Blockchain™ Council

Predecessors of Blockchain

DigiCash

- DigiCash Inc. was a company that deals with finance through electronic money founded by David Chaum, an American computer scientist and cryptographer in 1989.
- David Chaum made it possible by introducing a new mechanism called Blind Signature which plays a vital role in assuring the transactions 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 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”.
- HashCash appends a textual encoding of a hashcash stamp to the email header to prove that the sender utilized some CPU power in calculating the hashcash stamp which a spam is most unlikely to do.
- 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 0’s) 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 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, a computer engineer known for his contributions to cryptography and cryptocurrencies.
- He developed the Crypto++ cryptographic library, created the B-money cryptocurrency system, and co-proposed the VMAC message authentication algorithm.
- The smallest subunit of Ether, the wei, is named after him.
- B-money was proposed by Wei Dai as “Anonymous, Distributed Electronic cash system” in his white paper on the Cypherhunks mailing-list in November 1998.
- It was assumed that the "digital aliases" will be able to send and receive money through a decentralized network and even ensure the implementation of contracts among themselves without the involvement of a third party.
- Unfortunately, the B-Money project has not moved from the dead end after the implementation of the white paper.

E-Gold

- E-gold Ltd was a digital gold currency company 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.
- The company was at its peak during the year 2006 with more than $2 billion worth of spends per year which was momentarily equivalent to $71 billion USD.
- 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

- Bit gold is one of the most known decentralized virtual currency projects taken before blockchain. It was proposed by Nicholas (Nick) Szabo in 1998.
- The bitcoin and bitgold protocols are as similar as, at one instant, it is said that people thought that Nick is the anonymous bitcoin creator, Satoshi Nakamoto.
- The bitgold system that was proposed by Nick Szabo is non-fungible.
- The bit gold operates on a decentralized and distributed system instead of a centralized authority controlling its nerves.
- Dominic Frisby provided circumstantial evidence to believe that Szabo is the original Satoshi Nakamoto, but, as he admits that no proof is found. One day in July 2014, Szabo wrote an email to Frisby saying "I'm afraid you got it wrong doxing me as Satoshi, but I'm used to it."
- Nathaniel Popper, a famous journalist in The New York Times who was researching bitcoin wrote an article stating that "the most convincing evidence pointed to a reclusive American man of Hungarian descent named Nick Szabo."