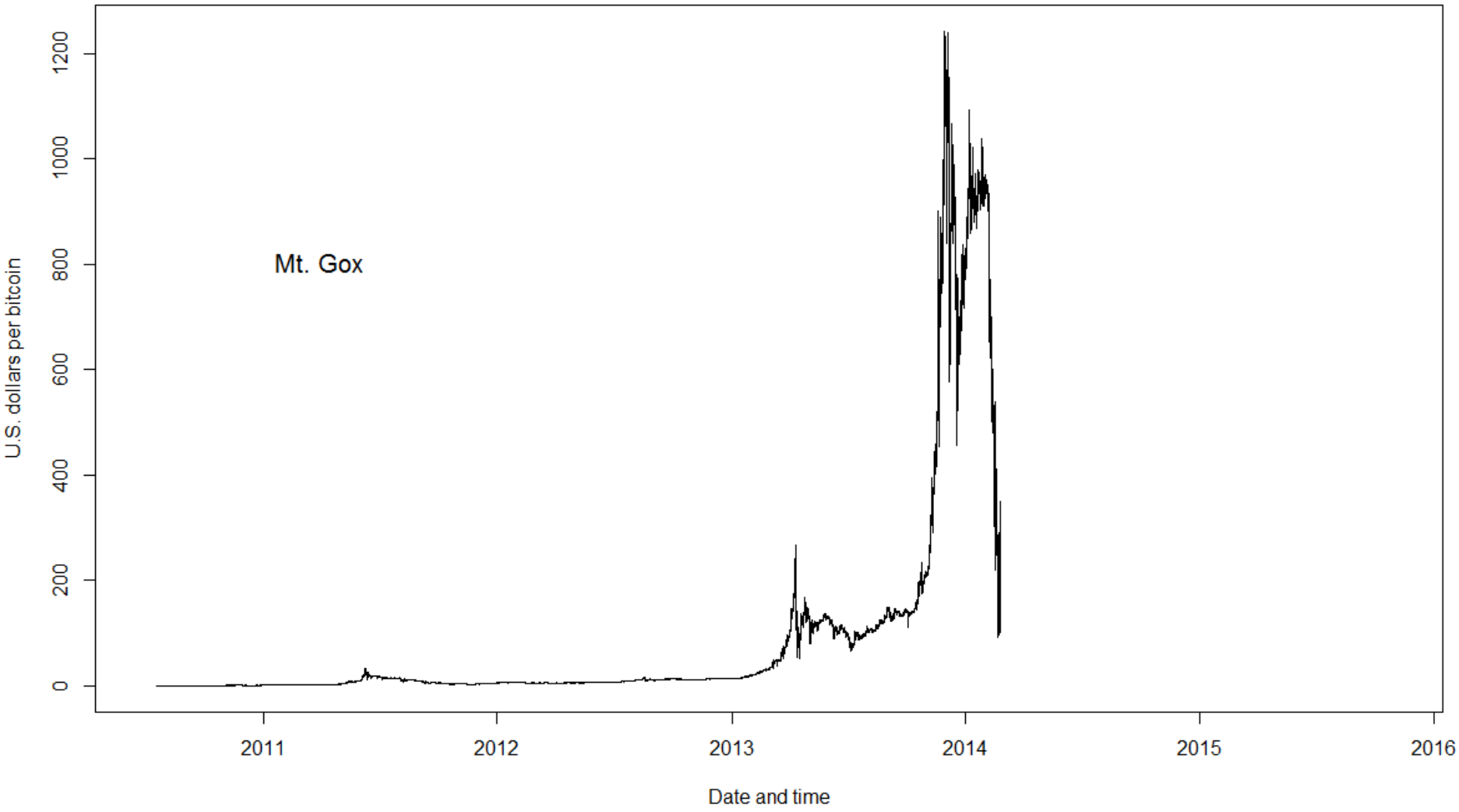
Bitcoin and Virtual Currencies

Gerald P. Dwyer
Clemson University
University of Carlos III, Madrid
Invited lecture at FMA meeting, October 2015

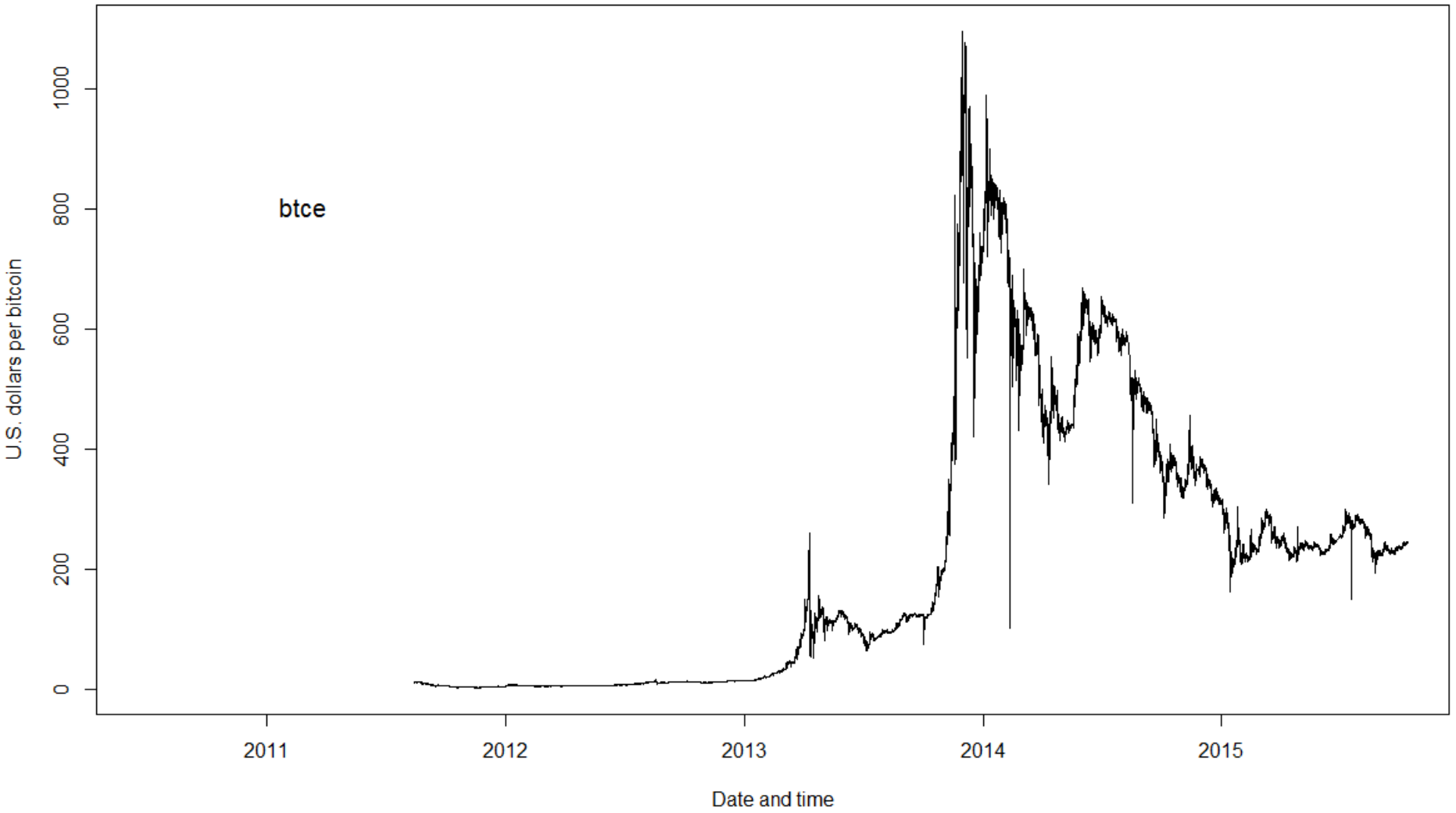
Bitcoin and Virtual Currencies and the Blockchain

Gerald P. Dwyer
Clemson University
University of Carlos III, Madrid

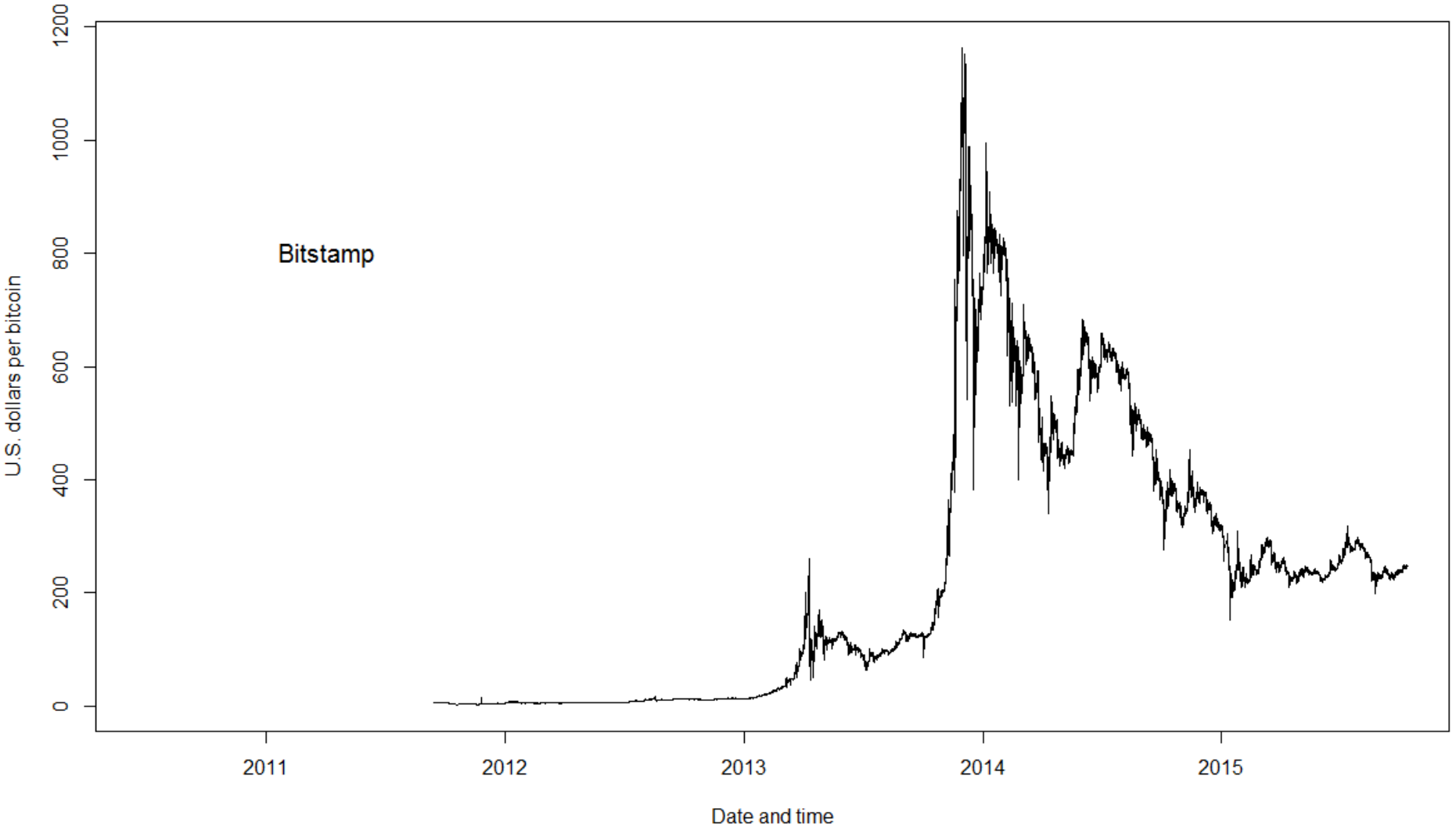
Price of Bitcoin
Mt. Gox Exchange
7/17/2010 to 2/14/2014



Price of Bitcoin
btce Exchange
8/14/2011 to 10/12/2015



Price of Bitcoin
Bitstamp Exchange
9/13/2011 to 10/12/2015



Introduction

- Digital currency has been next best thing since 1990s
- Digital currency is money which
  - Is an asset held by the owner of the money and not a liability of a financial institution
  - Can be used to buy something from someone else without the intervention of an outside party

Introduction

- Digital currency has been next best thing since 1990s
- Digital currency
- Virtual currency is another name for digital currency because the currency may have no physical representation other than bits and bytes

Introduction

- Digital currency has been next best thing since 1990s
- Digital currency
- Virtual currency
- Cryptocurrency
  - Digital currency with cryptography an important part of its implementation
  - Bitcoin and similar currencies

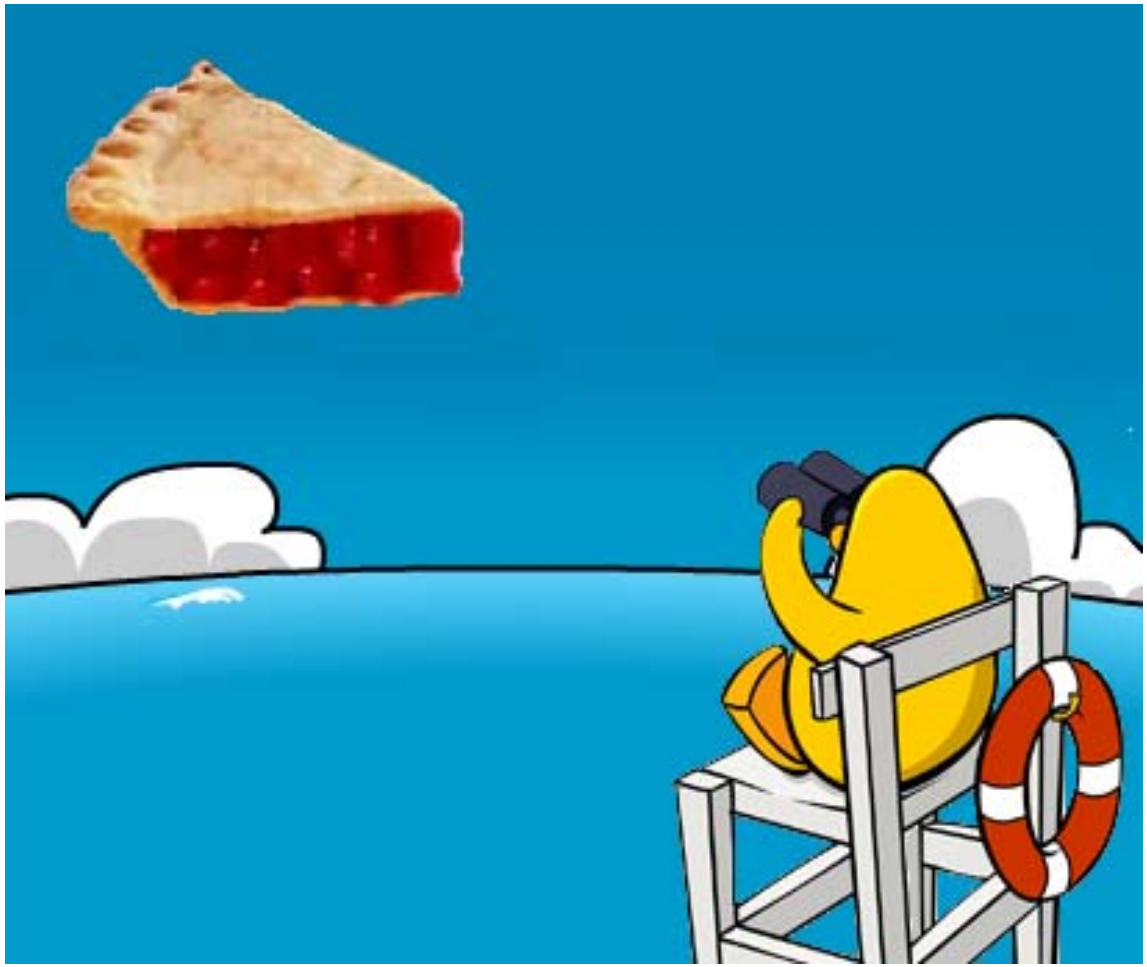
Introduction

- Digital currency has been next best thing since 1990s
- Digital currency
- Virtual currency
- Cryptocurrency
- Blockchain securely keeps track of changes in ownership of cryptocurrency

Bitcoin and the Blockchain in the Wall Street Journal

- Barclays Puts Big Banks One Step Closer to Bitcoin (9/2)
- Visa, Nasdaq, Others Invest $30 Million in Bitcoin-Related Startup (9/9)
- State Street Experiments with Blockchain for Institutional Banking (9/25)
- Blockchain is on the Agenda at State Street (9/28)
- UBS Working with Blockchain Prototypes (10/2)

Pie in the Sky?



Source: shadowproof.com

Computers

- “I see no reason why anyone would want a computer in their home.”
  - Kenneth Olsen, president of DEC, 1977

Cray Supercomputer 1979

Source: Deutches Museum

A 15-Times Faster Computer Today

Source: Samsung

Organization of Rest of Talk

- Use Bitcoin to make the discussion more concrete and precise
- Basic Issues
  - Supply
  - Demand
  - Equilibrium
  - Volatility
- Blockchain generally

Single Biggest Technical Issue for Digital Currencies

- Double spending

Source: gizmodo.com

Supply of Cryptocurrencies

- Bitcoin
- Litecoin
- Ripple

Economics of Bitcoin

- Demand
- Supply

Issues for Supply

- How created?
- What determines the nominal quantity of money?
- Who gets any revenue from creating money?
- How prevent double spending?

Origination of Bitcoin

- Satoshi Nakamoto
  - Paper in 2008
  - Details worked out in user group for programmers
  - Rules for supply
  - Fixed final number of bitcoins
    - 21 million
    - Actual quantity increases gradually over time
    - Rate of increase falling by about half every four years
    - Other currencies have other non-state-dependent rules

Supply of New Bitcoins

- “Miners” increase the number of bitcoins
- Mining is the solution of a computational problem
  - Requires work to solve the problem
    - Computer time
    - Electricity
  - Easy to verify that the problem has been solved
    - Hard to solve itself
- Software widely available
  - Open source

Double Spending

- How avoid double spending after created?
- Open-source software
- Peer-to-peer network

Client-Server Network

Peer-to-Peer Network

Maintaining the Record of Ownership and Transactions

- Why does anyone maintain a database?
  - All miners maintain such a database to know where they are in mining and to tell others
- Certification of a mining solution related to keeping record of transactions

Blockchain Is Record of Transactions

- Every transaction includes
  - Address to which bitcoins sent
  - Number of bitcoins sent
  - Digital signature of party sending the bitcoins

Basic Elements of Blockchain

- Each block in the blockchain is a record including
  - Address of party receiving transaction fee and new bitcoins
  - Hash of previous block
  - Transactions
  - Open field to alter hash (nonce)
    - Some other characters can be altered also

Miner Solves a Numerical Problem

- Compute hash of block's header which is less than or equal to a pre-specified value
  - Unique because transactions includes bitcoins to miner
- *h=H(M,nonce+other spaces)*
- *h* <= pre-specified value
- *Nonce* is set of spaces that can be altered, leading to altered *h*
  - The effect of changing nonce on *h* is unpredictable

A Bit of Detail about Maintaining the Record of Transactions

- Maintaining a record with a peer-to-peer network requires a protocol for coming to a consensus about transactions and solutions of mining problem
  - Keep chain of transactions
  - Resolve a block approximately every ten minutes
  - Longest chain is correct one

Maintaining the Record of Transactions without Mining

- Transactions fees
- Also motivates miners to include particular transactions

Who Decides Difficulty of Computational Problem?

- Solving computational problem and getting new bitcoins is a winner-takes-all game
  - Miners pool efforts in mining pools these days
- Difficulty such that a new block is finalized every 10 minutes
- Difficulty is set by consensus and announced by Gavin Andresen
  - Chief Scientist at Bitcoin Foundation
  - Satoshi Nakamura handed off leadership to him

Bitcoin Foundation and Leadership

- Software is open source
  - Anyone can take source code and start own currency
- Andresen and Bitcoin Foundation lead development and adherence to protocol
- Andresen worked for the Bitcoin Foundation for a while and no longer does

Anonymous?

- Not a design goal
- Not hard to collect information on activity of any address
- No
  - Reid and Harrigan (2013)
  - Ron and Shamir (2013)
  - Meiklejohn et al. (2013)

Demand for Digital Currency

- General trend toward digital representations of many things
- $5,000 of digital currency can be more convenient than 250 $20 bills
  - $300 of digital currency can be more convenient than 15 $20 bills

Demand for Digital Currency

- General trend toward digital representations of many things
- $5,000 of digital currency can be more convenient than 250 $20 bills
  - $300 of digital currency can be more convenient than 15 $20 bills
- Easier to smuggle bitcoins out of the country
- Silk Road
- Satoshi Dice

Value in Equilibrium

- Irredeemable paper money has a bad reputation
  - Full-bodied money
  - Digital representation does not improve issue
  - Free entry
- Is there an equilibrium in which digital currency has a positive value?
  - Marimon, Nicolini and Teles (2012)
  - Araujo and Camargo (2008)

Use in Exchanges for Goods and Services

- Not much evidence about that
  - There are analyses of transactions in blockchain but don't now what was traded for bitcoins
- Hill (Forbes, 2013) in San Francisco
- Couple in Utah
- Topic of discussion in Argentina
- Greece (Tsanidis, Nerantzaki, Karavasilis, Vrana, 2015)
- Silk Road

Uses in International Transfers

- Remittances
- Circumventing capital controls

Information from Blockchain

- Ron and Shamir (2013) analyze the blockchain through May 13, 2012
- Estimate turnover of bitcoins and identify "entities"
- Total transfers of about 423 million bitcoins
- About 3.7 million different addresses
  - About 1.9 million different entities with transactions
  - 609,000 additional addresses had never sent a bitcoin

Information from Blockchain II

- Distribution of transactions by entity highly skewed
  - 78 percent of all bitcoins were at addresses which had never sent a bitcoin to another address.
  - 97 percent of all entities have fewer than 10 transactions
  - 75 entities have at least 5,000 transactions

Information from Blockchain III

- Average entity held 3.7 bitcoins, although the distribution was very skewed
  - Average balance was about $100 at about $30 per bitcoin
  - 85 percent of all entities held less than 0.01 bitcoins
  - One entity held between 200,000 and 400,000 bitcoins worth about $6 to $12 million
  - About half of bitcoins were held by entities with 1,000 to 10,000 bitcoins

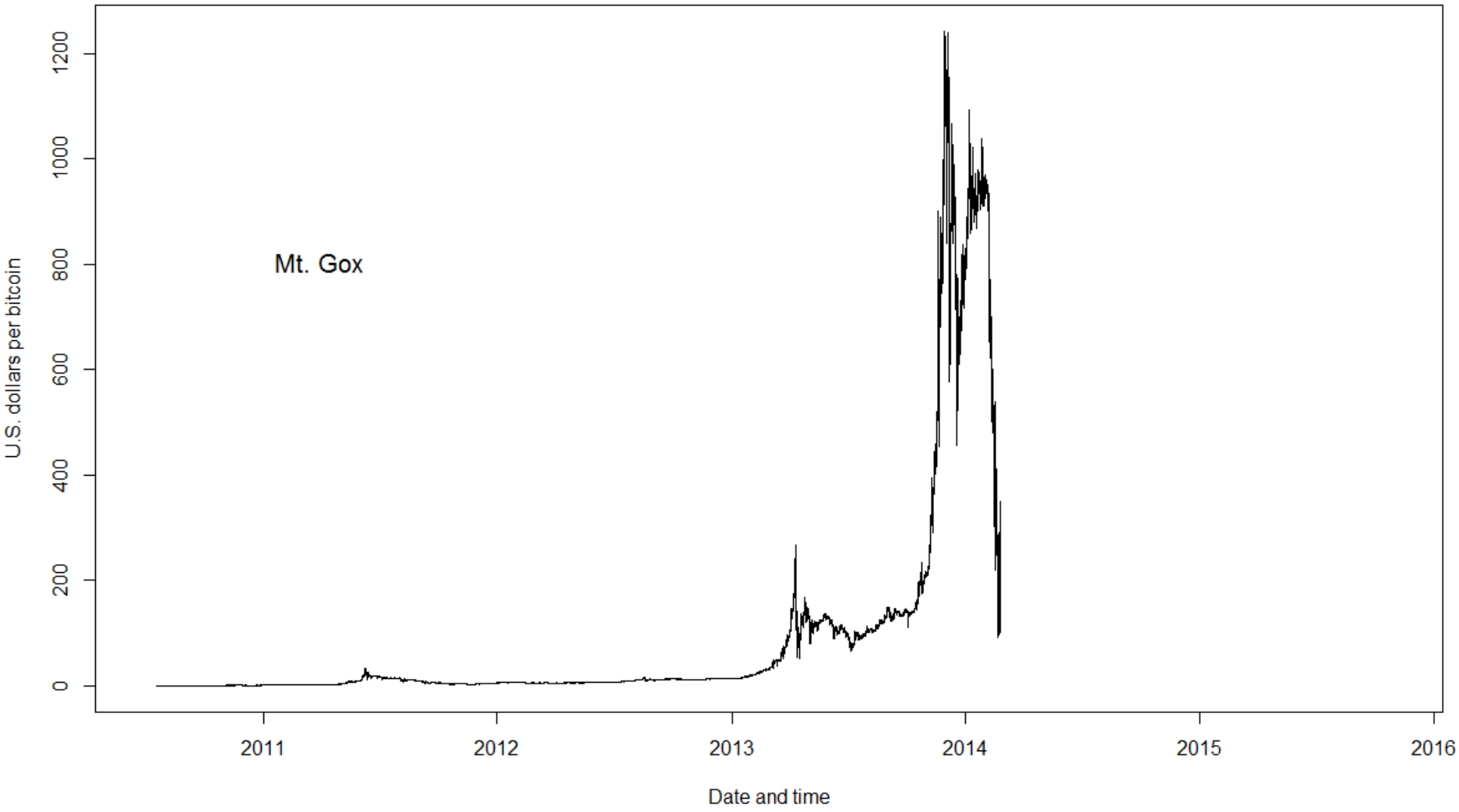
Trades of Bitcoins for Dollars

- Mt. Gox exchange in Tokyo
  - 7.7 million unique trades
- Btce
  - 22 million trades
- Bitstamp
  - 7.4 million unique trades

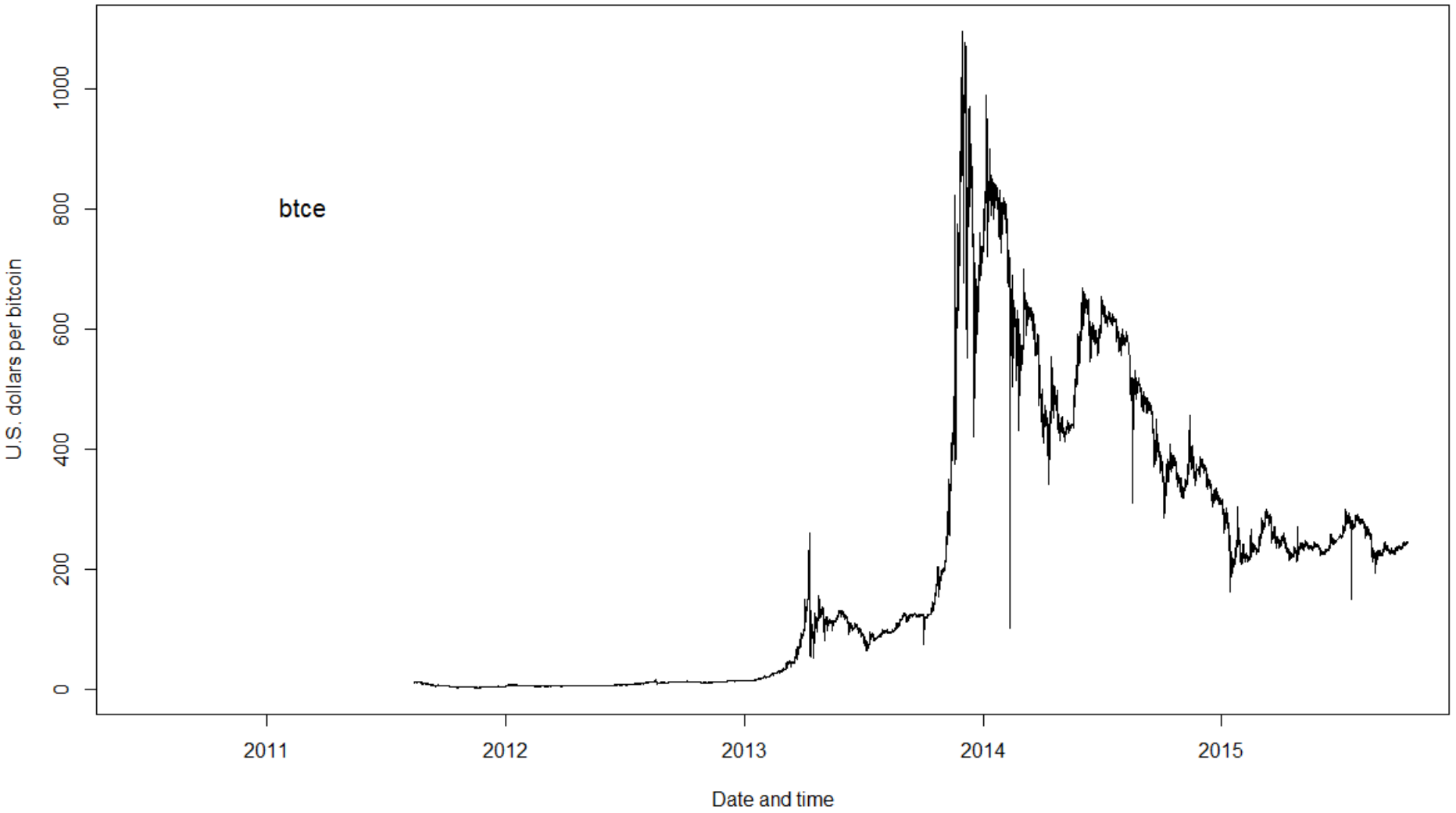
The Exchanges

- No brokers
- Limit orders and market orders
- Can see order book online and submit orders

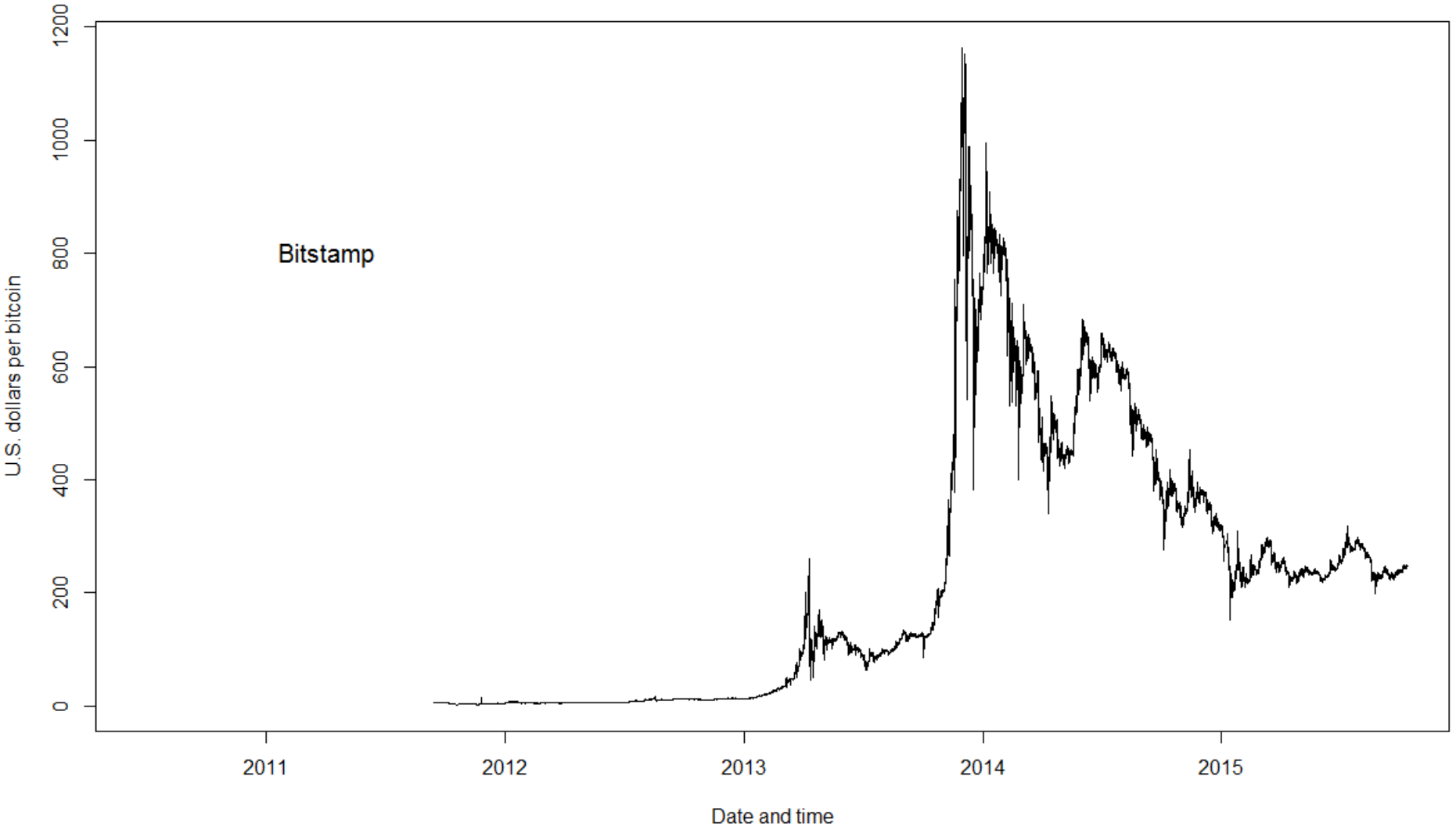
Price of Bitcoin
Mt. Gox Exchange
7/17/2010 to 2/14/2014



Price of Bitcoin
btce Exchange
8/14/2011 to 10/12/2015



Price of Bitcoin
Bitstamp Exchange
9/13/2011 to 10/12/2015



Price High or Low?

- October 31, 2015
- Value of bitcoins in dollars about $3.7 billion
  - Price about $250 per bitcoin
  - About 14.72 million bitcoins in existence in world
- M2 at end of September 2015 about $12.2 trillion
- Value of bitcoins worldwide about 0.03% of value of U.S. money

Price High or Low as Bank Reserves?

- U.S. bank reserves were $8.75 billion before Financial Crisis of 2007-2008
- Value of bitcoins about $3.7 billion
- About 42 percent of U.S. bank reserves

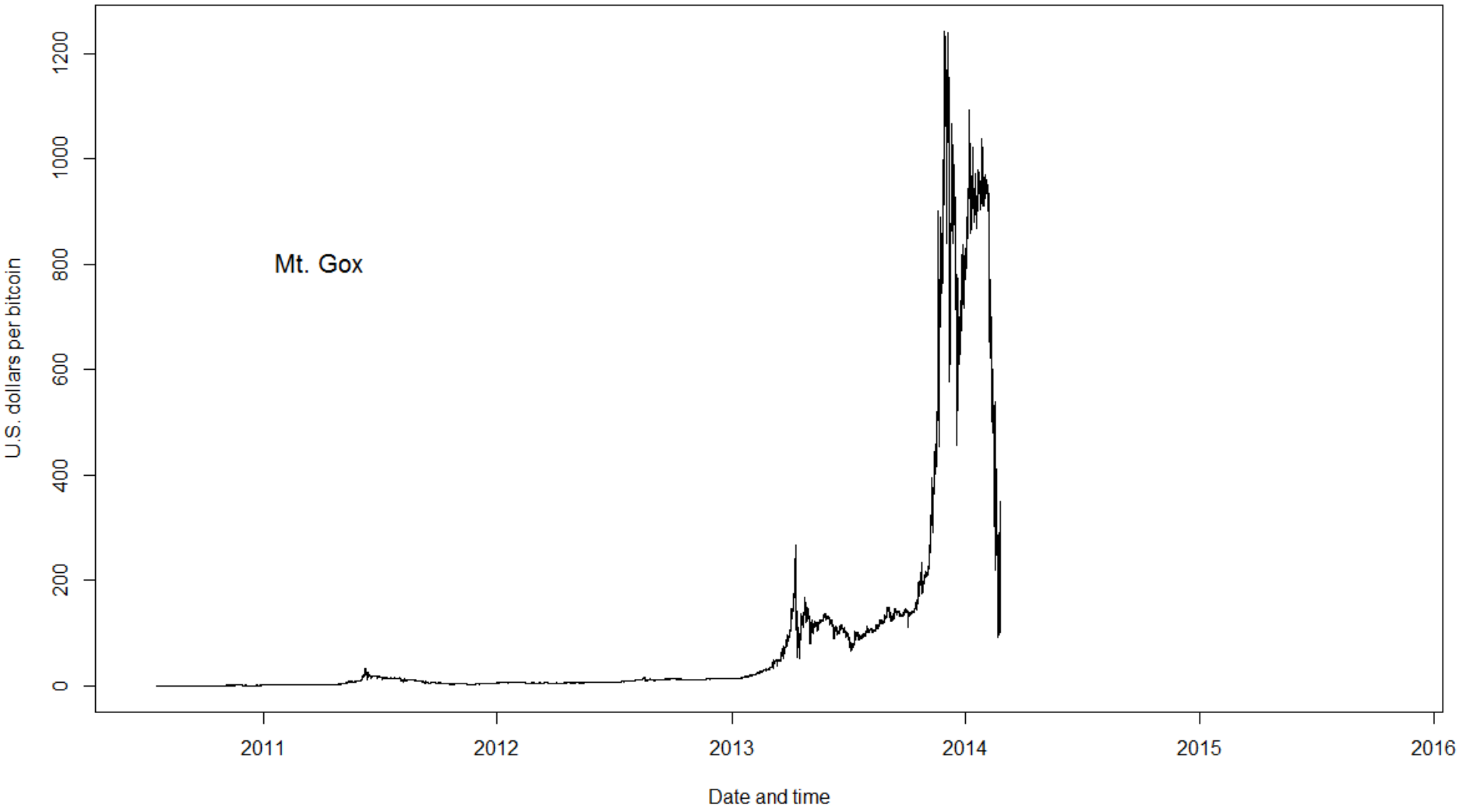
Price High or Low?

- Maximum of 21 billion bitcoins ever suggests that bitcoins likely to appreciate if used much in transactions
  - 0.03% of U.S. M2
  - 42 percent of U.S. reserves before financial crisis

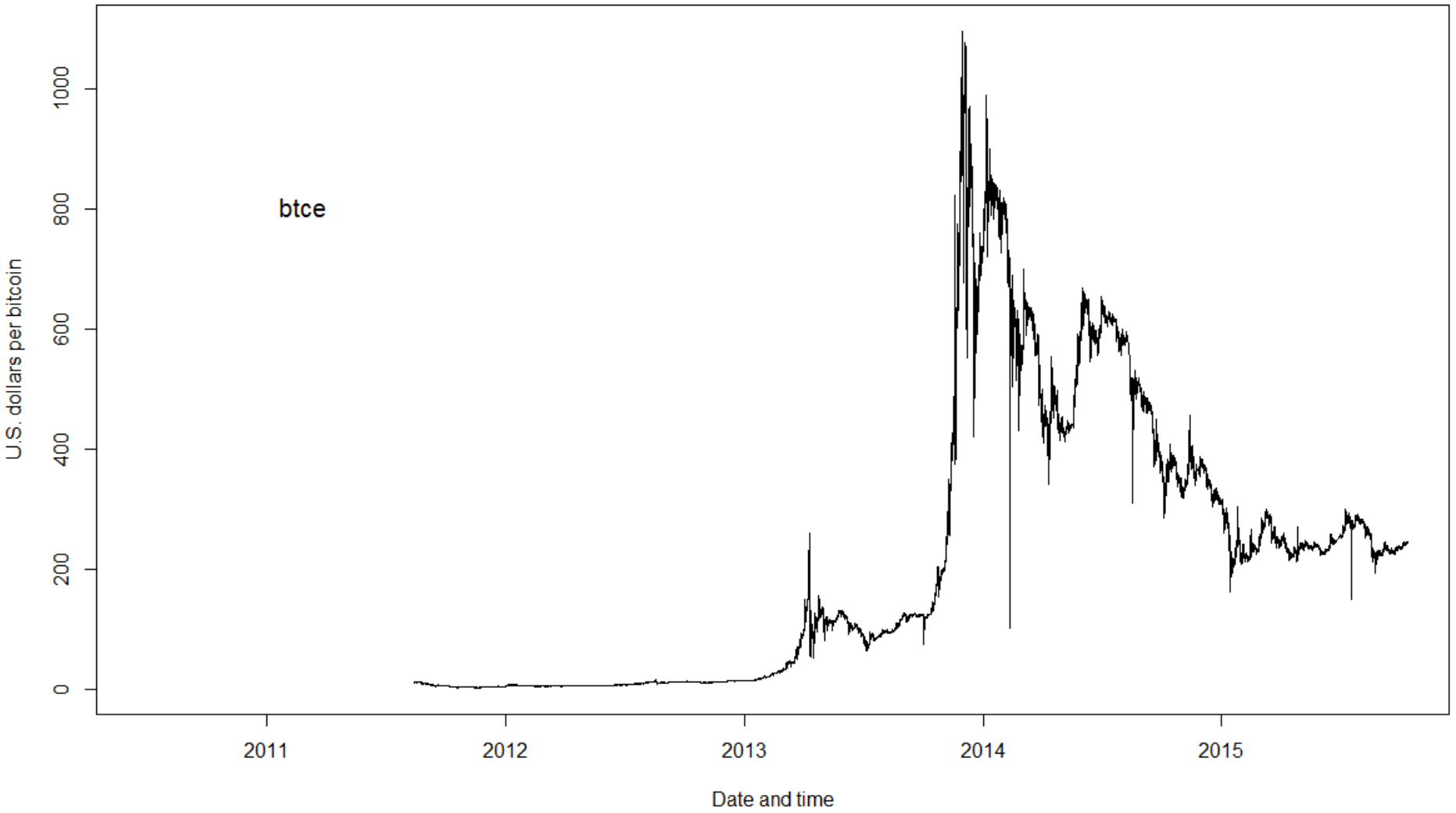
Volatility of Price versus Return

- Price is wrong metric for volatility
- Return is right metric for volatility

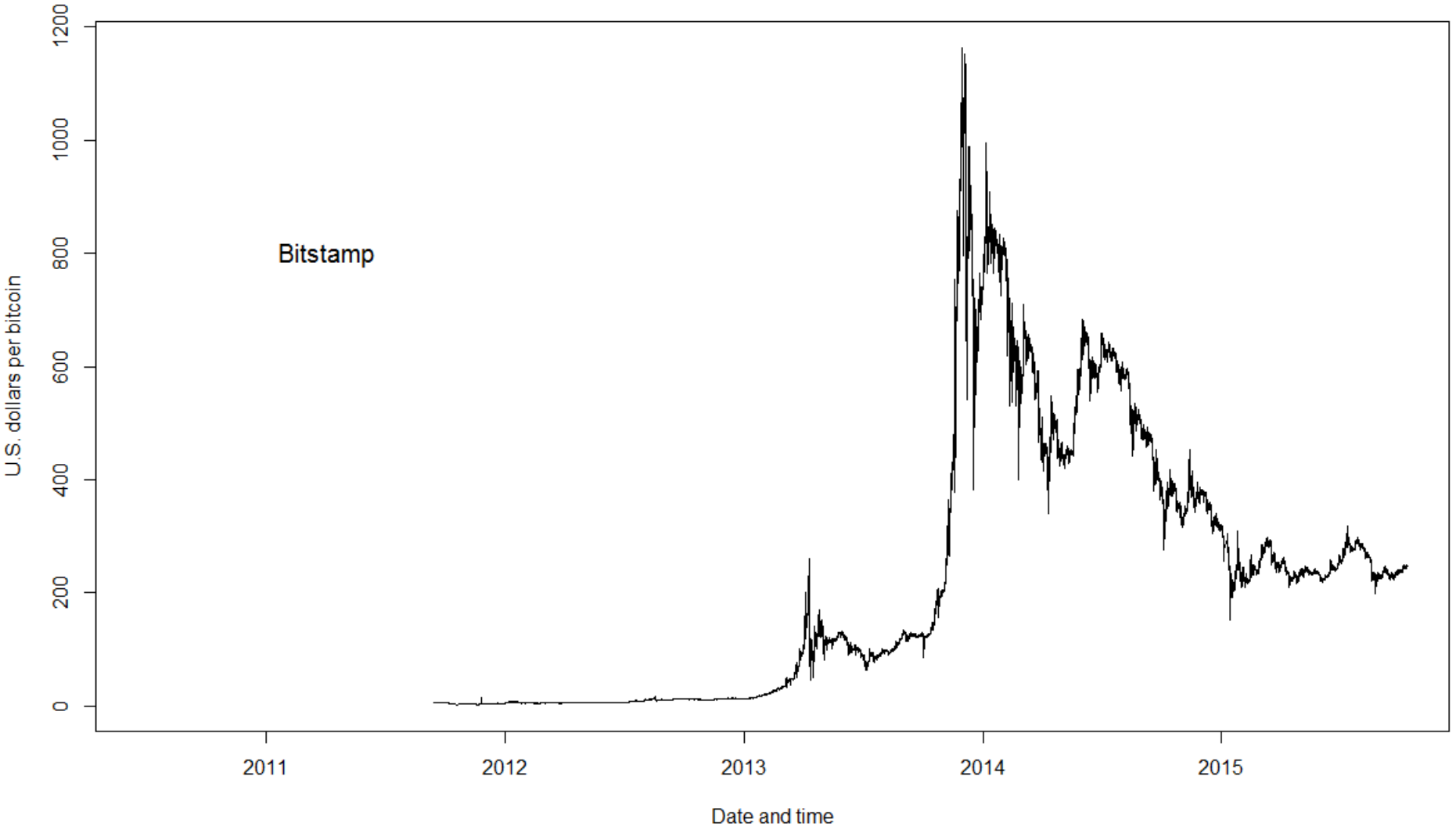
Price of Bitcoin
Mt. Gox Exchange
7/17/2010 to 2/14/2014



Price of Bitcoin
btce Exchange
8/14/2011 to 10/12/2015

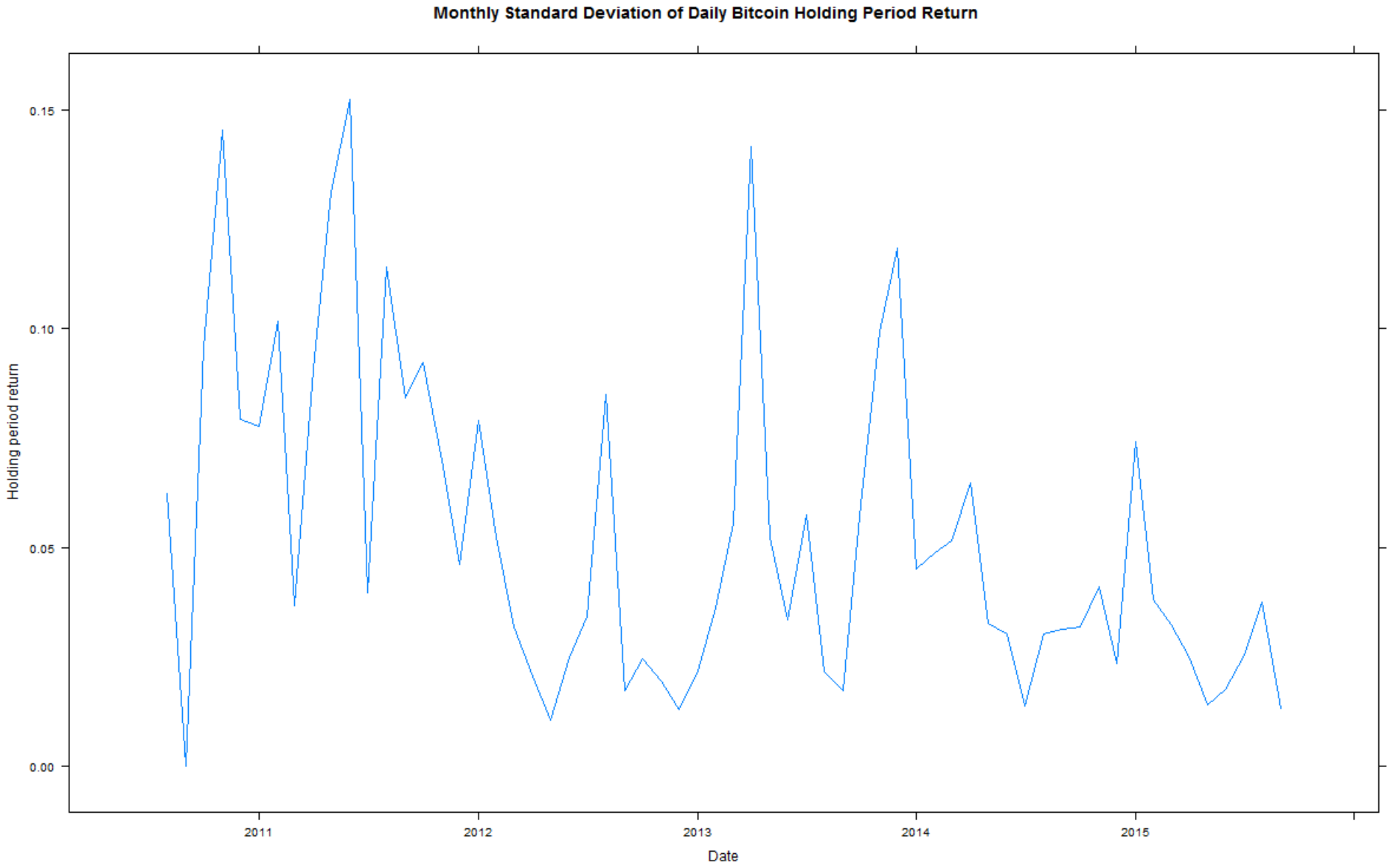


Price of Bitcoin
Bitstamp Exchange
9/13/2011 to 10/12/2015



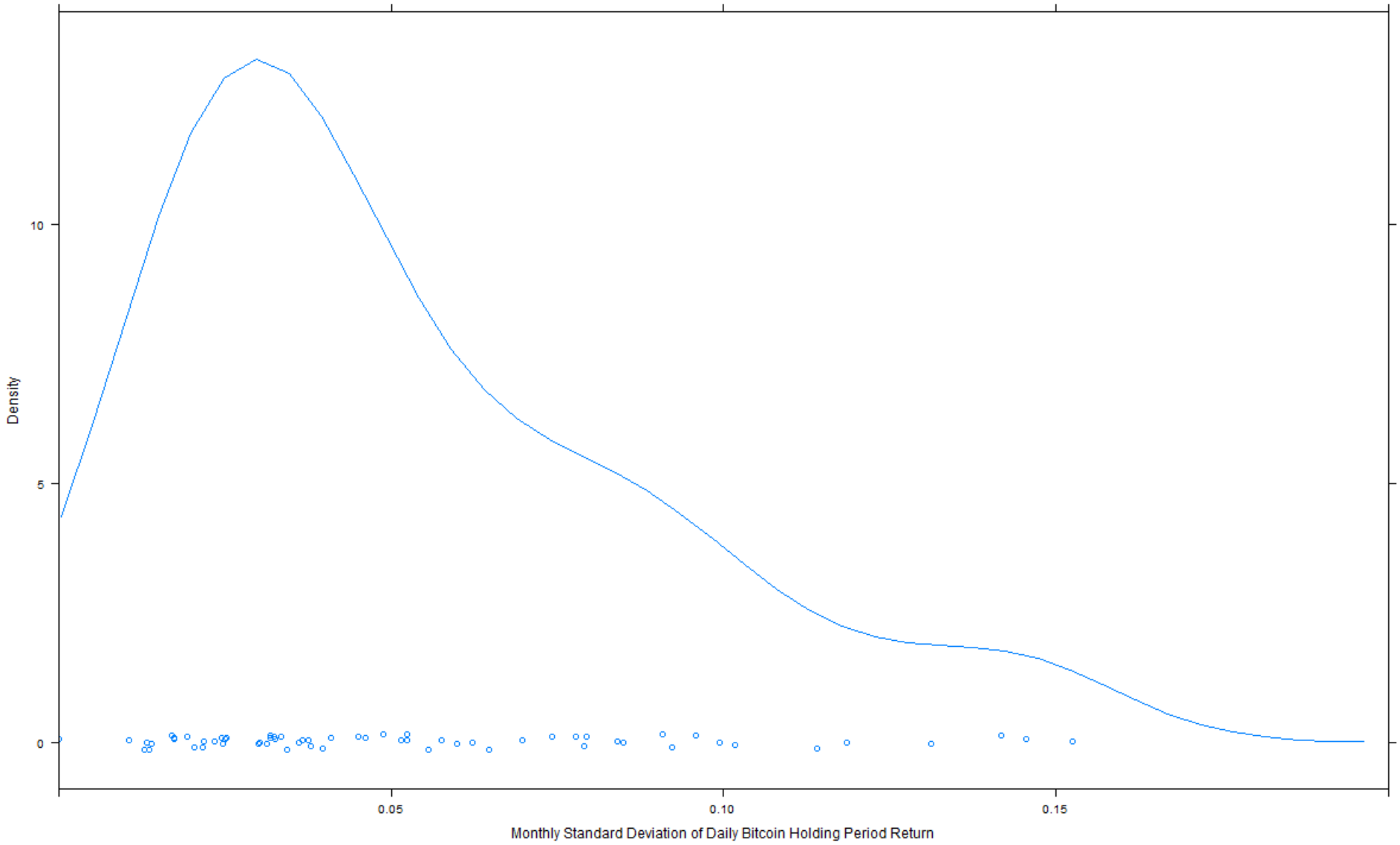
Volatility of Returns

Standard Deviation over Time



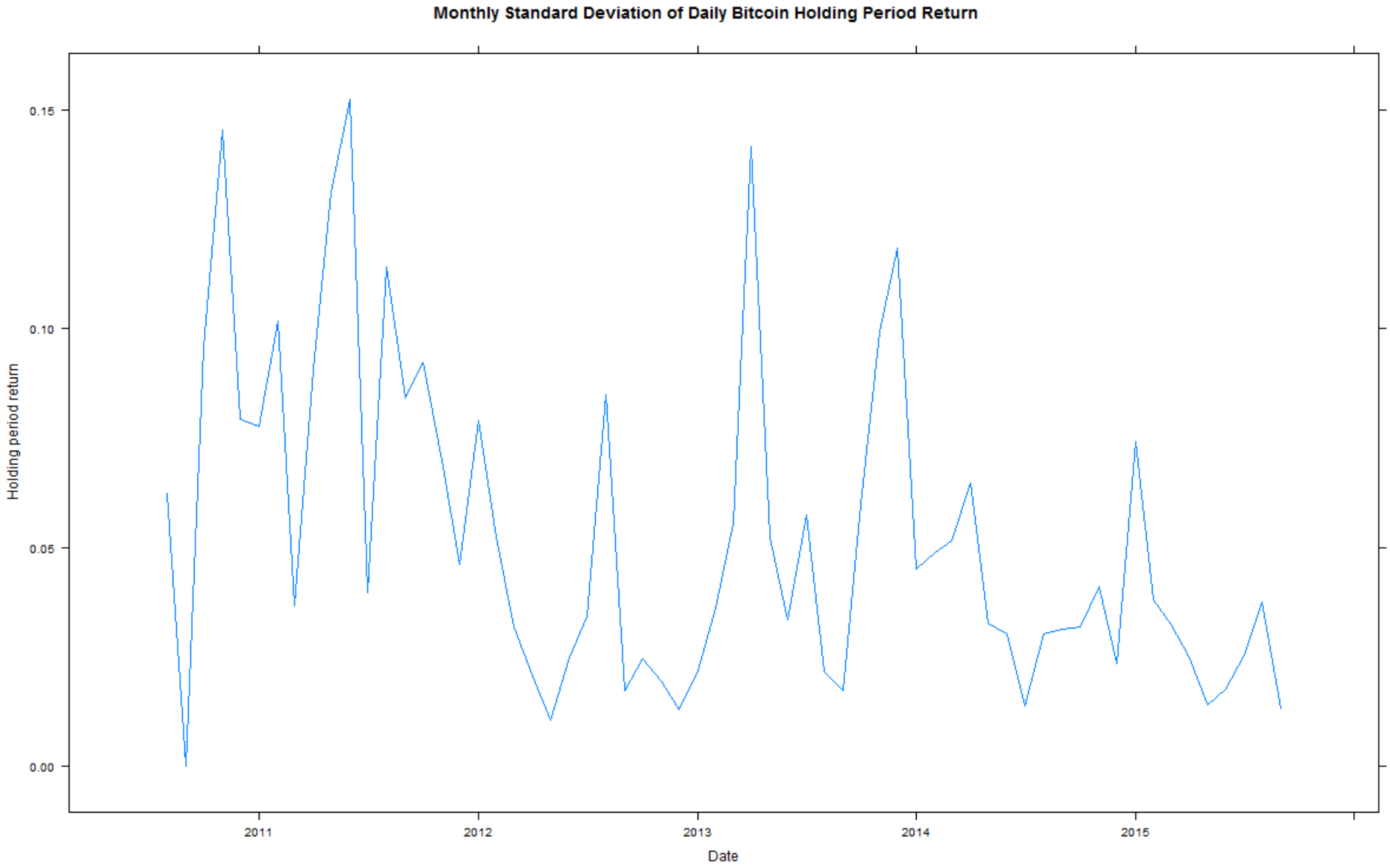
Volatility of Returns

Density

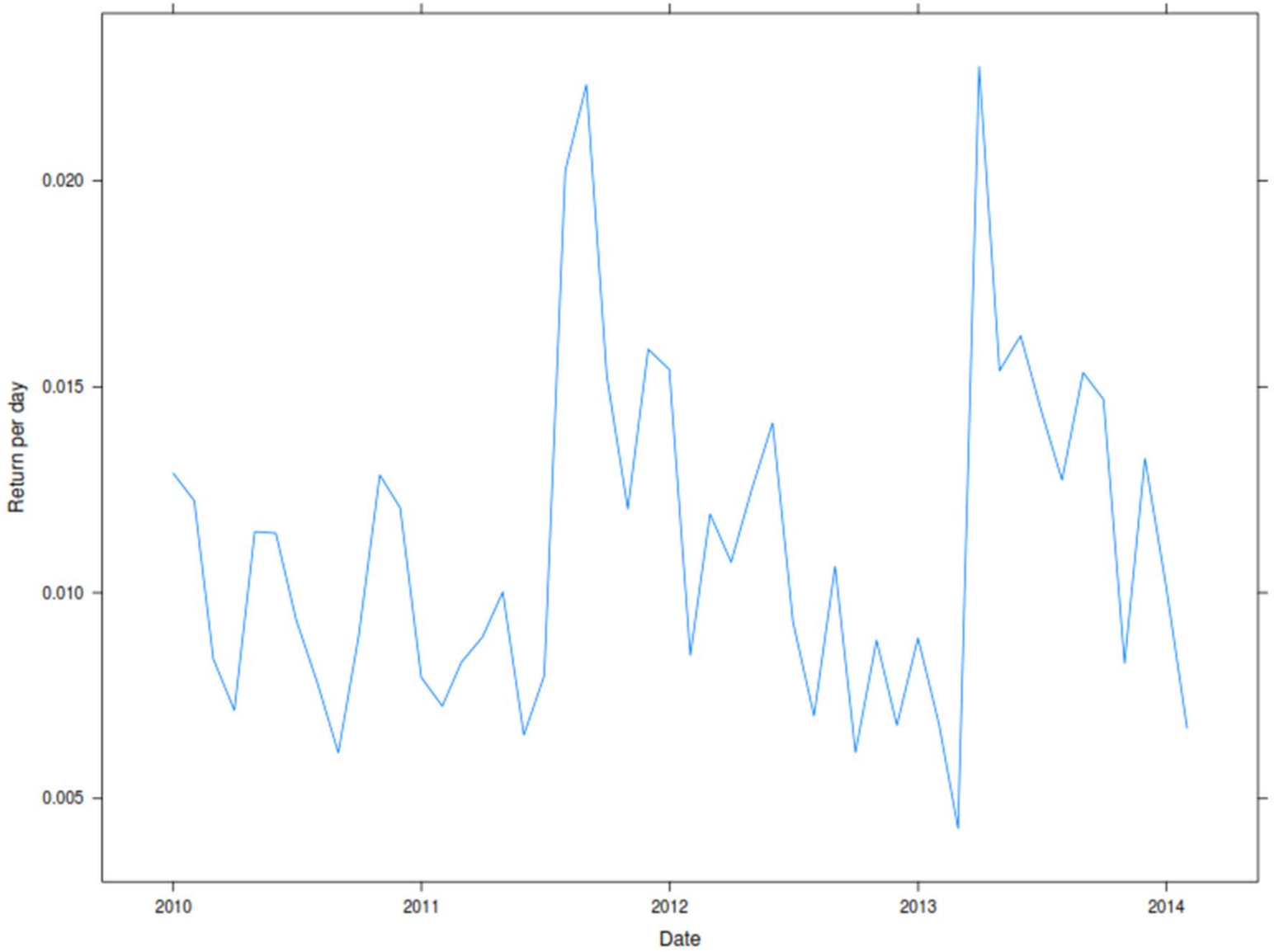


Volatility of Returns

Standard Deviation over Time



Volatility of Gold's Returns



Volatility of FX Returns

- 23 currencies with daily exchange rates provided by Federal Reserve Bank of St. Louis
- Monthly standard deviations of daily returns
- Minimum Hong Kong .0061% per day
- Maximum Venezuela 23.6% per day

Value Volatile?

- Not so much as to be highly volatile
- Not a unit of account generally either
  - Dell does not keep a stable price in bitcoins

Conclusion Bitcoin

- There is no fundamental flaw in Bitcoin that indicates its inevitable demise
  - Reputational equilibrium with knowable quantity
- Can have a positive value in equilibrium
- Free entry at zero marginal cost may be an issue but
  - Importance of liquidity
  - Identifiability of individual currencies

Conclusion Bitcoin

- Bitcoin is not obviously the ideal digital currency
  - Mining is not the only possible solution for creating bitcoins
    - Rule for creating money may waste resources
  - Fixed final quantity of bitcoins means continuing increases in price
    - Increase in demand
    - Loss of bitcoins

Conclusion Bitcoin

- Possible that people in U.S. will be paying their rent in bitcoins or another private digital currency
- I am dubious
  - People prefer to avoid exchange risk by having assets and liabilities in same currency
- Bitcoin and similar currencies are more likely to be used as base money for some transfers
  - Foreign exchange transactions
  - Remittances
- New asset class

Conclusion Bitcoin

- The blockchain and peer-to-peer impersonal verification of transactions is the big innovation
- Many open economic and financial questions
  - Game-theory solution of blockchain protocol
  - Operation of peer-to-peer exchange

The Blockchain in the Wall Street Journal

- Barclays Puts Big Banks One Step Closer to Bitcoin (9/2)
- Visa, Nasdaq, Others Invest $30 Million in Bitcoin-Related Startup (9/9)
- State Street Experiments with Blockchain for Institutional Banking (9/25)
- Blockchain in on the Agenda at State Street (9/28)
- UBS Working with Blockchain Prototypes (10/2)

The Blockchain

- What is all the discussion about?
- The blockchain is a peer-to-peer protocol for settling transactions
  - The Bitcoin protocol works for anonymous agents
  - Uses miners to settle transactions
  - “Trustless”
- The blockchain is called “blockchain” because it is a chain with blocks of transactions

The Blockchain

- Other possible uses besides Bitcoin
  - Settling other transactions
  - Contracts

Blockchain as Public Ledger

- The blockchain is a ledger of all transactions
- Transactions in Bitcoin are pseudo-anonymous
  - Address in blockchain is public
  - Don‘t know who has address, don’t know who did those transactions
  - If know who has address, know all transactions with by that person with that address

Blockchain and Payments

- The blockchain is an open protocol for settling payments across agents
  - No reason it has to be confined to Bitcoin
  - No reason it has to operate with miners competing
- Can operate with trusted agents
  - Real-time gross settlement
- Lots of issues
  - Prevent alterations
  - Finality

Blockchain and Ownership

- Author of book put a hash of the book's text on the blockchain before sending it to publishers
- Stock
  - NASDAQ is exploring using a blockchain for stock ownership
  - Obviously could use it for non-listed stocks
- Title to house
  - Legal issues

The Blockchain and Escrow

- Escrow on a house
  - Buyer transfers funds to bank of seller's agent
    - Returned if deal falls through
    - Cashed if house deal goes through or buyer backs out
    - Two of buyer's agent, seller's agent and buyer agree
- On blockchain
  - Put a "smart contract" for a transfer on the blockchain
    - Executed if two of these participants agree
    - Otherwise expires

Bitcoin and the Blockchain

- The blockchain is a big innovation
- Otherwise Bitcoin is similar to prior proposals
- The blockchain has the potential to alter many financial transactions

References

- Many papers on Bitcoin now
  - Economics and Computer Science
  - SSRN and Google Scholar
- My papers
  - "The Economics of Bitcoin and Similar Private Digital Currencies", Journal of Financial Stability, 2015
  - "Bits and Pieces: The Digital World of Bitcoin Currency", with Norbert Michel, Heritage Foundation Backgrounder
  - Blog, www.jerrydwyer.com/blog