
<td>758</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>21.7</td>
</tr>
<tr>
<td>FreshBTC</td>
<td>PL</td>
<td>8/11 – 9/11</td>
<td>3</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>21.7</td>
</tr>
<tr>
<td>Bitcoin7</td>
<td>US/BG</td>
<td>6/11 – 10/11</td>
<td>528</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>33.3</td>
</tr>
<tr>
<td>ExchangeBitCoins.com</td>
<td>US</td>
<td>6/11 – 10/11</td>
<td>551</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>34.3</td>
</tr>
<tr>
<td>Bitchange.pl</td>
<td>PL</td>
<td>8/11 – 10/11</td>
<td>380</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>21.7</td>
</tr>
<tr>
<td>Brasil Bitcoin Market</td>
<td>BR</td>
<td>9/11 – 11/11</td>
<td>0</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>24.3</td>
</tr>
<tr>
<td>Aqoin</td>
<td>ES</td>
<td>9/11 – 11/11</td>
<td>11</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>30.7</td>
</tr>
<tr>
<td>Global Bitcoin Exchange</td>
<td>?</td>
<td>9/11 – 1/12</td>
<td>14</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>27.9</td>
</tr>
<tr>
<td>Bitcoin2Cash</td>
<td>US</td>
<td>4/11 – 1/12</td>
<td>18</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>34.3</td>
</tr>
<tr>
<td>TradeHill</td>
<td>US</td>
<td>6/11 – 2/12</td>
<td>5082</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>34.3</td>
</tr>
<tr>
<td>World Bitcoin Exchange</td>
<td>AU</td>
<td>8/11 – 2/12</td>
<td>220</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>25.7</td>
</tr>
<tr>
<td>Ruxum</td>
<td>US</td>
<td>6/11 – 4/12</td>
<td>37</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>34.3</td>
</tr>
<tr>
<td>btctree</td>
<td>US/CN</td>
<td>5/12 – 7/12</td>
<td>75</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>29.2</td>
</tr>
<tr>
<td>btce.com</td>
<td>RU</td>
<td>9/10 – 7/12</td>
<td>528</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>27.7</td>
</tr>
<tr>
<td>IMEX.com</td>
<td>SC</td>
<td>7/11 – 10/12</td>
<td>2</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>11.9</td>
</tr>
<tr>
<td>Crypto X Change</td>
<td>AU</td>
<td>11/11 – 11/12</td>
<td>874</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>25.7</td>
</tr>
<tr>
<td>Bitmarket.eu</td>
<td>PL</td>
<td>4/11 – 12/12</td>
<td>33</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>21.7</td>
</tr>
<tr>
<td>bitNZ</td>
<td>NZ</td>
<td>9/11 – pres.</td>
<td>27</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>21.3</td>
</tr>
<tr>
<td>ICBIT Stock Exchange</td>
<td>SE</td>
<td>3/12 – pres.</td>
<td>3</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>27.0</td>
</tr>
<tr>
<td>WeExchange</td>
<td>US/AU</td>
<td>10/11 – pres.</td>
<td>2</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>30.0</td>
</tr>
<tr>
<td>Vircurex</td>
<td>US?</td>
<td>12/11 – pres.</td>
<td>6</td>
<td>no</td>
<td>yes</td>
<td>–</td>
<td>27.9</td>
</tr>
<tr>
<td>btc-e.com</td>
<td>BG</td>
<td>8/11 – pres.</td>
<td>2604</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>32.3</td>
</tr>
<tr>
<td>Mercado Bitcoin</td>
<td>BR</td>
<td>7/11 – pres.</td>
<td>67</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>24.3</td>
</tr>
<tr>
<td>Canadian Virtual Exchange</td>
<td>CA</td>
<td>6/11 – pres.</td>
<td>832</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>25.0</td>
</tr>
<tr>
<td>btccchina.com</td>
<td>CN</td>
<td>6/11 – pres.</td>
<td>473</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>24.0</td>
</tr>
<tr>
<td>bitcoin-24.com</td>
<td>DE</td>
<td>5/12 – pres.</td>
<td>924</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>26.0</td>
</tr>
<tr>
<td>VirWox</td>
<td>DE</td>
<td>4/11 – pres.</td>
<td>1668</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>26.0</td>
</tr>
<tr>
<td>Bitcoin.de</td>
<td>DE</td>
<td>8/11 – pres.</td>
<td>1204</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>26.0</td>
</tr>
<tr>
<td>Bitcoin Central</td>
<td>FR</td>
<td>1/11 – pres.</td>
<td>118</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>31.7</td>
</tr>
<tr>
<td>Mt. Gox</td>
<td>JP</td>
<td>7/10 – pres.</td>
<td>43230</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>22.7</td>
</tr>
<tr>
<td>Bitcurex</td>
<td>PL</td>
<td>7/12 – pres.</td>
<td>157</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>21.7</td>
</tr>
<tr>
<td>Kapiton</td>
<td>SE</td>
<td>4/12 – pres.</td>
<td>160</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>27.0</td>
</tr>
<tr>
<td>bitstamp</td>
<td>SL</td>
<td>9/11 – pres.</td>
<td>1274</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>35.3</td>
</tr>
<tr>
<td>InterSango</td>
<td>UK</td>
<td>7/11 – pres.</td>
<td>2741</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>35.3</td>
</tr>
<tr>
<td>Bitfloor</td>
<td>US</td>
<td>5/12 – pres.</td>
<td>816</td>
<td>yes</td>
<td>no</td>
<td>–</td>
<td>34.3</td>
</tr>
<tr>
<td>Camp BX</td>
<td>US</td>
<td>7/11 – pres.</td>
<td>622</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>34.3</td>
</tr>
<tr>
<td>The Rock Trading Company</td>
<td>US</td>
<td>6/11 – pres.</td>
<td>52</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>34.3</td>
</tr>
<tr>
<td>bitme</td>
<td>US</td>
<td>7/12 – pres.</td>
<td>77</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>34.3</td>
</tr>
<tr>
<td>FYB-SG</td>
<td>SG</td>
<td>1/13 – pres.</td>
<td>3</td>
<td>no</td>
<td>no</td>
<td>–</td>
<td>33.7</td>
</tr>
</tbody>
</table>

Survival Probabilities Wane Over Time

Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk

**Fig. 1.** Empirically-derived survival probability function for Bitcoin exchanges.

Mainstream Funding Could Help

In May 2013, BitPay announced a partnership with merchant gift card company Gyft, whose cards are offered by more than 50,000 U.S. retail locations. Under the Gyft/BitPay arrangement, consumers may spend bitcoins using the Android mobile version of Gyft’s merchant gift cards. In so doing, consumers may use bitcoins to buy from Target.com or Amazon.com, thus bringing the currency closer to mainstream use, though with a proprietary gift card in the middle.
Self-Regulation Emerges

DATA: Digital Asset Transfer Authority

Send & Share Large Files with Only a Web Browser

Large File Transfer
ShareFile/Large-File-Transfer

Free Trial: Large File Transfer. Voted Best for Business - Try Now!

bitcoin-square.com / By Stephen Reed / August 1, 2013

On July 30th, 2013, pioneers of the digital cryptography-based payments industry, including such names as Chris Larsen, CEO of OpenCoin; Tony Garlipp, CEO of BitPay, and Neij Kodz, CEO of BitStamp, jointly established the Digital Asset Transfer Authority, or DATA.

DATA aims to become a formal self-regulatory organization (SRO) for the "emerging payments and virtual currency" industry. The official announcement on info.dataauthority.org states that DATA will "develop best practice anti-money laundering, ... business and technical standards for the prudent and responsible conduct of payment transactions," continuing that the organization will work with authorities and industry stakeholders to "identify and address emergent public policy concerns and risks affecting (the virtual currency industry)."

READ MORE

August 4th, 2013 / Tags: assets, chris larsen, DATA, Neij Kodz, SRO, TONY GALLIPPIE, virtual currency / Category: Uncategorized

0 comments

Leave a message...

No one has commented yet.
Infrastructure Companies Offer Stability

BitPay has now helped over 10,000 merchants across the world accept payments in bitcoin.

The company, which was founded in 2011, only approved its 1,000th company this time last year, so it has experienced a huge surge in business over the past 12 months.

Of the merchants that use BitPay, some 50% are located in North America and 25% are in Europe. Over 90% of the merchants using the payment service provider are ecommerce businesses, and BitPay also counts blogging platform WordPress among its clients.

Tony Gallippi, co-founder and CEO of BitPay, said: “Our largest merchants are selling high-ticket items such as computers, electronics, jewellery, precious metals and bitcoin mining equipment.”

He went on to say these businesses are more likely to get hit by criminals using stolen credit cards, so they are attracted by the prospect of accepting bitcoins as doing so reduces their risk.
Your dollars are no good here.
Our mission is to grow the number of people using bitcoin, and merchants accepting it.

For Individuals
Enjoy the group buying power of the bitcoin community.

For Business
We accept bitcoin and pay you in dollars.
Interested in selling to our community of bitcoiners?

For Everyone
Build the bitcoin economy by creating short term deals available only in BTC.

Get in touch

Awesome Bitcoin deals?! Be the first to know!

Awesome Bitcoin deals?! Be the first to know!
6. Will Legal Issues be Resolved?

- FinCEN ruling applies Money Transmitter rules (e.g., AML, KYC)
- Other regulators jumping in (CFTC, SEC,…)
- Taxation issues loom (always a killer)
- Does the rush of legal scrutiny foretell the move to mainstream?
FINCEN Ruling Invokes Money Transmitter Rules

Individuals who merely exchange bitcoin for goods and services (and vice versa) are merely “users” of a virtual currency, not money transmitters.

Businesses that accept bitcoin from one person and send it to another are money transmitters, and are not exempt from money transmission regulation simply because they do not deal in fiat currency.

Individual bitcoin miners who convert their “created” coins to fiat are money transmitters, even though they never act “as a business,” nor accept value from one person to transfer it to a third person.

Any business that exchanges fiat currency for virtual currency – or even one virtual currency for another – is a money transmitter.

MTBs must enforce Anti-Money Laundering (AML) and Know Your Client (KYC) measures, identifying the people that they’re doing business with.

Source: CoinDesk
Other Regulators Jump In

**CFTC**
The US Commodity Futures Trading Commission (CTFC), which looks after financial derivatives, hasn’t announced regulation yet, but has made it clear that it could if it wanted to.

Various governments are considering whether to set rules for digital currencies such as bitcoin. In May 2013, Bart Chilton, one of five commissioners at the Commodity Futures Trading Commission, announced he was considering whether bitcoin should be subject to the agency’s rules. He had asked commission staff to explore whether consumers needed more protections given the bitcoin’s instability.

**SEC**
The US Securities and Exchange Commission (SEC) hasn’t issued solid regulations on virtual currencies, but its Office of Investor Education and Advocacy published an investor alert to warn people about fraudulent investment schemes involving bitcoin. In particular, it warned of Ponzi schemes, after charging Texas resident Trendon T Shavers, aka ‘pirateat40’, founder and operator of Bitcoin Savings and Trust, with allegedly raising 700,000 bitcoins by promising investors up to 7% weekly interest.
Taxation Issues Loom

- In 2009, the US Internal Revenue Service (IRS) posted information about the tax applications of using virtual currencies inside virtual economies, arguing that taxpayers can receive income from a virtual economy and could be required to report it as taxable income. However, it based this largely on guidance related to bartering, gambling, business, and hobby income.
- However, the IRS has not yet posted guidance on ‘open flow’ virtual currencies that can be used outside of virtual economies. In a 27-page report [PDF] published in May 2013, the US General Accounting Office (GAO) called for more guidance from the IRS on this issue.
- The IRS responded that its guidance could now be taken to cover virtual currencies as used outside of virtual economies. It added that it was also looking at the potential tax compliance risks posed by anonymous electronic payment systems, and was working with other federal agencies on the topic.
- In June 2013, the director of an IRS unit that investigates cyber threats also told the Financial Times that the use of “cyber-based currency and payment systems” to hide unreported income from the IRS is a threat that it was “vigorously responding to”. In short, don’t expect to evade taxes by earning bitcoins instead of fiat currency.

Source: CoinDesk
7. Applications for Treasury Departments?

- International transfers?
- Intra-company transfers?
- Tax ‘protection’ events and activities?
- Avoidance of repatriation complications?
- Procurement in ‘sensitive’ countries?
- Foreign exchange arbitration/protection?
- Hedging (including against central banks)?
BBD: Management Advising for the Digital Transacting Realm

dba CSI Management Services, Inc.
1386 Long Ridge Road
Stamford, CT 06903
and 1214 Querida Drive
Colorado Springs, CO 80909
(o) 203.968.1967
(c) 203-536.0588
email: stevemottusa@yahoo.com
website: www.betterbuydesign.com
Appendix A: Bitcoin Details

- Who created it?
- Did he/they cash in?
- How to acquire bitcoins
- How to store them
- Transactions tracked in a block
- Unique hash linking preserves validity
- ‘Proof-of-work’ prevents unrestrained mining
Who Created It?

- A software developer called Satoshi Nakamoto proposed bitcoin, which was an electronic payment system based on mathematical proof. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.
- Instead, bitcoin is created digitally, by a community of people that anyone could join. Bitcoins are ‘mined’, using computing power in a distributed network. This network also processes transactions made with bitcoins, effectively making bitcoin its own payment network.
- Satoshi published a paper via the Cryptography Mailing List in November 2008. He then released the first version of the bitcoin software client in 2009, and participated with others on the project via mailing lists, until he finally began to fade from the community toward the end of 2010.
- Does anyone know who he really was? No, but the detective techniques that people use when guessing are sometimes even more intriguing than the answer. The New Yorker’s Joshua Davis believed that it was Michael Clear, a graduate cryptography student at Dublin’s Trinity College. He arrived at this conclusion by analyzing 80,000 words of Nakamoto’s online writings, and searching for linguistic clues. He also suspected Finnish economic sociologist and former games developer Vili Lehdonvirta. Both have denied it.
An analysis by Sergio Lerner, an authority on bitcoin and cryptography, suggests that Satoshi mined many of the early blocks in the bitcoin network, and that his fortune in unspent coins is equivalent to at least $100 million.

What is he doing now?

No one knows what Satoshi is up to, but one of the last emails he sent to a software developer, dated April 23 2011, said “I’ve moved on to other things. It’s in good hands with Gavin and everyone.”

Source: CoinDesk
How to Acquire Bitcoins

You can buy bitcoins from regulated exchanges, or directly from other people selling them, either online, or on the street. You can pay for them in a variety of ways, ranging from cash to wire transfers, depending on who you are buying them from.

So, you’re interested in bitcoins, but you don’t want to invest in the mining equipment to generate your own (or perhaps the mining company only accepts payment in bitcoin, leaving you in a catch-22 situation). Clearly, you need to buy some bitcoins from someone else, but where do you start? Some shops in your city may display “Bitcoin Accepted Here” signs, but you don’t see any of them offering to sell you any.

1. Via ‘traditional’ Bitcoin exchanges (Mt. Gox, Bitstamp)
2. Over-the-counter exchanges (LocalBitCoins.com, Bitcoinary)
3. Direct Payments (CoinBase)
4. In-person (e.g., MeetUp.com)
5. Gift cards (gyft, Starbucks UK (IcedMocha), and Amazon (GiftcardBTC). Some sites, such as BitCC and Cryptcard, will exchange bitcoins for disposable prepaid debit cards.

Source: CoinDesk
How to Store Them

• Bitcoin wallets store the private keys you need to access a bitcoin address to spend your funds
• The form of the wallets depend on the device
• Securing and backing up wallets are essential (they are like money: if lost, too bad)
• Paper storage is also available

Source: CoinDesk
Transactions Tracked in a ‘Block’

- All transactions in a set period are collected into a list, called a block.
- Miners confirm those transactions, and write them into a general ledger.
- The GL is a long list of blocks, known as a ‘chain’; additions are communicated in updates to all participants.
- Miners examine each new block of transactions, applying a mathematical formula.
- The formula converts the information into a hash, which is stored at the end of the block chain.

Source: CoinDesk
Unique Hash Linking Preserves Validity

- It is very easy to produce a hash from a large amount of data, but each hash is unique. If you change just one character in a bitcoin block, its hash will change completely.
- Miners don’t just use the transactions in a block to generate a hash. Some other pieces of data are used too. One of these pieces of data is the hash of the last block stored in the blockchain.
- Because each block’s hash is produced using the hash of the block before it, it becomes a digital version of a wax seal. It confirms that this block – and every block after it – is legitimate, because if you tampered with it, everyone would know.
- If you tried to fake a transaction by changing a block that had already been stored in the blockchain, this would change that block’s hash. If someone checked the block’s authenticity by running the hashing function on it, they’d find that the hash was different from the one already stored along with that block in the blockchain. The block would be fake!
- Because each block’s hash is used to help produce the hash of the next block in the chain, tampering with a block would also change the next block’s hash. So tampering with a block would make the subsequent block’s hash wrong, too. That would continue all the way down the chain, throwing everything out of whack.
‘Proof-of-Work’ Prevents Unrestrained Mining

• That seals off a block—something that miners compete with each other to do
• Each successful hash earns the miner a reward of 25 bitcoin, and is communicated to the participants
• To avoid a deluge of mining, the protocol requires ‘a proof of work’: the hash has to look a certain way, it must have the correct number of zeroes at the start
• The form and content of a hash is unpredictable

Source: CoinDesk
Appendix B: A Tour of Digital Currencies

- Litecoin
- Namecoin
- Philadelphia Equal Dollars
- Ithaca (NY) Hours
- Linden Dollars
- Ven
- Feathercoin
- WebMoney
- Ripple
- PPcoin
- (many more—120 counted by BoozAllen’s Scott Dueck)
Litecoin: Bitcoin, but 4x More of Them

Litecoin

Aims to be easier to mine than Bitcoin, opens more often, and requires far less computer power. It is mined by a process that involves individuals using their computing power to roll digital dice. A certain rare combination of those dice will “unlock” a “block” of coins and those coins become the property of the miners.

It’s like Bitcoin’s cousin. Litecoin is another form of virtual currency based on the Bitcoin model, but with a higher limit: there can only be 21 million Bitcoins, but Litecoins can reach the mark of 84 million Litecoins.
A Namecoin like system was first described in 2010 and although it was created to be a cryptocurrency, today it’s mainly used as a decentralized DNS. Namecoin “is a cryptocurrency which also acts as an alternative, decentralized DNS, which would avoid domain name censorship by making a new top level domain outside of ICANN control, and in turn, make internet censorship much more difficult, as well as reduce downages”, it’s possible to read here.
Like the Berkshires region, Philadelphia also keeps promoting its local currency, called Equal Dollars. When you sign up to participate, you receive 50 Equal Dollars. Then, to earn more, you can offer your own possessions in an online marketplace, volunteer or refer friends.
“Ithaca Hours help to keep money local, building the Ithaca economy. It also builds community pride and connections. Over 900 participants publicly accept Ithaca Hours for goods and services”, it’s possible to read on the official currency’s website. Ithaca Hours is another form of hyperlocal currency, only usable in Ithaca, New York.
Second Life: Linden Dollars

Linden Dollars can only be used in the online community Second Life. This alternative currency can be bought with traditional currency or earned in other ways like selling goods or offering services to other community users.
Ven: Bid to be Global Currency

Ven is a global digital currency for everyone.

Debuted as a Facebook app in 2007; acquired by Thomson Reuters in 2011; trading available on half-million terminals; price set based on basket of currencies, commodities and carbon futures; Nike first to sell carbon offsets with Ven.
Feathercoin: 4X Bigger Than Litecoin

Investment vehicle with block reward of 200 coins, and a total limit of 336 million coins.

Visit us at: www.feathercoin.com

Source: dailydot.com
WebMoney: Russian, Very Private

Founded in 1998 as an in-system currency; Goods offered for sale, or “valuables of various legal nature” as they put it on their About page, are stored with “guarantors,” entities who agree to store valuable properties from bonds and transfer them when the WebMoney units are transferred. A benefit of WebMoney, and an aspect that makes it more of a payment system than an independent currency, is how it is tied to fiat currencies. One WMZ, for instance, is always going to be worth $1.00.
Ripple (Open Coin): Going Open Source

On July 2nd, Ripple.com announced the Bitcoin Bridge. This means that anybody with a ripple wallet can now send bitcoins to any bitcoin wallet. Like with other types of transfers on Ripple, you can originate the transaction in any currency, it will be exchanged into bitcoin at the best rate, and it will be delivered to the bitcoin address you indicated.

1. Enter a Bitcoin address.
2. Enter an amount.
3. Pick a currency.
4. Send.

Conclusion:

The Ripple Network will likely change the way money is handled in the world. By opening a Ripple Wallet, everybody gets access to the global currency market including digital currencies like bitcoin.

It works like email, but with money instead of messages. You can send and receive any currency like yen, pound, rubles, bitcoins or dollars. To and from
PPcoin, also known as PeerCoin and Peer-to-Peer Coin can be traded not only for fiat currencies but also for other digital currencies.

Like Bitcoin, Litecoin, and Feathercoin, PPcoin increases itself via mining. However, it uses a proof-of-stake system to prevent monopolies on the currency. Proof-of-stake ensures that if a miner, for instance, has 0.5 percent of the existing currency, he or she will only be allowed to mine 0.5 percent of the outstanding currency, making it much more difficult to secure a monopoly on the currency.

As over time the mining difficulty increases on a currency like Bitcoin, fewer people will mine. Eventually, one person or group could come to possess 51 percent of the currency.
Since, as Ars Technica notes, the system that vets the currency recognizes the blockchain that is recognized by the most mining nodes; once you secure 51 percent (and have the most mining nodes) you could theoretically produce counterfeit currency, something no one can do at present.

Source: dailydot.com