Storing Data, Inscriptions and Bitcoin Resiliency

Kostas Karasavvas

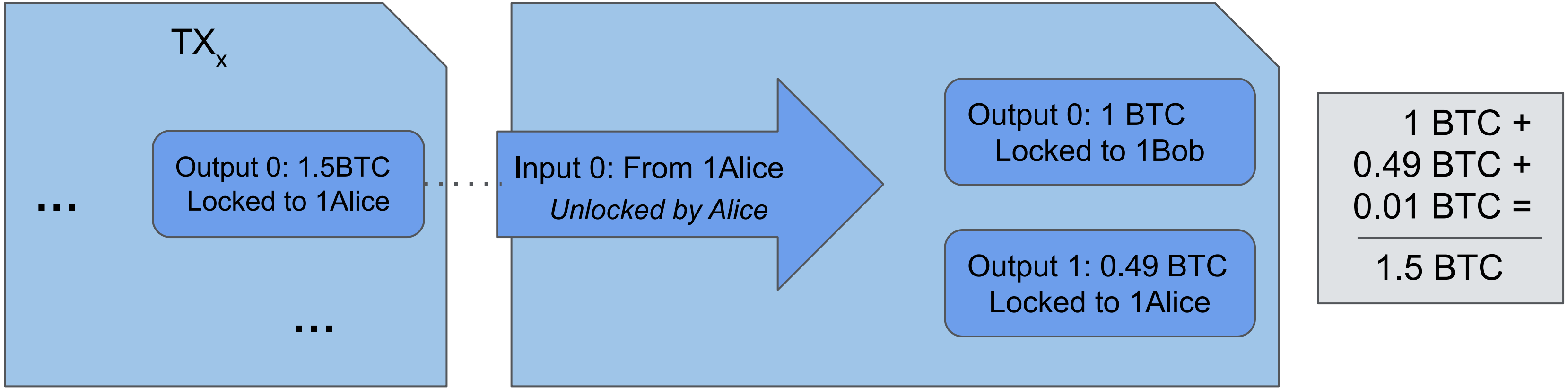
@kkarasavvas

Agenda

- Storing Data in Bitcoin
- Stored Data / Hidden Gems
- OP_RETURN Wars
- Inscriptions / NFTs on Bitcoin?
- Bitcoin Resilience
- Summary

Transactions and UTXOs Basics

- Funds are locked with scripts
    - they require an unlocking script to spend them
- Unspent Transaction Outputs are were the funds reside
    - they are tracked by every node



Transaction Validity vs Standardness

- A valid transaction does not need to be standard
- A standard transaction needs to also be valid
- Non-standard transactions are not relayed
- A miner can add valid transactions even if non-standard
- A simple user can only add standard transactions

Storing Data directly - OP_RETURN

- An opcode that allows storing a small amount of data into the blockchain
- Valid OP_RETURN transactions can be up to the block size limit (1MB)
  - and more than one per tx
- Standard OP_RETURN transactions can be up to 80 bytes
  - and only one per tx
- OP_RETURN outputs are ignored wrt UTXO set
  - this is important as it does not bloat the network

Storing Data indirectly

- Coinbase transactions
  - only for miners

- Fake addresses
  - unintended use

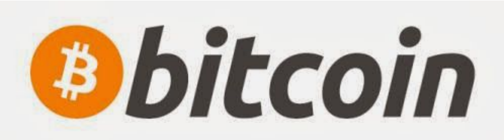
- Fake public keys in multi-signature outputs
  - unintended use

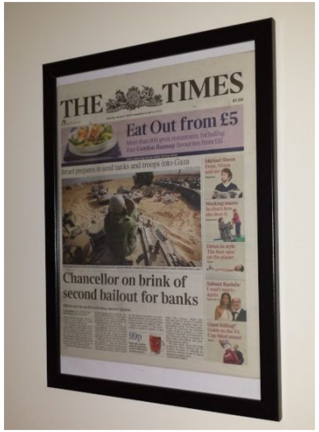
- Such transaction outputs are part of the UTXO set
  - network nodes are bloated (for ever!)

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 has been extracted as well…





THE TIMES

Eat Out from £5

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

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

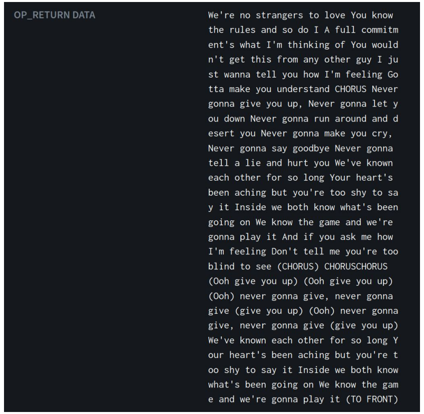
Bitcoin Trivia / Hidden Gems (?), cont.

- 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
    - Stored in OP_RETURN (>80 bytes)



OP_RETURN DATA

```
We're no strangers to love You know
the rules and so do I A full commitm
ent's what I'm thinking of You would
n't get this from any other guy I ju
st wanna tell you how I'm feeling Go
tta make you understand CHORUS Never
gonna give you up, Never gonna let y
ou down Never gonna run around and d
esert you Never gonna make you cry,
Never gonna say goodbye Never gonna
tell a lie and hurt you We've known
each other for so long Your heart's
been aching but you're too shy to sa
y it Inside we both know what's been
going on We know the game and we're
gonna play it And if you ask me how
I'm feeling Don't tell me you're too
blind to see (CHORUS) CHORUSCHORUS
(Ooh give you up) (Ooh give you up)
(Ooh) never gonna give, never gonna
give (give you up) (Ooh) never gonna
give, never gonna give (give you up)
We've known each other for so long Y
our heart's been aching but you're t
oo shy to say it Inside we both know
what's been going on We know the gam
e and we're gonna play it (TO FRONT)
```

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

OP_RETURN Wars

- Counterparty meta-protocol (layer 2)
  - Early 2014 (Bitcoin Core 0.9.0)
  - used to create assets on top of Bitcoin (other coins, NFTs, etc)
  - OP_RETURN allowed only 40 bytes back then, which, was not enough
  - used multi-signature outputs to encode the meta-protocol
    - thus bloating the network

- Accused of bloating the network by Bitcoin developers

- A proposal to increase the OP_RETURN limit to 80 bytes appeared

- After much debate it was not accepted by the Bitcoin developers

OP_RETURN Wars, cont.

- Counterparty continued using multi-signature outputs to store data
- Some nodes started filtering (censoring?) Counterparty transactions
- Counterparty changed the way the stored data to evade the filters
- Filters were updated …
- In 2016 (Bitcoin Core 0.12) the limit was increased to 80 bytes
    - Counterparty started using OP_RETURN

Segwit (v0)

- Segregates witness from transaction
  - several benefits like fixing transaction malleability
  - but now we are concerned only about blocksize

- 1MB limit

- 4MB weight limit
  - theoretical size with full segwit txs is ~2.8MBs

- Segwit txs have a 75% discount
  - the witness (spending) part !

Segwit (v0), cont.

- Maximum tx weight is 400kBs
  - standardness rule
  - note standardness for legacy size txs is 100kBs

- Maximum script size is 3600 bytes
  - standardness rule - consensus is 10000 bytes

- Maximum non-push opcodes is 201 per script

Taproot (v1)

- Removed the maximum script size limit
    - not 3.6kBs for standardness or 10kBs for consensus anymore

- Removed the 201 non-push opcodes limit per script

- These limits were removed to allow for more sophisticated scripts

Inscriptions / NFTs

- Indirect method to store data
- A taproot tx (output) is required
- A second tx spends it by including a really big script
    - the inscription is in the unlocking script (witness script)
- Because it is spent it does not burden the UTXO set

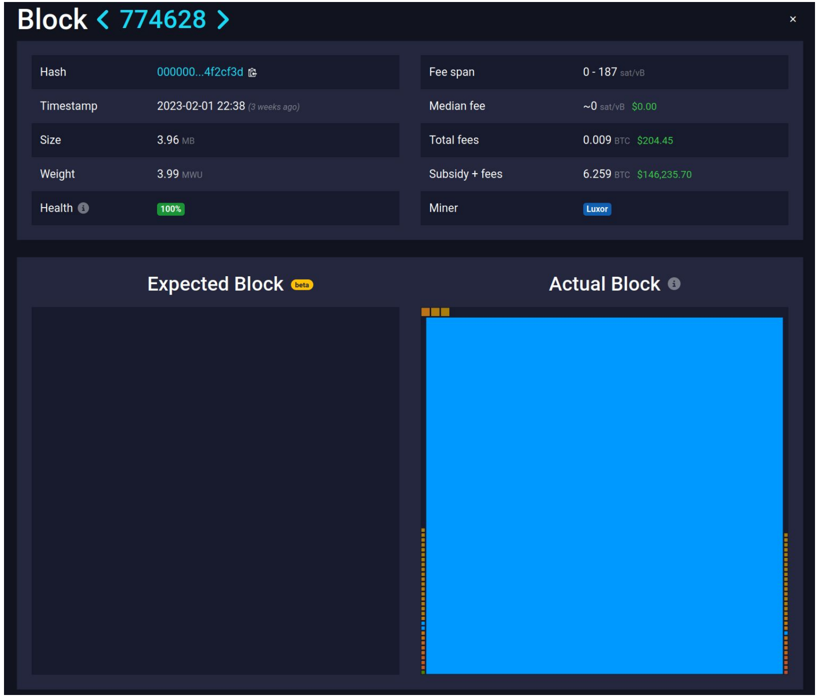
Inscriptions / NFTs, cont.

```
OP_FALSE
OP_IF
     OP_PUSH "ord"
     OP_1
     OP_PUSH "text/plain;charset=utf-8"
     OP_0
     OP_PUSH "max 520 bytes data - hex for binaries"
OP_ENDIF
```

… any other unlocking conditions…

Full blocks and Tx Fees

- Block 774628
  - 3.96MBs
- Several blocks >3MBs
- Miners received more tx fees
  - useful as reward decreases
- A couple of months after…
  - not that many inscriptions
  - one more use case



Block < 774628 >

Hash	000000...4f2cf3d	Fee span	0 - 187 sat/vB
Timestamp	2023-02-01 22:38 *(3 weeks ago)*	Median fee	~0 sat/vB $0.00
Size	3.96 MB	Total fees	0.009 BTC $204.45
Weight	3.99 MWU	Subsidy + fees	6.259 BTC $146,235.70
Health	100%	Miner	Luxor

Discussion

- Pushback from part of the community
  - Blockspace should be for transactions only
  - Now what?

- Suggestion to filter inscriptions
  - check for `OP_PUSH "ord"` etc
  - hmm, they tried that with Counterparty, remember?

- Should we try and censor txs in the only truly neutral platform?
  - No, we shouldn't.

- Can we really do it?
  - Probably not. That's the whole point of a neutral platform!

Discussion, cont.

- Should OP_RETURN be made free for all?
  - i.e. remove the standardness limit

- The witness script of inscriptions has a 75% discount.
  - thus, not a great incentive

- So what do we do?

Discussion, cont.

- The blockchain will get bigger though
  - and more difficult to be downloaded

- By default Bitcoin ignores validating unlocking scripts before certain checkpoints
  - can disable with `assumevalid=0`
  - still downloads everything but can prune as usual

- Note that it would be easy to not download them at all in the future
  - no plans for this!

Discussion, cont.

- What would happen if the inscriptions were not available in most nodes?
    - since they won't be stored before the latest checkpoint
- Are inscriptions equivalent to NFTs from other platforms?
- Blocks are not full anymore
    - is the craze over now?
    - will inscriptions still be here in 5 years from now?

Summary

- Bitcoin resiliency
  - neutral settlement layer
  - neutral in general
  - long-term future is based in healthy fee market

- Something to worry about?

Thank You

@kkarasavvas

Python Bitcoin Library (FOSS)

https://github.com/karask/python-bitcoin-utils

Bitcoin Programming Book (CC)

https://github.com/karask/bitcoin-textbook

Thessaloniki's Bitcoin and Blockchain Tech Meetup

https://www.meetup.com/BlockchainGreece-1/
@Thess_Bitcoin