e-Puzzles and Bitcoin

Konstantinos Karasavvas

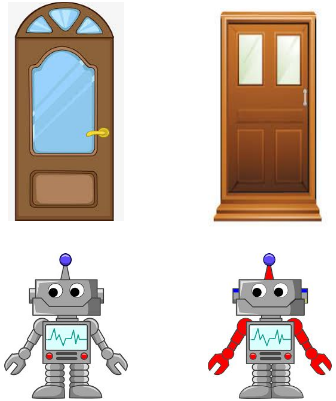
Logic Puzzles: The two robots

You are trapped in a room with two doors. One leads to certain death and the other leads to freedom. You don't know which is which.

There are two robots guarding the doors. They will let you choose one door but upon doing so you must go through it.

You can, however, ask one robot one question. The problem is one robot always tells the truth ,the other always lies and you don't know which is which.

What is the question you ask?



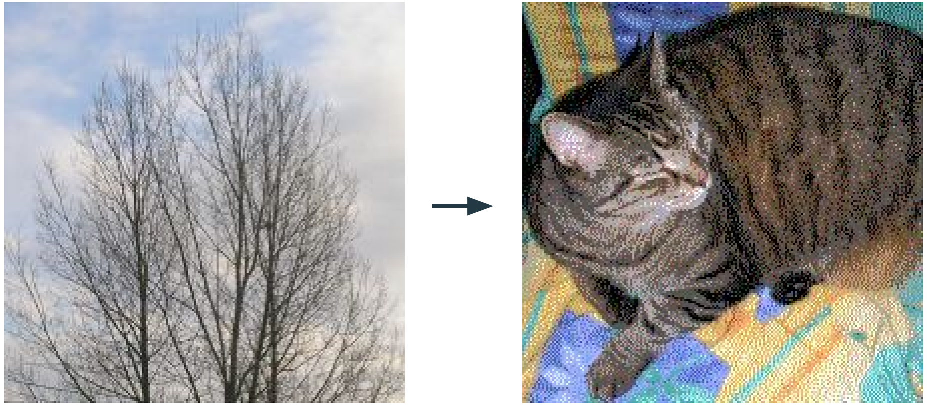
http://www.folj.com/puzzles/

Steganography puzzles

- Tattoo on person’s scalp
- Morse code knitted into clothing
- World War II microdots

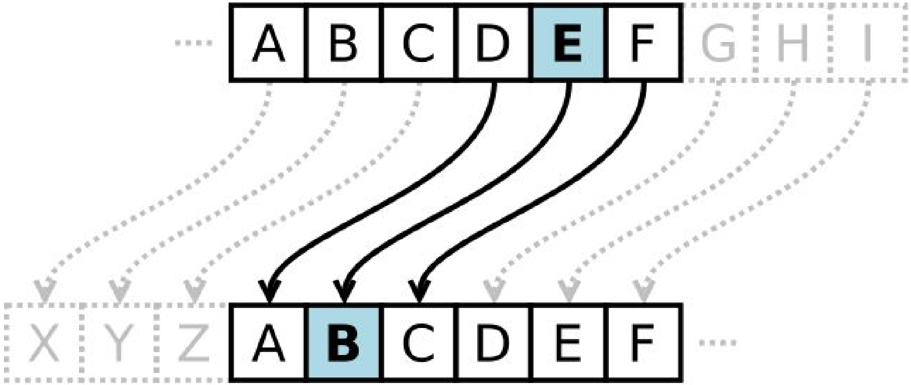
- Digital Steganography

The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization.



Cryptography puzzles

- Cryptanalysis puzzles
- From trivial…
  - Ceasar’s Cipher, ROT13
- … to advanced/modern
  - Symmetric / Asymmetric
  - Block / Stream
- NSA Puzzle Periodical



Cicada 3301

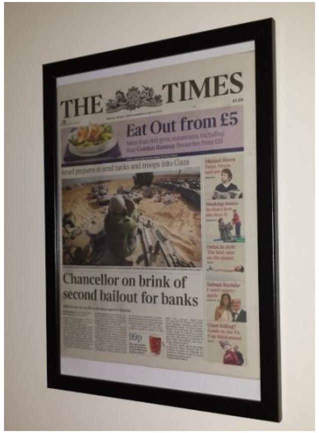
- The most elaborate puzzle of the internet age
  - 3 rounds of increased complexity
  - Jan 2012, Jan 2013, Jan 2014
  - Recruit “intelligent individuals”
  - Steganography, cryptography, logic, Mayan numerology, cyberpunk speculative fiction

  - https://en.wikipedia.org/wiki/Cicada_3301

Bitcoin Trivia / Hidden Gems

- Genesis Block (coinbase)
    - Hex for “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks/”

- Bitcoin’s logo have been extracted as well...



THE TIMES

£1.50

Eat Out from £5

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

99p

From Ken Shirriff's blog

Bitcoin Trivia / Hidden Gems, cont.

- Nelson Mandela tribute
  - in fake addresses!

Nelson Mandela (1918-2013)

"I am fundamentally an optimist. Whether that comes from nature or nurture, I cannot say. Part of being optimistic is keeping one's head pointed toward the sun, one's feet moving forward. There were many dark moments when my faith in humanity was sorely tested, but I would not and could not give myself up to despair. That way lays defeat and death." …

…

From Ken Shirriff's blog

Bitcoin Trivia / Hidden Gems, cont.

- Coinbase, (Saint) Eligius pool: Catholic prayers

  Benedictus Sanguis eius pretiosissimus. -- Benedictus Iesus in sanctissimo altaris Sacramento. -- Ave Maria, gratia plena, Dominus tecum. Benedicta tu in mulieribus, … -- ...and life everlasting, through the merits of Jesus Christ, my Lord and Redeemer. -- O Heart of Jesus, burning with love for us, inflame our hearts with love for Thee. -- Jesus, meek and humble of heart, make my heart like unto thine!

- Replies:
  - "Oh, and god isn't real, sucka. Stop polluting the blockchain with your nonsense."
  - "FFS Luke-Jr leave the blockchain alone!"

- And reply (link: Rick-rolling!):
  - "Militant atheists, http://bit.ly/naNhG2 -- happy now?"
    - Rick Astley - Never Gonna Give You Up

From Ken Shirriff's blog

Bitcoin Trivia / Hidden Gems, cont.

- XSS demo
  - Hex of output script of txid: 59bd7b2cff5da929581fc9fef31a2fba14508f1477e366befb1eb42a8810a000

```
<script>window.alert("If this were an actual exploit, your mywallet would be empty.")</script>
```

- Some Bitcoin explorers did not escape HTML tags … !?

From Ken Shirriff's blog

Bitcoin Trivia / Hidden Gems, cont.

- Len Sassaman tribute, Creature simulator in Basic, The original Bitcoin Paper, …
- Text from Bhagavad Gita, 1000 digits of pi, several images

- And… the Wikileaks cablegate data !
  - 2.5MB file (cablegate-201012041811.7z)
  - 130 separate txs, each containing 20k bytes
  - Each donating 1 Satoshi to Wikileaks

From Ken Shirriff's blog

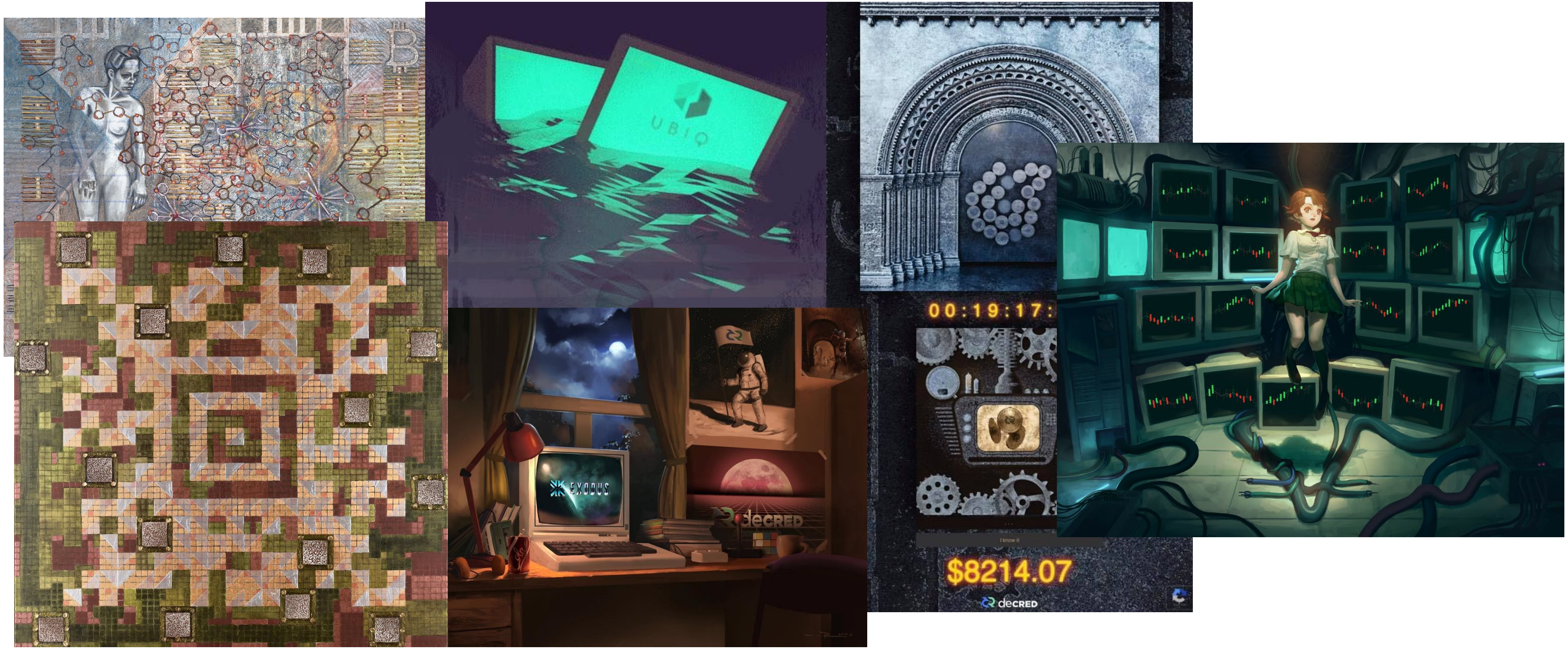
Bitcoin Puzzles

- Marguerite Christine art puzzles
  - *"The Legend of Satoshi Nakamoto"*
- Puzzle 1
  - June 2014
  - 3.4 Bitcoin treasure ($1,300 at the time)
  - dedicated group of 20 talented people
  - 2 weeks of work
  - 32-page solution explanation
  - Cody Wilson
    - defence distributed (eg. 3D guns)
  - Amir Taaki
    - hacker, programmer, activist
  - The duo initiated the Dark Wallet project (later forked into OpenBazaar)

Bitcoin Puzzles

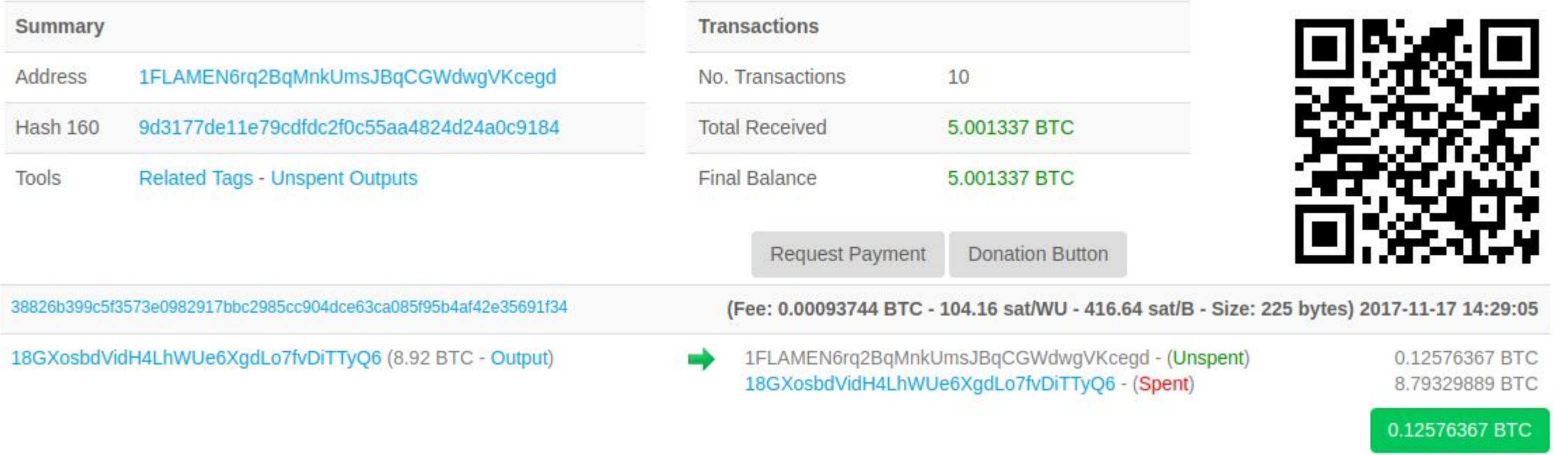
- Puzzle 2
  - *"The Legend of Satoshi Nakamoto"*
  - September 2014
  - 4.87 bitcoins reward
  - Unsolved
- Dedicated team of people
  - Forum, chats, etc. to coordinate
  - Still working to solve it!

More puzzles



Puzzle^2

- 4.87 bitcoins reward
- 17 November 2017
  - +0.125 BTC to the address 1FLAMEN6…



Summary	
Address	1FLAMEN6rq2BqMnkUmsJBqCGWdwgVKcegd
Hash 160	9d3177de11e79cdfdc2f0c55aa4824d24a0c9184
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	10
Total Received	5.001337 BTC
Final Balance	5.001337 BTC

38826b399c5f3573e0982917bbc2985cc904dce63ca085f95b4af42e35691f34 (Fee: 0.00093744 BTC - 104.16 sat/WU - 416.64 sat/B - Size: 225 bytes) 2017-11-17 14:29:05

18GXosbdVidH4LhWUe6XgdLo7fvDiTTyQ6 (8.92 BTC - Output) ➡ 1FLAMEN6rq2BqMnkUmsJBqCGWdwgVKcegd - (Unspent) 0.12576367 BTC
18GXosbdVidH4LhWUe6XgdLo7fvDiTTyQ6 - (Spent) 8.79329889 BTC

0.12576367 BTC

Meanwhile in a secret room... (1)

- Hmm, private keys are just 256bit numbers
- I will create thousands of random private keys
  - I will first get all addresses from the blockchain
  - If a corresponding Bitcoin address exists, I get the coins !!

Meanwhile in a secret room... (1)

- Hmm, private keys are just 256bit numbers
- I will create thousands of random private keys
  - I will first get all addresses from the blockchain
  - If a corresponding Bitcoin address exists, I get the coins !!

- Ehm, there are more combinations than the atoms in the universe…
  - Bummer, no coins for me

Meanwhile in a secret room… (2)

- Hmm, a lot of libraries allow you to create private keys from passphrases…
  - SHA256(`Kostas’) returns a 32 byte sequence that can be used as a key !
  - What if people used that and I can guess their passphrases ?!

Meanwhile in a secret room... (2)

- Hmm, a lot of libraries allow you to create private keys from passphrases…
  - SHA256(`Kostas’) returns a 32 byte sequence that can be used as a key !
  - What if people used that and I can guess their passphrases ?!
- Whoa! I got some valid private keys !!
  - "i find your lack of faith disturbing"
  - "these aren't the droids you're looking for"
  - "satoshi nakamoto"

Meanwhile in a secret room... (2)

- Hmm, a lot of libraries allow you to create private keys from passphrases…
  - SHA256(`Kostas’) returns a 32 byte sequence that can be used as a key !
  - What if people used that and I can guess their passphrases ?!
- Whoa! I got some valid private keys !!
  - "i find your lack of faith disturbing"
  - "these aren't the droids you're looking for"
  - "satoshi nakamoto"
- But but… already empty… most probably meant to be found !
  - Address creator’s claimed them, or
  - Others already guessed them and emptied them

Meanwhile in a secret room… (3)

- What if someone used a block hash as their private key?
  - Block height only

Meanwhile in a secret room… (3)

- What if someone used a block hash as their private key?
  - Block height only

- Whoa!
  - 46 addresses (2009-2016)
  - … all empty, not surprising

Meanwhile in a secret room... (4)

- What if someone used the merkle root as their private key?
  - Block height only

Meanwhile in a secret room... (4)

- What if someone used the merkle root as their private key?
  - Block height only

- Whoa… ok I will stop whoa-ing !
  - 6 addresses
  - … all empty

Meanwhile in a secret room… (4)

- What if someone used the merkle root as their private key?
  - Block height only

- Whoa… ok I will stop whoa-ing !
  - 6 addresses
  - … all empty

- What what… about transaction ids?
  - Some successes again … all empty again

Meanwhile in a secret room… (5)

- Now… what about hashing the hash of a phrase ?
    - SHA256(SHA256(“hello”)

Meanwhile in a secret room… (5)

- Now… what about hashing the hash of a phrase ?
  - SHA256(SHA256(“hello”)

- Yep! Several successes…
  - ‘sender’ x 2
  - ‘receiver’ x 2
  - ‘hello’ x 4 … and ‘hello’ x 65535
  - ‘password’ x 1975

Meanwhile in a secret room… (5)

- Now… what about hashing the hash of a phrase ?
  - SHA256(SHA256(“hello”)

- Yep! Several successes…
  - ‘sender’ x 2
  - ‘receiver’ x 2
  - ‘hello’ x 4 … and ‘hello’ x 65535
  - ‘password’ x 1975

- Yeah yeah… all empty.

Meanwhile in a secret room... (6)

- Now… what if the hash of an address is the private key of another address?
    - SHA256(1LGUyTbp7nbqp8NQy2tkc3QEjy7CWwdAJj)
        - 4300d94bef2ee84bd9d0781398fd96daf98e419e403adc41957fb679dfa1facd
    - Raw bytes that correspont to:
        - KyTxSACvHPPDWnuE9cVi86kDgs59UFyVwx2Y3LPpAs88TqEdCKvb
    - … which is the private key of address:
        - 13JNB8GtymAPaqAoxRZrN2EgmzZLCkbPsh

Meanwhile in a secret room... (6)

- Now… what if the hash of an address is the private key of another address?
  - SHA256(1LGUyTbp7nbqp8NQy2tkc3QEjy7CWwdAJj)
    - 4300d94bef2ee84bd9d0781398fd96daf98e419e403adc41957fb679dfa1facd
  - Raw bytes that correspont to:
    - KyTxSACvHPPDWnuE9cVi86kDgs59UFyVwx2Y3LPpAs88TqEdCKvb
  - … which is the private key of address:
    - 13JNB8GtymAPaqAoxRZrN2EgmzZLCkbPsh

- Bingo! (see? No whoa-ing!)
  - A lot of successes on this one!
  - … all zero balances (oh, well)

Meanwhile in a secret room... (6)

- Now… what if the hash of an address is the private key of another address?
  - SHA256(1LGUyTbp7nbqp8NQy2tkc3QEjy7CWwdAJj)
    - 4300d94bef2ee84bd9d0781398fd96daf98e419e403adc41957fb679dfa1facd
  - Raw bytes that correspont to:
    - KyTxSACvHPPDWnuE9cVi86kDgs59UFyVwx2Y3LPpAs88TqEdCKvb
  - … which is the private key of address:
    - 13JNB8GtymAPaqAoxRZrN2EgmzZLCkbPsh

- Bingo! (see? No whoa-ing!)
  - A lot of successes on this one!
  - … all zero balances (oh, well)

- But… hmm… the balances where emptied within minutes or **seconds** … !

Meanwhile in a secret room... (7)

- Why would someone create addresses and empty them… **seconds** later?
- A bot?
- This is getting serious…

Meanwhile in a secret room… (Theory 1)

- A coding error at some exchange or other software ?

- Could be … but too weird of a bug to cause such a predictive behaviour
  - … especially since someone is moving all the coins immediately
  - … maybe someone realized what was happening and created a bot?

Meanwhile in a secret room... (Theory 2)

- Someone installed malicious code to an exchange / wallet / etc.

- Why not include a salt when hashing the source public address?
  - SHA256(address + `some random salt')
  - Code reviews

- Quite clever actually
  - One could predict the next address/private key pretty easily

Meanwhile in a secret room... (Action 1)

- Bot that actively checks those addresses (which we can control)

Meanwhile in a secret room… (Action 1)

- Bot that actively checks those addresses (which we can control)

- After 48 hours 9.5 BTC are transferred to one of those addresses
  - $23k at the time !
  - But but… my bot did not transfer those coins properly !!

Meanwhile in a secret room… (Action 1)

- Bot that actively checks those addresses (which we can control)

- After 48 hours 9.5 BTC are transferred to one of those addresses
  - $23k at the time !
  - But but… my bot did not transfer those coins properly !!

- Yep, after 15 minutes the coins were gone…

Meanwhile in a secret room… (Action 2)

- Fixed bot…
  - 2 txs within 24 hours (< 0.1 BTC)
  - Did not want to raise any flags

- After 3-4 days a 0.3 BTC transaction appeared
  - After 7 days it was moved by their owner/bot

Meanwhile in a secret room... (Upgrading)

- More experimentation and upgrading
  - Hashing of addresses, transactions, block hashes and merkle roots were used for destination addresses/keys

- Re-running the bot revealed ~6 transactions per day !

Meanwhile in a secret room… (Endgame)

- Nov 12 2017
  - 9 BTC were transferred
- 17 November 2017
  - +0.125 BTC to the address 1FLAMEN6…
- Shortly after a reddit post (fitwear) was claiming theft of 9 bitcoins
  - Blockchain.info
  - Money was sent back (-0.125)
- Blockchain.info claimed that account was compromised
  - But, but… he took a lot of precautions

Meanwhile in a secret room… (Endgame)

- When a wallet is created several addresses are pre-generated
- Sending funds automatically sends change to one of those addresses (round-robin)
- It is possible that malicious code would send some of the change to new addresses
  - Generated by existing wallet addresses or transactions etc.
- Theft occurred immediately after fitwear sent 9 BTC to blockchain.info
  - From paper wallet !
  - He took a lot of precautions (typed key from paper wallet, 2FA, …)
- Blockchain.info did not find anything suspicious in their codebase
- “Going dark now....bye.”

Questions ?

Website:	www.kkarasavvas.com
Linkedin:	https://www.linkedin.com/in/kkarasavvas
Twitter:	@kkarasavvas
Email:	kkarasavvas@gmail.com
Bitrated:	https://www.bitrated.com/kostas
Keybase:	https://keybase.io/kkarasavvas