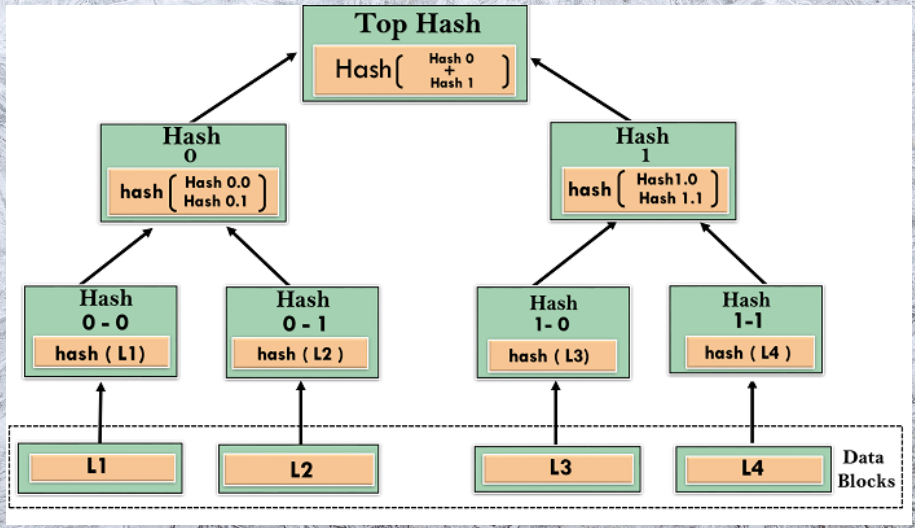
Blockchain Snippets

HISTORY OF BLOCKCHAIN

- THE BLOCKCHAIN TECHNOLOGY WAS DESCRIBED IN 1991 BY THE RESEARCH SCIENTIST STUART HABER AND W. SCOTT STORNETTA.
- THEY WANTED TO INTRODUCE A COMPUTATIONALLY PRACTICAL SOLUTION FOR TIME-STAMPING DIGITAL DOCUMENTS SO THAT THEY COULD NOT BE BACKDATED OR TAMPERED.
- THEY DEVELOP A SYSTEM USING THE CONCEPT OF CRYPTOGRAPHICALLY SECURED CHAIN OF BLOCKS TO STORE THE TIME-STAMPED DOCUMENTS.

- IN 1992, MERKLE TREES WERE INCORPORATED INTO THE DESIGN, WHICH MAKES BLOCKCHAIN MORE EFFICIENT BY ALLOWING SEVERAL DOCUMENTS TO BE COLLECTED INTO ONE BLOCK.
- MERKLE TREES ARE USED TO CREATE A 'SECURED CHAIN OF BLOCKS.' IT STORED A SERIES OF DATA RECORDS, AND EACH DATA RECORDS CONNECTED TO THE ONE BEFORE IT.
- THE NEWEST RECORD IN THIS CHAIN CONTAINS THE HISTORY OF THE ENTIRE CHAIN. HOWEVER, THIS TECHNOLOGY WENT UNUSED, AND THE PATENT LAPSED IN 2004.


Top Hash
Hash(Hash 0 + Hash 1)
Hash 0
hash (Hash 0.0 Hash 0.1)
Hash 1
hash (Hash1.0 Hash 1.1)
Hash 0 - 0
hash (L1)
Hash 0 - 1
hash (L2)
Hash 1- 0
hash (L3)
Hash 1-1
hash (L4)
L1
L2
L3
L4
Data Blocks

- IN 2004, COMPUTER SCIENTIST AND CRYPTOGRAPHIC ACTIVIST HAL FINNEY INTRODUCED A SYSTEM CALLED REUSABLE PROOF OF WORK(RPOW) AS A PROTOTYPE FOR DIGITAL CASH.
- IT WAS A SIGNIFICANT EARLY STEP IN THE HISTORY OF CRYPTOCURRENCIES. THE RPOW SYSTEM WORKED BY RECEIVING A NON-EXCHANGEABLE OR A NON-FUNGIBLE HASHCASH BASED PROOF OF WORK TOKEN IN RETURN, CREATED AN RSA-SIGNED TOKEN THAT FURTHER COULD BE TRANSFERRED FROM PERSON TO PERSON.RPOW SOLVED THE DOUBLE-SPENDING PROBLEM BY KEEPING THE OWNERSHIP OF TOKENS REGISTERED ON A TRUSTED SERVER.
- THIS SERVER WAS DESIGNED TO ALLOW USERS THROUGHOUT THE WORLD TO VERIFY ITS CORRECTNESS AND INTEGRITY IN REAL-TIME.

W. Scott Stornetta

Stuart Haber

- FURTHER, IN 2008, SATOSHI NAKAMOTO CONCEPTUALIZED THE THEORY OF DISTRIBUTED BLOCKCHAINS. HE IMPROVES THE DESIGN IN A UNIQUE WAY TO ADD BLOCKS TO THE INITIAL CHAIN WITHOUT REQUIRING THEM TO BE SIGNED BY TRUSTED PARTIES.
- THE MODIFIED TREES WOULD CONTAIN A SECURE HISTORY OF DATA EXCHANGES. IT UTILIZES A PEER-TO-PEER NETWORK FOR TIMESTAMPING AND VERIFYING EACH EXCHANGE.
- IT COULD BE MANAGED AUTONOMOUSLY WITHOUT REQUIRING A CENTRAL AUTHORITY. THESE IMPROVEMENTS WERE SO BENEFICIAL THAT MAKES BLOCKCHAINS AS THE BACKBONE OF CRYPTOCURRENCIES. TODAY, THE DESIGN SERVES AS THE PUBLIC LEDGER FOR ALL TRANSACTIONS IN THE CRYPTOCURRENCY SPACE.

Hal Finney

Satoshi Nakamoto