



Storing Data, Inscriptions and Bitcoin Resiliency

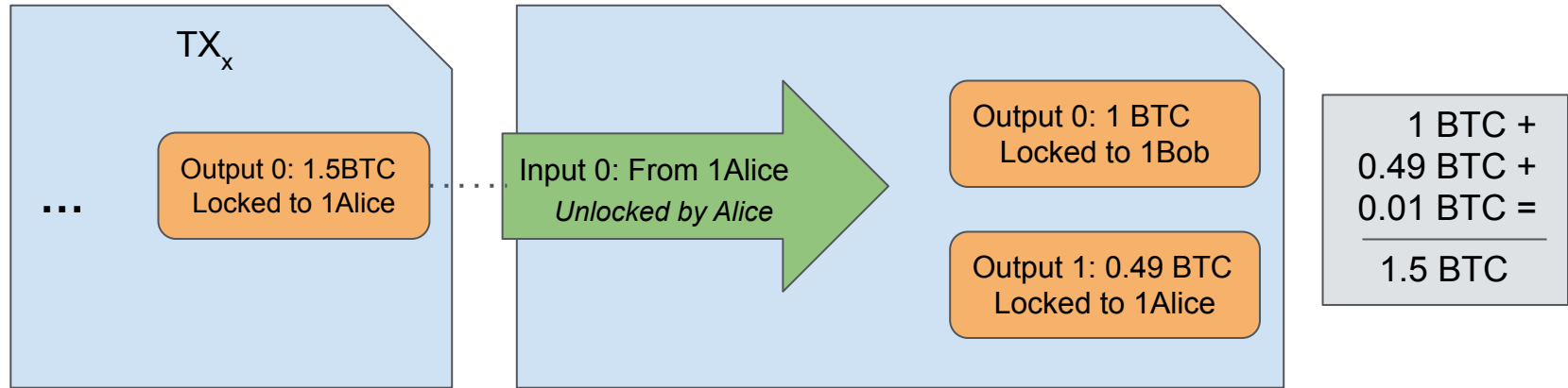


Agenda

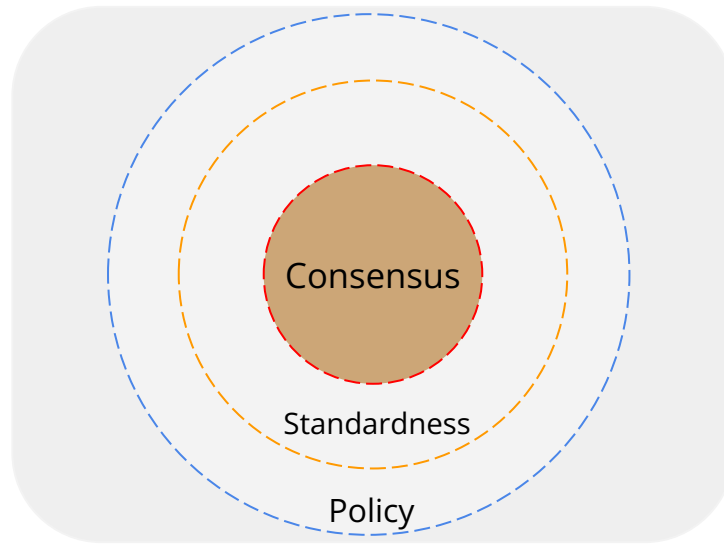
- Quick Introduction to basic concepts
- Different ways of storing data with examples
- Discuss Protocol's Resilience

Transactions and UTXOs Basics

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

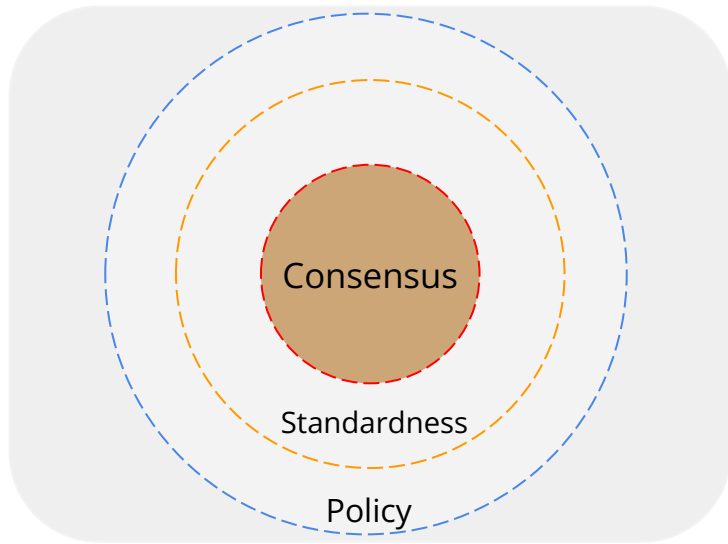


Transaction Validity vs Standardness



Node

Transaction Validity vs Standardness



Node

- A valid transaction does not need to be standard
- A miner can add valid transactions even if non-standard
- A standard transaction needs to also be valid
- Non-standard transactions are not relayed
- A 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 the UTXO set
 - this is important as it does not bloat the network

Storing Data indirectly

- Coinbase transactions
 - only for miners
 - genesis block

aed3754889f65dff83504fd0a8b78e1b69fc22c5396c67df23b0e607bf4e0d67

#0 Coinbase

SCRIPTSIG (ASM)	OP_PUSHBYTES_3 ef9c09 OP_PUSHDNUM_2 0 P_RETURN_240 OP_LESSTHAN OP_ABS OP_L ESSTHAN OP_PUSHDATA4 <push past end>
SCRIPTSIG (HEX)	03ef9c0952f09f909f4e5954696d65732030 392f4170722f323032302057697468202432 2e335420496e6a656374696f6e2c20466564 277320506c616e2046617220457863656564 732032303038205265736375652020144d69 6e6564200500ba5e4800
WITNESS	00000000000000000000000000000000 00000000000000000000000000000000
NSEQUENCE	0x00



Storing Data indirectly

- Coinbase transactions
 - only for miners
 - genesis block

```
aed3754889f65dff83504fd0a8b78e1b69fc22c5396c67df23b0e607bf4e0d67

#0 Coinbase

SCRIPTSIG (ASM)      OP_PUSHBYTES_3 ef9c09 OP_PUSHDNUM_2 0
                     P_RETURN_240 OP_LESSTHAN OP_ABS OP_L
                     ESSTHAN OP_PUSHDATA4 <push past end>

SCRIPTSIG (HEX)      03ef9c0952f09f909f4e5954696d65732030
                     392f4170722f323032302057697468202432
                     2e335420496e6a656374696f6e2c20466564
                     277320506c616e2046617220457863656564
                     732032303038205265736375652020144d69
                     6e6564200500ba5e4800

WITNESS              00000000000000000000000000000000
                     00000000000000000000000000000000

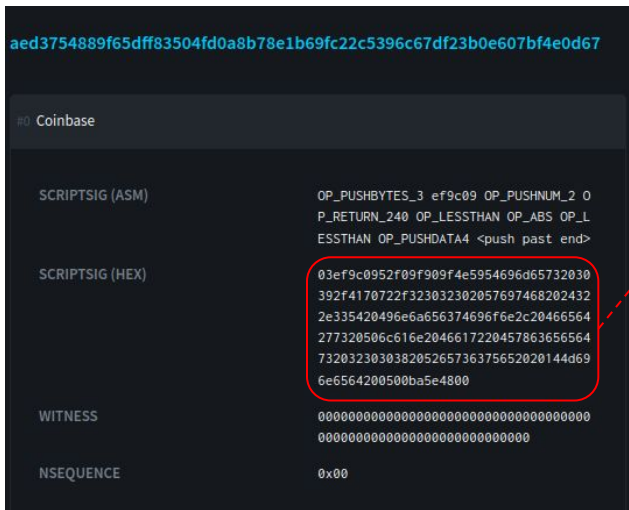
NSEQUENCE             0x00
```



04ffff001d0104455468652054696d65732030323f4a616e2f32303039204368616e63656c6c6f
72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73

Storing Data indirectly

- Coinbase transactions
 - only for miners
 - genesis block



04ffff001d0104455468652054696d6573203032f4a616e2f32303039204368616e63656c6c6f
72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73

EThe Times 03/Jan/2009 Chancellor on brink of
second bailout for banks

Storing Data indirectly

- Fake addresses
 - unintended use
 - tx 8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba

8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba		DETAILS	
7f4c19701b6e04967237506c3508a681718044c35a0711b0a06 0.1374500 BTC		147qlbMudFkgQJmndUjyWScs8MWe 0.0005500 BTC	
b42e763			
SCRIPTSig (ASM)	OP_PUSHBYTES_72 384502045408f817a7 a9f50bc5b1c27365e7e0b83802fa95172 f48220117ff9a6a0210b022780e612a5 0b0a731c4f40a0f9a4c427930a250a	TYPE	P2PKH
	36a6746a9229f81 OP_PUSHBYTES_33 830 04d0a6723336160785c9f10a24710408 6420006424411c31461818a	SCRIPTPubKey (ASM)	OP_HASH160 OP_PUSHBYTES_20 22 63306a2089c54083326520897306a9f 74 OP_EQUALVERIFY OP_CHECKSIG
SCRIPTSig (HEX)	4834502045408f817a7a9f50bc5b1c27 365e7e0b83802fa95172f48220117ff9a 042210b022780e612a50b0a731c4f40 0b0a731c4f40a0f9a4c427930a250a	SCRIPTPubKey (HEX)	76a0142333365c2089c5468652652089 73206eef748bac
	012036c80a6a723336160785c9f10a24710408 6420006424411c31461818a	SPENDING TX	Unspent
SEQUENCE	0xffffffff	1AN34gG2b6zpjG2Djw9pWbWmg 0.0005500 BTC	
PREVIOUS OUTPUT SCRIPT	OP_PUSH OP_HASH160 OP_PUSHBYTES_20 3a 9ac7f20a6c53830a0a4807786a07fa 14 OP_EQUALVERIFY OP_CHECKSIG (pub k)	TYPE	P2PKH
PREVIOUS OUTPUT ADDRESS	16LwQ8wNA1RqJQWngNc1mPq6JwN	SCRIPTPubKey (ASM)	OP_PUSH OP_HASH160 OP_PUSHBYTES_20 28 09a67208c08b0520a726147c20a08e9f 0a OP_EQUALVERIFY OP_CHECKSIG
		SCRIPTPubKey (HEX)	76a01468656a720a6c5986520726147c72 6a09a67208bac
		SPENDING TX	Unspent
		1BcwTRbndid3C3cdwagZnhdTuf 0.0005500 BTC	
		TYPE	P2PKH
		SCRIPTPubKey (ASM)	OP_PUSH OP_HASH160 OP_PUSHBYTES_20 24 070412070c6153050a0207a881742972 0a OP_EQUALVERIFY OP_CHECKSIG
		SCRIPTPubKey (HEX)	76a01474cf20a12070c6153050a0207a8 61742072658bac
		SPENDING TX	Unspent
		1AyMMCw4b3c1AuqQZpJ0rVYwC3kHps 0.0005500 BTC	

Storing Data indirectly

- Fake addresses
 - unintended use
 - tx 8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba

The screenshot shows a transaction with three outputs. The first output is a P2PKH script. The second output is a P2PKH script. The third output is a P2PKH script. Red dashed arrows point from the scriptPubKey (ASSEMBLY) fields of the first, second, and third outputs to a list of fake addresses on the right.

TYPE	SCRIPTPUBKEY (ASSEMBLY)
P2PKH	OP_DUP OP_HASH160 OP_PUSHBYTES_20 223339365ce2809c5468657265206973206e6f7468696e67206c696b652072657475726e696e6720746f206120706c61636550d0a20746861742072655
P2PKH	OP_DUP OP_HASH160 OP_PUSHBYTES_20 223339365ce2809c5468657265206973206e6f7468696e67206c696b652072657475726e696e6720746f206120706c61636550d0a20746861742072655
P2PKH	OP_DUP OP_HASH160 OP_PUSHBYTES_20 223339365ce2809c5468657265206973206e6f7468696e67206c696b652072657475726e696e6720746f206120706c61636550d0a20746861742072655

223339365ce2809c5468657265206973206e6f74
68696e67206c696b652072657475726e696e6720
746f206120706c61636550d0a20746861742072655

Storing Data indirectly

- Fake addresses
 - unintended use
 - tx 8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba

8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba

TXID	Amount
7f4c19701b6d092723709c3309a681718944c35a0711bda6	0.1374000 BTC

TYPE	SCRIPTPUBKEY (ASCI)	SPENDING TX
P2PKH	OP_PUSHBYTES_22 38450284508f817a7a9f59bc5b1c27365e7e0b83802fa9572f48220117ff9a60210b22781e612d5d9a731c4f46801f4a4127936a2c3a836a746a8229f81 OP_PUSHBYTES_33 830c4ef0e72233616b78d0c9f18ca7f4048f42c006424a11c51461818a	Unspent
P2PKH	OP_PUSHBYTES_22 38450284508f817a7a9f59bc5b1c27365e7e0b83802fa9572f48220117ff9a60210b22781e612d5d9a731c4f46801f4a4127936a2c3a836a746a8229f81 OP_PUSHBYTES_33 830c4ef0e72233616b78d0c9f18ca7f4048f42c006424a11c51461818a	Unspent
P2PKH	OP_PUSHBYTES_22 38450284508f817a7a9f59bc5b1c27365e7e0b83802fa9572f48220117ff9a60210b22781e612d5d9a731c4f46801f4a4127936a2c3a836a746a8229f81 OP_PUSHBYTES_33 830c4ef0e72233616b78d0c9f18ca7f4048f42c006424a11c51461818a	Unspent

223339365ce2809c5468657265206973206e6f7468696e67206c696b652072657475726e696e6720746f206120706c6163650d0a20746861742072655

"396\âThere is nothing like returning to a place that re

..mains unchanged to find the ways in which you yourself have altered.
— Nelson Mandela

Storing Data indirectly

- Fake public keys in multi-signature outputs
 - unintended use
 - tx 691dd277dc0e90a462a3d652a1171686de49cf19067cd33c7df0392833fb986a

691dd277dc0e90a462a3d652a1171686de49cf19067cd33c7df0392833fb986a		DETAILS				
2863c9cf4cd3c609c593ca9f1ede7029123dd42d25639d38a6c50ab4cd447		3.27114316 BTC				
SCRIPTSIG (ASM)		OP_PUSHBYTES_70 304682210bc8a4e0b3813a3c76d6762b1ae7d3e66f1a83ac9f7f986cb46861725e6971f02210bc3ba73111cf569b79d74baab787daa220e618e5ce464c1e5cf4d170f267d1d081 OP_PUSHBYTES_33 031e9c46ff60b20bc25c5f1cafd4ab5979c57022b28f6d99f63668827ae3	TYPE			
SCRIPTSIG (HEX)		49304682210bc8a4e0b3813a3c76d6762b1ae7d3e66f1a83ac9f7f986cb46861725e6971f02210bc3ba73111cf569b79d74baab787daa220e618e5ce464c1e5cf4d170f267d1d08121031e9c46ff60b20bc25c5f1cafd4ab5979c57022b28f6d99f63668827ae3	SCRIPTPUBKEY (ASM)			
NSSEQUENCE		0xffffffff	OP_PUSHNUM_1 OP_PUSHBYTES_65 1c2080087353455857696b96c65616b73204361626c6567617465204261636e757080a6361626c656761746520320313081320804313831312e37770a0a446f OP_PUSHBYTES_65 776e6c6cf61642074686520666f6c6cf7769e67207472616e73616374696f6e72077697468205361746f7368692046616d616d6f746f72720646f776e6c6cf61 OP_PUSHBYTES_49 420746f6f6c2077686963680a63616e20626520666f756e6420696e207472616e73616374696f6e20366335336364393837313139656339383731313965663739364364 OP_PUSHNUM_3 OP_CHECKMULTISIG		SCRIPTPUBKEY (HEX)	
PREVIOUS OUTPUT SCRIPT		OP_DUP OP_HASH160 OP_PUSHBYTES_20 d92de0838fc226a3387228bcb0b2ba892645b OP_EQUALVERIFY OP_CHECKSIG (g0pkh)	51411c2208007353455857696b96c65616b73204361626c6567617465204261636e757080a6361626c656761746520320313081320804313831312e37770a0a446f1776e6cf61642074686520666f6c6cf7769e67207472616e73616374696f6e72077697468205361746f7368692046616d616d6f746f72720646f776e6c6cf616420746f6c2077686963680a63616e20626520666f756e6420696e207472616e73616374696f6e20366335336364393837313139656637393643643556373936435616463636453ae		SPENDING TX	
PREVIOUS OUTPUT ADDRESS		1HcduyYUu1PpVazaknaTb8vZ8ScnfWbod	Unspent			
UNKNOWN		0.00000001 BTC				

Storing Data indirectly

- Fake public keys in multi-signature outputs
 - unintended use
 - tx 691dd277dc0e90a462a3d652a1171686de49cf19067cd33c7df0392833fb986a

<div>691dd27dc0e90a4e2a3d5a21171686de49cf19067cd33c7fd92383fb986a</div>	<div>DETAILS</div>
<div> <div>2663d48c4cd3c609593e911d7e029123d6d42d5639dc8f50a4a</div> <div>3.27114316 BTC</div> <div>cd447c</div> </div> <div> <div>SCRIPTSIG (ASM)</div> <div>OP_PUSHBYTES_73 3846822108ca8deeb3819a36767def2b1eafda866f1a83ac3f7f986cd48617256971f022108c3b8f3111cf5690797407a0a8782aa20a1b18c5c44c4e5c4d170f671d0b1 OP_PUSHBYTES_33 031e5cd4ef1b0b1e2b8a2c5c5f1ca0d4abf5979c578022b28f6d9996f9668827ae3</div> <div>SCRIPTSIG (HEX)</div> <div>43048022108ca8deeb3819a36767def2b1eafda866f1a83ac3f7f986cd48617256971f022108c3b8f3111cf569079740a0782aa220b18c5c44c4e5c4d170f671d0b1d0118181e5cd4ef1b0b1e2b8a2c5c5f1ca0d4abf5979c578022b28f6d9996f9668827ae3</div> <div>NSEQUENCE</div> <div>0xffffffff</div> <div>PREVIOUS OUTPUT SCRIPT</div> <div>OP_DUP OP_HASH160 OP_PUSHBYTES_20 d592d09c3f226a339f228b0c8a0b20a526450p_EQUILVERIFY OP_CHECKSIG (op4 h)</div> <div>PREVIOUS OUTPUT ADDRESS</div> <div>1HcAUQVUf7Fpvgzkn1T8u3Y2Scnf8Mod</div> </div>	<div> <div>UNKNOWN</div> <div>0.00000001 BTC</div> </div> <div> <div>TYPE</div> <div>SCRIPTPUBKEY (ASM)</div> <div>OP_PUSHBYTES_66 1c12880873503830990694c9010a7120a41e2c55671746520a61132637ab0ab36162655671746520a61132637ab0ab31313212637ab0ab446f OP_PUSHBYTES_55 6776e616c6f62407865520666f6cc6cf7896a672074261e738163746967e61207679740a20a31146f7380839a10e41e6d7746f72730a0577f89c5671 OP_PUSHBYTES_35 35420748f6f6c6207788963808a36162626250666f7756e4208092074261e738163746967e62083333333843338333131395654337314361140e305354 OP_PUSHBYTES_32 OP_CHECKSIGVERIFY</div> <div>SCRIPTPUBKEY (HEX)</div> <div>51411c20000733458857950a09e40410b32843616265761746520a611326370a0ab36162c65761746520a61132637ab0ab31312637ab0ab446f41776ecdf6164207488520666f6cc6cf7896a6720747201e738163746967e61207679740a20a31146f7380839a10e41e6d7746f72730a0577f89c567164776ecdf6164162074261e738163746967e6208333333384333833313139566573937643501646363</div> <div>SPENDING TX</div> <div>Unspent</div> </div>
<div>UNKNOWN</div> <div>0.00000001 BTC</div>	<div>UNKNOWN</div> <div>0.00000001 BTC</div>

1c2200007353455857696b696c65616b73204361626c6567617465204261636b75700a0a
6361626c65676174652d3230313031323034313831312e377a0a0a446f

776e6c6f61642074686520666f6c6c6f77696e67207472616e73616374696f6e732077697468205361746f736869204e616b616d6f746f277320646f776e6c6f61

6420746f6f6c2077686963680a63616e20626520666f756e6420696e207472616e7361637
4696f6e20366335336364393837313139656637393764356164636364

Storing Data indirectly

- Fake public keys in multi-signature outputs
 - unintended use
 - tx 691dd277dc0e90a462a3d652a1171686de49cf19067cd33c7df0392833fb986a

691dd277dc0e90a462a3d652a1171686de49cf19067cd33c7df0392833fb986a

2863c9cf4cd3c609c593c3e91fede7029123dd42d25639d38a6c50ab4 3.27114316 BTC

cd447

SCRIPTSIG (ASM)

OP_PUSHBYTES_73 38482210bc4e0d0b38 19a3c767de762b1ae7d3e66f1a83ac9f7f9 86cb4861725e8971f022100c30af311cf5 69b979740ab787daa220e618e5ce464c1e 5cf4d1707267d1d081 OP_PUSHBYTES_33 0 31e6c46ff60b20ac25c5f1e6e654ab597 8c578a22028f6d899f63668827ae3

SCRIPTSIG (HEX)

4938482210bc4e0d0b3819a3c767de762b1ae7d3e66f1a83ac9f7f986cb4861725e6 971f022100c30af311cf569b979740ab7 87daa220e618e5ce464c1e5cf4d1707267d 1d08121031e6c46ff60b20ac25c5f1e6e6 54ab5978c578a22028f6d899f63668827ae3

NSEQUENCE

0xffffffff

PREVIOUS OUTPUT SCRIPT

OP_DUP OP_HASH160 OP_PUSHBYTES_20 dd 92de8038fc226a3387228bcb0b20ba89264 5b OP_EQUALVERIFY OP_CHECKSIG (g2pk h)

PREVIOUS OUTPUT ADDRESS

1HcuayYfuiTpvazaknsTb8vZ8ScrfWld

UNKNOWN 0.00000001 BTC

TYPE

UNKNOWN

SCRIPTPUBKEY (ASM)

OP_PUSHNUM_1 OP_PUSHBYTES_65 1c2200007353455857696b696c65616b73204361626c6567617465204261636b75700a0a 6361626c65676174652d3230313031323034313831312e377a0a0a446f 776e6c6f61642074686520666f6c6c6f77696e67207472616e73616374696f6e732077697 468205361746f736869204e616b616d6f746f727320646f776e6c6f61 6420746f6f6c6c6f77686963680a63616e20626520666f756e6420696e207472616e7361637 4696f6e2036633533636439383731313965637393764356164636364

SCRIPTPUBKEY (HEX)

5141c2200007353455857696b696c65616b 73204361626c6567617465204261636b757 0a0a6361626c65676174652d323031303132 3034313831312e377a0a0a446f776e6c6f 61642074686520666f6c6c6f77696e672074 72616e73616374696f6e732077697468205 63746f736869204e616b616d6f746f727320 646f776e6c6f616420746f6f6c6c6f776869 63680a63616e20626520666f756e6420696e 207472616e73616374696f6e203663353363 64393837313139656373937643561646363 64536e

SPENDING TX

Unspent

UNKNOWN 0.00000001 BTC

1c2200007353455857696b696c65616b73204361626c6567617465204261636b75700a0a
6361626c65676174652d3230313031323034313831312e377a0a0a446f

776e6c6f61642074686520666f6c6c6f77696e67207472616e73616374696f6e732077697
468205361746f736869204e616b616d6f746f727320646f776e6c6f61

6420746f6f6c6c6f77686963680a63616e20626520666f756e6420696e207472616e7361637
4696f6e2036633533636439383731313965637393764356164636364

00 00 00 00 sSEXWikileaks Cablegate Backup

cablegate-201012041811.7z

Download the following transactions with Satoshi
Nakamoto's download tool which
can be found in transaction 6c53cd987119ef797d5adccd

Bitcoin Trivia / Hidden Gems (?)

- Coinbase, (Saint) Eligius pool: Catholic prayers

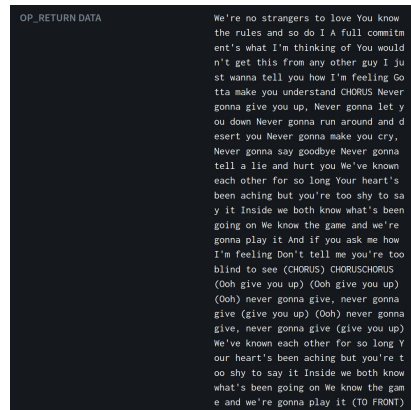
Benedictus Sanguis eius pretiosissimus. -- Benedictus Iesus in sanctissimo altaris Sacramento. -- Ave Maria, gratia plena, Dominus tecum. Benedicta tu in mulieribus, ...
-- ...and life everlasting, through the merits of Jesus Christ, my Lord and Redeemer. -- O Heart of Jesus, burning with love for us, 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)



Bitcoin Trivia / Hidden Gems (?), cont.

- Nelson Mandela tribute
 - in fake addresses!

Nelson Mandela (1918-2013)



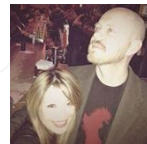
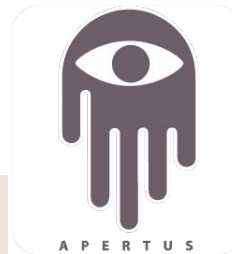
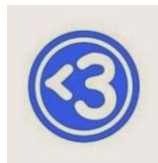
"I am fundamentally an optimist. Whether that comes from nature or nurture, I cannot say. Part of being optimistic is keeping one's head pointed toward the sun, one's feet moving forward. There were many dark moments when my faith in humanity was sorely tested, but I would not and could not give myself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

- Bitcoin's logo has been extracted as well...



Bitcoin Trivia / Hidden Gems (?), cont.

- The original Bitcoin Paper, Len Sassaman tribute, Creature simulator in Basic, ...
- 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



Storing Data indirectly

- Such transaction outputs are part of the UTXO set
 - network nodes are bloated (for ever!)
- OP_RETURN was the preferred way to store data
 - however, data amount was limited to 80 bytes

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 UTXO set
- Accused of bloating the network
- A proposal for an 80 bytes OP_RETURN
- Not accepted by the Bitcoin developers

OP_RETURN Wars, cont.

- Counterparty continued using multi-signature outputs
- Some nodes started filtering (censoring?) them
- Counterparty started to store data differently
 - Filters were updated ...
- Bitcoin Core 0.12 (2016): increased to 80 bytes
 - Counterparty started using OP_RETURN
- Indirect storage craze subsided
 - high fees

Segwit (v0)

- Segregates witness from transaction
 - several benefits, primarily fixing transaction malleability
 - but now we are concerned only about blocksize
- 1MB limit
- Segwit part of txs have a 75% discount
 - the witness (spending) part !
- 4MB weight limit
 - expected size with full segwit txs was up to ~2.8MBs

Segwit (v0), cont.

- Maximum tx weight is 400kB
 - standardness rule
 - note standardness for legacy size txs is 100kB
- Maximum script size is 3600 bytes
 - standardness rule - consensus is 10000 bytes
- ...

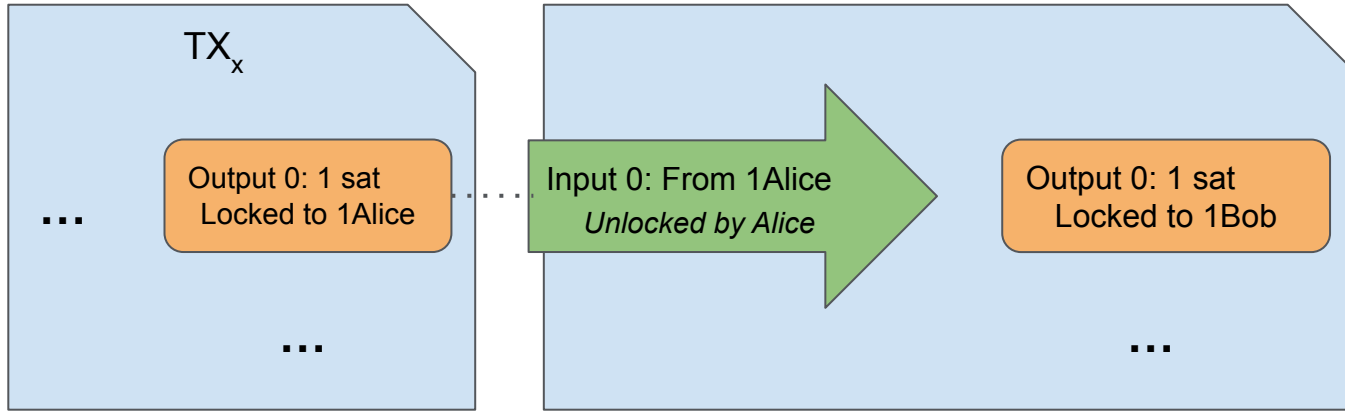
Taproot (v1)

- Removed the maximum script size limit
 - not 3.6kB for standardness or 10kB for consensus anymore
 - script size is limited by the block weight only
- ...
- These limits were removed to allow for more sophisticated scripts

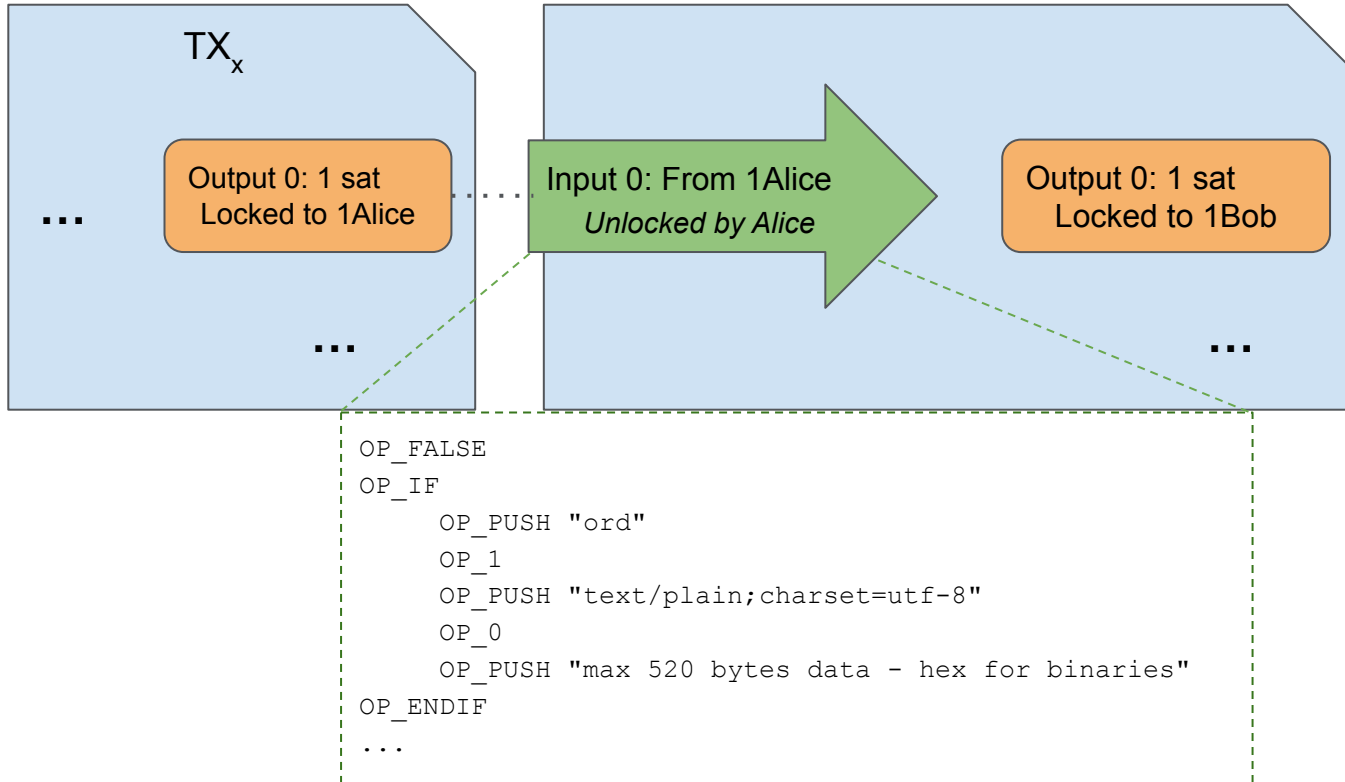
Inscriptions

- 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



Inscriptions



Inscriptions, cont.

OP_FALSE

OP_IF

OP_PUSH "ord"

OP_1

OP_PUSH "text/plain;charset=utf-8"

OP_0

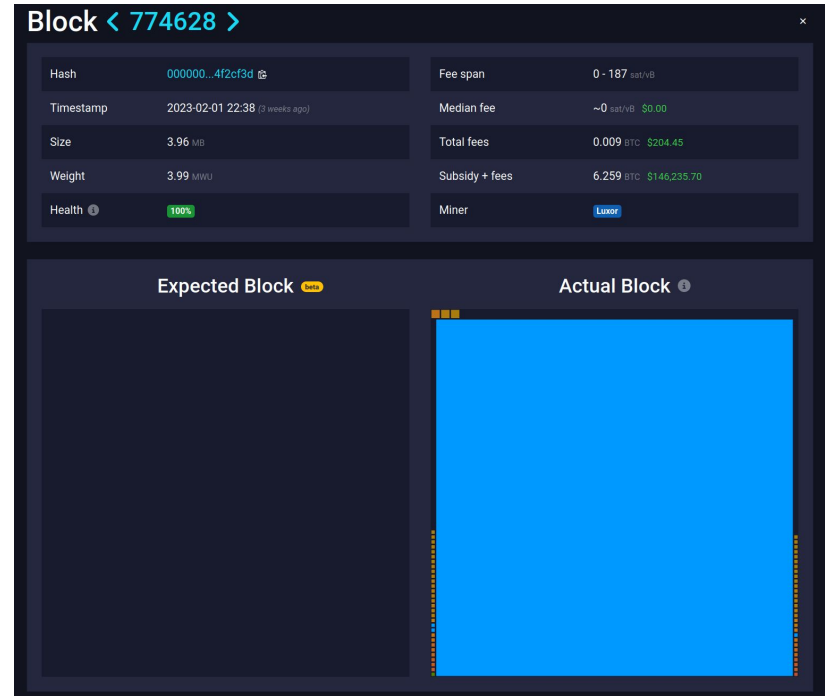
OP_PUSH "max 520 bytes data - hex for binaries"

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
- These are rare...
 - most blocks are 1.5-2MBs
 - hyped a lot
 - additional usage to increase fees



Full blocks and Tx Fees

(11 Apr 2024 @ 09.41 UTC)



Resiliency: filtering / censoring

- 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?
- Can we really do it?
 - Probably not.
- Should we try and censor txs in the only truly neutral platform?

Resiliency: blockchain size

- 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 possible to not download them at all in the future
 - no plans for this though

Resiliency: future of inscriptions

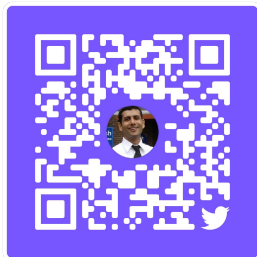
- Are inscriptions equivalent to NFTs from other platforms?
- Is the inscriptions craze over now?
- Will inscriptions still be here in 5 years from now?

Resiliency

- Unchecked storage was available before
 - market is always coming into an equilibrium
- Several meta-protocols and L2s
 - help sustainability via increased tx fees
- Bitcoin is a neutral settlement layer
 - probably the only one
- 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

