CRYPTOMASTER

WORKBOOK1

2023 VOLITION LABS

SESSION 1

01 UNDERSTANDING CRYPTO LANDSCAPE

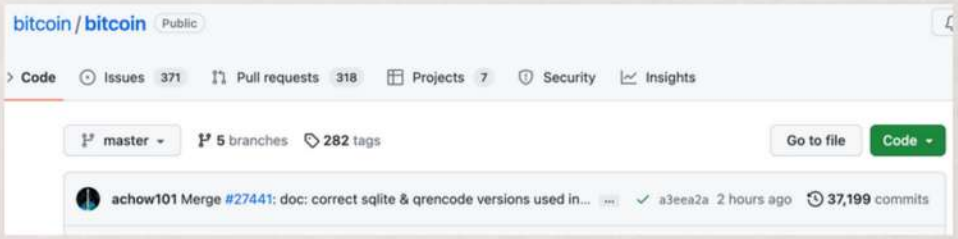
Currently there are over 9,000 crypto currencies listed on CoinMarketCap. To navigate these and to be able to independently assess them, focus on Bitcoin, the original cryptocurrency and blockchain. To understand Bitcoin, read the original whitepaper and the communications of its founder.

02 WHY SO MANY CRYPTO CURRENCIES?

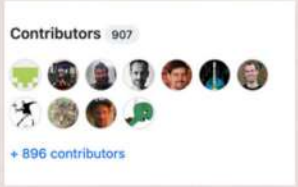
Bitcoin was developed as an Open Source project. Visit the Bitcoin github repository (repo) and see the history of commits and see the development history of since project launch in 2009.

The open source publishing of Bitcoin core has enabled developers to rapidly create their own alternative (alt) coins. Whilst some coins have been developed to bring new features, many are straight clones and can be launched with minimal coding knowledge.

The viability of a crypto project can in part be evaluated via analysis of its whitepaper and the activity in its github repository.



Taken from https://github.com/bitcoin/bitcoin



In contrast to the Bitcoin github repo, little development activity or the absence of a whitepaper could indicate a low level of unique project development of the project.

SESSION 1

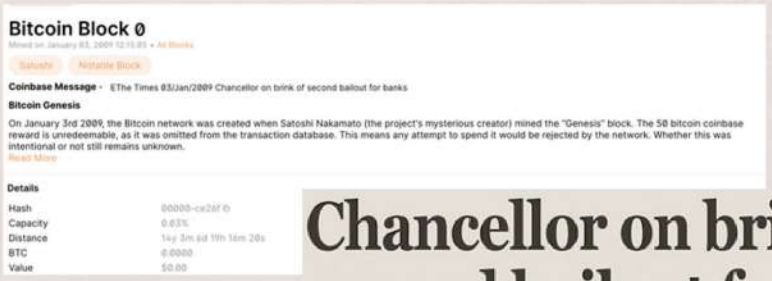
03 THE VISION BEHIND BITCOIN

While Bitcoin is sometimes viewed either as as an appreciating asset such as gold, or in some cases as an anonymous currency used to facilitate crime, in fact the whitepaper reveals that it was developed to provide an antidote to the centralized financial system by creating the world's first global, decentralized, peer to peer electronic cash system.

Bitcoin: A Peer-to-Peer Electronic Cash System

Server-based Peer-to-peer

While the whitepaper does not expressly speak of the issues associated with the involvement of politics in the economy, this is referenced by the inclusion of Times newspaper lead headline from 3 January 2009, the day that Bitcoin launched.



Taken from www.blockchain.com/explorer/blocks/btc/0

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 £37billion 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

99p

Pub chain cuts the price of a pint from £3.49 to 1989 levels

Business, page 47

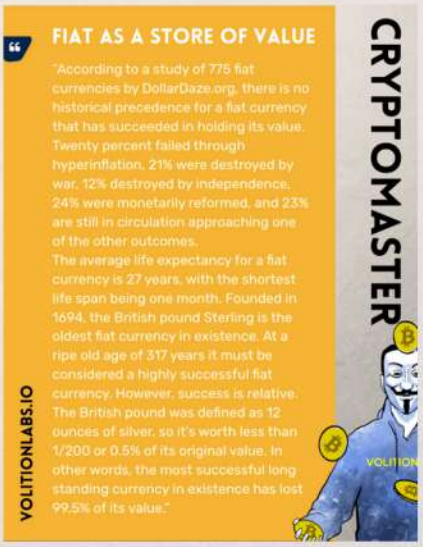
Continued on page 6, col 1
Leading article, page 2

SESSION 1

04 THE PROBLEM WITH FIAT CURRENCIES

According to a study of 775 fiat currencies by DollarDaze.org, there is no historical precedence for a fiat currency that has succeeded in holding its value.012 Twenty percent failed through hyperinflation, 21% were destroyed by war, 12% destroyed by independence, 24% were monetarily reformed, and 23% are still in circulation. The average life expectancy for a fiat currency is 27 years with the shortest life span being one month.

FIAT



Three great sources to understand the need for peer-to-peer currencies and the departure from the gorvenment controlled, fiat banking system include

1. The Creature from Jekyll Island - G Edward Griffin
2. The Money Masters documentary - Bill Still
3. America: From Freedom to Fascism - Aaron Russo

05 THE SECURITY OF BITCOIN

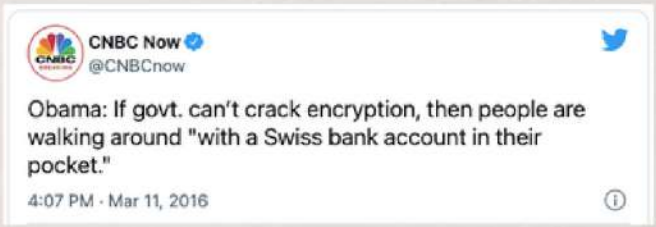
Another reason for public resistance to bitcoin is the belief that Bitcoin is vulnerable to attack by hackers or makes its users susceptible to fraud. In fact Bitcoin leverages military-grade security developed by NIST and utilized by the NSA. This strength of cryptographic component overrides the need for a trusted third party or intermediary such as the a bank or government.

Consumer confidence in Bitcoin as a store of value is demonstrated by Bitcoin's degree of market capitalization (market cap) as well as the amount of Bitcoin stored in the top 100 Bitcoin addresses.

Top 100 Richest Bitcoin Addresses

	Address	Balance △1w/△1m	% of coins
1	34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo wallet: Binance-coldwallet	248,597 BTC ($6,668,283,950)	1.28%
2	bc1qgdjqv0av3q56jvd82tkdjpy7gdp9ut8tlqmgrpmv24sq90ecnvqqjwvw97 wallet: Bitfinex-coldwallet	178,010 BTC ($4,774,876,485)	0.9189%
3	1LQoWist8KkaUXSPKZHNvEyfrEkPHzSsCd	119,347 BTC ($3,201,330,466)	0.6161%

In addition, the largest transaction on Bitcoin was made securely for over $1bn. Hence Obama referred to Bitcoin as providing the ability for users to have a 'Swiss bank account in their pocket'.



Name	Price	1h %	24h %	7d %	Market Cap
Bitcoin BTC	$30,134.64	▲0.36%	▲6.44%	▲8.20%	$582,892,700,945

The market capitalization of BTC demonstrates user confidence in BTC as a secure store or value. If the BTC was hacked at a base protocol level, the market price of BTC would crash and there would be a 'run on the currency' to exchange funds our of BTC. To date this has never happened.

SESSION 1

06 A TRANSPARENT BUT IMPENATRABLE SYSTEM

Despite the fact that all information on the blockchain is transparent and can be viewed easily on a blockchain explorer, the only way to access someone's bitcoin address and move funds to another is either to brute force the private key (computationally improbable) or obtain it directly from the owner.

Quantum computing is a consideration, but as yet there is no evidence of any computer successfully brute forcing SHA256. Despite this, some cryptocurrencies seek to be quantum resistant to address this apparent vulnerability.

07 PERSONAL RESPONSIBILITY & OPERATIONAL SECURITY

The migration from server-led (centralized) to peer-to-peer systems neccessitates a shift to personal responsibility in terms of operational security. The absence of a central authority means that there is no person or organization that can assist in the event that the private key to a Bitcoin address is lost.

It is estimated that as much as 20% of Bitcoin has been lost for ever. Therefore while hacking and theft of private is possible, in fact by far the majority of lost Bitcoin is due to personal error and mismanagement.

This includes keeping crypto on centralized exchanges that act as custodians of your cryptocurrencies and where access is not granted to your private keys.

MT Gox and FTX are examples of centralized that lost user funds.

08 BLOCKCHAIN AS A REVOLUTIONARY TECHNOLOGY

Cryptocurrencies leverage blockchain technology. This means that instead of transactions being recorded on one central server in the case of a highstreet bank, they are recorded on a decentralized ledger constantly being updated simultaneously on many different computers ('nodes') running the Bitcoin software. These nodes collectively provide one singleton state database that can be accessed and read by connecting to any node on the network.

Therefore regardless of which node your wallet connects to, it will receive the same information regarding the blockchain at any time.

Bitcoin's ability to do this makes it resistant to attack since even if all nodes in one continent were successfully shut down, your wallet would be able to connect to any other node on the network. If all nodes were taken off the internet, they would still contain a record of the blockchain. On reconnecting to the internet the network would re-sync and continue the process of recording transactions.

The Byzantine Generals' Problem as first solved by Bitcoin.

Blockchain provides a decentralized antidote to central data control, providing users with the ability to control and manage their own data, enabling a revolution in user-led data management.

SESSION 1

09 BLOCKCHAIN DEGREE OF DECENTRALIZATION

The degree to which a blockchain is decentralized reflects its resistance to what is known as a 51% attack. This refers to a situation when an attacker is able to control more than half of the network and therefore alter the state of the blockchain.

The security of a blockchain can therefore be viewed according to its resistance to a 51% attack. While the number of nodes is important, so is the cost of executing such an attack. Hence the value of a blockchain is often linked to its ability to resist this form of attack due to the associated costs of doing so.

10 EXPLORING THE BLOCKCHAIN

In contrast to electronic fiat currencies, blockchains provide transparent, publicly available records of transactions. The entirety of any blockchain can be searched via the relevant blockchain explorer. In this way, due to its informational transparency, Bitcoin is seen as pseudo-anonymous rather than anonymous. This has led to the development of a number of privacy coins.

Since the transactional history of an address is publicly available, it is good operational practice to use a new Bitcoin address each time when receiving Bitcoin. This function is made simple via a third party user interface called a wallet. Wallets manage users' keys and transactions while the crypto assets themselves reside on the blockchain.

Blocks are part of the data architecture of the Blockchain and can be thought of as data folders containing transaction data. Each block in Bitcoin has a maximum data storage capacity of 1MB. Since there are currently around 7800,000 blocks, the current size of the entire blockchain is less than 1TB of data, small enough to fit on a regular harddrive.

SESSION 1

Taken from www.blockchain.com/explore

Due to the decentralized nature of Bitcoin blockchain, all data recorded on the blockchain is theoretically immutable. Once a transaction is verified and recorded on the blockchain, it cannot be changed. However, users should be aware that the ability for a blockchain to remain censorship resistant is a hotly debated topic and has led to blockchain forks.

11 SCALING DEBATE (BLOCKSIZE WARS)

The decision to cap the size of Bitcoin blocks to 1mb resulted in a historic debate within the Bitcoin community regarding Bitcoin's ability to scale with proponents of Bitcoin as peer-to-peer cash wanting to increase the blocksize in order to enable Bitcoin to drive down transaction fees and become a global payment system to rival Visa. While BTC Bitcoin is able to process around 7 transactions a second, Visa processes some 1,700 transactions a second.

This scaling debate resulted in a hard-fork from BTC to Bitcoin Cash (BCH). On the new BCH chain the blocksize was originally set to 8mb (currently 32mb). A further fork was created from BCH to BSV which has a current blocksize of 128mb. As a result BSV has achieved 2.5m transactions in one block, putting it at a level of transactional capacity to rival Visa.

However, small block proponents argue that greater transactional throughput comes at the expense of security and increases the likelihood of a 51% attack on the network.

Therefore by way of contrast, BTC Bitcoin seeks to solve scalability issues via layer 2 (soft fork) solutions only, notably Segregated Witness (SegWit) and Lightning Network.

12 EXPLORING THE BLOCKCHAIN

In contrast to the fiat banking system, blockchains are transparent records of transactions. The entire blockchain can be searched via a blockchain explorer.

Since the transactional history of an address is publicly available, it is good operational practice to use a new Bitcoin address each time when receiving Bitcoin. This function is made simple via a third party user interfaces called wallets. Wallets manage users' keys and transactions while the crypto assets themselves reside on the blockchain.

Blocks are part of the data architecture of the Blockchain and can be seen as data folders that contain transaction data. Each block in Bitcoin has a maximum data capacity of 1MB. Since there are currently around 7800,000 blocks, the current size of the entire blockchain is less than 1TB of data, small enough to fit on a regular harddrive.

Taken from www.blockchain.com/explore

SESSION 1

13 THE BITCOIN GENESIS BLOCK

The first block mined on a blockchain is known as block 0 or the Genesis Block. In the case of Bitcoin this was mined by the creator, Satoshi Nakamoto.

Several thousand transactions have been made to the Genesis Block receiver address, even though Satoshi used each address just once. This is due to the fact that the genesis block address is utilized as a kind of wishing well transaction by Bitcoin users, as a method of asking for good luck when commencing their Bitcoin journey.


EZRA REGUERRA JAN 03, 2023

Community celebrates Bitcoin Genesis Day by sending BTC to the genesis block

The wallet address now contains around 68.56 BTC, which is worth around $1.1 million at the time of writing.

6363 Total views 34 Total shares Listen to article 2:24

Also we can see the second block (block 1) was mined 6 days after block 0, instead of the usual average 10 minutes, making a possible reference to the 6 days of creation in the bible.

In addition a reference to the Times Newspaper from 3.9.2006 is coded into the coinbase transaction, reinforcing the Bitcoin proposition as outlined in the original whitepaper.


THE TIMES

Eat Out from £5

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks