Money

Many areas had to be developed, invented, and refined before the blockchain could come to fruition and encompass the widespread mania it has today. Many of the sections that follow may seem disjunct, or even irrelevant upon first reading, but all have had some influence that led to the development of cryptocurrencies and blockchains.

The two main sources of motivation on the road to Bitcoin are Finance and Computing. The finance portion traces right back to early human civilisation and the development of money.

Early Trading Systems

Early humans could barter with their neighbours using goods or services on offer, but this quickly becomes cumbersome as values often do not align. In small tribes and families this is not a problem because the members trust each other. As societies or tribes get larger, inevitably there is interaction with another tribe whose members you do not trust. To resolve this peacefully elders of one tribe would negotiate with elders of another tribe, essentially keeping accounts of each other's debt (Graeber, 2011). This gives rise to two concepts that allow us to trust a neighbour: units of account and debt (Ferguson, 2008). However, a question remains: how do you conduct business with a tribe you've never met before? In the case that the elders have no previous history, how can they be trusted?

Cash

Cash offers a solution by enabling transactions between individuals who are unfamiliar and, thus, untrustworthy to each other. Myriad items throughout history have been used as cash such as gold, cowrie shells, woodpecker scalps, stone discs, and NZD$20 notes (Agha, 2017).

For a token to be considered cash, two conditions must be satisfied:

1. Someone must be willing to accept your token, and
2. The token must endure long enough to be transacted again.

For a token to qualify as an NZ$20 note, it must possess additional characteristics (Graeber, 2011):

- Affordability
- Availability
- Durability
- Fungibility
- Portability
- Reliability

Any token that has these properties in addition to being issued by the state is called fiat money. The advantages of a standardized cash transaction system extend beyond mere convenience—it also offers anonymity. You don’t know the history of your cowrie shell, or who previously used your $20 note. This applies into the future as well since your $20 note can't be traced back to you.

Q: Why would you care about that note being traced back to your transaction?

Finance

Finance evolved once systems for credit, debt, and value transfer (cash) gained widespread acceptance. The Medici family in 15th-century Italy revolutionized banking as meticulous money changers who adopted double-entry bookkeeping—where debits were maintained in one column and credits in another. This practice quickly became standard throughout Europe and remains so today (Ferguson, 2008). The concept of recording all account activity in a ledger is a fundamental characteristic of blockchain systems, including Bitcoin.

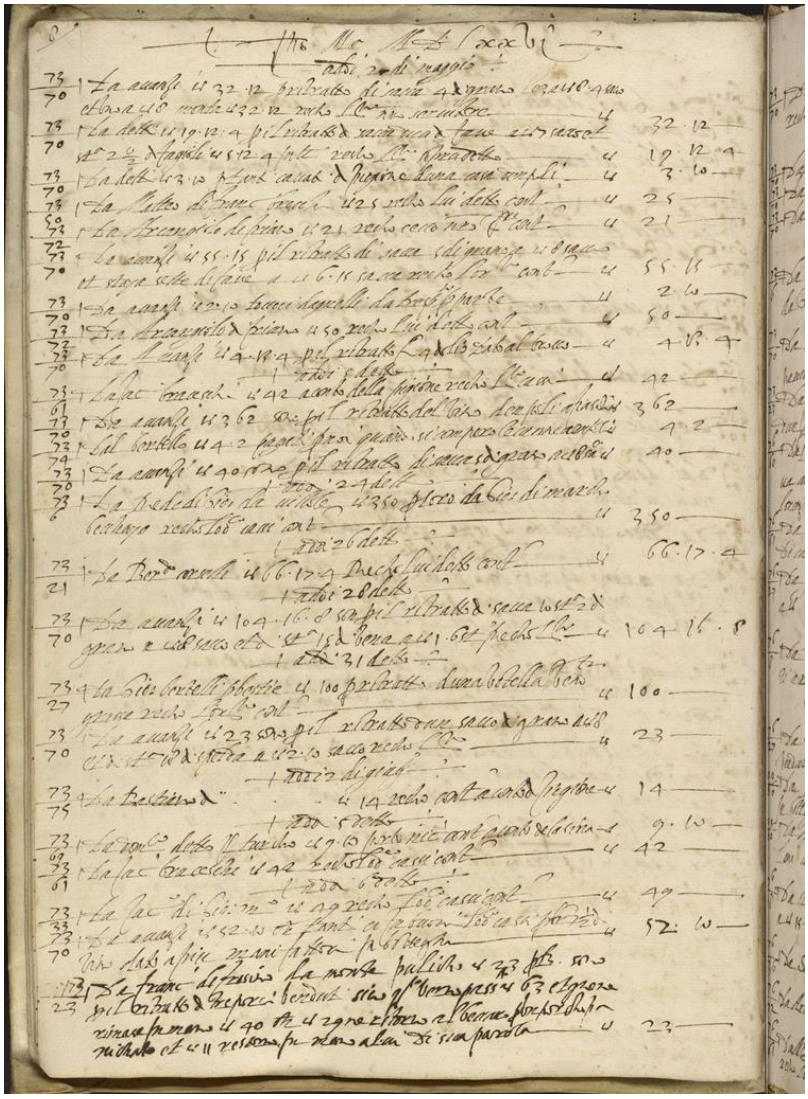

Figure: Medici Ledger of accounts from 1573. Source: University of Pennsylvania, OPENN Library.

It's not just the idea of a permanent ledger that bitcoin borrowed, but rather the motivation to create a system independent of the one pioneered by the Medicis in 15th-century Italy.

Traditional Banking System

The contemporary banking system leverages internet infrastructure and computing concepts such as relational databases and atomic transactions to operate on a global scale. With relevance to blockchain development, this system:

- Uses digital double-entry accounting,
- Has a centralised hierarchy and often distributed infrastructure,
- Maintains a permanent, but publicly opaque, record of transactions.

The bank serves as an intermediary, the final arbiter, of all transactions. The centralised architecture allows the bank to choose its customers, set fees, and even decide what to do with user deposits. Among other monopolistic behaviours, this leads to censorship and in the digital age, in addition to risks posed by hacks and breeches. Also, one may not want the bank to know exactly how and with whom you are transacting. As we learn more about the blockchain it will become apparent that Bitcoin transactions are not anonymous, rather they are considered pseudonymous. Although your name is not attached to a transaction, the address and activity associated with it is permanently recorded in the blockchain. Digital privacy is one of the most significant outcomes of the blockchain era.

P2P Digital Cash

The 80's & 90's saw many attempts to create a digital version of money that could have a token, both private and untraceable, treated as a bearer instrument, and resist the fragility associated with third-party issuers and verifiers. Some notable examples include David Chaum's work on *Untraceable Electronic Cash* (1988), Wei Dai's *b-money*, and Nick Szabo's *Bit Gold*.

Advancements in cryptography helped overcome many technical challenges, including those associated with digital signatures and hash functions. However, one issue remained unsolved: how can double-spending—a situation where someone spends the same digital coin twice—be prevented? A centralized authority could easily address this by checking someone's balance and updating it accordingly. However, in the absence of a centralized authority, this becomes a challenge; by the time you arrive at the second retailer your stolen card will be declined for insufficient funds or suspicious activity. Here the bank is saying, "You can only spend your dollar once."

Chaum, Fiat and Naor (1988) came up with a scheme for issuing unique digital coins that could be redeemed by a centralised authority in a way that conceals the user's identity. Anonymous digital cash. His scheme used what are called blind signatures and are clever because it means you can not reuse (double-spend) a digital coin. The double-spending problem is particularly difficult in the digital age because its so easy to copy a digital object (`ctrl+c`) and then turn around and offer it to many people while claiming it's unique. Chaum et al. commercialized his company, calling it DigiCash but it never caught on (Narayanan, 2016). One of the reasons was that it wasn't a truly peer-to-peer system still relying on the trusted thrid party.
The decentralized approach removes the bank entirely from the transaction and is one of the revolutionary ideas put forward by Satoshi in his whitepaper. This is the nature of *peer-to-peer*: I send you money without any entity, person, or corportion being involved.

Bitcoin

The Global Financial Crisis in the mid-2000's created significant hardship and the blame was put clearly on the banking sector. While changes were called for in how banks managed risk, there was also social disquiet amongst those that felt that banks controlled too much financial, and therefore, societal resources. In particular, libertarians called for an economic system free of the banking sector.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Figure: Header to Satoshi Nakamoto's description of p2p electronic cash (required reading) distributed via mailing list on October 31, 2008. Regarding historical timelines, Lehman Brothers bankruptcy was on September 15, 2008, said to be the "climax of the subprime mortgage crisis."
Source: https://en.wikipedia.org/wiki/Bankruptcy_of_Lehman_Brothers.

An anonymous individual, Satoshi Nakamoto, responded to this call by designing Bitcoin, a cryptocurrency. Despite the long history of digital cash systems, and notwithstanding the partial success of platforms like PayPal, many have failed to secure widespread support. Bitcoin's success seems in part to derive from its decentralised peer-to-peer system (the Bitcoin network) that provides complete transactions (bitcoin the cryptocurrency) without a singular or centralised banking authority.

Satoshi Nakamoto
48, Male
Japan

Share on Facebook
MySpace Tweet

Blog Posts
Discussions (5)
Groups
Videos

Satoshi Nakamoto's Apps

Figure: Satoshi Nakamoto's avatar on the P2P foundation site where he news of the first bitcoin reference implementation. Source: https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

The Bitcoin cryptocurrency architecture combines functions that provide coin creation, transactional cryptographic validation, and a highly redundant storage system that is publicly available, relatively anonymous, and incentivises users. An important measure that ensures cryptographically sound identification and verification of ownership is the use of SHA public/private key cryptography. This also provides a degree of anonymity, transactional integrity, and non-repudiation.

Distributed Systems

The key to solving the double-spend problem is to distribute the record of transactions to every participant in the network. In this manner every seller can verify independently that any buyer has the required unspent amount. Every new transaction is shared through the network with everyone else in a peer-to-peer (p2p) manner, rather than sending to a central server and having a gatekeeper update the accounts, this is handled at the individual level. This distributed ledger eliminates the need for centralized accounting and trust among users; no one needs to trust anyone else because the network consensus confirms the authority to spend coins.

Practically speaking, each peer in the network listens for new blocks of transactions, verifies them, and adds them to their own local database. Should two nodes have conflicting information because they received new blocks at slightly different times, or with different transactions in them, then the state is said to *fork*, and for a short time *both* forks are equally valid states. Resolving forks is expected and is the job of the consensus mechanism. Bitcoin resolves this issue using the longest chain rule. This means the node with the longest block chain is most likely to receive a new block and continue as the canonical chain. If a node falls behind, it abandons its chain and starts contributing to the longest one. This method of distributed system consensus is now known as *Nakamoto consensus*.

Because the chain is public you can do an inventory of nodes online at any given time. This also removes gatekeepers as anyone is free to join or leave whenever they want. Midway through 2023 the number of bitcoin nodes globally is about 45,000. (Compare this with centralized systems like Facebook and Twitter that keep your data on anywhere from 3-5 nodes.)

The Blockchain Data Structure

Where are objects stored in memory?

When a program writes to disc or memory, it typically uses a predetermined area allocated by the operating system at runtime. Since programs frequently write and rewrite to disc, the data can end up disorganized and scattered. Data structures help track the location of items in memory, including potentially other crucial information like the last element's location or the maximum quantity allowed. Here, we'll discuss two data structures: linked lists and trees (in a future lecture). These structures have simple visual representations but can be challenging to implement, hence all useful programming languages come equipped with built-in data structure operations.

Linked Lists

A linked list is a sequence of data that has a reference to previous or subsequent item. The figure shows a schematic for integer elements that are linked to a subsequent item in their list. A key property of lists is that there is no absolute reference to individual elements. To find an element in the middle, say 99, you have to start at the beginning (12) and then traverse the list. Additionally in this manner it is easiest to append elements to the end of the list and much more difficult to insert elements part way through.

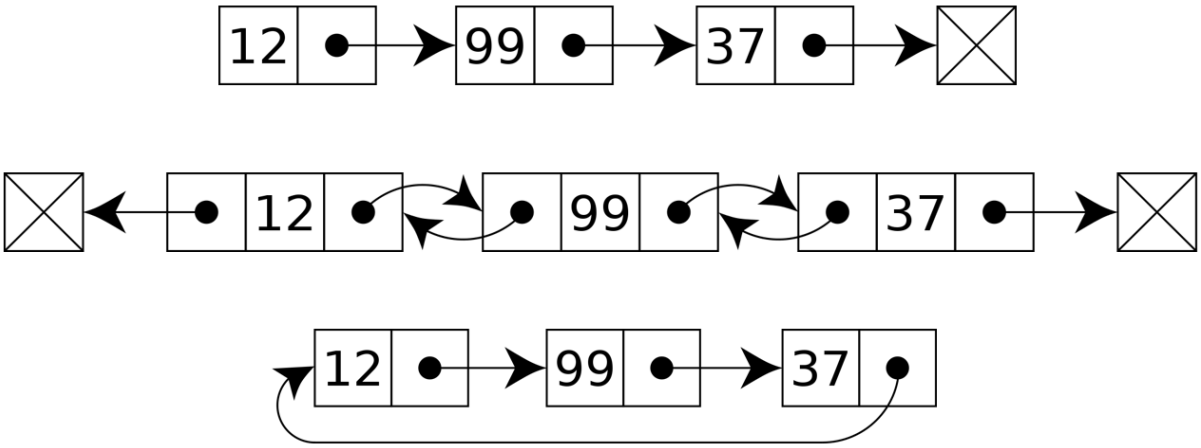

Figure: Various linked lists. Top: a standard implementation with a reference pointer to the next element. Middle: a doulble-linked list with previous and subsequent pointers. Bottom: a circular linked list with reference back to the first element. Source: https://en.wikipedia.org/wiki/Linked_list.

Linked Time-stamping

The blockchain itself, as the name suggests, is a chain of blocks that are linked together using cryptographic hash functions. The idea was not unique to cryptocurrencies. Haber and Stornetta (1991) describe a method to use one-way hash functions to digitally time-stamp documents and maintain privacy. This hashing system is used to order the blocks in a blockchain while maintaining block integrity and security over time.

If document A appears in the list before document B, then it can be concluded that A was published to the list earlier (in time) than document B. This is important because digital items such as timestamps can be forged. It is only in relation to the other documents in the list that we pinpoint a window in time when document A came into existence. An isolated document or moment in history is not nearly as valuable without the context in which that event happened. The blockchain doesn't just provide context, it provides the entire history.

Q: How can a blockchain maintain integrity without being vulnerable to forged timestamps?

Chains of Blocks

A blockchain is a data structure whereby a single block of data contains a hashed reference to a previous block. The chain of blocks can represent a chronological ordering of data as mentioned above. If blocks are appended regularly then the time-stamping effect can be as good as an actual time-stamp. When a new block is created it must include a reference pointer to the previous block in the chain, which, in turn contains reference to its previous block. An ordinary linked list would contain a pointer

referencing the object's address in memory. A blockchain reference is known as a *hash pointer* because it also includes a hash of the previous block.

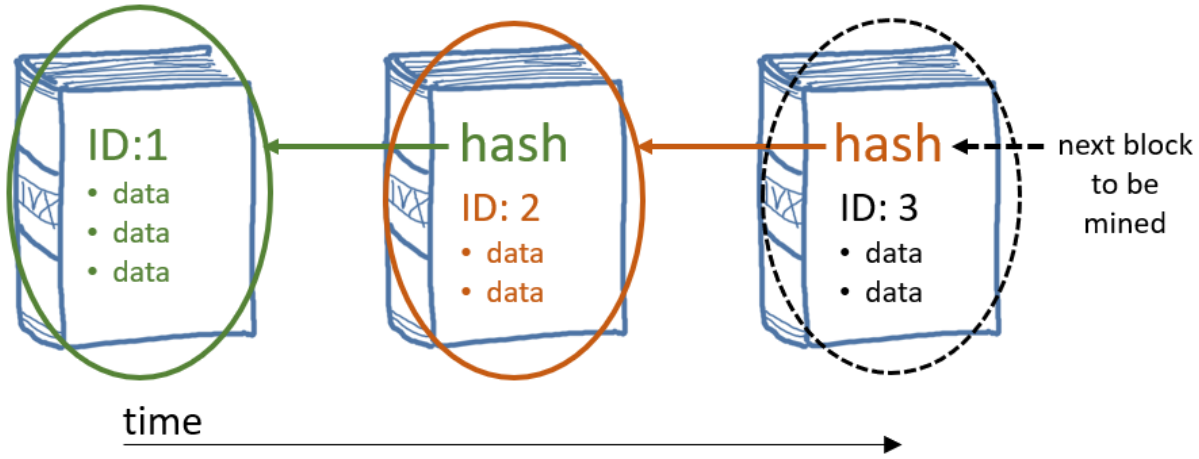

Figure: Each individual ledger is analogous to a block. When one book fills up, a new one begins, carrying over the account balances and thus linking the 'blocks'.

Bitcoin's primary purpose is to track transactions in a ledger (recall the double-entry accounting system popularized by the Medici family in Florence in the 1400s). The blockchain can be viewed as triple-entry accounting, where the third entry is the distributed copies maintaining consensus. In the figure, the second block contains a cryptographic hash of the first block, and the third block holds a hash of the second block, which, by definition, includes the first block's hash. This process is how the chain maintains its integrity.

The blockchain is a read-only public ledger of all transactions that have occurred within the cryptocurrency ecosystem and consists of a series of blocks that are created through proofing methods, such as proof-of-work (Back, 1997; and Nakamoto, 2008), proof-of-stake (Buterin, 2013 and Wood, 2014), or other unique methods or combinations of methods. The blockchain must be created one block at a time and mass deletion or appending of new blocks is not possible while maintaining the correct hash linking. If there are multiple new blocks to be added to the data structure, they must be added in series to create, and then preserve the total ordering.

What do these blocks look like?


```
        "hash":
"000000000000000000000534d3d2c7758fab39dabb98d23b954813379f053c580",
        "confirmations": 1,
        "strippedsize": 130543,
        "size": 174555,
        "weight": 566184,
        "height": 620229,
        "version": 536928256,
        "versionHex": "2000e000",
        "merkleroot":
"cdfc01a6d3a9f037670be9c17dba180e6b281764cb402ead941b2a439c1d801d",
        "tx": [
```

```
"9d6e152ab00bd22c4803a5cb2d393ac72cbf81d2d708802a52da2236f4a8f658",

"16e53bf67ccec6cd30460dd721a9a940791aa327a50ac99bcdb7a6bd7949fe54",

"e406e599aeb4974473bf9a4bcdcc5de35d15fac296acceb217779680ae927d91",

"d55c96ce6ccf995035338f4ded57850f307299b0756b44c61b2fe5e5c2c89a51",
                    ,
                    "...truncated...",
                    ,

"22ba973e71869d1e64cdd8572fa94754429d52d84bce61b2374f082606e02ec5",

"35525a4db6c1fdea573780c9726ceebcd71788db66d05b83e661d864820b59c6",

"8a2d96492dc0be984e5ee5d8641ff599f63cfbedc0041e3343fc7b76f4d75de0",

"c996d69ba1d780de851422cf27b7bf65bcfe1e77631d86fb508d79fd57a58ff5"
        ],
        "time": 1583366597,
        "mediantime": 1583365586,
        "nonce": 4225421315,
        "bits": "17122cbc",
        "difficulty": 15486913440292.87,
        "chainwork":
"0000000000000000000000000000000000000000d4bf930c8adffc9b1a4b136",
        "nTx": 350,
        "previousblockhash":
"00000000000000000070be3e6873e60481b5e3c71322c8ced8315f6e44edd6e"
```


The fields of block `620229` mined on March 05, 2020 in the Bitcoin blockchain. The transaction list has been truncated; this block has 350 transactions in total. The block ID is called *height* as if blocks are built on top of each other. Details of a block can be found in many third-party providers such as Blockchair.com, Blockchain.com, or btc.network.

Mining

The process of adding blocks to the chain is called mining. Bitcoin mining is down with proof-of-work computing and involves rewarding lucky miners with bitcoin(s)[1]. Mining is cruicial for the nodes in the Bitcoin network to stay in agreement, but also to generate new tokens for the system to use. This will be discussed at length in the lecture on consensus methods.

Cryptography

The 1980s saw a lot of research into the idea of being able to send a private digital message. Historically, this meant creating a cipher that converts a plaintext message into a ciphertext (encrypted message), sending the encrypted version, and the recipient has a matching cipher to enable them to decrypt the message. The key hurdle

to this setup is that the cipher has to be transported to the recipient among eavesdroppers. A digital cryptosystem also involves distributing your cipher through any number of third-party servers that could have spies monitoring the connection.