Predecessors of Blockchain

DigiCash

- DigiCash Inc. was a company that dealt with finance through electronic money. It was founded in 1989 by David Chaum, an American computer scientist and cryptographer.
- David Chaum made it possible by introducing a new mechanism called Blind Signature, which plays a vital role in assuring the transactions are made anonymously.
- The Blind Signature disguises (blinds) a transaction before it submits to the network and the blinded signature is verified publicly with its original form i.e., unblinded form as a regular signature.
- The company declared bankruptcy in 1998 and eventually sold their assets to another digital currency company called Ecash Technologies. Ecash Technologies was eventually acquired by InfoSpace on Feb. 19, 2002.

HashCash

- HashCash is an email filter based on a proof-of-work system to figure out spam mails and DoS (Denial-of-Service) attacks. Adam Back developed HashCash in the year 1997 and a formal documentation was released in the year 2002 in the paper “HashCash - A Denial of Service Counter Measure”.
- In HashCash, the sender calculates a hashcash stamp which is appended to the email header. This is done to make sure the sender has utilized some CPU power to calculate the stamp.
- Spammer is unlikely to spend resources to calculate the stamp, as the number of email increases, the computation power increases exponentially.
- HashCash uses a 160 bit SHA-1 encryption scheme. The PoW used by the HashCash is designed to have the first 20 bits to be zeroes thus leaving 2^140 combinations.

HashCash

- The header of the HashCash looks similar like:

  X-Hashcash: 1:20:1303030600:anni@cypherspace.org::McMybZIhxKXu57jd:ckvi

- The header contains:
  - **ver:** It is used to represent the version of HashCash.
  - **bits:** The number of bits that are used as "partial preimage" that means the zero bits are present in the hashed code.
  - **date:** The date and time when the sender sent the messenger and is represented in the format of YYMMDD[hhmm[ss]].
  - **resource:** Resource is the data in the string format that is being transmitted which could be an IP address or email address or something else.
  - **ext:** It is an optional field which is used to represent the extension used. It is ignored in the version 1.
  - **rand:** It is just a string of random characters that are encoded in base64 format.
  - **counter:** This field represents the binary counter of the hashcash that is encoded in base64 format.

B-Money

- B-Money is an early age distributed cash system proposed by Wei Dai. He developed a cryptographic library-Crypto++. He also co-proposed the VMAC message authentication algorithm.
- B-money was proposed by Wei Dai as “Anonymous, Distributed Electronic Cash System” in his white paper in November 1998.
- B-money was introduced to create a free financial system over the internet with basic principles similar to modern cryptocurrency. It was presumed that without involving any third party the digital aliases of money will move freely via the decentralized network.

E-Gold

- E-gold Ltd was a digital gold currency company that operated under Gold and Silver Inc.
- The company was founded by Douglas Jackson and Barry Downey in 1996.
- It was one of the earlier companies that tried to establish digital currency, but it used gold and other precious metals, mostly silver as the underlying currency as they are globally acceptable.
- E-gold lets users create an account on their website and deposit money in the denomination of grams of gold or silver mostly and provide instant transfers of gold to other accounts.
- E-gold faced many hurdles such as security issues, digital scams, cyber attacks, systemic problems as the technology available during the era was primitive.
- During the early 2000s, the feature of immediate settlement implemented by e-gold was recognized and it rose as the key for the emergence of peer-to-peer transactions of digital rights of an asset such as in smart contracts.

Bitgold

- Bitgold is one of the most known decentralized virtual currency projects taken before Blockchain. It was proposed by Nicholas (Nick) Szabo in 1998.
- It is aimed to address the common problems in financial system, where transaction flow was largely dependent on trust on both the recipient and third party involved.
- The Bitcoin and Bitgold protocols are very similar. They both run on a Byzantine Fault Tolerant (BFT) consensus based, peer-to-peer decentralized network.
- The Bitgold system, proposed by Nick Szabo is non-fungible.