Bitcoin, Blockchain and cryptocurrency

What's the fuss all about? By Gail Chatziyakoumis August 2018

Blockchain adoption means

- you can buy without a merchant
- bet without a bookie
- get insurance without an underwriter
- access finance and loans without a bank
- trade without an exchange
- purchase commodities without a broker
- have law without lawyers, courts and judges
- create assets without an issuer
- audit without an accountant or auditor
- get funding without a Venture Capitalist
- secure escrow without an agent
- have internet without an Internet provider (ISP)
- verify records without a notary
- establish reputation and credit without a credit agency
- create identity without government.

When Bitcoin started

The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto.

In Oct 2008 , a white paper was published titled "Bitcoin: A Peer to Peer Electronic cash system".

It was implemented the following year by Nakamoto as a core component of the cryptocurrency Bitcoin.

The words *block* and *chain* were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, *blockchain,* by 2016.

Natamoto created the first block himself and he embedded the words

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

Blockchain fundamentals

- The Bitcoin program creates a maximum of 21,000,000 bitcoins (digital money) across time
- It records all there ongoing transactions in a file called the blockchain.
- The bitcoins only exist in the blockchain record
- The bitcoin program is open source -anyone can read the instructions to the computer
- The bitcoin program is free to put (download) onto your computer
- Thousands of computers are running the program keeping it secure
- It's anonymous -no names are included only account numbers
- Anyone can see the blockchain on the internet and check its contents

BLOCKS

- Instead of one continuous file of ongoing transactions the information is broken into blocks
- The block is the reason the data is considered secure and trustworthy
- A block is created and added to the blockchain approx every 10 minutes
- Each block is created when a maths puzzle is solved
- Each block is said to have been mined when it is created
- Each block creates bitcoins
- Each block includes bitcoin transactions of already created bitcoins
- The first computer to solve the puzzle wins the mining reward
- The mining rewards are the newly created bitcoins and fees for transactions
- Each block is numbered and timestamped
- The winning computer adds the block to blockchain file and all other computers copy it.
- Each block is linked through a maths process to every previous block

Original block rewards in 2009 where 50 bitcoins and after 4 years it halves so 25 in 2013 and in 2017 it was 12.5. The last bitcoin will be mined in 2140AD.

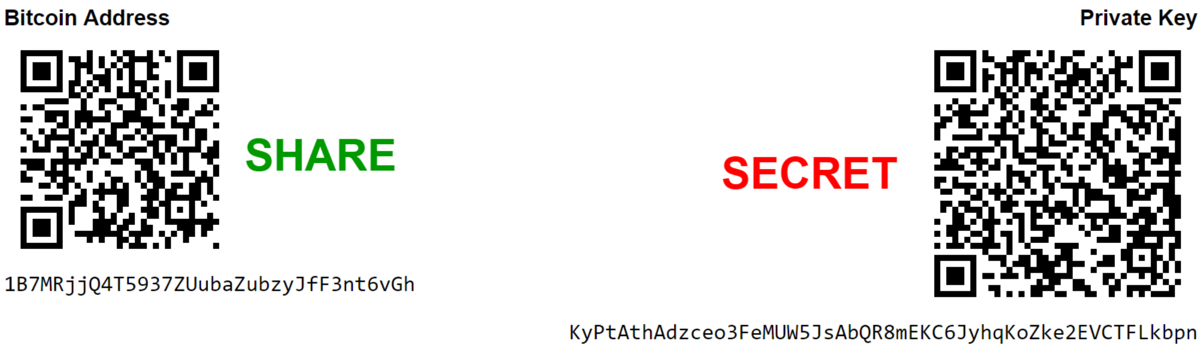
Simulted blockchain

Block 1	9/8/2018 2.18pm Account 614		Bal 50 BTC

Block 2	9/8/2018 2.21pm Account 832		Bal 50 BTC
Prev Block characters 38			

Block 3	9/8/2018 2.25pm Account 175		Bal 50 BTC
TX1	Account 832		Bal 48.999 BTC
	Account 222		Bal 1 BTC
	Account 175	TX fee	Add 0.0001BTC
Prev Block Characters 60			

Pairs to access the blockchain



Bitcoin Address

SHARE

1B7MRjjQ4T5937ZUubaZubzyJfF3nt6vGh

Private Key

SECRET

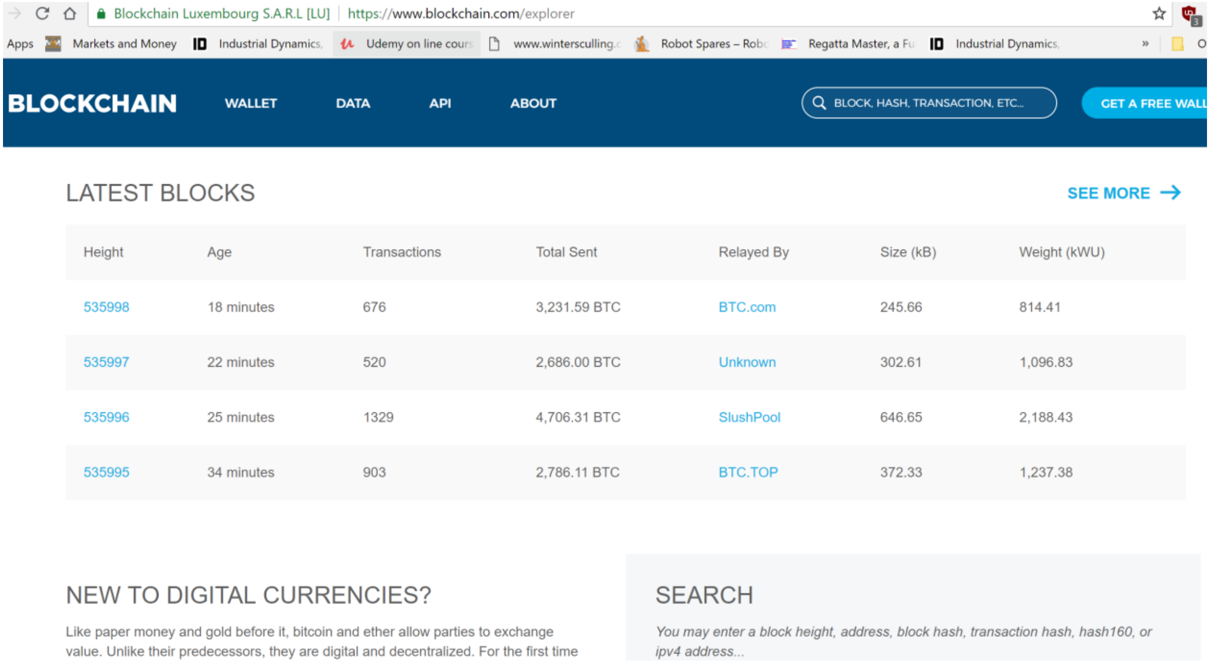
KyPtAthAdzceo3FeMUW5JsAbQR8mEKC6JyhqKoZke2EVCTFLkbpn

The bitcoin address is what we called account no in our simulation. The secret key is needed to do transactions and you can create a key pair (a bitcoin address and Private key) at this website.

https://www.bitaddress.org were you can go to make you

The Bitcoin blockchain in action

At this website https://www.blockchain.com/explorer



LATEST BLOCKS

SEE MORE →

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
535998	18 minutes	676	3,231.59 BTC	BTC.com	245.66	814.41
535997	22 minutes	520	2,686.00 BTC	Unknown	302.61	1,096.83
535996	25 minutes	1329	4,706.31 BTC	SlushPool	646.65	2,188.43
535995	34 minutes	903	2,786.11 BTC	BTC.TOP	372.33	1,237.38

NEW TO DIGITAL CURRENCIES?

Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time

SEARCH

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

SMART CONTRACTS

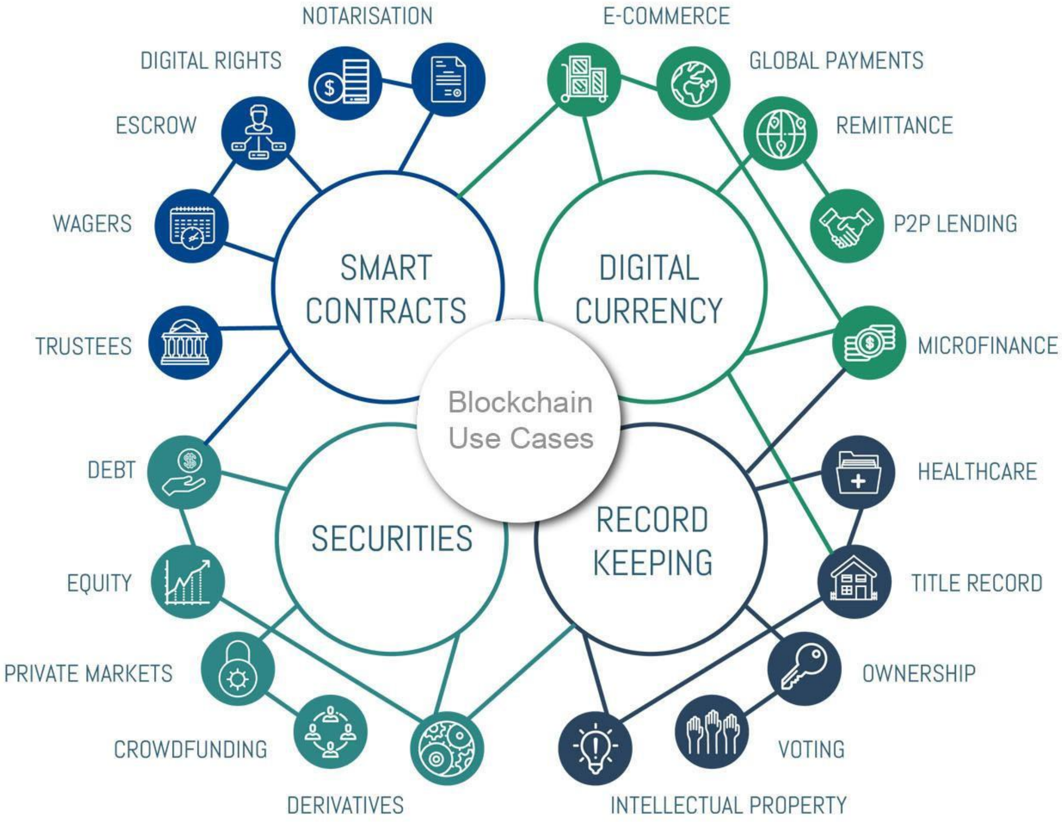
Ethereum is a Blockchain that you can add computer instructions to that do something to the blockchain when something happens.

For example if you own something listed on the blockchain.

You could make a contract to sell it to someone else that automatically sends that ownership to them upon receiving the payment from them.

They can trust that the sale will happen because they can see the smart contract inside the blockchain.

The main cryptocurrency with this ability is Ethereum but there are others.



TOKENS

Instead of a bitcoin the same idea can be used to tokenise things- Made in smart contracts

Currently there are 2 types of tokens- ones that are all the same and ones that are all unique.

Tokens that are the same are used to pay for services e.g. the way you buy a ticket or coin to get on a ride

You can buy access to computer power or file space .

Unique tokens represent an asset like a painting or house or a digital cat.

These are often the basis of ICO- Initial Coin Offerings

Examples of blockchain

https://www.mivote.org.au/

MiVote is an information platform that presents you with a variety of perspectives on all major issues up for debate in the Australian Parliament and many others that affect our lives, via the MiVote App. The MiVote App enables you to make an informed, well rounded decision and have your say on where you want our country to go. Putting REAL change at your fingertips.

Blockchain uses in trade

Blockchain is about to revolutionise shipping and boost trade by $US1 trillion

https://www.afr.com/business/transport/shipping/blockchain-is-about-to-revolutionise-shipping-and-boost-trade-by-us1-trillion-20180419-h0z0fg

Blockchain in Remittance

https://cointelegraph.com/news/backed-by-major-vc-firms-the-bitcoin-remittance-app-abra-is-set-to-launch-next-month

Essentially, Abra is a peer-to-peer version of today's remittance service providers. Instead of having to visit physical locations or outlets to receive or send money, that can be inefficient for individuals based on the countryside or rural areas, users can simply send remittances using their mobile phones to any recipients who will then receive the payment from Abra tellers all across the world.

Blockchain used to trace Almonds from Australia to Germany

https://youtu.be/TqB9gSEc-5o

A blockchain used to give refugees an provable identity

https://www.cnbc.com/video/2018/05/13/blockchain-refugees-identity-wfp-un.html

Decentalized Autonomous Organisation DAO

Is bound by rules created by its founding members that can evolve via consensus protocols , written into a set of contracts that run via computer code.

https://youtu.be/ETfaSaywXqM

https://youtu.be/Pyi8-qm02hs

So in conclusion

We can expect to see the use of blockchain , smart contracts and DAO's increase overtime because it solve the basic problem of TRUST, that's what all the fuss is about.

Thank you for your attention – any questions.

Learn more by reading "The Truth machine" by Micheal J Casey and Paul Vigna

Or visit the Blockchain Centre 85 City Road Southbank 3006

https://blockchaincentre.com.au/