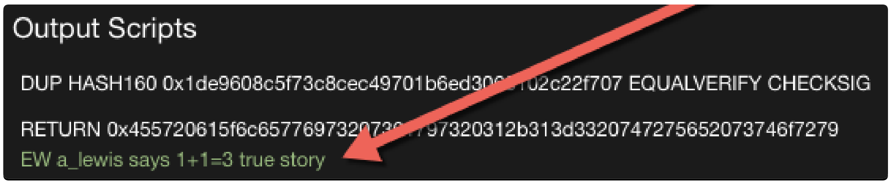
Bits on blocks

Thoughts on blockchain technology

Just because it’s on a blockchain it doesn’t mean it’s true

Posted on May 19, 2016 by antonylewis2015



Output Scripts

```
DUP HASH160 0x1de9608c5f73c8cec49701b6ed30[illegible]02c22f707 EQUALVERIFY CHECKSIG

RETURN 0x455720615f6c6577697320[illegible]97320312b313d3320747275652073746f7279
EW a_lewis says 1+1=3 true story
```

This short article attempts to explain what people mean when they are talking about blockchains being a “single source of truth”. In classic Chinese Whispers style, the narrative has become confused about what is meant by “truth”.

This is currently relevant to discussions in the insurance industry where blockchain enthusiasts may be eager to promote blockchains as a solution to the problem of verifying if something has happened or not.

Here, I permanently recorded on Bitcoin’s blockchain a non-truth about the world.

Graffiti box

When you make a bitcoin transaction, you have the opportunity to type in a short amount of text in a field called OP_RETURN. This gets

Follow Blog via Email

Enter your email address to follow this blog and receive notifications of new posts by email.

Enter your email address

Follow

Top Posts & Pages

A gentle introduction to blockchain technology
A gentle introduction to smart contracts
I aim to write accessible articles about blockchai…
A gentle introduction to bitcoin
A gentle introduction to Ethereum
A gentle introduction to bitcoin mining
The pros and cons of internal blockchains
So you want to use a blockchain for that?
Inside Bitcoin's blockchain
A gentle introduction to immutability of blockchains

Recent Posts

A gentle introduction to Ethereum
The emergence of blockchains as Activity Registers
So you want to use a blockchain for that?

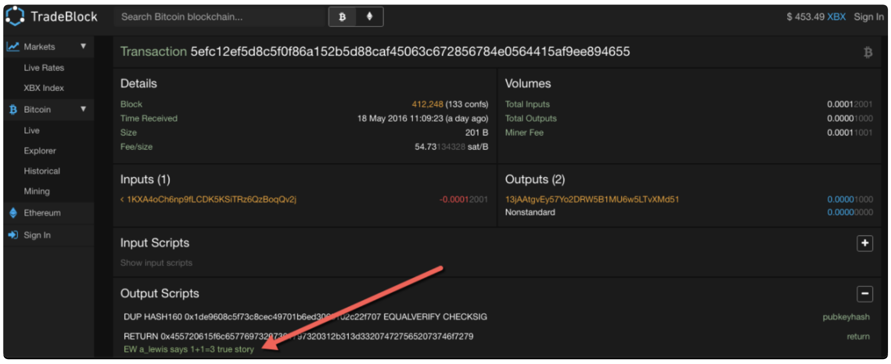
submitted with the transaction and is stored on bitcoin's blockchain when the transaction is included in a block.

This is similar to the free-text field in a banking payment where you can type a short note like an invoice number or some initials.

If it's on a blockchain…

Here's an example of a transaction where OP_RETURN has been used (hat tip to Eternity Wall):

https://tradeblock.com/bitcoin/tx/5efc12ef5d8c5f0f86a152b5d88caf45063c67285



Transaction 5efc12ef5d8c5f0f86a152b5d88caf45063c672856784e0564415af9ee894655

Details

Block 412,248 (133 confs)
Time Received 18 May 2016 11:09:23 (a day ago)
Size 201 B
Fee/size 54.73134328 sat/B

Volumes

Total Inputs 0.00012001
Total Outputs 0.00001000
Miner Fee 0.00011001

Inputs (1)

< 1KXA4oCh6np9fLCDK5KSiTRz6QzBoqQv2j -0.00012001

Outputs (2)

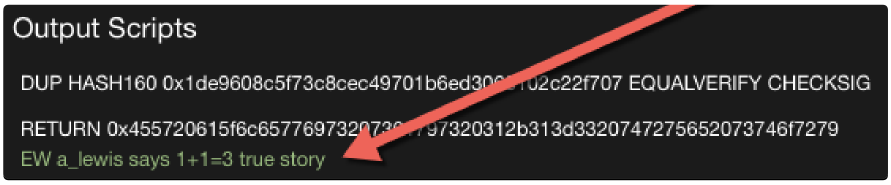
13jAAtgvEy57Yo2DRW5B1MU6w5LTvXMd51 0.00001000
Nonstandard 0.00000000

Input Scripts

Show input scripts

Output Scripts

```
DUP HASH160 0x1de9608c5f73c8cec49701b6ed30   02c22f707 EQUALVERIFY CHECKSIG    pubkeyhash
RETURN 0x455720615f6c657769732073   97320312b313d3320747275652073746f7279    return
EW a_lewis says 1+1=3 true story
```



Output Scripts

```
DUP HASH160 0x1de9608c5f73c8cec49701b6ed30   02c22f707 EQUALVERIFY CHECKSIG
RETURN 0x455720615f6c657769732073   97320312b313d3320747275652073746f7279
EW a_lewis says 1+1=3 true story
```

Notice that at the bottom there is a permanent record on bitcoin's blockchain with the comment:

> *a_lewis says 1+1=3 true story*

This is "on the blockchain" which some will have you believe makes it "true".

However it's not true on two counts:

1. One plus one does not equal three
2. I (a_lewis) didn't actually say this

So what *is* true? What *was* validated?

Well, inclusion into a valid block means that the transaction was valid – ie it passed some technical requirements (the size of the data was below a

KPMG Report on Consensus: Interview with co-author George Samman

No, "Blockchain" is not a solution looking for a problem

Follow me on Twitter

Tweets by @antony_btc

Antony Lewis Retweeted

Todd McDonald
@Mcdtv

forgot to share @R3CEV read buff.ly/2fl1QMZ w @gendal @zooko @antony_btc @SYFNews #blockchain #tailgating

The Weeke…
Our regular …
r3cev.com

31 Oct

Antony Lewis
@antony_btc

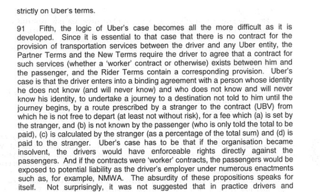
I leave my fingerprints on everything I touch and most borders I cross. You think it is a smart idea for them to control my money?

29 Oct

Antony Lewis Retweeted

Leigh Day
@LeighDay_Law

"The logic of #Uber's case becomes all the more difficult as it is developed" and "The absurdity of these propositions speaks for itself."



strictly on Uber's terms.

91 Fifth, the logic of Uber's case becomes all the more difficult as it is developed. Since it is essential to that case that there is no contract for the provision of transportation services between the driver and any Uber entity, the Partner Terms and the New Terms require the driver to agree that a contract for such services (whether a 'worker' contract or otherwise) exists between him and the passenger, and the Rider Terms contain a corresponding provision. Uber's case is that the driver enters into a binding agreement with a person whose identity he does not know (and will never know) and who does not know and will never know his identity, to undertake a journey to a destination not told to him until the journey begins, by a route prescribed by a stranger to the contract (UBV) from which he is not free to depart (at least not without risk), for a fee which (a) is set by the stranger, and (b) is not known by the passenger (who is only told the total to be paid), (c) is calculated by the stranger (as a percentage of the total sum) and (d) is paid to the stranger. Uber's case has to be that if the organisation became insolvent, the drivers would have enforceable rights directly against the passengers. And if the contracts were 'worker' contracts, the passengers would be exposed to potential liability as the driver's employer under numerous enactments such as, for example, NMWA. The absurdity of these propositions speaks for itself. Not surprisingly, it was not suggested that in practice drivers and

28 Oct

Antony Lewis
@antony_btc

Will Banks Get Onboard with Cryptocurrencies? greenwich.com/blog/will-bank…

maximum threshold, the signature was valid, etc) and some business requirements (bitcoins weren't created out of thin air, etc). That so much is true.

The block creator (self-reported as CKPool Kano) validated the transaction and included it in block number 412,248. Later, 5,500 or so nodes (according to Bitnodes at time of writing) all agreed that this transaction, and the text within it, was valid and occurred. Each full node has recorded this on their copies of the blockchain.

However the validation done on the content was limited to some technical checks (like message length) and clearly not the logic of the comment (1+1=3) or if the the event actually happened in real life (it didn't).

When people talk about a single source of truth, they should really be talking about a single, mutually agreed, version of record, but being careful that this is not over-sold as "truth" or "fact".

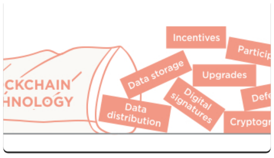
Spread the knowledge:

99 3

★ Like

One blogger likes this.

Related



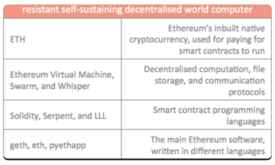
A gentle introduction to blockchain technology

In "blockchain"

So you want to use a blockchain for that?

There are good reasons and bad reasons to use blockchains. In conversations with people thinking about

In "blockchain"



resistant self-sustaining decentralised world computer

ETH	Ethereum's inbuilt native cryptocurrency, used for paying for smart contracts to run
Ethereum Virtual Machine, Swarm, and Whisper	Decentralised computation, file storage, and communication protocols
Solidity, Serpent, and LLL	Smart contract programming languages
geth, eth, pyethapp	The main Ethereum software, written in different languages

A gentle introduction to Ethereum

In "blockchain"

This entry was posted in bitcoin, blockchain and tagged blockchains, fact, hype, myth, truth. Bookmark the permalink.

← Confused by blockchains? Revolution vs Evolution

Interview on Brett King's Breaking Banks →

via @GreenwichAssoc

27 Oct

Antony Lewis
@antony_btc

#zcash day today and drug dealers all over the world are cheering! #bitcoin

27 Oct

Categories

- bitcoin (11)
- blockchain (19)
- digital tokens (6)
- Epicenter Bitcoin (2)
- ethereum (5)
- Events (2)
- fintech (2)
- industry workflow tools (2)
- infographics (2)
- interview (1)
- introductions (9)
- kyc (2)
- mining (3)
- nutshell (4)
- smart contracts (4)
- thought (5)
- Uncategorized (1)

Search …

Blogroll

- Cryptonomics
- Ethereum blog
- Future of Finance
- GavinTech
- Hacking, Distributed
- Hashing It
- Of Numbers
- Organ of Corti
- Stealing from smart people
- Two Bit Idiot

3 thoughts on “Just because it’s on a blockchain it doesn’t mean it’s true”

lordtravistyblog says:

May 21, 2016 at 1:54 am

The old short piece of text in OP_RETURN!

★ Like

↪ Reply

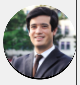
Jer0enH says:

July 4, 2016 at 4:39 pm

How does this relate to something like virtual notary, where the explicit goal is to record some ‘truth’ even to be used as proof in legal situations?

★ Like

↪ Reply



antonylewis2015 says:

July 4, 2016 at 4:58 pm

I think that the idea of hashing a document and storing the hash on a timestamped blockchain serves as a proof of existence of the document at that point in time, which may be useful eg to prove that I didn’t write last year’s entry in my diary yesterday. However hashing docs doesn’t preclude hashing every card in a pack then producing the “correct” one for climax of the trick.
Separately, notaries serve to affirm that a copy of a document is a true copy, I don’t think they generally certify that the original is genuine, but I could be wrong. If the doc or the hash is cryptographically sighed by the issuer, then that would add value as to how genuine the document is, ie proof of provenance as opposed to just proof of existence.

★ Liked by 1 person

↪ Reply

Leave a Reply

Enter your comment here...