DIGITAL CASH: BITCOINS AND CRYPTOLOGY

DANIEL SEGAL

CRYPTOCURRENCY

WHAT IS CRYPTOCURRENCY?

- A digital currency that derives its value and security from cryptographic principles
- Difficult to counterfeit & trace
- Utilize public and private keys for transfer

THE VALUE IN CRYPTOCURRENCY

- Not regulated by a central bank
- Market forces drive value

Chart from bitcoincharts.com

ATTEMPTED CRYPTOCURRENCIES

- Many cryptocurrencies have failed
  - Qubic
  - TimeKoin
  - BBQCoin
  - Coiledcoin
- Currencies fail when system is broken or not enough users participate
- Bitcoin (BTC) is only current successful cryptocurrency

THE BITCOIN: BASICS

SATOSHI NAKAMOTO

- Introduced bitcoins in a paper (2008)
- Nakamoto is a presumed pseudonym for a person or group of people
- Currently no confirmed identity
  - Posted to forums from a German IP address
  - Active times corresponded with somebody in EST
  - Uses British formatting, but American spelling
  - Has since stepped down from public eye
- Wrote and maintained bitcoin client, “mined” first bitcoins on January 3, 2009

GOALS OF BITCOIN

- Eliminate need for a central authority
- Enable easy transfer of bitcoins between individuals
- Create a secure & private economy

OBSTACLES TO BITCOIN

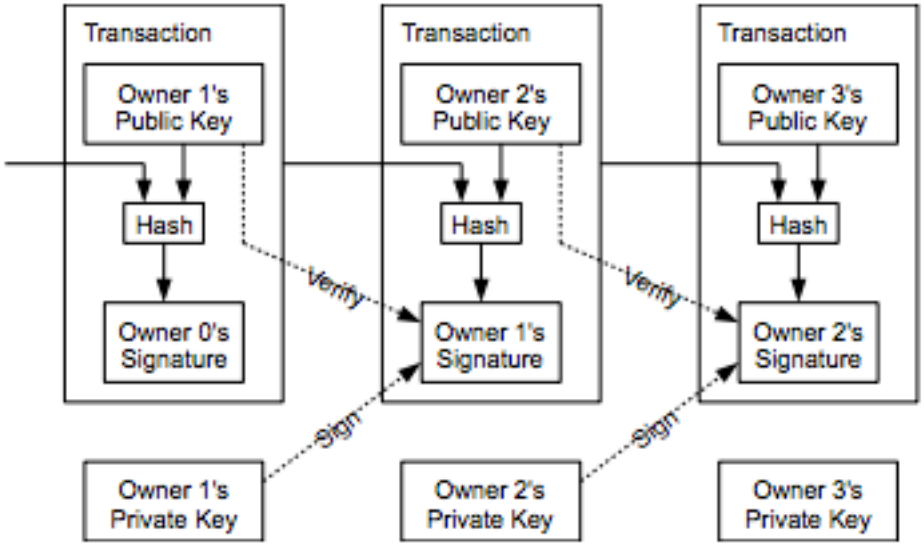
- Double Spending Problem
  - Digital “coins” (character strings) are easy to reproduce, how do you prevent somebody from spending those coins multiple times

- Sybil (51%) Attacks
  - Since no central authority, users need to agree on validity of transaction. If a malicious user controls 51% of the network (via processing power or number of identities), they can overrule honest users

THE BITCOIN: IMPLEMENTATION

SOLUTION: THE BLOCK CHAIN

- “Block chain” is bitcoin’s answer to these problems
- Every user has record of every transaction and helps verify these transactions
- Longest chain is assumed to be correct

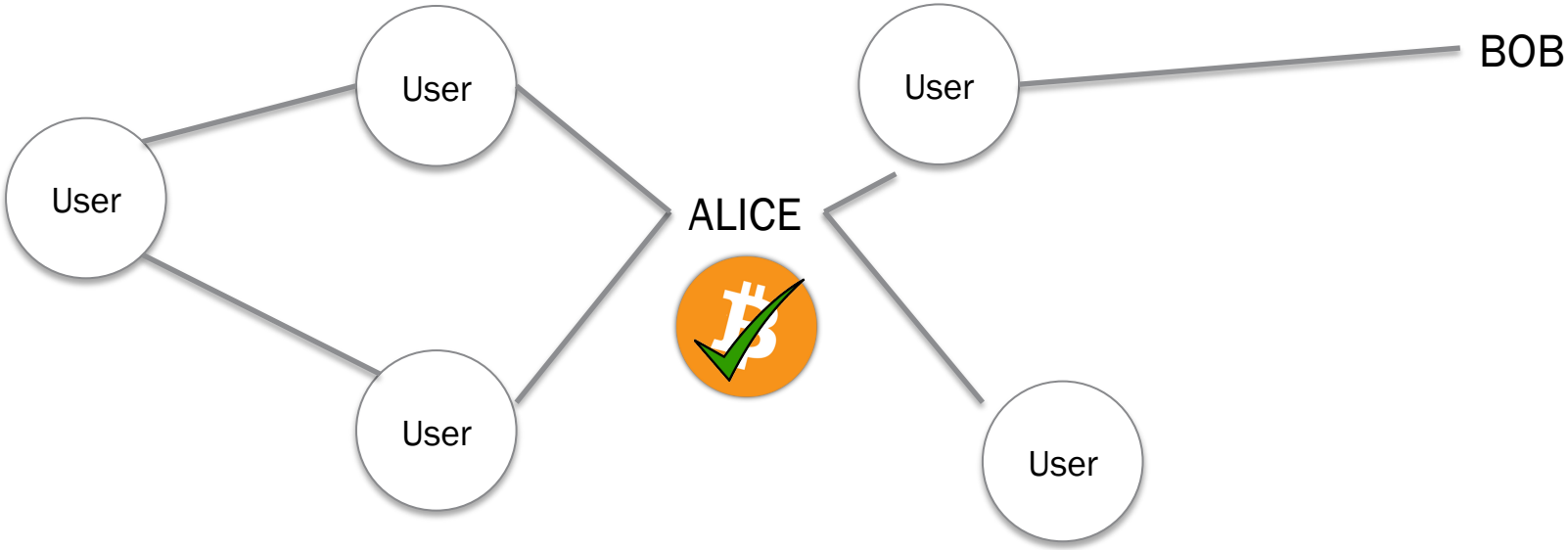


A BITCOIN TRANSACTION

Step 1) Alice decides to pay a sum of bitcoins to Bob

Step 2) Alice signs the transaction with her private key

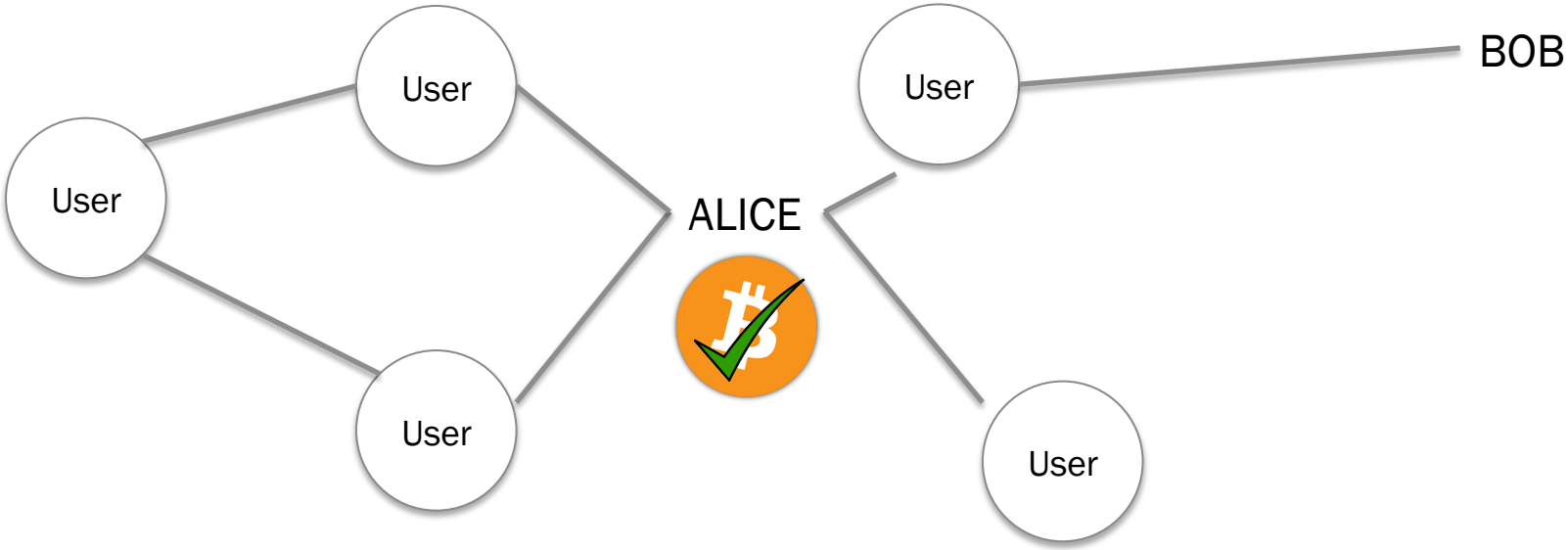
Step 3) Alice's client notifies other clients of the transaction



A BITCOIN TRANSACTION

Step 4) Each node competes to solve a computationally hard problem (this problem will be described later)

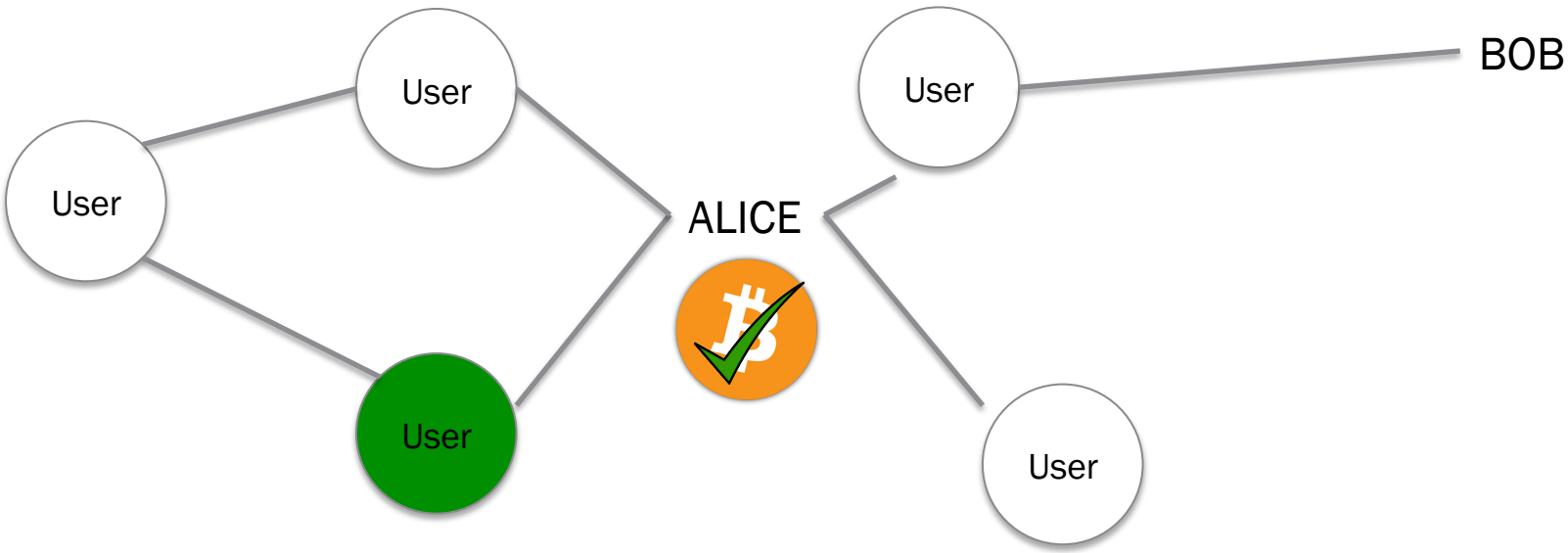
Step 5) A node broadcasts that it has found a solution



A BITCOIN TRANSACTION

Step 6) Each node verifies the solver node's solution

Step 7) The transaction authorized and added the the block chain



THE BITCOIN: MATHEMATICS

THE HASHES

- Two different types of hashes used
  - SHA-256
    - 256 bit SHA-2 (Secure Hash Algorithm, Generation 2)
    - Designed by National Security Agency (NSA), published by National Institute of Standards and Technology in 2001
  - RIPEMD-160
    - 160 bit RIPEMD variant (RACE Integrity Primitives Evaluation Message Digest)
    - Designed academically, published in 1996
- Both currently believed to be secure

THE HASHES

- SHA-256 used for creating aforementioned difficult problem (stay patient, we will get to this soon)
  - Always used twice (hashed value is hashed again)
- RIPEMD-160 used for bitcoin address
  - Used after value has already been hashed by SHA
  - Useful for shorter digest size
  - Address is user's bitcoin "wallet
  - Alice transfers bitcoins to Bob by sending them to his address

THE SIGNATURE

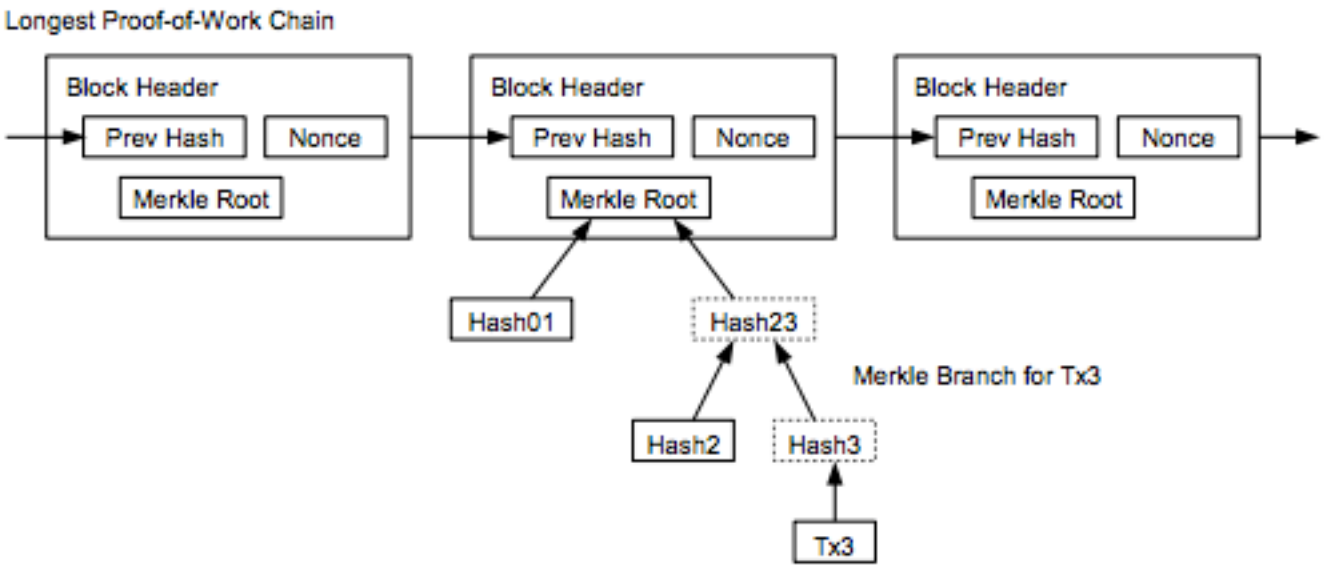
- Alice uses the elliptic curve digital signature algorithm (ECDSA) to sign transactions
  - Uses secp256k1 curve given in Standards for Efficient Cryptography
    - 128 bits of security
    - Over a 256 bit field
    - Comparable in strength to 3072 bit RSA

THE TRANSACTION

- Signature releases bitcoins from previous transaction (i.e. whenever the bitcoins were transferred to Alice)
- Can only be authorized by current owner's private key
- Transaction contains amount and destination address

THE BLOCK CHAIN

- Proofs of work stored as Merkle (Hash) Tree
- Allows old leaves to be deleted
- Can verify transaction by attempting to insert into place in block chain



THE “HARD” PROBLEM (FINALLY)

- Find a value which, when double hashed by SHA-256, begins with n zeroes where n is set by the bitcoin network in proportion to amount of processing power available (more power = hard problems)
  - Keep incrementing a nonce (k in this example) stored in the transaction block until find an appropriate value

    k = 1 SHA-256: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

    k = 2 SHA-256: d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35

    .
    .
    .
    .
    .

THE “HARD” PROBLEM (FINALLY)

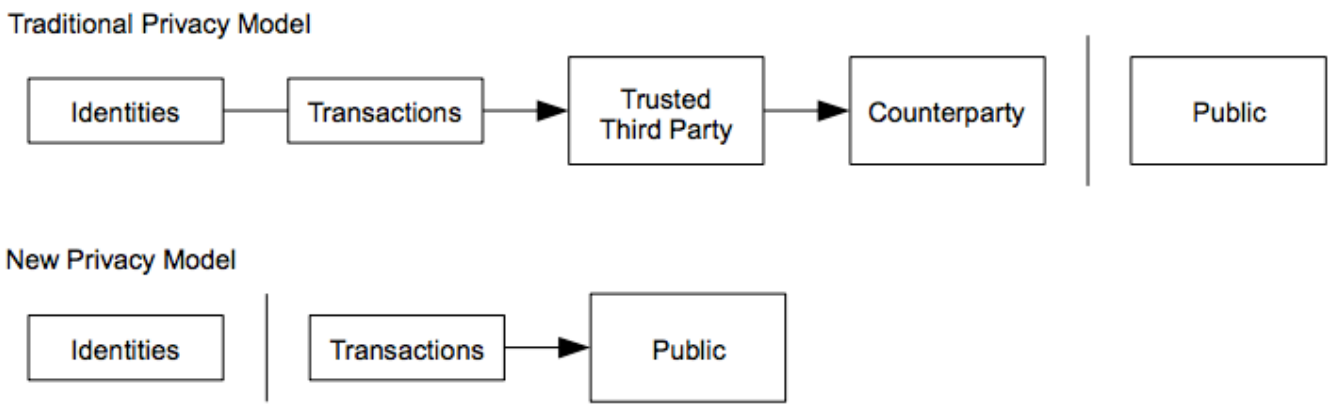
- Entire network can solve a problem every 10 minutes
  - 62.118 x 10^{12} hashes per second
- Would take an individual several weeks – months (currently)

BITCOINS: PRIVACY & SECURITY

HOW PRIVATE ARE BITCOIN TRANSACTIONS

HOW PRIVATE ARE BITCOINS

- Bitcoin network makes efforts to remove user identifiable information
- Never transmit to a person, just to a hashed address
- Security is contingent on address not being linked to person
  - As bitcoins grow in popularity, government agencies might start building databases



HOW SECURE ARE BITCOINS

Very

(until you add people into the mix)

HOW SECURE ARE BITCOINS

- All of bitcoins cryptographic functions are provided by established and vetted algorithms (SHA-256, ECDSA)
- Only one vulnerability identified so far:
  - Bug found in transaction log that did not properly verify transactions which overflowed transaction size
  - Two users generated 184 billion bitcoins in a day
  - Protocol was updated, transaction reversed

HOW SECURE ARE BITCOINS

- All malicious attacks on bitcoins have been focused on peripheral trading sites and wallets
- Users store their bitcoin wallet online to avoid loss, malicious users gain access
- Trading websites have been exploited (mass sell offs) to manipulate market value of bitcoins

PREVENTING 51% ATTACKS

- By design, bitcoin network is 1 vote per CPU instead of 1 vote per IP
- Malicious user would need to control 51% of processing power, and then could only double-spend own money, can't create money
- Since longest chain accepted as correct chain

  p = probability honest node finds next block

  q = probability attacker finds next block

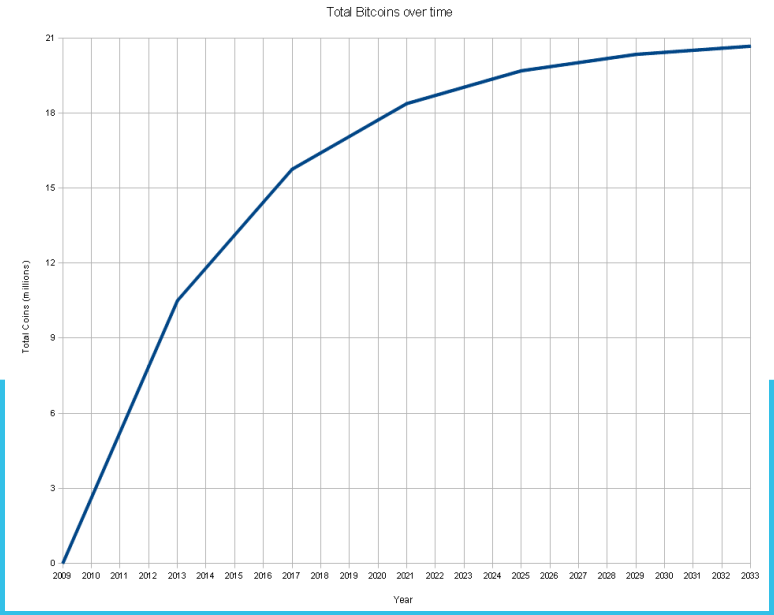
  q_z = probability attacker can catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

DIGITAL CASH, ANALOG MARKET

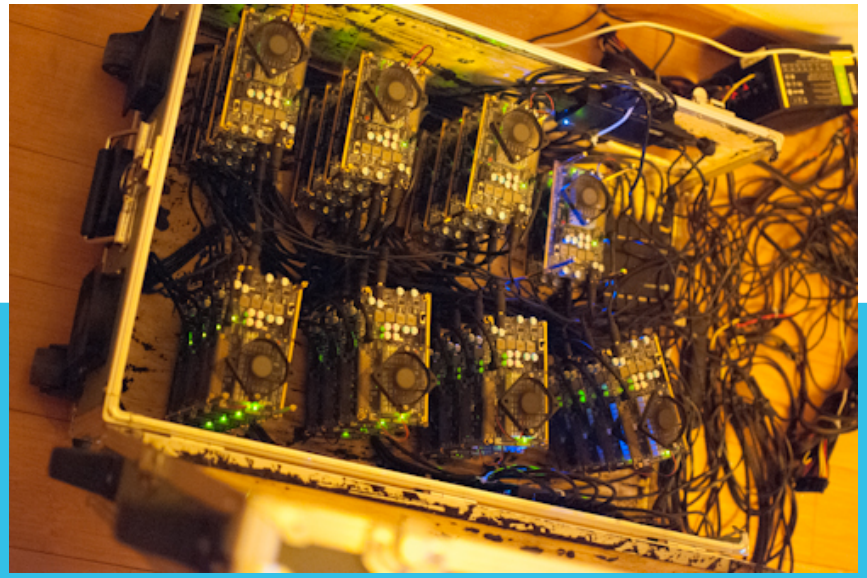
WHERE DO BITCOINS COME FROM?

- Mining
  - Every time a transaction is verified, node that verified it gets a predetermined number of bitcoins
    - Started at 50BTC
    - In March, dropped to 25BTC
  - BTC limited to 21 million, intended to last until 2140



MINING BITCOINS

- Difficult for individual user to mine bitcoins at this point
- People are building machines specifically to mine bitcoins
  - GPU heavy machines
  - Top commercial devices can try ~60 billion hashes per second
- Balance performance against energy costs (current estimates of $150,000 in power used daily mining bitcoins)
- Many users join mining “pools”, contribute computing power for portion of block payout



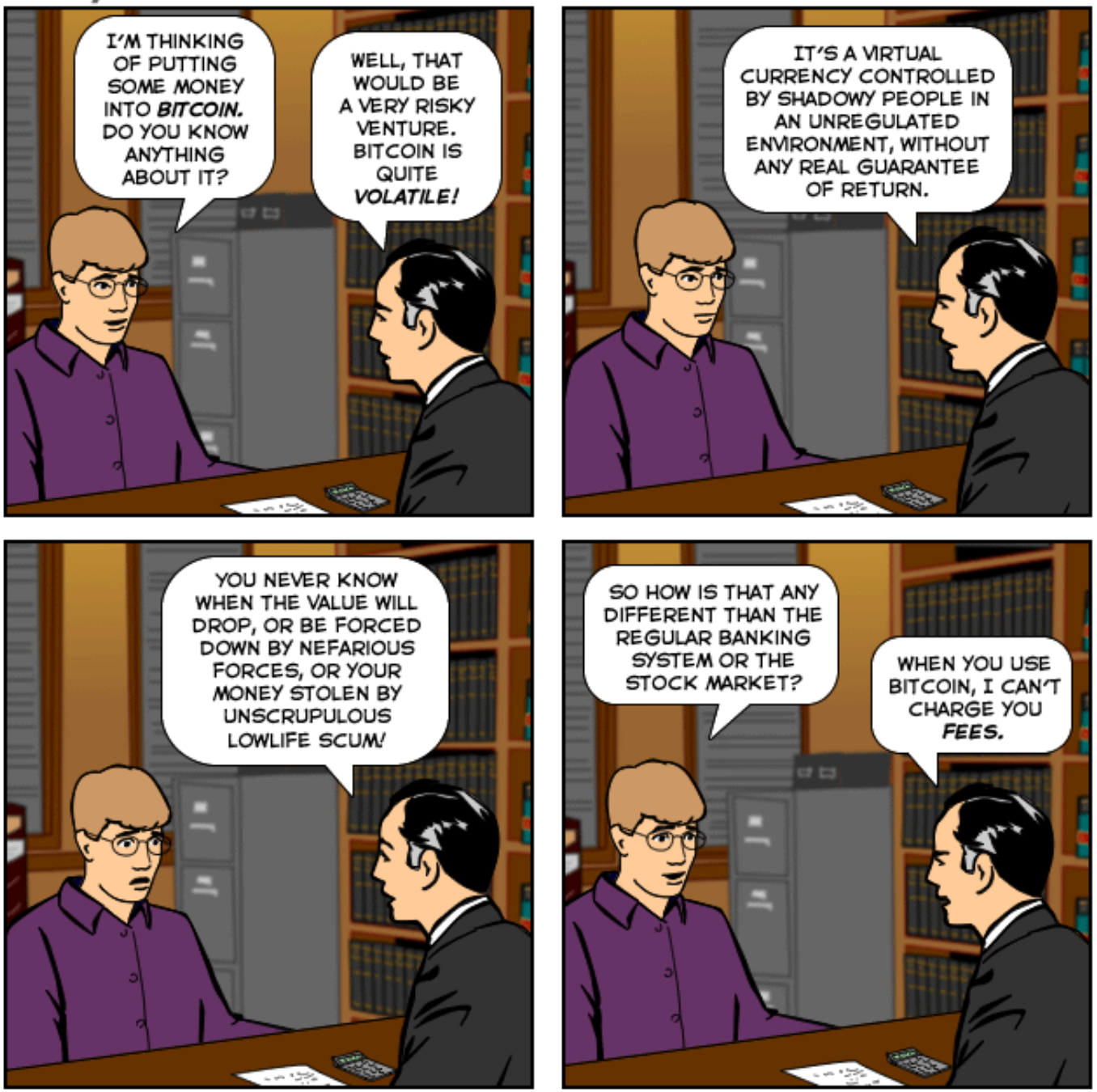
WHAT CAN YOU BUY WITH BITCOINS

- First purchase made with bitcoins was on May 21st 2010. A Florida programmer gave a man in England 10,000 BTC to order him a pizza from Papa Johns.
- Many niche companies are starting to accept bitcoins
  - Web services (VPN, web hosting)
  - Gambling
  - A dental practice in Seattle
  - Alpaca socks (0.2487 BTC)
- Most people are treating bitcoin as an investment

TRADING BITCOINS

- Several exchanges have been created
- Largest is Mt. Gox (www.mtgox.com)
  - Handles 70% of bitcoin trading
  - Over past year has handled $550,704,696.11 of currency

by Nitrozac & Snaggy




Bitcoins


Dotcom Bubble


Dotcom Bubble Pops

QUESTIONS?