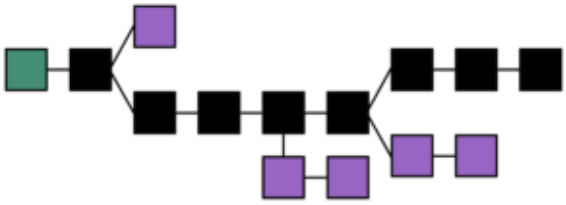
Trust me (we'll get to know each other later) – Tagline: blockchain re-invents who and how we trust



Ills.: nl.wikipedia.org

I've been mulling a wry title for this piece. The passage of deliberation punctuated by flocks of green avians (yes, parrots and in Amsterdam!) dissecting the blue, blue firmament on their screeching way to somewhere possibly exotic, only to pivot and rush back the way they had come mere moments later.

The struggle is to find the depth of pith required to compliment the hint of wit that will sustain attention beyond a headline. 'Trust me (again)' comes close as does 'Trust re-invented'. 'Trust 2.0' is potentially smirk worthy but only to those, perhaps, for whom Web 3.0 or Industry 4.0 elicit a familiar nod.

Trust me, this was the best I could do.

Most of us trust someone or something: a distant cousin on your mother's side, a company, an institution, or even the government. Agreed, it was not strictly necessary to add the word 'even' when mentioning the government and yet…

Trust runs through us like Brighton through rock. It's free and freely given. It's easily and frequently betrayed only to be given again.

And so…

We trust that the barber is no Sweeney Todd; that government will safeguard state pensions; that the late-night Uber driver is, honestly, just an Uber driver; that the limited-edition Warhol is not, on inspection, a Wharwhole; that the heating engineer can distinguish a water pipe from a gas pipe; that the eviction

technician barring entry to Koooolers Nightclub will not sell the enforced copy of your ID to X-Ron3023, a denizen of the dark-web and a close associate of NightKnightBungie100-2; that the recently promoted (former) assistant VP now has access to the executive bathroom on the top floor.

We need trust. The moment maker. The oil in the works. What is there without trust? And I implore you to keep in mind that trust starts with truth and ends with truth, fear leads to more fear, and trust leads to more trust, and we must surely all concur that to be trusted is a greater compliment than being loved. Trust Hemmingway to weigh in with 'The best way to find out if you can trust somebody is to trust them.'

All good. Not a jot of critique from my side. Old school trust. Built over decades, augmented by endorsements of others. The trusted and tested and true assured reliance on character and values and judgement, our innate ability and strength to see the truth of someone or something leading us have confidence (unscientifically, some might say) that our best interests will be represented, or at the very least not compromised.

It's been a battle – a losing battle – to maintain my willingness to trust those making increasingly frequent requests for, yes, my trust. You can trust us with your profile data, they cry; you can trust our claim that the coffee-famer received a living wage in the production of this premium product; that the energy powering my microwave is not only green but the greenest; and that this cod was sustainably caught in the North Sea using the latest ecologically friendly gear and the discard (read: disposing of dead fish that you'd rather not have caught) was negligible.

Sceptical? Should you find a moment in your local supermarket to peruse the little letters and labels printed on the packaging en route past Dairy and Fresh to where Linda waits patiently at the checkout, you'll surely agree that the credibility of these claims is enhanced by cutting-edge keywords that include (but are not limited to) WiggleWoggle certified, artisan organic, free range (define range) and farm fresh(ness) – whatever that means.

Further doubts may be placated by a plethora of QR codes and high-quality logos and, without a shred of hesitation on my part, I'd like to state for the record that many of these logos go way beyond clipart.

Look, we're a few paragraphs in and I've not mentioned blockchain which has not been easy. Don't ask or expect me to defend the many (but not all) justifiable claims that cast blockchain in a poor light. Decades must pass before blockchain's battered reputational half-life decays to the point of defying detection.

Blockchain. Disruptive? Disreputable? I need to move on as, otherwise, this post will assume book-length dimensions as I attempt to parry what many are thinking. My plea, humbly made, is that you will accept that blockchain is a 'thing' and that we'll save other discussion for later.

[Author's note: the remainder of this article contains numerous dangerous bends in train of thought, and a range of concepts and terms invented by nerds whose average age is twenty-three. Continue reading only under medical advisement].

How can blockchain replace old school trust? What could possibly supplant the handshake, the written agreement, the unshakeable faith in a bond handed down the generations?

The answer is that blockchain cannot replace any of these things.

Rather, blockchain facilitates alternative forms of trust. Trust between parties that have never met, who have not heard of one another, who do not like each other, who compete with each other and – I'm just putting it out there – do not trust each other. Blockchain facilitates trustless transactions where a distributed network of 'verifiers of truth' (nodes) guarantee both the execution of transactions between parties (liveness) as well as the integrity of transactions following agreement (consensus).

Furthermore, blockchain requires no mediating (meddling?) third-party as an enabler and, as a result, there is no centralised authority needed to deny or refuse or scrutinise or record any transaction or interaction between two parties. Humans are not involved in consensus forming and, as a result, there is no opinion-based influence and no ad-hoc bias. Given the same set of inputs, the blockchain will consistently resolve in the same manner each time of asking. Trust me on that.

In considering how blockchain helps reinvent trust, we need to first dispel the notion that blockchain and cryptocurrency are synonymous. The repute of the former tarnished by the ponziness of the latter. Take transactions for example.

The first and best-known blockchain network was named ‘Bitcoin’, while the first and best-known cryptocurrency was named ‘bitcoin’ (the branding agency has a lot of explaining to do). And the first transaction involved a bitcoin token on the Bitcoin network.

The term ‘transaction’ can also mislead. A transaction could, indeed, refer to a payment from one party to another. However, a transaction my involve the transfer of intellectual property, or of a digital work of art (NFTs are the new black, digital scarcity and ownership guaranteed), or the verification of a claim such as the right to drive, your age (remember Koooolers), relevant skills (remember the heating engineer), your academic credentials, certain rights (remember the former assistant VP), or sustainable fish (remember the cod).

Two examples suffused with a sprinkling of geek-speak will either pave the way to your ‘ah-ha’ moment or reinforce existing beliefs that old-school trust is all you can trust.

Koooolers Nightclub
You’re at the door of Koooolers Nightclub. Midnight. The bouncer needs to see your ID. He turns to make a copy of your driving license on an ancient Xerox 1048 circa 1984. Copy? “Yes, mate. Company policy. Any other questions?” It’s raining and you don’t have any other questions. In order to gain entry to this den of partyness, you’ve just entrusted – to a stranger – your full name, your photograph, date of birth, place of birth, your driving license number, your social security number, how long you’ve had your licence, and an overview of the vehicles you are permitted to drive when all that is really required to enter Kooolers is a check on if you are old enough, not even how old you are. If we think this through, you’ve also given away your physical location confirming that you are not home, your preference for a down-market nightclub, and indicated your willingness to part with personal data at the request of someone wearing a tight suit. Self sovereign identity (SSI) is an approach to digital identity management gives individuals control of their digital identities using, often, blockchain to secure and protect privacy. SSI would change the above scenario as follows: a scan of your face would match against the blockchain secured and encoded biometrics of your ID document (this offers a proof that you are the holder of the ID based on the permission you’ve granted to perform this verification just once for this specific task). In this manner, you have verified yourself against a credential (your driving license) issued by a trusted party (the Government). You would also need to give

permission to establish that your age is above the minimum age required to enter Koooolers. In this case, the same credential can be used as your date of birth is also an element of your driving license data secured on the blockchain. It checks out and moments later you are swapping stories with a retired wrestler while the barman inexpertly assembles a watery cocktail replete with maraschino cherry and tiny umbrella.

Cranking up the geek-factor a tad, the Koooolers scenario demonstrates an application of non-interactive zero-knowledge proofs that require no interaction between the issuer of a credential (the Government) and the verifier (Koooolers) to establish the veracity of a claim (you are old enough). Using SSI in combination with zk proof technology, you have been able to prove your claim without giving away any data that you'd rather keep private.

Supermarket.
It's true. Sustainably caught cod tastes better than other cod. And even if it doesn't, it feels like it should and, as you've paid a premium for this ecologically friendly product, you'll exercise your deity-given right to believe whatever you want about the taste.

But let's move beyond the sustainability claims on the packaging: tiny letters, even smaller logos, certifications from bodies you've never heard off, a web address here, a QR code there. We are asked to trust in so many claims these days that, in order to determine which are genuine, something more is required. What follows is a cod-inspired thought experiment: a fishing boat in the North Sea. The captain, somewhat nervously, has deployed imaging and sensor-technology on his boat that captures 20 data points every thirty seconds. A trip of 16 hours would record 38400 micro-measurements on salinity, humidity, line tension, fuel consumption and a host of other metrics. Real-time processing of this data in the cloud using buzz-word compliant artificial intelligence, big data analytics, image recognition and other cool techniques provide two types of output. Firstly, actionable insights that benefit the captain immediately by suggesting, for example, adjustments to set ups, gear choice, and speed which positively impact the profitability of this trip; secondly, the cloud-based analytics will provide sustainability proofs. This latter output forms the basis of establishing verifiable sustainability claims that cod-fans can rely on. A boat can prove it has not strayed outside of mandated fishing grounds (without revealing where, specifically, it fished), that the weight of fish caught has not exceeded the amount

of fish landed (without revealing how much was caught), that discard is within regulatory tolerance, that bycatch is limited, that the gear used did not damage marine ecology. These claims can be cryptographically secured on the blockchain and made available – at the captain's discretion – to those asking for proofs.

A picky point of clarification is required here. We are talking about proofs and the role of blockchain in creating trust in claims. We are not implying that blockchain is a synonym for database. More plainly stated, blockchain is not better at being a database than, say, a database. Blockchain offers an immutable, auditable (and often) public trust layer enabling claims to be verified. In this cod example, the data, outputs and insights are all owned and controlled by the boat captain. ZK technology, as used in the Kooooolers example, allows for minimal reveal without giving away information a captain would rather keep confidential.

This means that (downstream), consumers can trust in sustainability claims. Furthermore, this means that (upstream), regulators can trust in claims of sustainable fishing practices and can act (regulate) based on traceability and verification rather than on aggregate modelling and assumption.

We started talking about trust and ended up with blockchain. How did that happen?

My hopes for readers that made it this far are two-fold. Firstly, that you (now) regard blockchain as a real and unstoppable and disruptive technology and, secondly, that trust in a technology that reinvents trust is more than purely tautological.

–

Mike Russell is Senior Lecturer and Researcher at the Amsterdam University of Applied Science and at Northumbria University. Since gaining a PhD in man-machine interaction from the University of Wales, Russell has waited decades for blockchain's arrival. During this intervening period, he has pretended to be a software developer for ITT (Amsterdam), directed the European Management Lab for CTP (Amsterdam), dabbled as an invited researcher at Hitachi Central Research Labs (Tokyo), and taught informatics at Griffith University (Brisbane). Russell's current research interests relate primarily to blockchain and something: blockchain and defi, blockchain in the supply chain, blockchain and the metaverse, blockchain and philanthropy.