<table>
<thead>
<tr>
<th>Principles</th>
<th>Policy</th>
<th>Management</th>
<th>Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>P</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>R</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>O</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **M**      | • External Accounts (BB)  
             • Internal Accounts (NN)  
             • Automatic Adjustment  
             • Active Adjustment (Fiscal, Monetary, Exchange, Wage)  
             • Structural Reforms  
             • BBNN at the industry level  
             • Automatic and Active Adjustment | • Decision Rules  
             • Product Markets  
             • Financial System  
             • Macro Prudential Regulation  
             • Fiscal and Monetary Institutions |
| **I**      | • Consistent Designed  
             • Market Inefficiency | • Demand Institutionality | • Public Choice  
             • Social Insurance  
             • Unacceptable outcomes  
             • Property Rights |
| **S**      | • Social Aspirations  
             • Political Aspirations  
             • Standards of Living (SP)  
             • Message  
             • Representation  
             • Transparency  
             • Accountability  
             • Political Influence  
             • Community Reach  
             • Corruption  
             • Commitment versus Involvement | • Demand Institutionality | • Social & Personal needs  
             • Political Voice & Representation  
             • Justice & equality  
             • Individual & Civil rights |
| **E**      | • Environmental (EE)  
             • Regeneration and Harvesting  
             • Waste Generation and Recycling  
             • Technology Improvement and Stocks  
             • Demand Control  
             • Biased Technological Improvement  
             • Biased Consumption Mixture  
             • Market Interventions: Prices and Quotas  
             • Production Mix  
             • Inputs Mix (Materials & Energy)  
             • Living at the Margin of the Unmeasurable | • Demand Institutionality | • Regulation (Markets, Prices, Quotas)  
             • International Coordination |
Currency, CryptoCurrencies, and BitCoin
# Physical Properties of Currency

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Divisible</td>
<td>A currency must be divisible so that units of its value can be paid to match the value of your purchase.</td>
</tr>
<tr>
<td>Scarce</td>
<td>Money has to be sufficiently rare. If the medium of the currency is easily obtainable or reproducible, it will have little worth and be easily counterfeited.</td>
</tr>
<tr>
<td>Portable</td>
<td>For a currency to be convenient, it must be portable.</td>
</tr>
<tr>
<td>Uniform</td>
<td>Every unit of a currency must be equal in value. Diamonds are not fungible because there are other properties of a diamond that makes it worth more or less than any other diamond.</td>
</tr>
<tr>
<td>Durable</td>
<td>Money must not have a property that allows it to decay over time. Any perishable items are a good example of this: Apples, Spices, Tea, Milk, etc.</td>
</tr>
<tr>
<td>Acceptable</td>
<td>Trusted and accepted by all</td>
</tr>
</tbody>
</table>
Currency

- **Economic Properties**
  - **Store of value**
    - Money must be able to be reliably saved, stored, and retrieved – and be predictably usable as a medium of exchange when it is retrieved.
    - The value must remain relatively stable over time.
  - **Medium of exchange**
    - Used to intermediate the exchange of goods and services.
    - For comparing the values of dissimilar objects.
    - Standard of deferred payment
      - Money is an accepted way to settle a debt.
      - When debts are denominated in money, the real value of debts may change due to inflation and deflation.
  - **Unit of Account**
    - A unit of account is a standard numerical monetary unit of measurement of the market value of goods, services, and other transactions.
      - Divisibility
      - Fungibility
Barter

Courtesy of FREE to use clip art. Source: Clipart Finders.
Goods *BECOME* Money

- Acceptable
- Durable
- Portable
- Scarce
- Divisible
- Recognizable

Peacefully and voluntarily, markets choose money.
Gold Storage -> Paper Receipts

<table>
<thead>
<tr>
<th>Gold Claims</th>
</tr>
</thead>
</table>

England, 17th Century

This image is in the public domain. Source: [Wikimedia Commons](https://commons.wikimedia.org/wiki/File:Gold_Storage.png).

Screenshot © Paul Grignon, 2006. All rights reserved. This content is excluded from our Creative Commons license. For more information, see [https://ocw.mit.edu/help/faq-fair-use/](https://ocw.mit.edu/help/faq-fair-use/).
Payment System

• Infrastructure
  – Operational network
  – Clearing system
  – Governed by laws, rules and standards
  – Links bank accounts for monetary exchange

• Security
  – Identification
  – Verifiability
  – Reversibility

• Payments
  – Instead of physical cash uses other instruments
    • Traditional
      – Checks and Money orders
    • Newer
      – Debit card, credit card, electronic transfers, internet banking, e-commerce
Public Ledger

- A very easy way to have a clearing system: public ledger written in stone!
  - Every transaction is written in stone
  - Everybody can verify
  - Transactions are not reversible
  - Hard to commit fraud (need another stone)
- Bitcoin has the same features....
What makes a good...

<table>
<thead>
<tr>
<th>Currency?</th>
<th>Payment System?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust</td>
<td>Trust</td>
</tr>
<tr>
<td>No counterfeiting</td>
<td>Verification of ownership</td>
</tr>
<tr>
<td></td>
<td>Verification of transaction</td>
</tr>
<tr>
<td>Anonymity</td>
<td>No Anonymity: Control Criminal Behavior</td>
</tr>
<tr>
<td>Clearing Automatic</td>
<td>Fast</td>
</tr>
<tr>
<td></td>
<td>Low Transaction Cost</td>
</tr>
<tr>
<td>Managed by Central Bank to deal with demand shocks</td>
<td>No Monetary or Fiscal Policy tool</td>
</tr>
<tr>
<td>Denomination of Contracts</td>
<td>No Denomination</td>
</tr>
<tr>
<td>No issue with Liquidity</td>
<td>Exchange System to guarantee liquidity</td>
</tr>
<tr>
<td>Peer to Peer</td>
<td>Needs Clearing System</td>
</tr>
</tbody>
</table>
BitCoin
What is Bitcoin?

• A peer-to-peer internet currency that allows decentralized (verification) transfers of value between individuals and businesses.
  – **Bitcoin** is the system
  – **bitcoins** are the units

• In economic terms
  – An International Currency
  – An international clearing system
  – A payment system/network
Creating a currency from scratch

• Motivation
  – Distrust of financial institutions
  – Transaction costs
  – CB Manipulation

• Primary concerns
  – Transaction security
  – Double spends
## Stripping down BitCoin

### How a macroeconomist thinks about the elements of BitCoin?

<table>
<thead>
<tr>
<th></th>
<th>How it is?</th>
<th>How it should be?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>Ledger</td>
<td></td>
</tr>
<tr>
<td>Clearing Transactions</td>
<td>BlockChain</td>
<td></td>
</tr>
<tr>
<td>Clearing House</td>
<td>Miners</td>
<td></td>
</tr>
<tr>
<td>Currency of Transaction</td>
<td>BitCoin</td>
<td></td>
</tr>
<tr>
<td>Currency</td>
<td>BitCoin</td>
<td></td>
</tr>
<tr>
<td>Form of Transaction</td>
<td>P2P + Anonymous</td>
<td></td>
</tr>
</tbody>
</table>
Transaction security

• Two levels of verification
  – Source is legitimate
  – Coins are legitimate

• Encryption
  – Public and private key verification ensures the legitimacy
TheoryCoin: (coins to ppl)

Encryption

**Input**

- Fox
  - cryptographic hash function
  - Digest: DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

- The red fox jumps over the blue dog
  - cryptographic hash function
  - Digest: 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

- The red fox jumps over the blue dog
  - cryptographic hash function
  - Digest: 8FD8 755B 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

- The red fox jumps over the blue dog
  - cryptographic hash function
  - Digest: FCD3 7FDB 5AF2 C6FF 915F D401 COA9 7D9A 46AF FB45

- The red fox jumps over the blue dog
  - cryptographic hash function
  - Digest: 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C
Double spends

• If the money is just digital codes, why not copy and paste to make more money?
  – Timestamps
    • Each transaction is packaged and publically recorded in the order it was carried out.
  – Hashes
    • The time-stamped group of transactions are given a unique algorithmically derived number
  – Block chain
    • Transactions are recorded in a community-built record of all transactions that acts as a proof-of-work.
    • Computers connected to the network accept the longest chain as accurate.
Digi-cash: Remittances

• anonymous
• secure (no double-spending)
• only transfer (no creation/storage)

...and bankrupted in 1999
The advent of Bitcoin

• 2009: **Bitcoin announced** by Satoshi Nakamoto
  – Pseudonym for person or group of person

• 2009-2011: slow start...

• 2011-2013: Silk Road and Dread Pirate Roberts

• End 2013: **Bitcoin price skyrockets**
  – and the world notices!
Elements of Bitcoin

- **Individuals**
  - Wallet (accounts)
  - Identity is anonymous
    - Private Key (sk)
    - Public Key (vk)

- **Transactions**
  - Peer-to-peer (decentralized)
  - Digital Signatures
  - Verification of “identity”
  - All transactions are public

- **Transaction Block**
  - List of transactions that are unrecorded

- **Transaction Block Chain**
  - List of transactions that have been recorded: Public Ledger

- **Miners**
  - **Objective**
    - Validate Transactions
      - Clearing house
    - Record transactions
      - Solve a complicated mathematical problem
      - Proof – of – work
  - **Remuneration**
    - When a block of transactions is recorded
    - Transaction fees
Elements of Bitcoin

Bn-1
T1: P1 a coins to P2......
T2: P1 b coins to P3......

Bn
T3...
T4...

Bn+1
T5...
T6...
Miners

• Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions.
  – This ledger of past transactions is called the block chain as it is a chain of blocks.
  – The block chain serves to confirm transactions to the rest of the network as having taken place.
  – Bitcoin nodes use the block chain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere.

• Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady.
  – Individual blocks must contain a proof of work to be considered valid.
  – This proof of work is verified by other Bitcoin nodes each time they receive a block.
  – Bitcoin uses the hashcash proof-of-work function.

• The primary purpose of mining is to allow Bitcoin nodes to reach a secure, tamper-resistant consensus.
TheoryCoin: How to transfer money

\[ m_1 = \text{"P3 gives coin 3 to P1"} \]
\[ s_1 = \text{Sig(stk3, } m_1) \]

\[ m_2 = \text{"P3 gives coin 3 to P2"} \]
\[ s_2 = \text{Sig(stk3, } m_2) \]
What info is in the transaction?

<table>
<thead>
<tr>
<th>Field Size</th>
<th>Description</th>
<th>Data type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>version</td>
<td>uint32_t</td>
<td>Transaction data format version</td>
</tr>
<tr>
<td>1+</td>
<td>tx_in count</td>
<td>var_int</td>
<td>Number of Transaction inputs</td>
</tr>
<tr>
<td>41+</td>
<td>tx_in</td>
<td>tx_in[]</td>
<td>A list of 1 or more transaction inputs or sources for coins</td>
</tr>
<tr>
<td>1+</td>
<td>tx_out count</td>
<td>var_int</td>
<td>Number of Transaction outputs</td>
</tr>
<tr>
<td>9+</td>
<td>tx_out</td>
<td>tx_out[]</td>
<td>A list of 1 or more transaction outputs or destinations for coins</td>
</tr>
</tbody>
</table>

The block number or timestamp at which this transaction is locked:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not locked</td>
</tr>
<tr>
<td>&lt; 5000000000</td>
<td>Block number at which this transaction is locked</td>
</tr>
<tr>
<td>&gt;= 5000000000</td>
<td>UNIX timestamp at which this transaction is locked</td>
</tr>
</tbody>
</table>

If all TxIn inputs have final (0xffffffff) sequence numbers then lock_time is irrelevant. Otherwise, the transaction may not be added to a block until after lock_time (see NLockTime).
TheoryCoin: Proof of Work

1. Everyone **tries to solve** a puzzle

2. The **first one** to solve the puzzle **gets 1 TC**

3. The solution of **puzzle $i$** defines puzzle $i+1$
TheoryCoin: Proof of Work

The puzzle:
given L, find R such that \( T = 0^d \)

*S aka Proof-of-Work*
TheoryCoin: Proof of Work

L = 011001100101010....
R = ??????....

T = 000000...0000xxxxxx

Public Ledger
- Previous hash
- New transactions

Hash for next block

d elements are zero

- Trial and error
- The more zeros the harder the problem: $2^d$ transactions
TheoryCoin: (coins to ppl)
How to create money

x₀ = Start!
x₁ = (P₁, i₁)
x₂ = (P₂, i₂)
x₃ = (P₃, i₃)

* aka the blockchain

SolvePuzzle(L) {
  repeat {
    R = my_name || i++
    T = H(L, R)
  } while (T ≠ 0ᵈ)
  return R
}
Problems

• Disclaimer: I am extremely affected by my research on law enforcement!
  – What is the purpose of the “coin”?
  – Why the remuneration to the miners is a tax on all holders, as opposed to a tax on each transaction?
  – Why the transactions need to be anonymous?
    • I understand confidentiality but anonymity?
Anonymity

• Volume and Weight of Cash
  – 1 Billion dollars in “new” 20 dollar bills
    • 50 million notes
    • Stack of 5km (3.11 miles)
    • Volume of 52 thousand litters (1.7 times a typical container)
    • Weights 50 tons
  – In BitCoin?
Payment System with Fixed Exchange Rate: Dollars as Collateral

One Bitcoin is a claim on one Dollar

Objectives of exchanges:
- Guarantee value of claims in the Bitcoin world
- Guarantee liquidity
- Guarantee convertibility

Miners:
- Payment CANNOT be paid by creation of Bitcoins
- Remuneration exclusively based on transaction fees
  - Constant “fee” charged per block
Payment System with Flexible Exchange Rate: Dollars as Collateral

One Bitcoin is a NOT claim on a Dollar.

Exchanges
- Inflation Targeting rules
  - Exchange rate risk
  - CPI target
- Pure payment system
  - International Transfers need to be arranged in the formal Banking system
  - Accounts might not need to be anonymous
- Remuneration
  - Taxes on participants
  - Capitalization of central exchange

Miners
- Payment CANNOT be paid by creation of Bitcoins
- Remuneration exclusively based on transaction fees
  - Constant “fee” charged per block
Payment System with Flexible Exchange Rate: Dollars as Collateral

Demand Shock: BBNN

Active Monetary Policy requires a tightening after a boom and a loosening after a recession

Supply Shock: BBNN

Active Monetary Policy should validate the new equilibrium. No need to “fight” the economy
What are the problems?

• Money Management
  – Good monetary policy needs active management of the money supply
    • Shocks to the aggregate demand need to be accommodated
    • Shocks to the aggregate supply should not be accommodated
  – Bitcoin has a parsimonious printing
    • This means that the adjustment occurs through inflation and deflation
    • Asymmetry: Cost of lowering prices and wages is larger than the cost of increasing prices and wages

• Criminal behavior
  – Anonymity and confidentiality is good for small transactions
  – Verifiability and openness is good for financial transactions

• Lack of reversibility
  – Some transactions need to be reversed (flash crash, and human error)

• What is Bitcoin?
  – A decentralized clearing system
  – A decentralized system of payments
  – A decentralized currency
## What I would do?

<table>
<thead>
<tr>
<th></th>
<th>How it is?</th>
<th>How it should be?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Documentation</strong></td>
<td>Ledger</td>
<td>Ledger</td>
</tr>
<tr>
<td><strong>Clearing Transactions</strong></td>
<td>BlockChain</td>
<td>BlockChain</td>
</tr>
<tr>
<td><strong>Clearing House</strong></td>
<td>Miners</td>
<td>Miners</td>
</tr>
<tr>
<td><strong>Currency of Transaction</strong></td>
<td>BitCoin</td>
<td>BitCoin</td>
</tr>
<tr>
<td><strong>Currency</strong></td>
<td>BitCoin</td>
<td>Basket</td>
</tr>
<tr>
<td><strong>Form of Transaction</strong></td>
<td>P2P + Anonymous</td>
<td>P2P</td>
</tr>
</tbody>
</table>

Remuneration in fee-for-use not money creation

Fixed to a single currency or a basket

Confidential but NOT Anonymous
Technical Slides
TheoryCoin: How to transfer money

(Digital) Signatures

– Only you can sign
– Everyone can verify
– You cannot deny

Give coin 3 to Schmittlein

Roberto
TheoryCoin: How to transfer money

"Your pin code"
secret key
message

Gen
message, signature

"Your username"
public key

Sign
accept/reject

Verify
TheoryCoin:
How to transfer money

$m = "P3 \text{ gives coin 3 to P1}"
\>
s = \text{Sig}(sk3,m)$

If $\text{Ver}(pk3,m,s) = \text{accept}$ and P3 owns coin 3 then return accept

$x_0 = \text{Start!} \quad x_1 = (P_1, i_1) \quad x_2 = (P_2, i_2) \quad x_3 = (P_3, i_3)$
TheoryCoin:
How to transfer money

\[ m_1 = \text{“P3 gives coin 3 to P1”} \]
\[ s_1 = \text{Sig}(sk_3, m_1) \]

\[ m_2 = \text{“P3 gives coin 3 to P2”} \]
\[ s_2 = \text{Sig}(sk_3, m_2) \]

* aka double spending
TheoryCoin: How to create money
(Double Spending)
TheoryCoin: How to store money

Main Idea:
Record **transfers** in the **blockchain**
How is money created in Bitcoin?

• New block every ~10 mins
  – $d$ adjusted every ~2000 blocks

• $H = 2^{\text{SHA2}}$

• Initial reward: 50 BTC
  – Halved every ~4 years (now 25 BTC)