Taylor Spencer
Advanced Technical Writing
Dr. Frith
05/13/15

# Final Project Outline

1. Introduction – What is Bitcoin?
   a) Bitcoin is a revolutionary invention.
      - What is Bitcoin, you might ask?
        - Bitcoin is described as "a purely peer-to-peer version of electronic cash" backed by an "ongoing chain of hash-based proof-of-work" (Nakamoto, 2008a, p. 1).
        - People who want to use Bitcoin can install a program on their computer that implements the Bitcoin protocol or create an account on a website that runs the Bitcoin client for its users (Grinberg, 2011, pp. 4–5).
        - To prevent users from double-spending their Bitcoins, the Bitcoin system records every transaction made with Bitcoin, and sends it to every node in the network, creating "a distributed system with no single point of failure" (Maurer, Nelms, & Swartz, 2013, p. 4; Nakamoto, 2009).
      - While users of Bitcoin can see a record of all transactions from all accounts, they cannot trace these transactions to individual users (Grinberg, 2011, p. 6).
        - These records are stored in the blockchain (Eyal & Sirer, 2014, p. 1).

   b) How is Bitcoin valuable?
      - Bitcoins have no intrinsic value, but they are considered valuable because they are computed from increasingly difficult math problems whose supply diminishes by one half almost every four years (Smith & Weismann, 2014, p. 2).
      - The process of creating these Bitcoins is called mining, where people run a software that solves difficult cryptographic problems, called a Bitcoin miner, on their computers (Harvey, 2015, p. 4; Taylor, 2013, p. 2).
        - The supply of Bitcoin is tied to the rate of discovery of prime numbers by the miners, and is promised never to exceed 21 million Bitcoins (Van Alstyne, 2014, p. 2).
      - Most mining occurs in pools where people join forces in reward for a cut of a new block of Bitcoin (Harvey, 2015, p. 4).
        - These pools are necessary because the many professional engineers and programmers that mine for Bitcoin serve to prevent average ordinary people from individually mining Bitcoin on their computers (Iwamura, Kitamura, & Matsumoto, 2014, p. 7).

   c) Bitcoin has a long, storied history filled with interesting characters, growth and collapse, and conspiracies.
      - Let's start with the whitepaper that started it all.

Taylor Spencer
Advanced Technical Writing
Dr. Frith
05/13/15

2. The History of Bitcoin
   a) Invention
      - On November 1, 2008, a person, under the alias of Satoshi Nakamoto, posted a paper to the Cryptography mailing list detailing a completely peer-to-peer cryptocurrency system (Nakamoto, 2008b; Taylor, 2013, p. 2).
        - This crytocurrency system would have five main properties: There would not be a mint or any other trusted parties, new coins would be made from a Hashcash-style proof-of-work, participants could be anonymous, a peer-to-peer network would be used to prevent double-spending, and the network used to prevent double-spending would be powered by the same proof-of-work used for new coin generation (Nakamoto, 2008b).
      - However, this person did not sit back and leave this idea as theory; they worked on an implementation of this cryptocurrency until, on January 3, 2009, they had created the "Genesis Block", or the first Bitcoin ("Bitcoin Block #0," 2009; Šurda, 2014, p. 3).
        - This person continued to tweak and perfect this software until February 11, 2009, when they made a post to the P2P Foundation forum to announce the release of Bitcoin, an open-source implementation of this peer-to-peer cryptocurrency (Nakamoto, 2009).
   b) Period of Relative Obscurity
      - However, Bitcoin would continue to languish in relative obscurity for a good while longer.
        - This obscurity, however, meant that the coins were undervalued and could be purchased in large amounts for very little money.
      - In 2009, Gavin Andresen, a coder from New England, did just that: To promote Bitcoin, he bought 1,000 Bitcoins for $50 and created a site called the Bitcoin Faucet, where he gave away his Bitcoins in increments of .05 BTC per user (Grinberg, 2011, p. 9; Offer, 2014, p. 3).
      - On May 22, 2010, another milestone for Bitcoin was made: Laszlo Hanyecz, a programmer from Florida, purchased two pizzas for 10,000 Bitcoins, in what is widely considered to be the first purchase made with Bitcoin (laszlo, 2010; Offer, 2014, p. 3; Šurda, 2014, pp. 4–5).
        - In hindsight, this purchase may have been ill-advised, as according to Wolfram Alpha, this amount of Bitcoins is now worth $2.359 million US dollars ("10,000 BTC to USD," n.d.).
        - Incidentally, you can now buy a pizza with Bitcoins from PizzaForCoins.com, though for much less than Laszlo paid for his two pies (Luther & Olson, 2013, pp. 5–6).

Taylor Spencer
Advanced Technical Writing
Dr. Frith
05/13/15

c) Bumpy Road
- The road to prominence for Bitcoin, however, would prove to be a long and hard road, with many bumps along the way.
- On August 6, 2010, a vulnerability was found in the Bitcoin software and was exploited to create 184 billion Bitcoins and send them to two people (Firică, 2014, p. 39).
  - Within hours, this costly bug was fixed, a new version was pushed out to the Bitcoin network, and the erroneous transactions were erased from the ledger (Firică, 2014, p. 39).
- However, the government was beginning to take note of Bitcoin.
  - Later that year, the Financial Action Task Force put out a report warning that digital currencies could be used as a financing mechanism by terrorist groups (Financial Action Task Force, 2010).
  - While this report never mentioned Bitcoin by name, it mentioned many of its aspects, including anonymity and exchanges.

d) Rise to Prominence
- Almost on cue, people and services began to take advantage of Bitcoin's anonymity.
  - On June 14, 2011, WikiLeaks, the site made famous for leaking 251,287 U.S. diplomatic cables, began taking Bitcoin donations after its accounts were frozen, eventually taking in approximately 3,889.91 Bitcoins, or $958,800 US dollars, from its public address alone ("3,889.91677164 BTC to USD," n.d., "1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v," n.d.; Greenberg, 2011; WikiLeaksVerified account, 2011).
  - Additionally, Silk Road, a Tor darkweb site exposed by Gawker on June 1, 2011, but undoubtedly existing earlier, allowed people to buy and sell drugs with Bitcoin, at least until October 2, 2013, when the FBI shut it down and arrested its owner (Chen, 2011; Christin, 2013, p. 2; Thomas, 2013).
- These events, however, caused many people to learn about Bitcoin for the first time, suggesting that, for Bitcoin, any publicity is good publicity.

e) Series of Hacks and Crashes
- However, a series of hacks and crashes would soon come that would test Bitcoin even more than before.
  - First, what was then the largest Bitcoin exchange, Mt. Gox, would be hacked by a mischievous individual, who would reduce the price for Bitcoin to 1 cent and transfer 25,000 Bitcoins into a single account (Mick, 2011).
  - This would be followed by Bitomat, then the third-largest Bitcoin exchange, having to shut down after losing their Bitcoin wallet and the 17,000 Bitcoins in it ("New Bitcoin Crisis?," 2011).

    - Shortly after this, MyBitcoin would fall victim to a hack, causing them to lose 78,000 Bitcoins, or 51 percent of their deposits ("New Bitcoin Crisis?," 2011).
  - This unfortunate series of events likely caused the value of Bitcoin to crash from $33 all the way down to $2.51 (Bonn, 2011).
    - Mt. Gox would eventually recover from this attack, and even buy Bitomat and absorb their clients' losses, but this wouldn't be the first time Mt. Gox would suffer losses, and next time they wouldn't be so lucky (Dotson, 2011; McMillan, 2014).

f) Milestones
  - While Bitcoin users were reeling from a series of collapses and crashes of the cryptocurrency's institutions, Bitcoin itself quietly passed a milestone.
    - On June 24, 2011, with the mining of block 133056, the difficulty of mining Bitcoin climbed over 1,000,000 for the first time ("Bitcoin Block #133056," 2011; Taylor, 2013, p. 3).
  - During this time, Bitcoin would pass another milestone: It would go mobile.
    - On July 19, 2011, the first Bitcoin transaction over NFC would occur (Blackman, n.d., p. 3).
    - This would be followed by the release of the first Bitcoin app, BitCoins Mobile, on July 22, 2011 by Intervex Digital (Blackman, n.d., p. 3).
  - Additionally, a culture would start to develop around Bitcoin.
    - 2011 would see the first Bitcoin Conference and World Expo, and the first European Bitcoin Expo, and in 2012 the first issue of Bitcoin Magazine would be published (Blackman, n.d., p. 3).

g) From Saving to Spending
  - All this means that more businesses would begin to accept Bitcoin, causing the habits of Bitcoin holders would shift from saving to spending their Bitcoins.
    - In the early days, this would consist primarily of legally-questionable services, such as Satoshi Dice, a gambling site, which would account for approximately 50% of Bitcoin transactions around 2012 (Hurlburt & Bojanova, 2014, p. 3; Meiklejohn et al., 2013, p. 8).
  - But as the currency grew, more local and online businesses, from Overstock.com to a Subway in Allentown, PA, began to accept Bitcoin (Luther & White, 2014, p. 6; Morganteen, 2013; Van Alstyne, 2014, p. 1).
    - Bitcoin provides several advantages for businesses, including a lack of transaction fees (Halligan, 2014).
    - Additionally, it gives these businesses an advantage over their competitors, causing customers to come from miles and spend more (Halligan, 2014; Morganteen, 2013; Van Alstyne, 2014, pp. 1–2).

h) Today
- This takes us to the present day.
  - Bitcoin is accepted by a fair amount of businesses, both online and offline, and there are even Bitcoin ATMs, where Bitcoin holders can exchange their Bitcoins for cash or vice versa, though they are not nearly as widely available as bank ATMs (Jervis, 2014; Luther & White, 2014, p. 6; Morganteen, 2013; Van Alstyne, 2014, p. 1).
- However, Bitcoin remains threatened, both by hackers and by government agencies, as I will detail later in this paper.

3. Spin-off Currencies

a) Of course, anything that is successful is bound to inspire followers, and Bitcoin is no exception.
- In fact, Bitcoin's nature as open-source software serves to encourage this, as anyone can fork the Bitcoin software, stick a new face on it, and say they have released a new cryptocurrency.
- However, there are two cryptocurrencies that are of particular importance because they have managed to gain a significant following: Litecoin and Dogecoin.

b) Litecoin
- Litecoin is a Bitcoin fork designed to be more easily mined with typical hardware found in homes (Sprankel, 2013, p. 14).
- Litecoin was introduced in late 2011 (Zhang & Song, 2014, p. 26), and it differs from Bitcoin in three ways.
  - First, while Bitcoin has a 10-minute block generation time, Litecoin has a 2.5-minute block generation time, and while Bitcoin halves its mining rewards at 210,000 blocks, Litecoin doesn't half its mining rewards until 840,000 blocks (Sprankel, 2013, p. 14).
  - Last, but not least, while Bitcoin uses SHA256, Litecoin uses scrypt, which moves the mining load from the computer's CPU to its memory (Morris, 2014, p. 12; Sprankel, 2013, p. 14).
- Litecoin is the second-largest cryptocurrency by market capitalization, second to only Bitcoin (Zhang & Song, 2014, p. 9).

c) Dogecoin
- Dogecoin was introduced on December 8, 2013 when Jackson Palmer and Billy Markus, after having a beer, bought Dogecoin.com and adapted an unsuccessful cryptocurrency called "Bells" to the Doge Internet meme (McGuire, 2013; Zhang & Song, 2014, p. 30).
  - After they posted the currency on Reddit, its popularity took off so quickly they couldn't even amass a pile of Dogecoins for themselves (Gilbert, 2013; McGuire, 2013; ummjackson, 2013).

- Dogecoin is like Litecoin, except for some important differences.
  - While Litecoin has a 2.5-minute block generation time, Dogecoin uses a 1-minute generation time for its blocks (Zhang & Song, 2014, p. 30).
  - Also, Dogecoin randomly distributed the mining reward for its first 145,000 blocks, but it now gives a static reward for each block (Zhang & Song, 2014, p. 30).
- A major use of Dogecoin is to "tip" users small amounts for posts on Reddit and Twitter for posts they found helpful (McGuire, 2013).
- Dogecoin has also been used for numerous fundraising efforts, including to send the Jamaican bobsled team to the Sochi winter Olympics and fund wells for clean water in Kenya (Hern, 2014; Hickey, 2014).

4. Bitcoin Threats, Enemies, and Challenges
   a) For all the success Bitcoin and its spinoffs have achieved, Bitcoin faces numerous threats.
   b) Flaws in Bitcoin
      - The first threat to Bitcoin regards its value.
      - If too many blocks of Bitcoin, or any other cryptocurrency, can be mined, it cannot be trusted as a store of value, for the cryptocurrency would no longer be scarce (Eyal & Sirer, 2014; Houy, 2014, p. 4).
      - As stated earlier, this happened to Bitcoin once.
        - On August 6, 2010, someone exploited a vulnerability in the Bitcoin software to create 184 billion Bitcoins and send them to two people (Firică, 2014, p. 39).
        - Within hours, this bug was fixed, and the erroneous transactions were erased from the ledger (Firică, 2014, p. 39).
      - This never happened to Bitcoin again, which suggests that Bitcoin is quite secure on this front.
   c) Mt. Gox Bankruptcy
      - The second threat to Bitcoin regards its institutions.
      - Over the course of the cryptocurrency's existence, countless Bitcoin exchanges have gone broke, losing customers Bitcoins in the process, the largest of these being Mt. Gox.
        - From February 9 to February 11, 2014, Mt. Gox suffered a series of malleability attacks that caused it to suspend withdrawals (Decker & Wattenhofer, 2014, p. 6; Shirriff, n.d.).
      - This suspension of withdrawals was be followed by a claim that the problem was being fixed and Mt. Gox would resume withdrawals soon (Decker & Wattenhofer, 2014, pp. 6–7).
        - However, depositors would never see their Bitcoins again, as on February 23, Mt. Gox would disappear from the Internet, only to be followed up on February 28 by

Mt. Gox filing for bankruptcy (Decker & Wattenhofer, 2014, p. 7; Trautman, 2014, p. 100).

- The once-mighty Mt. Gox had fallen.

- However, this just scratches the surfaces of Mt. Gox's problems.
- As mentioned before in the paper, Mt. Gox had fallen once before.
  - On June 13, 2011, Mt. Gox was hacked by a mischievous individual, who reduced the price for Bitcoin to 1 cent and transfered 25,000 Bitcoins into a single account (Mick, 2011).
- While Mt. Gox, by all indications, had appeared to recover from this attack, it was suffering from bigger problems that emanated from its CEO's, Mark Karpeles's, ego.
  - Mark Karpeles, who had taken it upon himself to rewrite the site's backend software, made everyone run code changes through him, and didn't use any version control for the site's software (McMillan, 2014).
  - This meant bug fixes, including security fixes, would not be applied for weeks, while that previously untested changes would be pushed out to Mt. Gox's customers without any way to undo them (McMillan, 2014).
    - To quote one unnamed insider, "[It] was a complete mess." (McMillan, 2014)
- Additionally, Mt. Gox had just had $5 million seized from their account because they had neglected to register with the U.S. government as a money transmitter, and Mt. Gox was being sued for $75 million because they had not held up to their end of a business agreement with a U.S. company called CoinLab (McMillan, 2014).
  - While all this was going on, CEO Mark Karpeles was focused on opening the Bitcoin Cafe, a stylish hangout next to Mt. Gox's offices and within walking distance of Tokyo's largest train station, where one could buy a French quiche and a coffee with Bitcoins (McMillan, 2014; Mochizuki, 2014).
- In short, Mt. Gox was clearly mismanaged by a CEO who let his ego get in the way of running his business.
  - Hopefully Bitcoin will recover from the collapse of this badly mismanaged exchange.

d) Governments vs Bitcoin

- The third threat to Bitcoin regards its legality.
  - This may be the most credible threat to Bitcoin.
- Of course, it is unsurprising to see dictatorships like China moving against Bitcoin, as Bitcoin can be used to anonymously fund opposition and human rights groups (Sanders, 2014, p. 4; Shubber, 2013).
  - But more worrysome is the attacks made on Bitcoin by democratically-elected governments such as the United States.

Taylor Spencer
Advanced Technical Writing
Dr. Frith
05/13/15

- Their stated reason is the potential for malevolent and criminal use of Bitcoin, which, given its anonymity, is definitely a possibility, as we have seen with Silk Road (Ferrara, 2013).
    - However, there is a good case to be made that the real reason Bitcoin is being targeted is that it threatens the status quo.
- Bitcoin is decentralized, and therefore, a harder target to impose regulation on than a centralized digital currency (Karlstrøm, 2014, p. 4).
    - The most notable effect of this is that entities can't be banned from receiving Bitcoin donations, a property that Wikileaks has taken full advantage of ("1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v," n.d.; Greenberg, 2011; WikiLeaksVerified account, 2011).
- Also, Bitcoin is designed to be anonymous, which serves to prevent intimidation from keeping donations from flowing to controversial and/or targeted organizations.
    - Granted, it is possible for someone to be tracked to a transaction, if the government can determine that person's Bitcoin address, but Bitcoin allows for users to have multiple addresses, lessening the impact of such an identification (Glaser, Zimmermann, Haferkorn, Weber, & Siering, 2014, p. 3; Hobson, 2013, p. 4).
- Last, but not least, the circulation of Bitcoin is limited to 21 million Bitcoins, which separates it from government-backed fiat currencies, where new money can be printed to finance government spending, albeit at the cost of inflation (Hobson, 2013, p. 3).
- Bitcoin's creator, Satoshi Nakamoto, admits Bitcoin's appeal to libertarians himself, stating "It's very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though." (Nakamoto, 2008b)
- Therefore, it's only natural that Bitcoin would be an anathema to power-hungry politicians for the same reason it's appealing to libertarians: It's decentralized, it's somewhat anonymous, and it has a finite limit, meaning it can't be printed for the sake of government spending.
- Whether these governments are successful in shutting down Bitcoin, or whether Bitcoin is allowed to disrupt the financial sector and the agencies that regulate it, will be the big question.
    - I can only hope Bitcoin survives, for the potential it has to change things would be something I would hate to see die.