Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin

Blockchains are an exciting new development, but the devil is in the detail

Nikolai Hampton (Computerworld)
05 September, 2016 09:00

Much of what you've heard about the blockchain revolution is nothing but snake oil and marketing spin. This new technology has been touted as the cure-all for performing secure and trusted transactions. The mere mention

of the word blockchain sends fintech and banking execs into frenzy.

Australia Post even threw its hat into the blockchain ring in early 2016 when it revealed it intended to use blockchains to store identities. Australia post also recently made a submission to a Victorian government committee conducting an inquiry into electronic voting. The submission suggested that it could use 'blockchain' technology, but provided no detail on how or why a blockchain would improve the electronic voting process. The finance and banking sector is also investing in the technology.

The whole blockchain phenomenon started with the success of Bitcoin – a type of digital 'cash' that uses various cryptographic processes to secure transactions between untrusted third parties, without the need for a central authority or bank.

While the blockchain is indeed a critical part of the Bitcoin security model, it is no silver bullet. The hype surrounding the blockchain buzzword greatly exaggerates what blockchains are, and totally neglects the complex interplay of many critical technology components that work together to

make Bitcoin secure.

So, what is the blockchain?

The blockchain is a distributed ledger book of all Bitcoin transactions. This means there's no single database of records. The distributed nature of the blockchain also helps to secure it because the Bitcoin community collectively agree on all transactions; there's no central authority that can block or reverse payments.

Imagine it as a physical book where each page contains about ten minutes of Bitcoin transactions. After 10 minutes of transactions, the page is stamped with a special serial number (a hash), and glued permanently into the ledger book.

Everyone can be assured that the transaction list in the ledger book is secure and complete because nobody can insert, modify or delete a transaction without tearing out the page. The serial number hash makes this process very difficult because it ensures all pages are mathematically 'locked' (or chained) together. If any content on a previous page is modified, the serial numbers will no longer align, and everyone would know that

Related Whitepapers

How to proactively manage cyber security threats

something hinky is going on.

The only way to alter a transaction in the blockchain book is to tear out the page containing the transaction, plus all the following pages. Then alter the transaction on the original page, and then re-print every subsequent page, creating a new hash, and then gluing all of those pages back into the book. Bitcoin transactions are secure because it's just too much work to modify them!

Buying a pizza with a blockchain

If I'm spending $10 at Lizza's Pizzas, I can 'broadcast' a message to all Bitcoin users, requesting that they make a note of my transaction in the current block. Because the blockchain is open for inspection, Lizza can watch the blockchain until she sees my payment recorded. Furthermore, because the blockchain is secure against tampering, Lizza can be confident that the transaction is complete – there's no way I could scam her and steal $10 worth of pizza.

More from EMC »

If someone were to examine the blockchain after my transaction with Lizza, they'd see that her account had $10 in it that came from my account. When Lizza wants to spend $4.50 on a magazine from Nate's News, Nate inspects the blockchain to confirm that Lizza has enough money in the account to cover the $4.50 transaction, and then watches for Lizza's transaction in the blockchain.

The blockchain ledger book verifies the money in Nate's account through the linkage from Nate to Lizza to me (and so on). This is how all transactions are chained together; every transaction is linked to all previous transactions through the history of blocks in the blockchain.

Blockchain protecting transactions

It's clear that even with our naïve and simple 'blockchain book', it's not worth trying to scam a $10 pizza or a $4.50 magazine. The work required outweighs the value of what's being protected. But, Bitcoin transactions come in all shapes and sizes; for example, a gambling website was sold

for US$11.5 million worth of Bitcoin in 2013.

While I wouldn't bother trying to skip out on a $10 pizza, if I could easily reverse a million dollar sale I might think about it.

Baked in security

A simple blockchain is nothing more than a list of transactions that is chained or linked together using novel data structures, and some basic cryptographic principles. Anyone can make a blockchain, and create blocks. My little old laptop can make millions of blocks every second, they just wouldn't be secure like Bitcoin's blocks.

This is where the subtly between blockchains and security is lost. Bitcoin isn't secure because of blockchain; it is secure because the effort and cost of subverting its blockchain is greater than the value of what's being protected. The effort and cost that protect Bitcoin comes in the form of time, computing power and electricity.

READ MORE

Report of Census review expected this month

The effort is dictated by the rules that are ‘baked in’ to what Bitcoin is. The rules provide mathematical certainty from how transactions are ‘signed’ through to how much ‘proof of work’ needs to accompany a block.

There are many parts to the Bitcoin rulebook, and each and every part is essential to the scheme’s overall security; no single element (including the blockchain) is enough to secure Bitcoin transactions.

Mining blocks is expensive work

The Bitcoin rules are enforced by thousands of Bitcoin ‘miners’ that compete against each other to record transactions and create new blockchain entries. The miners all race to calculate a block’s hash value, which can only be found by brute force (using trial-and error).

The miners make blocks by gathering end-user transactions (my $10 pizza order for example), combining them and calculating hashes. When they discover blocks that match Bitcoin’s rules they add the block to the chain, and collect a reward.

Unlike our paper-ledger-book example, the difficulty in creating a single block is immense. It (currently) takes the collective efforts of many thousands of miners testing 1.6-million-million-million hashes per second to discover one ‘block’ every 10 minutes; they’re working at a speed that’s equivalent to 130-billion 'average' desktop computers working in parallel. These mining computers are real devices, taking up real physical space, and they collectively consume gigawatts of real power.

Economics and mathematics — blockchain armor

The massive effort required to 'break Bitcoin' is what protects it. It is the reason that the blockchain is secure. As each block is added, a lot of work needs to be done; for blocks that are lower down in the chain, that work is multiplied for every subsequent block added to the chain.

Even if an attacker managed to harness gigawatts of computing power (or subvert half of the thousands of miners working to create Bitcoin blocks), the attacker would still only have a marginal advantage. The theoretical ‘51 per cent attack’ against the Bitcoin

network improves the probability of controlling the 'next' block. But, using such an attack to re-write history (many blocks) is still almost impossible.

It's the rules that govern the integrity of a bitcoin block that secure the blockchain. The rules ensure that the computing power required to tear out a recent block, alter a transaction, then re-create all subsequent blocks is more than any attacker and even most governments could amass.

Read more: Menlo Security seeks to isolate web-borne threats

The Punchline

Blockchain technology and solutions are tantalising. Without doubt, many new technologies will be built upon the blockchain concept in the years to come. But, the blockchain alone isn't what creates security. The questions for private or proprietary blockchains are how will you protect your chain and why is a blockchain better than running an ordinary database?

The Bitcoin blockchain is protected by the massive group mining effort. It's unlikely that any private blockchain will try to protect records using gigawatts

of computing power — it's time consuming and expensive. Within a private blockchain there is also no 'race'; there's no incentive to use more power or discover blocks faster than competitors. This means that many in-house blockchain solutions will be nothing more than cumbersome databases.

There is also no need for a '51 per cent' attack on a private blockchain, as the private blockchain (most likely) already controls 100 per cent of all block creation resources. If you could attack or damage the blockchain creation tools on a private corporate server, you could effectively control 100 per cent of their network and alter transactions however you wished.

Sure, blockchains are an exciting new development, but the devil is in the detail. Without a clear security model, proprietary blockchains should be eyed with suspicion.

Nikolai Hampton holds a Master's Degree in Cyber Security and is a director of Impression Research. He consults on matters of privacy, security, digital forensics, and incident response. His focus is on the correct application of cryptography. He is passionate

about educating business on complex security issues. Follow Nikolai on Twitter: @NikolaiHampton

Tags Blockchain security Bitcoin cyber security

More about Australia Post indeed News Twitter

0 Comments

Read next

A series of tubes: What's next for home automation

Scientists look at how A.I. will change our lives by 2030

FBI Perspective On the Status and Evolution of Global Cybercrime

CSO Online

In pictures: Computerworld Exchange Breakfast: Accelerate Your Digital Transformation

Inside UNSW's quantum computing laboratory

Use the internet? This Linux flaw could open you up to attack

'It can be done easily by anyone in the world,' one researcher says

Use the internet? This Linux flaw could open you up to attack

'It can be done easily by anyone in the world,' one researcher says