Record: 1

7 myths about the Bitcoin blockchain. By: Connolly, Byron. CIO (13284045). 4/15/2016, p1-1. 1p. Abstract: The article discusses seven common myths about Bitcoin blockchain technology. These include the common belief that blockchain is a general purpose database, that the blockchain can be decoupled from the currency or digital token, and that Bitcoin transactions are anonymous, instantaneous and absolute. Also mentioned is the reality that integrity of the ledger is defined by the majority of hashpower, not the number of distinct nodes in the peer-to-peer network. (*AN: 114546216*)

Database: Business Source Complete

7 myths about the Bitcoin blockchain

Sydney

There's some confusion around what the Bitcoin blockchain can and can't do. Gartner analysts list 7 common myths about Bitcoin blockchain technology.

Everyone's talking about the Bitcoin blockchain -- a global, distributed ledger of transactions for the Bitcoin digital currency -- allowing for peer-to-peer payments over the Internet.

According to a Gartner definition, the Bitcoin blockchain is "an authoritative record of Bitcoin transactions, and is not stored in, or controlled by, a central server." Instead, transaction data is replaced as a whole across a peer-to-peer network of thousands of coins. The Bitcoin blockchain is being applied across many industries in areas such as the Internet of Things, digital rights management, and global payments. But among all the global noise, there is some confusion around what it can and can't do. In a report published this month, Gartner analysts Ray Valdes, David Furlonger, and Fabio Chesini shared seven common myths about the Bitcoin blockchain.

Myth 1: The blockchain is a magical database in the cloud

The blockchain is not a "general purpose database" but rather it is conceptually a flat file -- a linear list of simple transaction records, the analysts said in the report. "This list is 'append only so entries are never deleted, but instead, the file (currently about 50 gigabytes), grows indefinitely and must be replicated in every node in the peer-to-peer network (thereby introducing scalability and latency issues)."

Myth 2: The integrity of the ledger is defined by the majority of nodes in the peer-to-peer network

The reality is that its integrity is defined by the majority of "hashpower" (the computational resources used in data mining) not the number of distinct nodes in the network, the analysts said. "This means that a single sufficiently powerful entity on the network can 'outvote' the rest of the nodes," the report said.

Myth 3: The ledger represents an irrevocable record

This is pragmatically correct, the analysts said, but it is "theoretically possible for a party to accumulate enough hashpower to rewrite the record all the way back to the Genesis block (the first block of a blockchain)." "Such an action would work against the incentives of the usual participants in the Bitcoin ecosystem because it would destroy all user confidence in the blockchain technology and the commercial economy it supports," the report reads.

Myth 4: Blockchain technology is scalable to the level of a global economy

This is not just a myth, but more widespread perception today as people become aware of scalability issues relating to the current form of the Bitcoin technology stack, the analysts said. Due to its design, the network can only handle a relatively small number of transactions per second. "This number is due to the constraint of a maximum block size of one megabyte, combined with around a 10-minute confirmation delay per block which, depending on the average transaction size, results in a maximum capacity of seven transactions per second (tps)," the analysts said in the report. "Actually, due to the increasing size of transaction records, this number has been decreasing and is now estimated at less than three tps, a small number compared to the peak capacity of, say, the Visa network at 47,000 tps or Nasdaq's potential of 1 million tps," the analysts said.

Myth 5: The blockchain can be decoupled from the currency or digital token

Some financial institutions considering using blockchain are saying they don't care about the currency, only the blockchain. But in its present form, bitcoin is a key part of the blockchain, the analysts said. "The blockchain is simply a list of bitcoin-dominated transactions. Also, the design of the consensus mechanism relies on the currency providing the incentive for miners to confirm transactions. "Therefore (as some members of the bitcoin community have said), anyone who states that the currency is not important and can be ignored in favour of the blockchain, does not understand the technology and how it works," the analysts said.

Myth 6: Bitcoin transactions are anonymous, instantaneous and absolute.

"In the bitcoin technology stack, participants in transactions are pseudonymous," the analysts said.

"Regarding transaction speed there is, by design, a minimum 10-minute latency in confirming transactions, and pragmatically, one could wait for an hour for confirmation. "Transactions on the blockchain are probabilistic rather than absolute, in that it is theoretically possible for an attacker to build an alternative chain (a data fork) that would allow double spending. Unless the attacker has a majority of hashing power, this will not succeed."

Myth 7: The blockchain is a decentralised system.

The original design was a decentralised peer-to-peer network, but in practice the blockchain has become more centralised, the analysts said. "The number of peer-to-peer nodes on the network has dropped steadily at about 15 per cent per year," they said. "Mining is conducted in large part (about 80 per cent) by only four mining pools, which are all based in China. "Any two of these four could theoretically collude and would together constitute a majority of the computational resources (hashpower) needed for mining,

and could then control the updating of the distributed ledger."

~~~~~~~~

By Byron Connolly

~~~~~~~~