Infospectives

STRAIGHTFORWARD PRIVACY & SECURITY

CORPORATE SECURITY

Blockchains: Embedding Integrity (a.k.a Blockchain for beginners with an InfoSec twist)

BY INFOSPECTIVES ON JANUARY 5, 2016 · (LEAVE A COMMENT)

Blockchains are tackling the 'I' in the holy InfoSec CIA trinity (Confidentiality, Integrity, and Availability, not the government agency), more simply and robustly than anything that's gone before.

However they are also a source of banker panic, intense speculation, stereotyping critique, an impending

vendor feeding frenzy, and (more than anything else) confusion.

No wonder big corporations and financial institutions are spending LOTS of time and money looking into this. Time and money that could turn into very expensive purchasing mistakes if IT, security, procurement, and all other related professionals don't grasp the fundamentals and implications.

So, provoked by a vendor FinTech pitch (http://www.americanbanker.com/bankthink/explore-the-blockchain-ignore-the-bitcoin-maximalists-1077657-1.html) and critique of it (http://webonanza.com/2015/11/04/sorry-r3-but-you-still-dont-get-it/) thrown my way by Jan Winter (@janwinterBTC (https://twitter.com/janwinterBTC)), here's my first look at blockchains* as a transactional concept, with an initial muse on security implications.

Disclaimer: Despite getting an expert to review before publishing, this is not intended to be a seminal post adding to the definitive store of blockchain knowledge. It's for readers who are also at a starting point in their understanding, and my future clients.

If pros don't 'get' this, our peers and employers are at very real risk of being fleeced for want of due and sensible diligence. So, if you have something to add, go for it.

A few months back I was sat on a train checking Twitter and caught sight of an article about one of Ethereum (http://www.ibtimes.co.uk/setting-your-own-central-bank-just-start-ethereum-1532146)'s fund raising rounds. It triggered something: A deep and intense feeling that economic history was in the process of being written.

Of course I knew about Bitcoin and even basic blockchain concepts, but that provoked me to spend many hours doing research. Since then mainstream media coverage seems to have snowballed (even allowing for the Baader-Meinhof effect (https://en.wikipedia.org/wiki/List_of_cognitive_biases#Frequency_illusion)). Most notably attached to implications for Financial Technology (FinTech), and banking more generally. What hasn't been super-common is clarity and common sense.

The what and why of blockchains

First a couple of things that a blockchain is not:

- An application
- A technology
- An algorithm
- A method of encryption
- A proprietary product.

It utilises some of the above, but it doesn't come – in and of itself – in a vendor stamped package. Anyone telling you otherwise is lying.

What it is:

It is indisputably a rare change to information storage and processing plumbing. In essence it hardwires the history of information. Be that information with it's own inherent value (e.g. cryptocurrency and intellectual property), or information about asset ownership, and ownership changes.

Blockchains are also, in their basic form, open source. A piecing together of earlier open source concepts and code as outlined in a now famous paper (https://bitcoin.org/bitcoin.pdf) written by Bitcoin's founder, Satoshi Nakamoto (who's real identity is still a source of intense speculation (https://en.bitcoin.it/wiki/Satoshi_Nakamoto)).

EDIT June 2016: Now slightly less – The New Yorker on Craig Wright (http://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is), Australian entrepreneur claiming he's the man, plus ongoing questions raised.

In other words it's a new iteration of the Trusted Third Party (TTP) (https://en.wikipedia.org/wiki/Trusted_third_party) concept. For financial transactions your traditional trusted intermediary is a bank. For property purchases it's a lawyer. For secure browsing it's a certificate authority (validating that HTTPS padlock). In the blockchain it's the enforcer of chain rules, and the distributed network of transaction validators.

Don't be blinded by the technobabble and hype. Good due diligence and procurement principles still 100% apply. This isn't magic. If vendors can't simply demonstrate how a solution solves your problems, how it will work in your environment…you will be complicit in pulling very expensive wool over executive eyes.

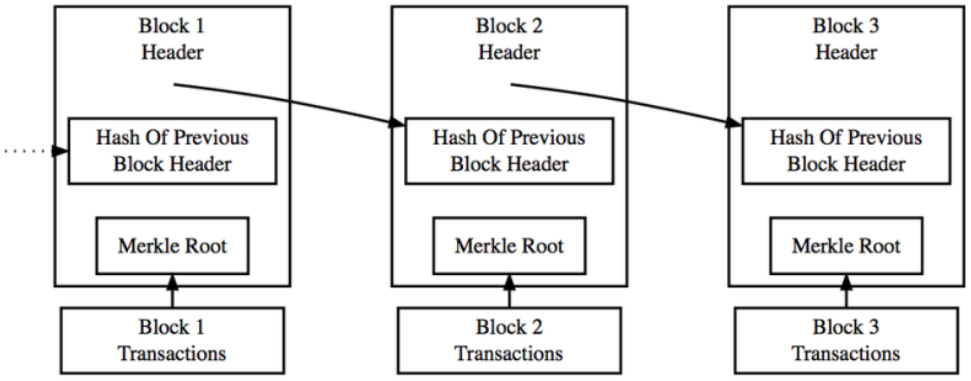
Beginning to see why fee and interest earning financiers are getting jumpy?

How does it do all that?

Transaction data is written into a block (in computing terms, that's a small chunk of space on a disc in a computer somewhere…just like all the other data in the world). What distinguishes the block from everything else you create and save are the
tamper resistant timestamps and unique identifiers: A

transaction includes a hashed record of recent valid transactions, summary transaction info, address of the creator (also usually cryptographically hashed), block timestamp, and hash of the block preceding it (hence the chain). Hashes, very simply are alphanumeric strings generated by applying an algorithm to block contents (for those smarter than me here's the elliptic, scalar, modulo and hexy maths (http://www.coindesk.com/math-behind-bitcoin/)).

The Merkle Root (mentioned in the diagram below), is nothing to do with Angela. It's a name given to that final 'hash of all hashes' in a block…the master identifier if you will.



Simplified Bitcoin Block Chain

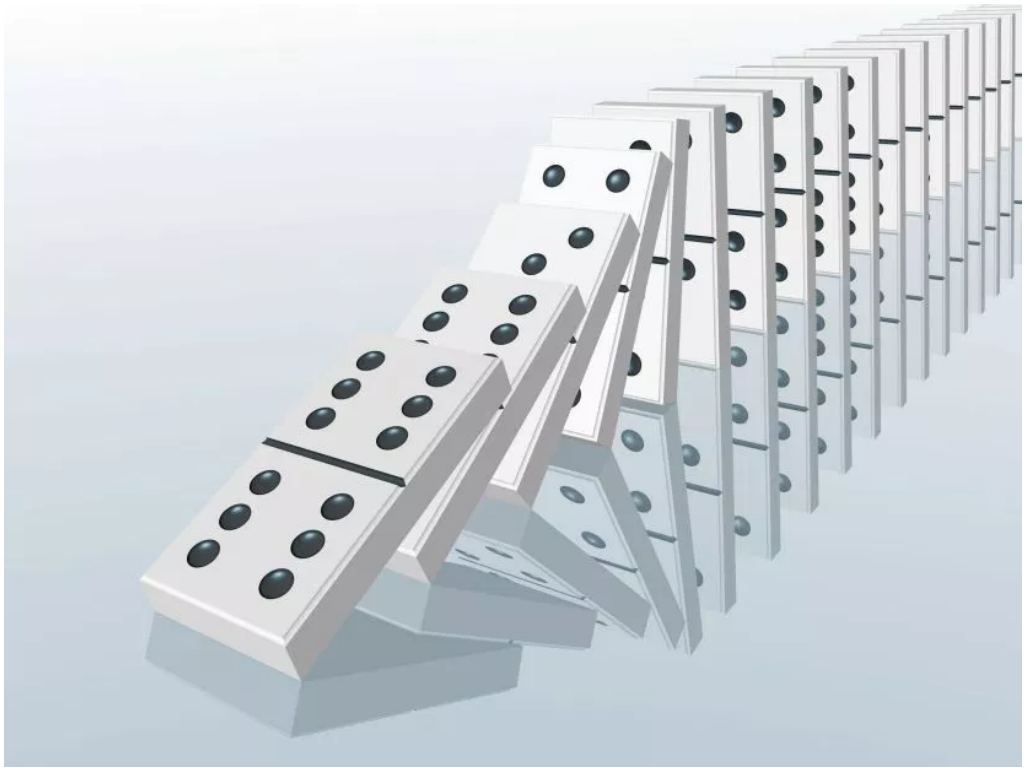
A new block can only be created when certain criteria are met. Criteria based around the algorithm. Block miners run calculations using big numbers for as long as it takes to produce a hash that meets chain creator requirements. That takes significant processing power. Criteria for cryptocurrency have also been designed to future proof that difficulty. If hashes are found too fast (Bitcoins are produced at a rate of roughly 1 every 10 minutes), the requirements get harder. Thus, with stylish simplicity, they, and other competing firms like Primecoin (https://bitcoin.org/bitcoin.pdf) (who claim to speed, but also future proof hash creation through clever use of special classes of prime numbers), allow for the inexorable increase in available processing oomph, and

prevent inflation in cryptocurrency markets that would result from overproduction.

Hashes can be, with sufficient processing power and time, reverse engineered without private keys to get at the hidden plaintext. But, as things currently stand (assuming robust chain creation criteria, evolution of criteria to match future processing capability, and proper implementation), you'd likely die before you succeed.

Once written and added to the chain it would therefore take significant money and time to replace blocks. And (to correct errors, or add information), you **have** to replace them. Blocks don't change. The fact of the replacement is recorded in the chain along with the new information.

Branches and integrity checking dominos



That's the story for a single isolated block. Now you have to wrap your head around implications for long branching chains. If a way down the road a problem is found with an historical transaction, each and every block referencing the original transaction will have to be

replaced or the hashes will be invalid (based as they are on previous blocks' hashes). An integrity checking domino effect. From that point on a branch is created. One chain becomes two. The second containing new information. As new blocks get added, the new chain becomes longer than the old, and shorter chains become dormant (or 'expired' in blockchain parlance).

What doesn't change (and this is the fundamental and critical point), is the history. The What, Who, and When of changes is a persistent record, linked always to the originating and branched chains of the oldest parent transaction. In Bitcoin's world that's the Genesis Block, created by Santoshi (https://en.bitcoin.it/wiki/Satoshi_Nakamoto) in November 2009.

Why is this a paradigm shift?

To grasp that you simply have to consider what's gone before. First there were paper records. I had a couple of A2 leather-bound ledgers rescued from banks my parents worked in (both blank I should hastily add). In them, before the days of computers, the end of day banking books were balanced by hand with the help of adding machines. In the land registry, property rights were painstakingly written in legalese documents that grew as ownership changed. Records were then stored in giant warehouses, and retrieved when needed with the help of card indexes.

If asset ownership or transactions were questioned, you had to hope no-one had tinkered with the index, file location, or files themselves. That's without allowing for typos, calculation errors, or intentional amendments during creation of originals. As for tracing transaction history back to origins…lots, and lots, and lots of legwork.

Then there were computers. Records scanned or manually entered into machines. Database schemas and unique identifiers replacing card indexes. Entries changing slowly for property, and in nanoseconds for transactions in the global money markets.

Data now accessible by a dramatically wider range of people with variably well control access. Logs of access, changes, and transactions also subject to variable control. Most auditors asking about log integrity are told about standard access management, ropy database permissions, and what can be done to retrospectively investigate database problems. There's little inherent control of the type blockchains inject with their structure and hashed contents.

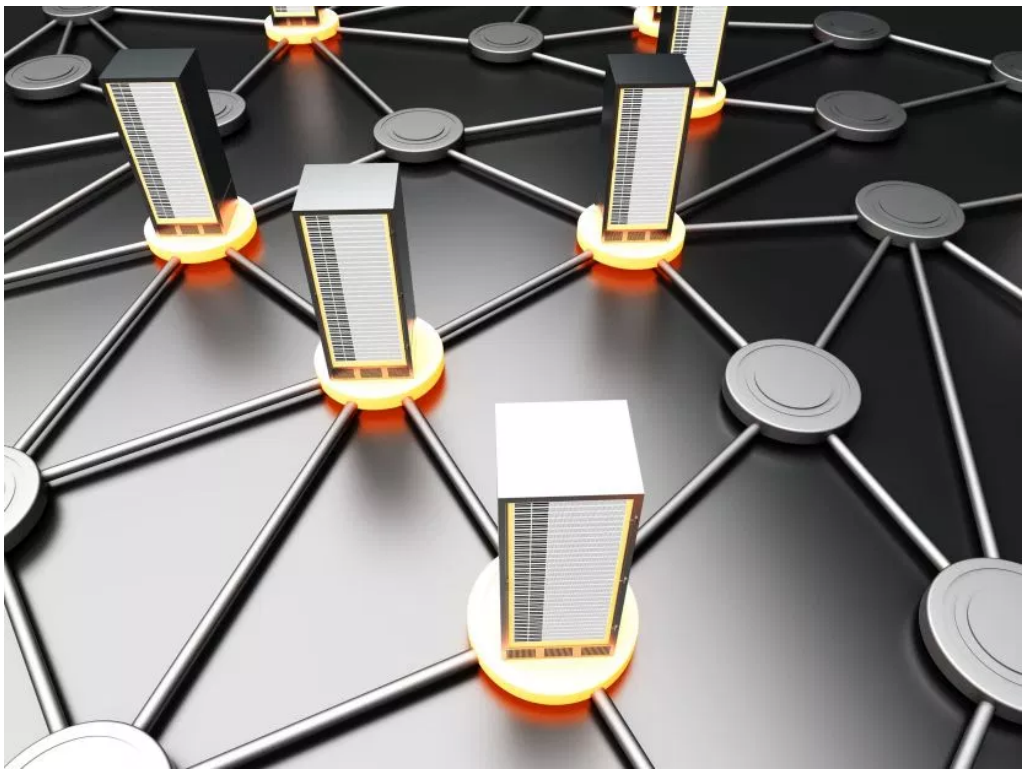
Then came criminals working to steal or alter stored versions of the truth (actually not a continuum, as soon as there were computers there were folk trying to break into them). That's been coupled with an unforeseeable explosion in data scooping interfaces and data scooped. All presenting huge challenges for tracking, correlation, analysis, and protection. Not least when trying to force legacy (sometimes decades old), formats and systems, into our modern regulatory and technical environments.

Anyone with more than a passing interest in tech and security is aware of the fragility of networks, how much of our data is in others' hands, and the newish mantra "Assume you have been hacked". When you put all that in the context of data identifying you as rightful owner of your bank account or house, it takes on a whole other significance. Something with which identity theft victims (http://www.forbes.com/sites/laurashin/2014/11/18/someone-had-taken-over-my-life-an-identity-theft-victims-story/) agonisingly empathise.

But banks are the most secure places... surely

Yes, in most cases, they are. But they are also (like every business with tech designed, implemented, maintained, and used by humans), fallible, as recently highlighted by a review (http://www.infosecurity-magazine.com/news/uk-online-banking-logon-pages/) of their online logon pages. And the target painted on them is huge. More determined and sophisticated effort is made to hack and defraud banks than any other type of business. Your business and personal banking fees reflect the cost of buying, implementing, and running hard core controls. An enormous part of that cost comes from tech and bodies employed to validate asset ownership, tame data stores, and ensure integrity of records.

And that's where the distributed-ledger-like blockchain comes in



Beyond what I've explained so far is the distributed nature of that transaction validation. We are not talking about Blockchain Inc sitting on top of mammoth data centres, grafting to check each submitted transaction and churning out new blocks. The work of block validation (mining) is outsourced with incentives for production. And anyone can become a Bitcoin miner (http://www.pcadvisor.co.uk/how-to/internet/how-mine-bitcoins-generate-money-bitcoin-mining-terrorism-3515249/) with a bit of processing power and time to learn. Points of entry are called nodes and via APIs they take copies of the blockchain that are constantly updated. A consensus about transactee and transaction validity is reached by multiple nodes by checking pre-existing information in the distributed copies of the chain. A virtual and unanimous vote on what becomes the next link.

Protection against conflicting concurrent updates is also built-in. One block follows another and references what goes before. If a Bitcoin owner attempts to sell the same currency to two purchasers, one transaction will trump the other by getting written into the chain first. The second fails on validation, because the transaction history shows they now longer own that part or whole

Bitcoin. If the node writing the transaction processes the wrong one offline dispute resolution can swing into action and a change will get written as a transaction later.

In rare cases, for a valid transaction, miners produce different compliant hashes almost simultaneously and two blocks are created. When the next related transaction takes place, the previous block it refers to is the one built on. The single block branch with the other hash is orphaned. Conflicting transactions therefore do not become part of the mature blockchain dataset.

In other words, while being both public and anonymous, transaction integrity is protected better than ever before, and no single entity has control. If that hasn't yet blown your mind, think harder about it.

Implications

- **International financial transactions:** SWIFT, SEPA, transfer charges…meh. If your recipient accepts cryptocurrency, none of that applies.
- **Domestic financial transactions:** Ditto.
- **Other transactions:** If you want a mutually protective way of keeping abreast of all kinds of digital exchanges – here's a solution.
- **Contracts:** Want a persistent, verifiable, version-controlled record of your agreements – Bob's your uncle
- **Code control:** Bingo – Versions recorded, verified and maintained

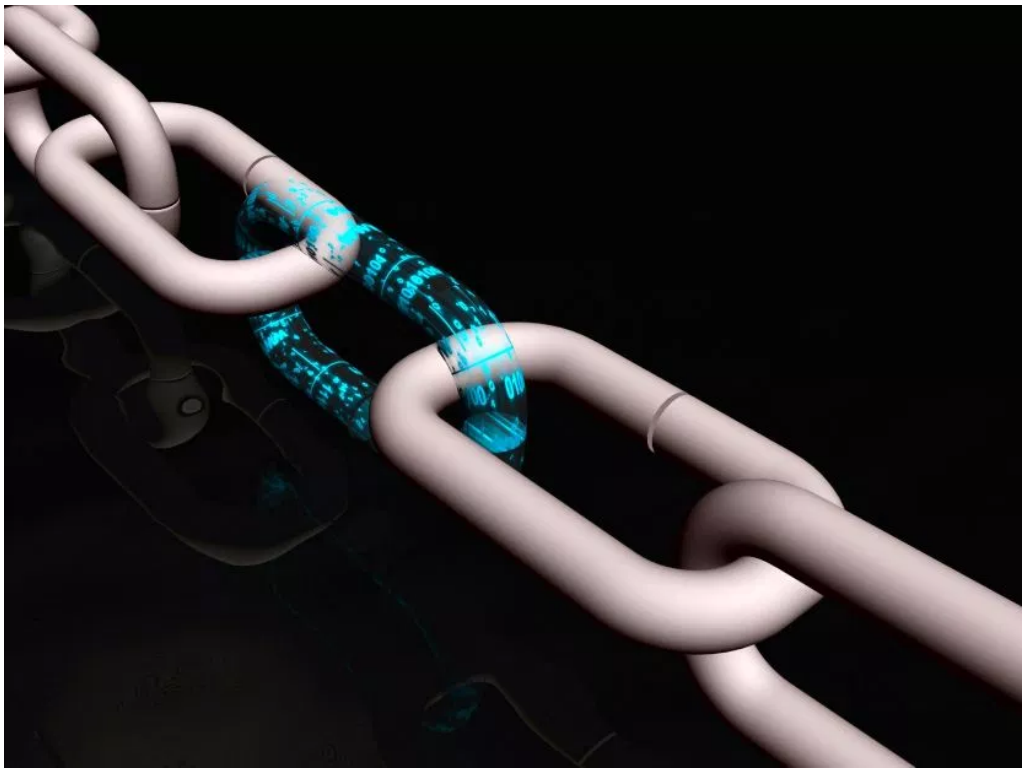
That's my truncated list, but there's far more exciting stuff about potential usage of Bitcoin's blockchain in this video from Bitcoin Properly (http://bitcoinproperly.org/#sthash.g4QWPGAc.dpbs), broader speculation from Scott Rosenburg (https://medium.com/backchannel/how-bitcoins-blockchain-could-power-an-alternate-internet-bb501855af67#.ugegrdagc) via

Backchannel, and lay-person friendly coverage in this BBC Radio programme

Future Proofing: The Blockchain (http://bbc.in/1J3txg8)

The latter also includes a mind-blowing suggestion related to the 'trust-less' model blockchain theoretically enables: Blockchain as foundation of a governmentless state (you may want to get a beer or something stronger before trying to wrap your noggin round that).

Other things it doesn't do, and concerns about what it does



While the implications are huge, there are key things it was never designed to do. It does not check the identity of asset owners before a first transaction is submitted. It just maintains the relationship between asset owner and transactions over time. Initially validating an individual's entitlement to transact, and their ownership of referenced assets stored outside the blockchain, happens independently.

In other words; If trading Bitcoins, you might be doing business with a drug baron. If that doesn't send your moral compass into a spin, you can rest assured that the drug baron possesses the currency promised and can't pretend the trade didn't happen.

In this Lawfare podcast (http://www.reuters.com/article/us-spying-juniper-idUSKBN0UN07520160109) Nick Weaver (senior staff researcher at the International Computer Science Institute in Berkeley, California and staunch Bitcoin sceptic), gives his own take on Bitcoin basics, and whether it's really an historic financial opportunity, massive criminal problem, or something else entirely: a waste of everyone's time and money.

He argues (to protect everyone from fraud), electronic transactions need to be reversible, which Bitcoin transactions are not…without the private keys. He talks a lot about Chinese domination of Bitcoin generation and Chinese coal being burned to power what he dubs "useless work" a.k.a hash generation.

Bitcoin enforces decreasing production returns (currently 25 Bitcoins, plus transaction fees) to combat mining monopolies. The bitcoin protocol (https://en.wikipedia.org/wiki/Bitcoin_protocol) specifies that the reward for adding a block will be halved approximately every four years (here's a counter point (http://senior staff researcher at the International Computer Science Institute in Berkeley, California) for the environmental – if not political and fraud – concerns). Eventually, the Bitcoin reward will decrease to zero – transaction fees will be all folk get – and the limit of 21 million bitcoins will be reached in around 2140. That doesn't however combat ponzi schemes (where Bitcoin investors are paid returns out of money invested by others, rather than any actual earnings), another key theme in the podcast.

Nick's primary argument is that criminals see opportunities for returns far beyond Bitcoin market

value (due to the anonymous and therefore criminal-friendly aspects of exchange), so racing to reap and control coins through production
offers dark opportunities that justify a loss-making investment in production means. Together with potential for market instability (including DDoSing or spamming to disrupt transactions), he argues Bitcoin will never evolve into a value-stabilised competitive currency. Instead it will die a death through breaking or being regulated out of existence…and so what? According to Weaver only criminals, crypto/techno anarchists, and a few misguided venture capitalists will really mourn it.

As I said earlier on, blockchain (as distinct from Bitcoin), is just plumbing. Digitally innovative and game-changing plumbing, but plumbing nonetheless…

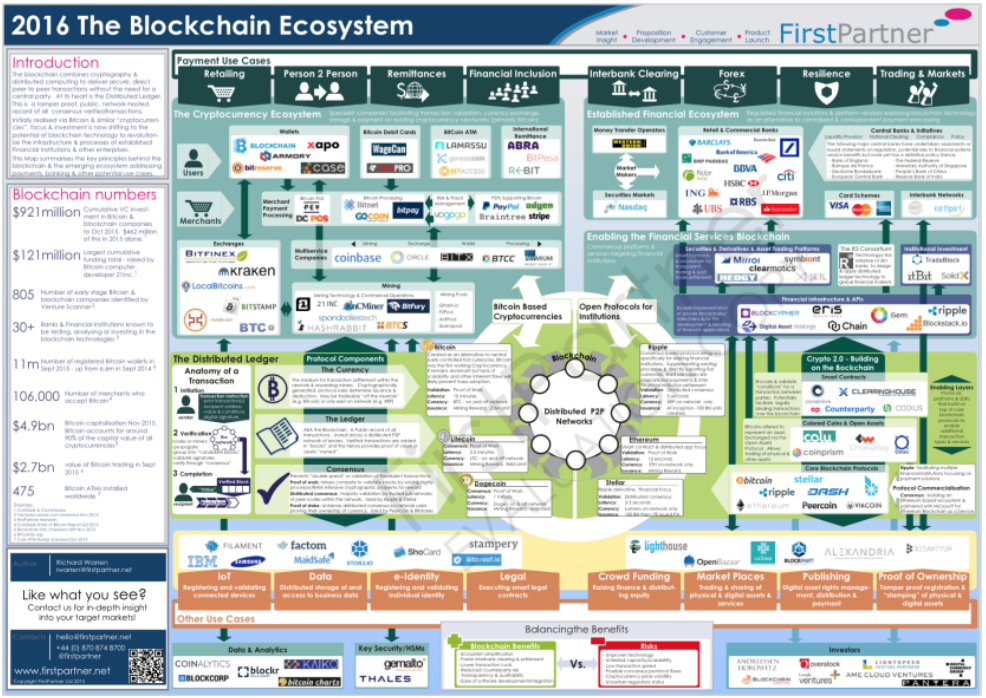
…and there's the impending storm

While big businesses of all flavours can see the undoubted benefits of blockchain related solutions, they're not sure where it starts and ends. Cue vendors falling over themselves to sell 'Blockchain Plus' or (as I've seen it called by a few folk), blockchainware. Perhaps packaged with tools to perform that pre-transaction identification and authentication step (a must for regulated finance industries). Companies maybe missing the fact that vendors bringing them easily consumable and 'credible' blockchain expertise, might not have a scooby do about the true ins, outs, and resources required to securely provide the shiny extras.

It will be easy to become overwhelmed by people milking the enticing idea of cutting out traditional transaction-validating fee-charging middle men, or blockchain-esque ways to inject wedges of extra protection for all kinds of information integrity.

Don't be blinded by the technobabble and hype. Good due diligence and procurement principles still 100% apply. This isn't magic. If vendors can't simply demonstrate how a solution solves your problem, if vendors ignore work needed to get data into a fit state to be preserved in a blockchain, if vendors gloss over the identity and asset ownership verification (Garbage In Garbage Out is as true here as it ever was), if vendors don't confirm and accept liability for making it work in your existing environment, if vendors don't assess and demonstrate future scalability capacity, performance, and run budget required…you will be complicit in pulling very expensive wool over executive eyes.

For a related and also slightly mind blowing view, have a look round the now octopus-like ecosystem that's developed so far (thanks to @blkchninstitute for the cephalopod analogy and pointing me at this First Partner infographic)



Click on the image to expand

Far from equally prolific are the professionals who can differentiate between blockchain flavours, good and bad implementations, inherent value-add, and hastily-

cobbled branded bolt-on (the reason this post exists). Bolt-ons that may very well bleed away hoped-for savings and inject unforeseen vulnerabilities. Much like the disappointment many suffered when buying cloud solutions, only to find arms-length oversight, and lack of orchestration to make cloud meet their requirements, equalled a loss of advertised benefits.

For those who want to learn more about blockchains and other cryptocurrency related technologies, this Coursera course (https://www.coursera.org/course/bitcointech) has been recommended by a number of my contacts.

Back to good old C, I & A

So, given this has turned into War and Peace, more musing on security to come later. Except to stress again that the benefits of blockchain are mostly, in security terms, around integrity. The frequently ignored part of that security triumvirate. Availability, in the widely distributed model, is also protected. Your data store is everywhere. But it doesn't guarantee confidentiality. Confidentiality depends upon the implementation, maintenance, algorithm used, and management of cryptographic keys (among other things). Here's Kaspersky's take (http://insidebitcoins.com/news/kaspersky-and-interpol-say-blockchain-is-vulnerable/31578) on what can go wrong.

More generally, everything is only as secure as the behaviour of people who design, build, maintain and use it. Mt Gox were bankrupted (http://www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/) following 'technical problems' resulting in loss of 850,000 Bitcoins. That underlines my point in mile high neon. And, in blockchainville, the number of people involved is exploding. An explosion that will come with lots of of important security lessons to learn.

A big thank you to @01101O10 (https://twitter.com/01101O10) a.k.a. cryptocurrency developer a.k.a blockchain alchemist a.k.a. all round super-smart good guy, for reviewing this for me.

*Blockchain, blockchains, block chain, the blockchain – usage varies wildly. For the sake of this post, where I'm talking about 'it' as a concept/method, I've used 'blockchain' throughout.