How Bitcoin Works: A Non-Technical Introduction

Token Money

- Represented by a physical object such as a banknote, coin, traveler's cheque, etc.
- Without the token, the value is lost.
- No intermediary required for spending
- But: requires faith in the ISSUER, usually a government

Notational Money

- Represented by a notation in a ledger, passbook or database
- E.g., a bank account:
- Notational money cannot be lost
- BUT: requires an intermediary (bank or clearing house) for spending
- ALSO: requires faith in the MAINTAINER of the ledger
Hybrid Money

- Requires BOTH a token AND a ledger account
- Example: personal cheque, Octopus card

- Can be lost AND requires faith in the ISSUER
- AND requires an intermediary (bank or clearing house) for spending

Virtual Money

- No token
- No ledger
- No issuer, no government backing (or supervision)
- No intermediary required for spending

- Is this even possible?
- Who creates the money? Why is it money?
- Without a token or ledger, how do you know how much you have? What is its value?
- How does "spending" occur?
- How do you know the spender is the owner?
- What prevents spending the same money twice?

Analogy: Real Estate

- Land ownership is defined by a “chain of title,” a sequence of deeds leading from the original owner to the present owner

- Deeds are recorded in the Land Registry
- Ownership determined by searching the Registry
- The Land Registry is, in effect, a ledger holder
- If the Registry is altered, ownership can be lost
- Double-selling is prevented by timestamps

Distributed Registry

- Suppose we broadcast ALL deeds to thousands of nodes of a decentralized public network?
- IF the deeds are genuine AND the network members agree on the chain of title, THEN we can tell who owns a piece of property
- Ask the network and count the responses! If a majority say that V is the owner, then he is.
- There must be enough honest members that false responses cannot dominate
- This registry is not under government control
Creating a Currency

- Land is not portable and can’t be “spent”
- Let’s use valuable scotch whisky as money

Scotch as Money

- As long as there’s a market for expensive scotch, it will have value
- Scotch drinkers will be able to drink it or trade it
- The value will depend on supply and demand
- Problem: it’s very heavy, can’t be carried easily

Solution: A Scotch Bank

- Deposit your bottles in a bank
- The bank promises to hand over your bottle when you ask for it
- To prove ownership, they let you keep the label unique to your bottle:
  - When you transfer the label, you transfer ownership
  - The labels act as money!
  - The labels are “backed” by scotch
Disaster: Scotch is OUTLAWED!

- The Department of Health finds that scotch is poisonous, possibly fatal
- The government orders all of it destroyed, even in your bank
- You have scotch labels but your bank has no more scotch
- What happens to the value of the labels? No longer "backed" by scotch bottles
- Probably declines, but not to zero

The Label Virtual Currency

- Assume one label is now worth HKD 100.
- You can’t carry all of them around
- You can’t spend them on the Internet
- Let’s “virtualize” them
- Instead of labels, just store their serial numbers in a cellphone app:

Spending

- To spend a label, you just send its number over the Internet or bump phones
- Problem: you might still have it, but your digital wallet could delete it to prevent double spending
- Problem: How does the recipient know it’s genuine?
- Problem: Who controls the issuance of the numbers?
- Problem: What stops forgery?
- SOLUTION:
  - Make creation of numbers expensive (deters forgery)
  - Limit generation to a fixed quantity of serial numbers
  - Maintain ownership records in a distributed network

Hash Functions

- A “hash” is a short function of a message
- BUT: a hash is not uniquely reversible
- Many messages have the same hash

Hash function $H$ produces a fixed size hash of a message $M$, usually 128-512 bits

$h = H(M)$
One-Way Hash Functions

- Hashes are easy (fast) to compute but computationally difficult to invert
- Should not be able to find any message corresponding to a given hash
- Bitcoin uses a well-known published hash function SHA-256, which produces 256-bit hashes

\[ h = H(M) \]

What is a Bitcoin Really?

- No physical object, not even a character string
- A chain of digitally signed transaction records leading from the original owner to the current holder
  - (Very similar to a chain of land deeds)
- The transaction records contain
  1. hashes that are difficult to find AND
  2. virtual owner IDs, called addresses
- There is NO bitcoin registry, NO centralization
- Bitcoin chains are broadcast to everyone
- Anyone can verify them

Bitcoin Protocol

- Bitcoin was invented in 2008 by an anonymous person or team called “Satoshi Nakamoto”
- The bitcoin protocol for generating and exchanging bitcoin is implemented in publicly available, open source software
- Anyone can obtain and run a bitcoin client

How Bitcoin Works 1

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.
Bitcoin Addresses

- Bitcoin software generates bitcoin addresses of 25-44 characters for users
- Sample address: 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ
  (The address is actually an elliptic curve public key, 44-character key as secure as a 7000-bit RSA key.)
- To send bitcoins, user specifies a receiving address and amount, and clicks “send”
- To receive bitcoins, just tell the sender your address!
- Addresses are not registered to users. A user can have a different address for every transaction.

Bitcoin Mining

- Bitcoin chains begin with data “mined” by performing a large number of hash function computations
- A “miner” tries many different (e.g., 10^15) numbers, trying to find one whose hash value is less than a given threshold
- Success is rewarded with bitcoins
- The threshold declines over time (determined by the protocol)
- Bitcoin hashes are progressively more difficult to find
- There will never be more than 21 million bitcoins. Divisible into units as small as 1/100 millionth of a bitcoin
Possible Vulnerabilities

• No way to reverse a transaction without the payee’s cooperation
• Transaction malleability (alterability)
• Should to wait 60 minutes or more to confirm a large transaction
• Software bugs
• Bank robbery by hackers (e.g. Mt. Gox)
• Malware attacks against wallets
• Government attempts to control
  – Silk Road raided by US FBI in Oct 2013
• Competing digital currencies easy to create

Bitcoin in Hong Kong

• This created speculation that HK would become a hotbed of Bitcoin activity

The New York Times

Apparent Theft at Mt. Gox Shakes Bitcoin World

The most prominent Bitcoin exchange appeared to be on the verge of collapse late Monday, raising questions about the future of a volatile marketplace.

On Monday night, a number of leading Bitcoin companies jointly announced that Mt. Gox, the largest exchange for most of Bitcoin’s existence, was planning to file for bankruptcy after months of technological problems and what appeared to have been a major theft. A document circulating widely in the Bitcoin world said the company had lost 744,000 Bitcoins in a theft that had gone unnoticed for years. That would be about 6 percent of the 12.4 million Bitcoins in circulation.

While Mt. Gox did not respond to numerous requests for comments, and the companies issuing the statement scrambled to determine the exact situation at Mt. Gox, which is based in Japan, the news helped push the price of a single Bitcoin below $500 for the first time since November, when it began a spike that took it above $1,200.

Hong Kong Monetary Authority says it won’t regulate Bitcoin

Posted on 17 November 2013.

The Chinese Banking Regulatory Commission and the Hong Kong Monetary Authority (HKMA) won’t regulate Bitcoin. The last time Bitcoin Examiner talked about this possibility, the commission was still looking into regulation and possible framework. However, the HKMA has publicly announced, in the meantime, that Bitcoin doesn’t belong to its jurisdiction.

The information was revealed this Friday (15) by the authority’s chief executive, Norman Chan, quoted on Geek Empire through an article published by Brian Cohan. While this Hong Kong institution has the responsibility of “promoting the stability and integrity of the financial system, including the banking system”, it won’t be tackling Bitcoin regulation.

• This created speculation that HK would become a hotbed of Bitcoin activity

afab news

‘First’ physical Bitcoin retail store opens in Hong Kong

HONG KONG: A shop selling the virtual Bitcoin currency has opened in Hong Kong, as fresh concerns grew in Asia over the currency’s viability and security.

Touting itself as the world’s “first” physical Bitcoin retail store, Hong Kong-based exchange AnxBTC said it could help raise the popularity of the crypto-currency.

It came on the day that Japanese Bitcoin exchange Mt.Gox was forced to file for bankruptcy protection, saying it had lost nearly half a billion dollars’ worth of the digital currency in a possible theft.

Analysts have warned that the lack of government support and security risks may fuel further uncertainties for the digital currency.

Late last year, the People’s Bank of China (PBoC), the nation’s central bank, ordered financial institutions not to provide Bitcoin-related services and products while cautioning against its potential use in money laundering.

Vietnam has also banned its banks from handling Bitcoins, saying the virtual currency is not legal tender in the communist nation.

Japan’s finance minister said earlier he had always thought Bitcoin was suspect and that the country might take action following the Mt.Gox debacle.
Octopus + Bitcoin?

Bitcoin spreads tentacles as Octopus sniffs the bait

Crane Cheung

Wednesday, January 15, 2014

Octopus chief executive Simon Cheung Yu-fung said the firm does not rule out accepting Bitcoin immediately even as a Hong Kong Monetary Authority official regards it as a virtual commodity, not a virtual currency.

A heated debate took place at the Asian Financial Forum on Bitcoin - an emerging virtual currency that has seen its valuation soar and usage expand around the globe. Even Octopus, which operates a smart card payment systems across the SME market, showed interest.

"More people will be attracted to use Bitcoin and the currency was accepted by online merchants as a method of payment," Cheung said. "We don't exclude the possibility that one day our customers may want to use Bitcoin to add value to their Octopus cards."

His comments triggered strong opposition from HKMT executive director for financial infrastructure Gordon Lee Kin-yung who said Bitcoin is not yet a virtual currency.

"Bitcoin fails to meet two preconditions as a virtual currency: acceptance on the part value and confidence in the issuer," Lee said. "It is just a virtual commodity."

He said that there are only a few online vendors that accept Bitcoin, but large companies, such as real estate developers and automobile manufacturers, will not be interested when they see products.