An introduction to Bitcoin and Blockchains

James Campbell

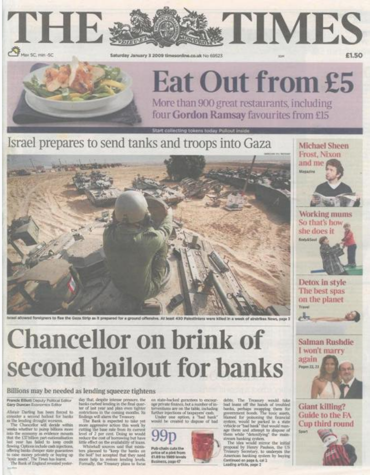
March 20, 2018

Department of Mathematics
Cardiff University

History and Background

Bitcoin: The first Blockchain

- Outlined in October 2008 by Satoshi Nakamoto [15]
- Network online January 2009 [5]
- First transaction for physical goods in May 2010



THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£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

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.89 to 1989 levels Business, page 47

Definition

A Transparent, Public, Distributed, Append-Only Ledger

- Unknown

The Ledger

From	To	Amount (£)
	…	
Amy	Ben	13.65
Ben	Tesco	1.01
Lidl	Amy	492.50
	…	

Tell Me More...

Hash Function

A hash function is any function that can be used to securely map data of arbitrary size to data of fixed size.

Cryptographic Hash Functions have some useful properties:

- Deterministic and Fast
- Non-Invertible
- Collision Resistant
- Avalanche Effect

A Block

- An Index
- Some Data
- Nonce
- Hashable

Mining a Block

A Block is not valid unless it's Hash satisfies a certain criteria.

A Blockchain

Link Blocks together (in a chain) by including the Hash of the previous Block.

A Blockchain

Link Blocks together (in a chain) by including the Hash of the previous Block.

What happens if an attacker attempts to edit some previous data?

Tell Me More...

The Blockchain Process

1. A user creates an addition to the ledger

The Blockchain Process

1. A user creates an addition to the ledger
2. This is broadcast to the entire network

The Blockchain Process

1. A user creates an addition to the ledger
2. This is broadcast to the entire network
3. Nodes in the network attempt to create a Block

The Blockchain Process

1. A user creates an addition to the ledger
2. This is broadcast to the entire network
3. Nodes in the network attempt to create a Block
4. The new Block is added to the Blockchain and broadcast to the Network

The Blockchain Process

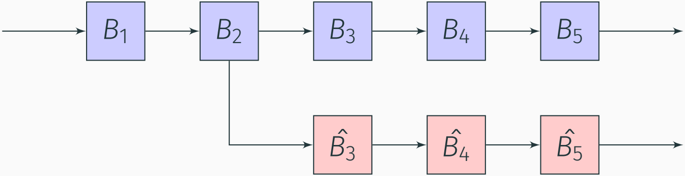
1. A user creates an addition to the ledger
2. This is broadcast to the entire network
3. Nodes in the network attempt to create a Block
4. The new Block is added to the Blockchain and broadcast to the Network
5. The process repeats

The Blockchain Process

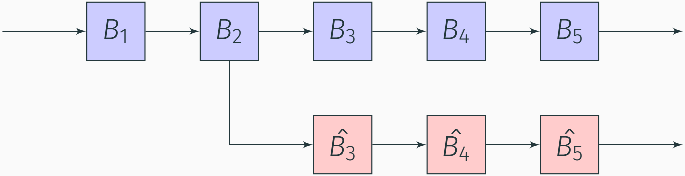
1. A user creates an addition to the ledger
2. This is broadcast to the entire network
3. Nodes in the network attempt to create a Block
4. The new Block is added to the Blockchain and broadcast to the Network
5. The process repeats

Nodes in the network use the longest Blockchain available

A Malicious Node



A Malicious Node



The network is secure provided that no single malicious attacker controls more than half the hashing power.

Tell Me More About Bitcoin...

Unanswered Issues

- What incentive is there for Good nodes?
- How are Bitcoins created?
- Proof of Ownership

Coinbase Transaction

Every Block includes a transaction that has no sender, only a recipient.

Coinbase Transaction

Every Block includes a transaction that has no sender, only a recipient.

The recipient is the Node that found the correct Nonce to validate the Block.

Coinbase Transaction

Every Block includes a transaction that has no sender, only a recipient.

The recipient is the Node that found the correct Nonce to validate the Block.

Called the Block Reward (which decreases over time).

Public/Private Key Pairs

Bitcoin addresses are Public Keys.

Public/Private Key Pairs

Bitcoin addresses are Public Keys.

Every transaction must be signed by the Private Key that is paired with the senders Public Key.

Public/Private Key Pairs

Bitcoin addresses are Public Keys.

Every transaction must be signed by the Private Key that is paired with the senders Public Key.

Anyone can easily verify that a transaction was created by the sender **only**.

Tell Me More...

Further Reading (Bitcoin Related)

- Myths [10, 1]
- Environmental Impact of Bitcoin [3, 16, 22, 11]
- Merkle Trees [18, 14]
- Segwit and Lightning Network [7, 12, 23, 13]

Further Reading (Future of Blockchain)

- Proof of Stake [6, 19]
- Smart Contracts [4, 9]
- DAG currencies (IOTA, Nano, ByteBall) [20, 8, 17]
- Hashgraph [2, 21]

Thank you...any questions?

References

May 2016. URL: https://www.nasdaq.com/article/top-10-myths-about-bitcoin-cm620562.

Leemon Baird. *THE SWIRLDS HASHGRAPH CONSENSUS ALGORITHM: FAIR, FAST, BYZANTINE FAULT TOLERANCE.* May 2016. URL: http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf.

JP Buntix. *Bitcoin Network’s Electricity Consumption Is Lower Compared to Printing Money*. URL: https://themerkle.com/bitcoin-networks-electricity-consumption-is-lower-compared-to-printing-money/.

frozeman et al. *The Ethereum Wiki*. ethereum, Mar. 2018. URL: https://github.com/ethereum/wiki.

Genesis Block. URL: https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c

Investopedia. *Proof of Stake (PoS)*. May 2017. URL: https://www.investopedia.com/terms/p/proof-stake-pos.asp.

Investopedia. *SegWit (Segregated Witness)*. May 2017. URL: https://www.investopedia.com/terms/s/segwit-segregated-witness.asp.

jimmco. *ByteBall vs IOTA - battle of two DAG cryptocurrencies*. June 2017. URL: https://steemit.com/cryptocurrency/@jimmco/byteball-vs-iota-battle-of-two-dag-cryptocurrencies.

Lukas K. *This is How Smart Contracts and Ethereum Work. Brief Introduction*. July 2017. URL: https://medium.com/startup-grind/gentle-intro-to-blockchain-and-smart-contracts-part-2-30a6c9a40946.

George Kikvadze. *Seven Myths of Bitcoin*. Mar. 2018. URL: `https://medium.com/@BitfuryGeorge/seven-myths-of-bitcoin-2e3a66d37e64`.

Nicole Kobie. *How much energy does bitcoin mining really use? It's complicated*. URL: `http://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use`.

Charlie Lee. *My Vision For SegWit And Lightning Networks On Litecoin And Bitcoin*. Jan. 2017. URL: `https://segwit.org/my-vision-for-segwit-and-lightning-networks-on-litecoin-and-bitcoin-cf95a7ab656b`.

- Waee Digital Ltd. *Segwit Bitcoin and Lightning Network Explained*. URL: https://www.anythingcrypto.com/guides/segwit-bitcoin-lightning-network-explained.

- *Merkle Tree - Bitcoin Glossary*. URL: https://bitcoin.org/en/glossary/merkle-tree.

- Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. URL: https://bitcoin.org/bitcoin.pdf.

- Elaine Ou. “No, Bitcoin Won’t Boil the Oceans”. In: *Bloomberg.com* (Dec. 2017). URL: https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think.

- Serguei Popov. *The Tangle*. Oct. 2017. URL: https://iota.org/IOTA_Whitepaper.pdf.
- Shaan Ray. *Merkle Trees*. Dec. 2017. URL: https://hackernoon.com/merkle-trees-181cb4bc30b4.
- Ameer Rosic. *Proof of Work vs Proof of Stake: Basic Mining Guide*. Mar. 2017. URL: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.
- Peter Ryszkiewicz. *IOTA vs NANO (RaiBlocks)*. URL: https://hackernoon.com/iota-vs-raiblocks-413679bb4c3e.

George Samman. *A New Approach to Consensus: Swirlds HashGraph*. URL: http://sammantics.com/blog/2016/7/27/hashgraph-consensus.

steembusiness. *Bitcoin Mining - A Critical View On Its Environmental Impact!* Dec. 2017. URL: https://steemit.com/bitcoin/@steembusiness/bitcoin-mining-a-critical-view-on-its-environmental-impact.

Aaron van Wirdum. *Understanding the Lightning Network, Part 1: Building a Bidirectional Bitcoin Payment Channel*. URL: https://bitcoinmagazine.com/articles/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791/.