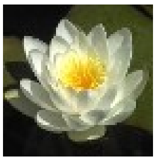
blockchain



what is it?

A blockchain is a list of records that once verified, is virtually impossible to change. Packets of digital information form a ‘block’, and the blocks are linked together chronologically in a ‘chain’. A Blockchain can be used for transferring things (digital assets) securely between individuals, without the need for a centralised authority, such as a bank or a state. Each block contains a number of transactions / records, plus additional info such as dates, participants (anonymous digital signatures), and some encryption called a ‘hash’, produced by an algorithm, and unique, to distinguish that block from every other block in existence. Put another way, it’s a distributed database (or ledger), with cryptography built in, so that anything written to it is secure, without having to trust individuals or institutions. Bitcoin and other cryptocurrencies are not blockchains – they’re based on blockchain technology.

In the early 80s, David Chaum proposed an electronic payment system with ‘blind signatures’, for privacy and prevention of criminal activities. He founded Digicash to implement this system in 1990 – but it still required a bank to verify transactions. In the late nineties, Wei Dai (b-money) and Nick Szabo (Bit Gold) proposed distributed systems, without central verification, and Adam Back proposed Hashcash, to prevent spam (the Hashcash algorithm is still used in Bitcoin). Hal Finney used Hashcash to develop ‘proof of work’ tokens, that verified transactions through the solving of puzzles by computers, which is the basic idea behind blockchain. The first blockchain was built in January 2009 by Satoshi Nakamoto (a pseudonym – the identity of the inventor is still unknown), who sent the first Bitcoin to Finney.

Blockchain was all about cryptocurrencies until Ethereum arrived in 2015, which allowed application code to be run on blockchain. Blockchain applications beyond cryptocurrencies are still minimal, although those applications do exist – such as registering land ownership.

Cryptocurrencies are the best known application of blockchain technology.

what are the benefits?

Blockchain transactions are transparent, immutable, irreversible and can occur securely between people who don’t know or trust each other. Transactions in the conventional (fiat) economy require mediation between parties for trust; a mutual credit economy involves known and trusted participants (payments in cash are immediate and irreversible too, but come with a whole new raft of logistical problems).

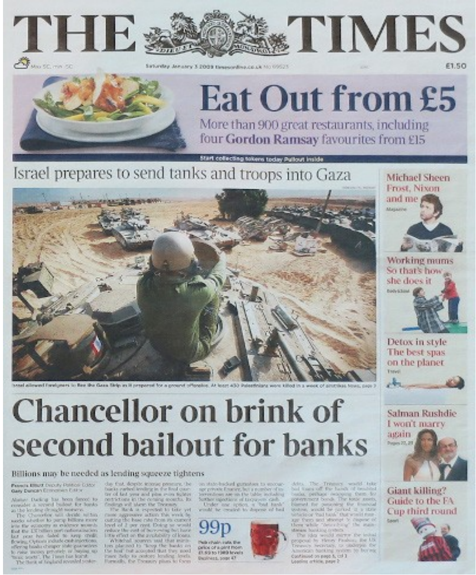
People can transact with each other without middlemen. This removes the extra cost of banks, and helps disperse some of the massive concentration of money in the banking sector. This is good for democracy too. As Supreme Court Justice Louis Brandeis said: ‘We can have democracy or we can have great wealth concentrated in the hands of a few, but we can’t have both.’ In the first (‘Genesis’) block, Nakamoto embedded this text: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” – which has been interpreted as a critique of the banking system. Bitcoin doesn’t require banks or bank bailouts.

Because blockchain is distributed technology, it means that we don’t need a central authority for trust. This has a lot of potential – perhaps for distributed governance, so that we don’t need centralised authority at all – removing the risk that that centralised power be seized, or bought by concentrated wealth (actually, this one is less of a risk than a reality in today’s world). This was a strong motivation for the blockchain pioneers.

No-one can ‘own’ the blockchain technology – it’s open source (and can be found in GitHub, an open source code repository). It’s about the freedom to know, rather than to own.

Blockchain can help prevent fraud. The Honduran land registry was put on the blockchain to stop gangsters making fraudulent claims on farmers’ land, and politicians claiming beachfront properties. Estonia is doing some funky things with the blockchain too, such as blockchain-registered digital passports. There have been scams and thefts involving cryptocurrencies, but this isn’t the fault of the blockchain – it’s to do with errors in the writing of applications.

A downside is that the ‘proof of work’ consensus algorithm used by Bitcoin, Ethereum and other currencies requires a lot of energy. Some cryptos are now moving to an algorithm called ‘proof of stake’, which doesn’t require number-crunching, and requires a tiny fraction of Bitcoin’s energy use. Examples include EOS and FairCoin; but there are technical challenges with this kind of algorithm, which is why they’re not so prevalent.



THE TIMES

Saturday January 3 2009 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

99p

Times headline, Jan 3 2009. This text was included in the first blockchain, indicating that anti-bank sentiment was a motivation for its anonymous inventor.

what can I do?

Every blockchain has an associated crypto token, so for transaction fees, you need a digital wallet, a plug-in to your browser, and when you submit something, you have to digitally sign your transaction. For more technical people, the barriers aren't high, but the geekiness of blockchain is probably what's holding it back.

Author Melanie Swan (see resources), describes Blockchain 1.0 – for cryptocurrencies; Blockchain 2.0 – for financial applications (not just crypto, but also share dealing, token exchanges etc.); and Blockchain 3.0, on which any applications can be run, beyond finance. Ethereum is an example of Blockchain 2.0 / 3.0, with an associated cryptocurrency called Ether. It's different from Bitcoin and other cryptos in that you're able to run any application code, in theory to do anything you like, on the Ethereum blockchain itself.

She, and other enthusiasts, see blockchain as the solution to all the world's problems. We wouldn't go that far, but we can see its benefits in lots of situations. For example, it's often claimed that most humanitarian aid or charity donations end up in the wrong hands because of corruption. It's difficult to prove, but it would be clear if this were true if transactions happened a blockchain.

For developers, blockchain involves interesting problems like cryptography, decentralised consensus, writing applications, open source and economic and political philosophy. You can write applications to blockchains like Ethereum, so that non-technical users can interact with it; or you can copy the Bitcoin code from Github, modify it to create your own blockchain, name it, get it online, and then initiate the first transaction, which would form part of the Genesis block for your new blockchain. You could then work with others, including beginners, and show them how to use your blockchain. For the uninitiated, if you've been advised that a blockchain is the thing you need for your business (for example), talk to a blockchain developer. It's a new and growing industry. But you can have a go at using cryptocurrencies without so much technical expertise.

If you're of a geeky persuasion, and think you'd like to be a blockchain developer, a good place to start is web3js.readthedocs.io. There are courses, or you can learn by doing. You could volunteer on open source projects – contact our advisor Steve (below), who is often looking for volunteers.

resources

- lowimpact.org/blockchain for our advisor, plus more info, courses, links & books, including:
- Melanie Swan, *Blockchain*
- Don & Alex Tapscott, *Blockchain Revolution*
- Roger Wattenhofer, *Blockchain Science*
- bit.ly/3bs9eO5 – Nakamoto's 2009 white paper
- github.com/bitcoin/bitcoin – Bitcoin's open source code
- coinmarketcap.com: list of crypto tokens associated with blockchains

Huge computer banks do the puzzle-solving involved in 'proof-of-work' algorithms used to generate Bitcoin. 'Proof-of-stake' algorithms use far less electricity.

Feel free to upload, print and distribute this sheet as you see fit. 220+ topics on our website, each with introduction, books, courses, products, services, magazines, links, advice, articles, videos and tutorials. Let's build a sustainable, non-corporate system.

facebook.com/lowimpactorg **Lowimpact.org** **twitter.com/lowimpactorg**

Registered in England. Company Ltd. by Guarantee no: 420502