The Irresistible Rise of Online Cryptographic Currencies

Dr George Danezis
University College London
<gdanezis@ucl.ac.uk>

Payment Instruments and Currencies

- Payment Instruments: Mechanism of how we transfer value.
  - Cash.
  - Letters of credit.
  - Cheques.
  - Bank transfer.
  - Debit card.

- Each payment instrument has a cost:
  - Actual monetary cost.
  - Handling cost.

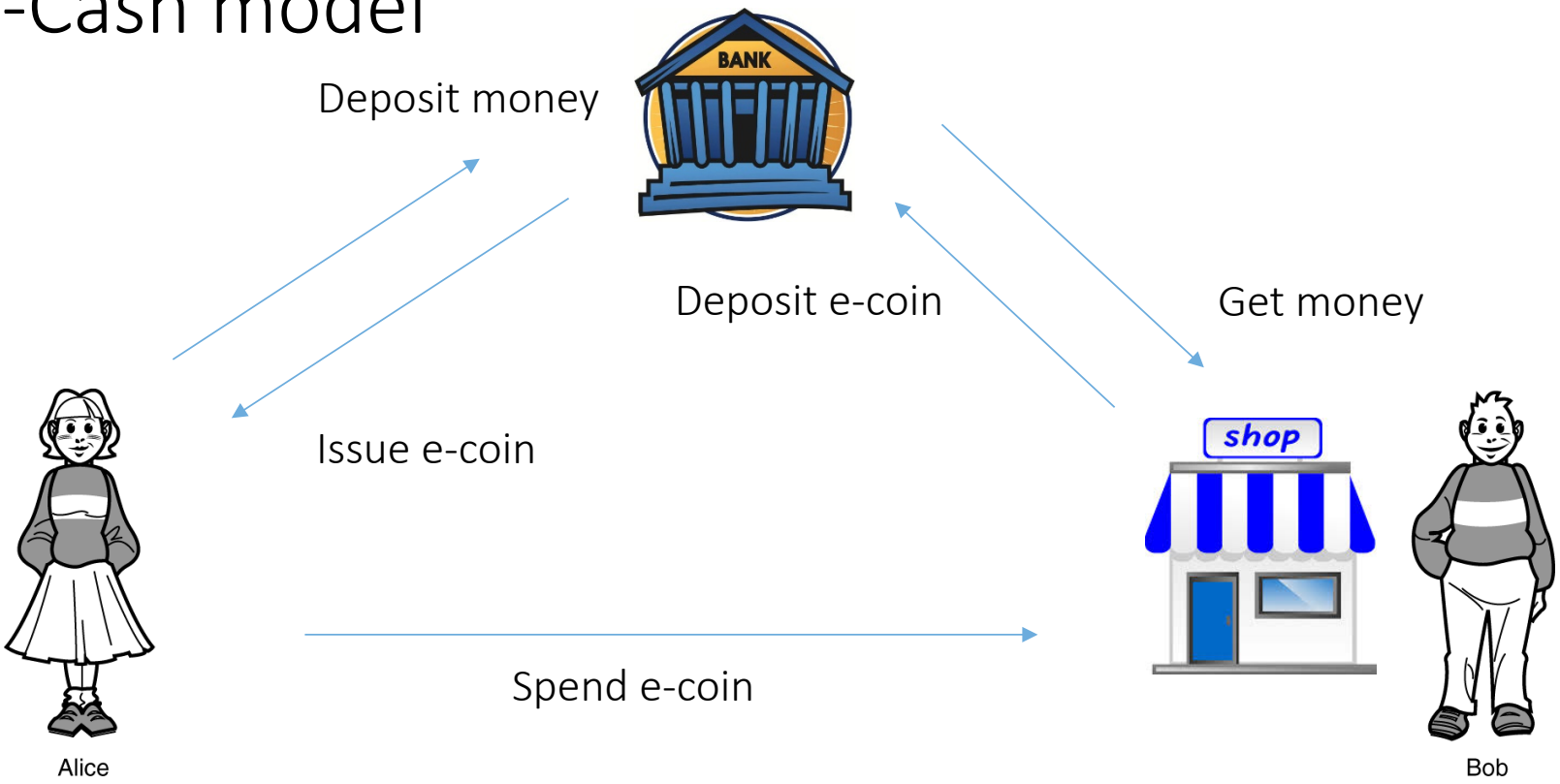
- Different instruments provide different security properties:
  - Integrity / authenticity
  - Privacy (i.e. cash vs. bank payments)

Cryptographic Payments

- Mainstream banking:
  - Europay, MasterCard and Visa (EMV) protocols.
  - Interoperation of Cards, Point of Sale terminals (PoS), Automatic teller machines (ATM).
  - First standard EMV 2.0 in 1995.
  - Uses tamper-resistant hardware, symmetric crypto and (maybe) digital signatures.

- Research & Development:
  - Digicash: Start-up of David Chaum (started 1990, bankrupt 1998).
    - Inventor or selective disclosure credentials. Visiting Prof. at KU Leuven!
    - Anonymous cash using cryptography – double spending prevention.
    - Long line of research on efficient e-cash: we know how to do this.
    - Model: central issuer of coins, in national currency denominations.

E-Cash model



- Key message:
  - We know how to do this extremely efficiently.
    - Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya: **Compact E-Cash**. EUROCRYPT 2005: 302-321
  - Properties:
    - High authenticity– no double spending.
    - Privacy: Shop and Bank cannot tell who customer was.
  - However:
    - **Not a new currency – This is not what this talk is about!**
    - Centralized "Bank" service to issue and deposit (and hold real value)

Currencies

- A way of :
  - Storing and remembering value (money).
  - Across time.
  - Across exchanges.

- "Fiat" money:
  - Has no intrinsic value aside its value as a currency.
  - Gold, cigarettes, mobile phone credits are **not** fiat currencies.

- It facilitates exchange
  - Acts a **unit of value** for exchanges.
  - Economically efficient alternative to barter (goods-for-goods) or commodity money (gold). (However: not a historical progression)

Bruce Champ, Scott Freeman, Joseph Haslag. Modelling Monetary Economies. (3rd Edition) Cambridge University Press.

Key problems in running a monetary system (I)

- The **money supply**:
  - It may go up, down or stay the same.
  - Money is like a "commodity":
    - If demand for money outstrips supply:
      Deflation -- value of money goes up. Value of goods goes down.
      Incentives to hoard – bad for transactions and productivity.
    - If demand lower than supply:
      Inflation – value of money goes down. Goods go up.
      Incentives to spend, or find alternative investment (turn into Capital).
    - Tension: the fairest system is if the money supply stays the same, no matter what the fluctuations in supply/demand are. (However this is not best for economic growth).
  - Key Question: **Who has control of the money supply in a currency?**
    - (UK: Bank of England)
  - Key Question: **Who gets the new money? Who deletes the old money?**

Key problems in running a monetary system (II)

- The memory:
  - Key Question: **How do we make sure we will always remember who has how much money?**
- The initial allocation:
  - If money is like a good: How do we bootstrap it?
  - Key Question: **Who has it to start with? (Does it matter?)**
- Bonus issue:
  - **How can I start my own currency?**

Early days: MojoNation

- Peer-to-peer file storage service.
  - Currency “Mojo”
  - Started around 2000 – stops operation in 2002.
  - Employed Bram Cohen (BitTorrent) and Zooko.
- Peers could chose to request a payment for a service.
  - Hope, self-regulating rates of requests and service.
  - Initially: Determining prices in the absence of a Market mechanism: Hard!
- Second price-auction at each server:
  - Client requests are all queued.
  - A second price auction is ran to determine which blocks to accept to store.
  - Clients need set a maximum number of Mojos they wish to pay to store.
- By 2002 the service experiences an economic meltdown.

The MojoNation economic catastrophe

- Economic catastrophe:
  - In 2005 CEO Jim McCoy says: “For core messaging protocols (e.g. our "Hello" message used to establish a connection) some clever users figured out that they could steal everyone else's credits by setting an outrageously high price for responding to this message. **Responding to this problem required us to hand out more credits to existing users**.”
- Daniel A. Nagy concludes:
  - “First, they allowed some unbacked currency into the market -- **mojo was handed out without any service in exchange**.”
  - “Then prices started crawling up, as those gouging the prices **did not feel the pressure of diminishing demand**.”
  - “Suddenly, precisely as described above by Jim, the operators found a system with an insatisfiable thirst for mojo, and **they had to keep pumping mojo into it, just to keep it running**. Classic case of a runaway hyperinflation, IMO.”
- What do we see here?
  - Uncontrolled creation of “money” by a central authority. (Money supply)
  - Unprincipled distribution of this new money around clients. (Distribution)
  - Market mechanism failure (as a result it is argued) – or because clients provided no value.
  - Service doom.

https://financialcryptography.com/cgi-bin/mt/mt-comments.cgi?entry_id=572

BitTorrent

- Zooko (2005) writes:
  - "Several of the ideas in BitTorrent can be understood as radical simplifications of ideas in Mojo Nation."
  - "One such perspective is to think of BitTorrent's tit-for-tat incentives as being **time-limited**, **file-specific**, and **non-transferrable** bilateral accounting."

- In 2001 Bram Cohen starts writing BitTorrent.
  - Tracker and peers cooperate to host (seeders) / download (leech) a large file.
  - Tit-for-tat mechanism: benefits from repeated interaction.
    give preferential service to peers that have provided you with a block.
  - Form of barter? Or bilateral accounting and local (time, file) currency?

- No need for a "full" currency.

Theory: Does the initial allocation matter?

- Say you rule with majesty a mythical land with no monetary system:
  - You generate 1000 coins – the only you will ever make (fixed supply).
  - Who do you give them to?
    At random? To your cronies? You keep them? To those with land?

- Coase theorem (1991 Nobel Prize in Economics)
  - "If trade in an externality is possible and there are sufficiently low transaction costs, bargaining will lead to an **efficient outcome regardless of the initial allocation** of property"
  - i.e. to an economist it does not matter!

- What does "efficient" mean?
  - It means that the money will be held and flow to where value was generated.
  - NOT: that the outcome of who holds the money will be the same.
  - In fact the initial allocation does determine who can generate the value!
  - E.g. An allocation where one party holds all the value and all the money is efficient.
    - MojoNation: the parties that stored the blocks ended-up holding all the Mojo.

- From a personal, welfare and a macroeconomic perspective (how to grow your economy) initial allocation matters.

Interlude: Chartalism

- The "state theory of money"
  - Money as a good with limited supply is rubbish!
  - "fiat currency has value in exchange because of sovereign **power to levy taxes on economic activity payable in the currency** they issue".
  - Thus: fiat currency acquires it value through the legitimacy / violence of the state.

- Argument against:
  - A number of value stores have value, without a state backing them. (although cigarettes, … may not be good examples due to use value)
  - Bitcoin!

- Interesting because:
  - Easier to start an electronic currency if you can **force some demand for it**.
  - Example: Linden dollars – **require all payments in Second life to be in Linden dollars**, and also issue them against other currencies.

Allocating “new” money, deleting “old” money

- When the money supply fluctuates:
  - Who gets the new money?
  - Who deletes their money?

- Options:
  - Give / delete money to those that already have money.
  - Give / delete money to those that do work.
  - Give / delete money at random, or equally to all.

- All of those have their own problems:
  - More money to those with money is unfair to “new generations” or those that did not have time to accumulate wealth.
  - More money to those with work is unfair to the “old generation” since it devalues their stored value.
  - At random or universally is “OK”. But who is “all”?

- Problem: **There is no constituency in an on-line voluntary currency**!
  - Uniformly or “at random” makes no sense without a fixed set.
  - Sybil attacks!

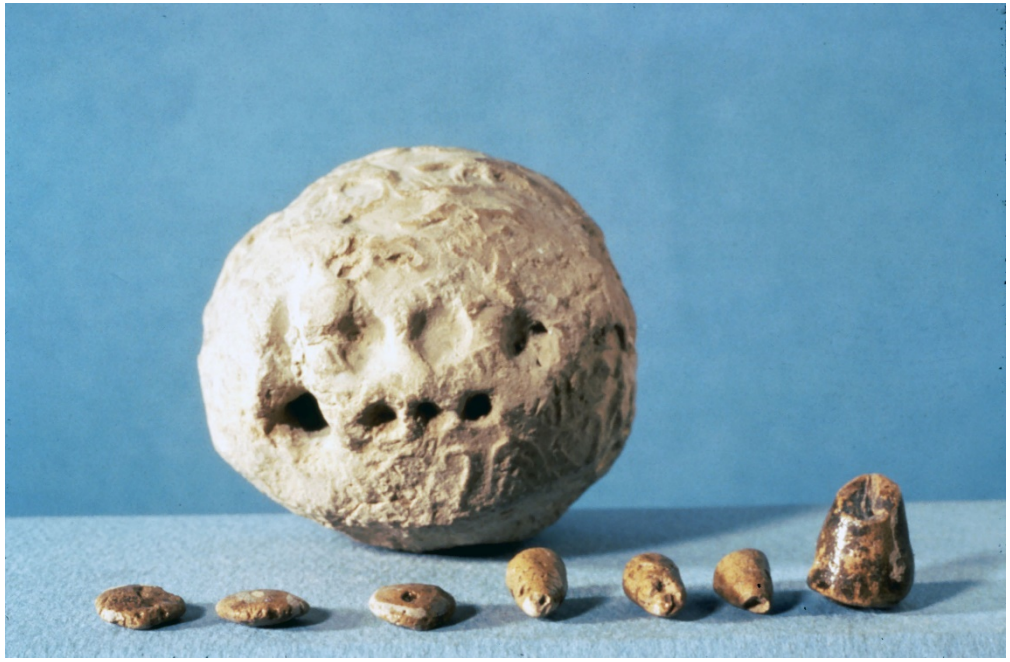
Bootstrap trust in a currency

- Money is merely memory:
  - There is a well understood amount + supply.
  - All other transactions act to transfer from one person to another.
  - No money is created or destroyed as part of the transaction.

- A high-integrity, high-authenticity, high-availability **append only log**.
  - Sufficient to implement money in theory.
  - Start by marking who has what money.
  - Enter a log entry for each transfer.
  - Voila!

- Two aspects of trust:
  - How do you know the “memory” will not be lost?
  - How do you know anyone will care about the money tomorrow?

Maintaining memory



The origins of writing

"Envelope and contents from Susa, Iran, circa **3300 BCE**."

"Each lenticular disc stands for "a flock" (perhaps 10 animals). The large cone represents a very large measure of grain; the small cones designate small measures of grain."

Tensions between centralized and de-centralized ways to remember value exchanges, debts, and what is due.

- Centralization: (Clay tablet) Economies of scale, high-integrity, vulnerable.
- Decentralized: (Coins) High-availability, difficult to destroy as a system, forgery.

(Image provided courtesy of Denise Schmandt-Besserat and Musée du Louvre, Département des Antiquités Orientales.)

At the beginning not money, but Debt.

- How do you ensure
  - That people “want money now”
  - Believe in the future people “will want” money

- Answer: You (the overlord) **only interact in money** – using you monopoly of violence.
  - **Coercion**: you make it “legal tender” in exclusivity with all other currency.
  - **Taxation**:
    - You owe land: you pay money for tax every year. (Not part of the crop!)
    - You have windows: you pay money for tax every year.
    - You trade or barter: you pay money per transaction. (Not a fish!)
    - You need a permit: you pay money.
  - **Payments**: You also pay in money for work done or goods to the state.

Pure state or Chartist theory of money

- Result: everyone needs money, and value it.
  - You believe you and other will want it in the future.

- Note: You only need to bootstrap.
  - After people believe that a fiat currency will persist there is no need for coercion to use it to mediate exchanges.

Pure exchange theory of money.

- Problem: cyber-currencies do not have taxation or coercion powers.

David Graeber. **Debt: The First 5,000 Years.** Melville House.

Centralized power is necessary! (maybe)

- Thesis: A centralized authority is necessary
  - Manage the money supply – it has to come from somewhere.
  - The supplier needs to have credibility and legitimacy to not abuse the supply.
  - Manage the initial allocation, and subsequent allocation.
  - Possibly create a constituency to allocate new money.
  - Bootstrap through coercion or taxation or buying power (chartalism).
  - Maintain the ledger of who holds what amount:
    - Fabricate and issue unforgeable coins.
- How could you perform all these functions without involving a centralized legal power with powers of coercion?
- However, centralization is also not without problems.

Case study: e-gold

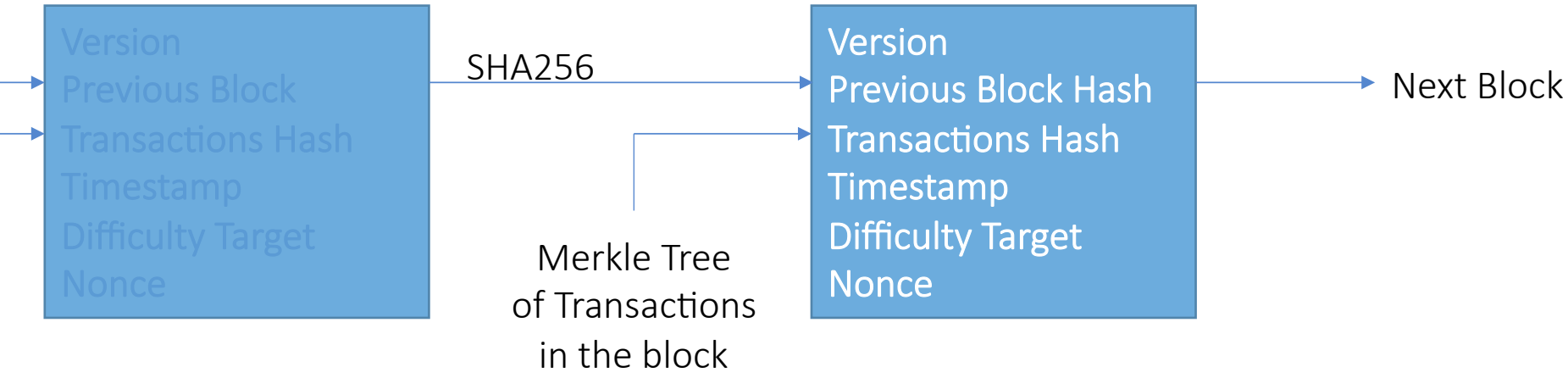
- Established in **1996**.
  - 1 million user accounts by **2002**.
- Features:
  - Centralized ledger of transactions.
  - Currency backed by real commodity, gold.
  - Network of international e-gold resellers.
- E-gold becomes a crime magnet:
  - Difficult to identify customers.
  - Easy to transfer internationally.
- Changing legal ground:
  - US Patriot Act (2001) requires money transmitters to be regulated.
  - In 2006-8 DOJ: money transmitter for any value system, not just money.
  - In **2008** directors face charges of money laundering and operating without a licence.
    They are found guilty and get away with fines, and suspended sentence.
    Asserts liquidated: $90M in gold (more than the central banks of bottom 1/3 countries).
  - California (2010) and other states: all digital value transfer systems are money transmitters.
- Lesson: **Centralization brings (legal) fragility**, unless it is backed by the state (even then).

Bitcoin (BTC)

- Paper in late October **2008**.
  - Released as open source software in 2009
  - Pseudonymous developer Satoshi Nakamoto.
  - Disappears in mid-2010.
  - He is estimated to have about 1M BTC.

- Bitcoin features (as in the original email):
  - `Double-spending is prevented with a peer-to-peer network.`
  - `No mint or other trusted parties.`
  - `Participants can be anonymous.`
  - `New coins are made from Hashcash style proof-of-work.`
  - `The proof-of-work for new coin generation also powers the network to prevent double-spending.`

Memory: the block chain



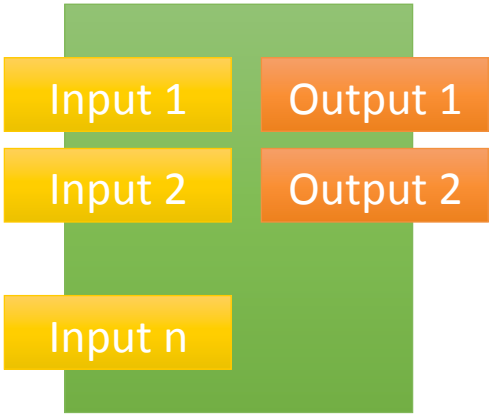
- A **block chain** storing all **transactions** is maintained by all.
- The last block is sufficient to guarantee the integrity of the full chain.
  - They form a hash tree of other blocks and transactions.
- The longest chain is recognized by all as the authoritative chain.
  - Blocks have some validity constraints that make them acceptable to all.

Transactions

Each input address signs the transaction.

The address and key must previously be in the block chain.

The full value of each address is input.



Transaction

Specify an output value and public key to transfer funds to.

Typical: Transfer and change

(Remaining go to miner as transaction fees to be included.)

- Bitcoins are transferred between addresses.
  - Address is identified by hash of public key
  - Private key used to sign transactions to spend coin.
  - Security property: authorization!
- Special transactions …

Where BTC money lives?

- Money lives in a **wallet**.
  - Wallet – stores the secret key for all user BTC addresses.
  - Secret keys are just bit sting.
  - If seen by an adversary they can transfer coins away from you.
  - **Bitcoin Theft**!
- Where do you put the wallet?
  - On client software. Downside: you get hacked – “bye bye” BTC.
  - On services. Exchanges and wallet services.
    - The service gets hacked – everyone’s money is stolen.
  - In hardware: a market in its infancy but growing
    - Parallel to Hardware Security Modules.
- Key insight: Hacking now allow you to steal money!
  - So are bad random number generators for the addresses.

Money supply: hashcash

- Hashcash (Adam Back):
  - Make users find hash collision to rate limit supply in distributed manner.
  - Original use: DoS prevention.

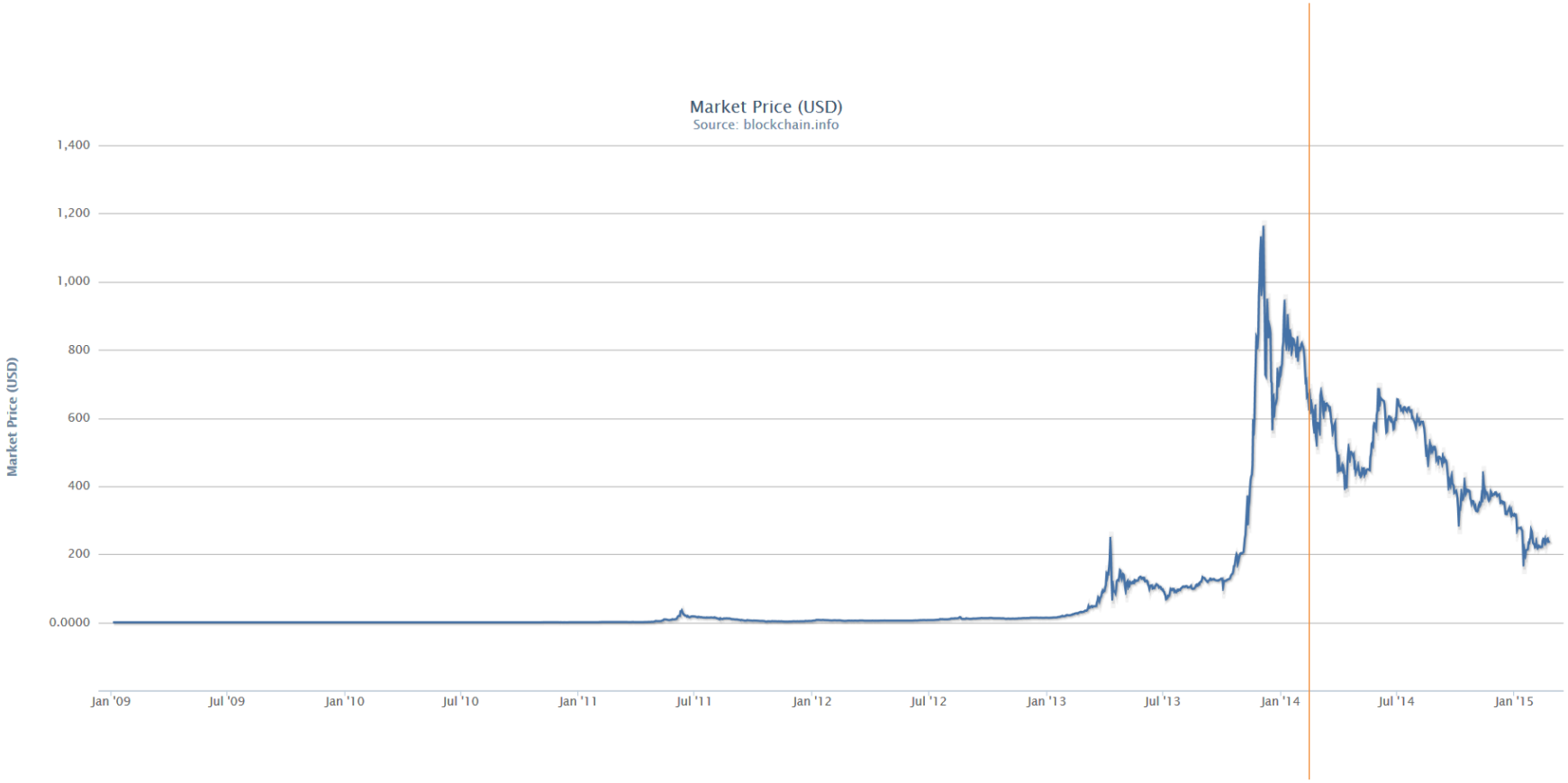
- Who controls the money supply?
  - Convention in code.
  - **Mining**: Take all advertised transactions and try to make a block.
  - A block is made using the previous block, transactions and nonce.
  - Hash of valid blocks need to be smaller than a target difficulty agreed by all.
    - Lottery
  - Difficulty level – tuned for 1 block every 10 minutes.

- Details
  - A single special transaction is within each block to create new Bitcoins.
  - How many depends on the length of the block chain.
  - **Bitcoins in existence will never exceed 21 million.**
  - After that? Transaction fees should kick in to provide incentives to mine.

Double spending prevention

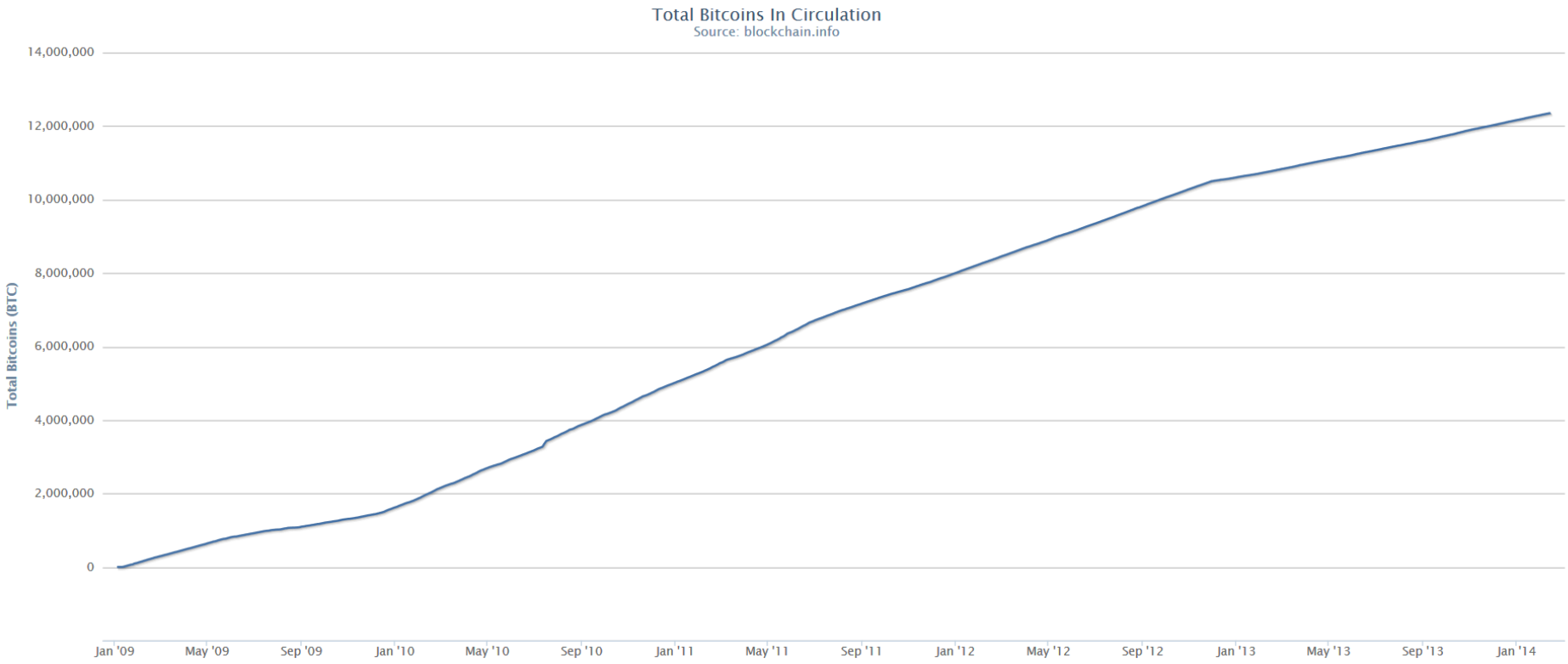
- Each transaction is **broadcast** to all miners in the network.
  - Massive peer-to-peer broadcast network.
- Miners only include, in the new block calculation, transactions that do not have inputs already spent.
- Other miners check blocks for double-spending, otherwise block is invalid.
- After a transaction has been included in a mined block it has received one confirmation.
  - Usually clients wait for 6 confirmations to consider a transaction confirmed.
  - 1 block = 10 min means 1 hour wait.

How much is a BTC worth?



SecAppDev 2014

Total BTC in circulation



About 12M BTC out of a maximum of 21M BTC have been mined in 5 years.
Rate of BTC / mining will slow down as more BTC are mined:
25BTC per block today, 6BTC per block by 2020.

Other key numbers

- 60K transactions per day (Feb 2014).
  100K transactions per day (Feb 2015)

- **$1.5M daily transaction volumes. (Feb 2015)**

- 22 500 000 GH / second (SHA256) (Feb 2014)
  329 000 000 GH / second (SHA256) (Feb 2015)

The cost of leaderless consensus

- A hidden consensus protocol:
  - Whichever coalition has **most hash power, has control of the block chain**.
  - Intuition: the conventional one will win.
  - Note merely demonstrating, actually using.
  - 329 000 000 GH/s is a significant cost.

- Equipment:
  - Rival estimates $40 per GH/s for specialized equipment.
  - In Dec 2013, 6M GH/s were added
  - $240M in equipment alone in Dec 2013.
  - This is not performing any useful task!

- Electricity + Networking costs.

How secure is the consensus?

- Hashing is like a lottery: you draw random numbers.

- NOT winner takes all:
  - If you have 10% of hashing power.
  - You also have 10% probability of sealing the next block.

- Therefore a block may be constructed that injects / removes certain transactions.
  - Best practice: wait for multiple blocks to confirm transactions.
  - Probability of a small minority creating successive ones is small.

Is Bitcoin really anonymous?

- BTC flows from “address” to “address”.
  - **Pseudonymous – not tied to a human, just a secret key.**
- However:
  - Exchanges accept national money and provide BTC.
  - Those nowadays implement “know your customer” policies
    (Or payments can be traced if done via conventional banking)
  - Once money is **in BTC you can follow money flow chains**.
  - Again it goes into normal banking system when it leaves.
- Forensic accountancy tricks:
  - Each transaction has many inputs, but two outputs:
    The recipient.
    The change address – this is the same as the sender.
  - Many small change addresses are consolidated to buy big things.
  - Result: can trace, and group, addresses per owner over time.
- In fact: **everyone can do investigations on public graph**.

Tracking thefts (1)

- From: UCSD

"A Fistful of Bitcoins: Characterizing Payments Among Men with No Names"

- Case Study 1:
  - The Betcoin gambling site was hacked in April 2012
  - 3,171 BTC were stolen in total (2902, 165, 17, and 87 BTC).
  - Did not move until March 15 2013 (bitcoin goes up)
  - Aggregated with other small addresses into one large address
  - Then began a peeling chain.
  - After 10 hops, a peel went to Bitcoin-24,
  - And in another 10 hops a peel went to Mt. Gox;
    in total, 374.49 BTC go to known exchanges, all directly off the main peeling chain, which originated directly from the addresses known to belong to the thief.

Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, Stefan Savage:
A fistful of bitcoins: characterizing payments among men with no names. Internet Measurement Conference 2013: 127-140

Tracking thefts (2)

- Case Study 2: Bitfloor theft
  - Large peels off; several initial peeling chains were then aggregated, and the peeling process was repeated.
  - Nevertheless, by manually following this peel-and-aggregate process to the point that the later peeling chains began, systematically followed these later chains and again observed peels to multiple known exchanges.
  - The third peel off one such chain was 191.09 BTC to Mt. Gox, and in total we saw 661.12 BTC sent three popular exchanges (Mt. Gox, BTC-e, and Bitstamp).

- Case Study 3:
  - Thief stole bitcoins by installing a trojan on the computers of individual users
  - Unable to confidently track the flow of the stolen money
  - Most of the stolen money did not in fact move at all
  - Of the 3,257 BTC stolen to date, 2,857 BTC was still sitting in the thief's address, and has been since November 2012.

- Conclusion: It is very **hard to exfiltrate the proceeds of crime** at scale.

See: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

How to make Bitcoin anonymous?

- Proposal: ZeroCoin (http://zerocoin.org/)

- Key idea:
  - Each Address has a hidden serial number and a key.
  - When spending, you have to release the serial number and sign with the key.
  - You also **prove that the serial number and key are in the block chain**.
  - **Without revealing where**!

- Security properties:
  - Integrity: Zero-knowledge proof that serial and key are in the block chain.
  - Double-spending prevention: check that the serial is not already used.

Transaction Maleability

- Major exchanges suspend operations in Feb 2014!

- What is the problem:
  - Transaction: Addresses In, Addresses Out, signatures, and other metadata.
  - Signature is generates on critical fields: In, Out, volumes.
  - Transaction ID is generated on all fields, critical and not critical.
  - Result: transaction ID could be changed.

- So?
  - There has been a rise in the volume of changed Transaction IDs.
  - Speculation of fraud:
    - Customer makes a transaction using an exchange, with TID1.
    - Then it changes it so that TD2 is registered in the blockchain.
    - Then it calls customer support claiming that TD1 is not in the chain.
    - The exchange re-issues the transaction – and double pays.
  - Morality: Make sure your IDs are bound to the items and have high integrity.

Bitcoin as a currency

- **Who has control of the money supply in a currency?**
  - By convention it follows a well understood and committed curve.
  - Will max out.
  - Convention enforced by software.
- **Who gets the new money? Who deletes the old money?**
  - No money is deleted (if you want a laugh: go suggest random deletions!)
  - Money is created by hashing blocks and adding them to the block chain.
  - The Miner gets the new coin.
- **How do we make sure we will always remember who has how much money?**
  - Large block-chain is recorded by all.
  - Authoritative one is the longest – race for aggregate CPU power.
- **Who has it to start with? (Does it matter?)**
  - Satoshi Nakamoto.
- **Where did the demand come from?**
  - …

Philosophy & research problem

- **Can we avoid the Bitcoin waste**?
  - Is that even a problem? (Is bitcoin more expensive than cash?)
  - What about only hashing one day a year?
  - What about running an election / consensus protocol?
  - What about running a non-inflationary currency?

- Not so simple!
  - Problem of constituency.
  - Everyone who could hash is part of Bitcoin.
  - Who is otherwise entitled and who is not? (e.g. election)
  - Confirm transactions?

- Centralization:
  - Are exchanges not becoming too centralized?
  - Are some mining operations not becoming too powerful? (% of pool)

The future of on-line currencies

- Regulator attention cannot be avoided:
  - US: Bitcoin friendly – for the moment.
  - China: Not so much.
  - How it can be regulated depends on the mechanism – decentralization.

- Rapid evolution of payment instruments and mechanisms:
  - Banks and EMV are dinosaurs.
  - Bitcoin can act as a backing currency to innovate in payments and finance.
  - Whatever works will become mainstream.
  - **Prediction: in 20 years the Euro or Pound will "look like" bitcoin (digital).**

- Is there room for more than one on-line currency?
  - Litecoin, Dogecoin, and and all that?
  - Unclear: bootstrapping problem – lucky Cyprus crisis – gambling & drugs markets benefited Bitcoin growth.
  - What Benefit? Better anonymity? Cheaper to run?

- **Is a zero-governance currency possible?**