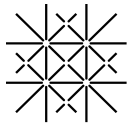


University of Basel

Center for Innovative Finance

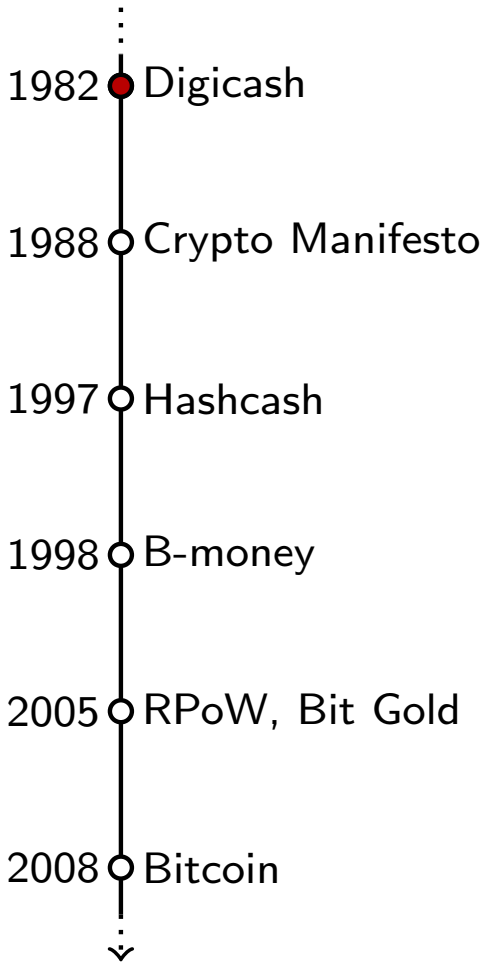
Bitcoin, Blockchain and Cryptoassets

History of Digital Money

Prof. Dr. Fabian Schär
University of Basel

Release Ver.: (Local Release)
Version Hash: (None)
Version Date: (None)

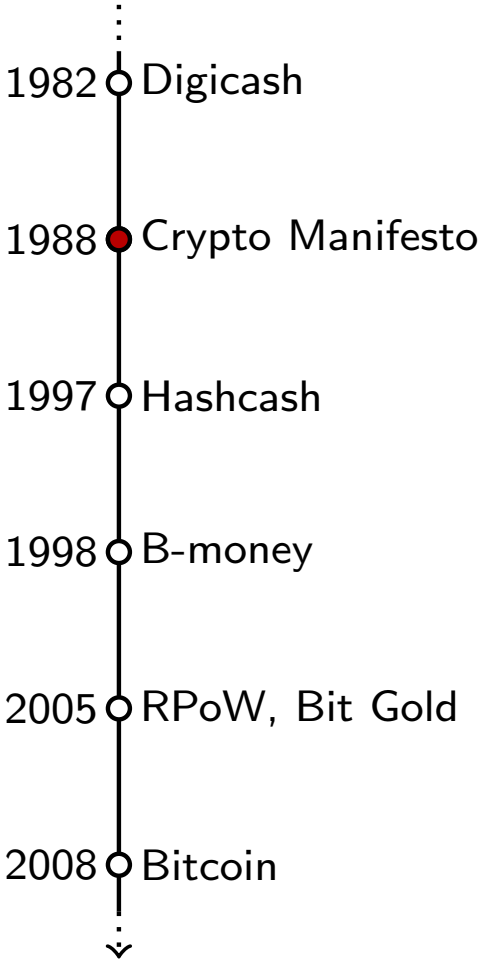
Before Bitcoin



Digicash - David Chaum

- Concern: Electronic means of payment significantly limit privacy and traceable payment flows may generate sensitive data.
- Goal: Virtual monetary unit that imitates the anonymity of cash.
- Monopolized money creation and centralized settlement.
- Central bank blindly signs monetary units.

Before Bitcoin



Crypto Anarchist Manifesto - Tim May

Link

The Crypto Anarchist Manifesto

Timothy C. May
tcmay@netcom.com

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

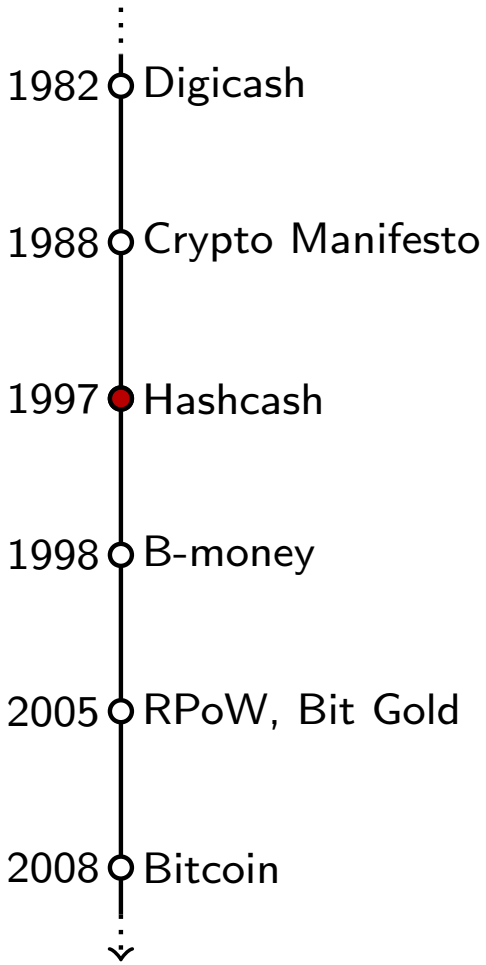
The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

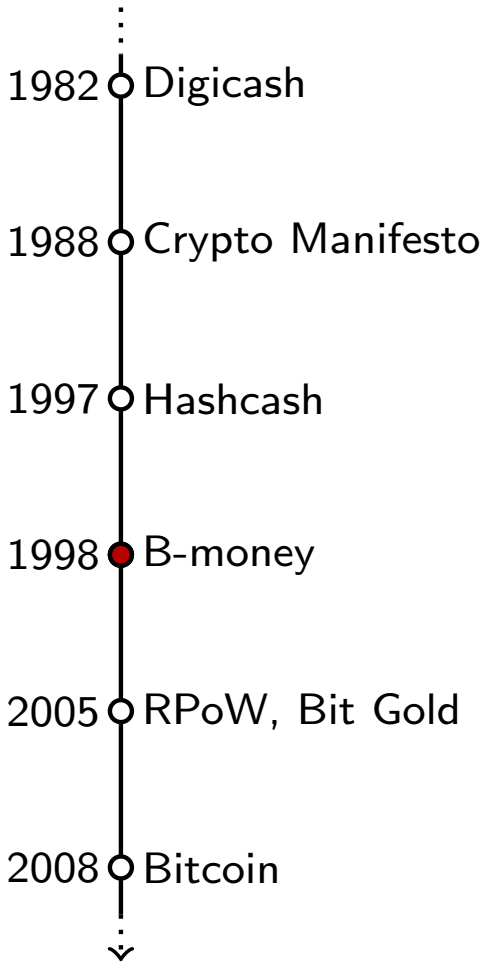
Before Bitcoin



Hashcash - Adam Back

- Originally proposed as a mechanism for anti-DoS and spam email.
- Introduced concept of artificial costs.
- "The idea of using partial hashes is that they can be made arbitrarily expensive to compute (by choosing the desired number of bits of collision), and yet can be verified instantly." [1]

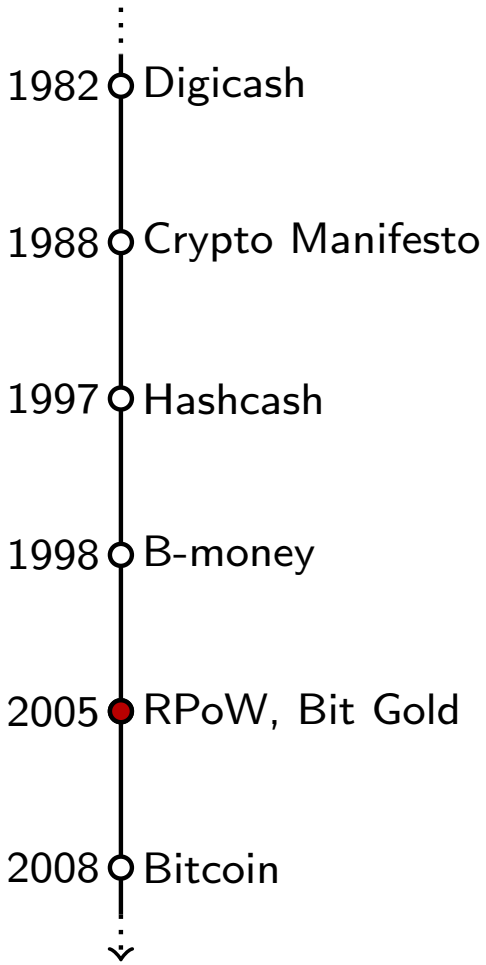
Before Bitcoin



B-money - Wei Dai

- Thought experiment
- Assumption: Existence of an untraceable network.
- Senders and receivers are identified only by digital pseudonyms. (i.e. public keys)
- Transaction legitimacy guaranteed by signature with associated private key.
- Participants keep separate registers with the current balances of all pseudonyms.
- Competitive money creation by solving numerical puzzles that are hard to compute but easy to verify.

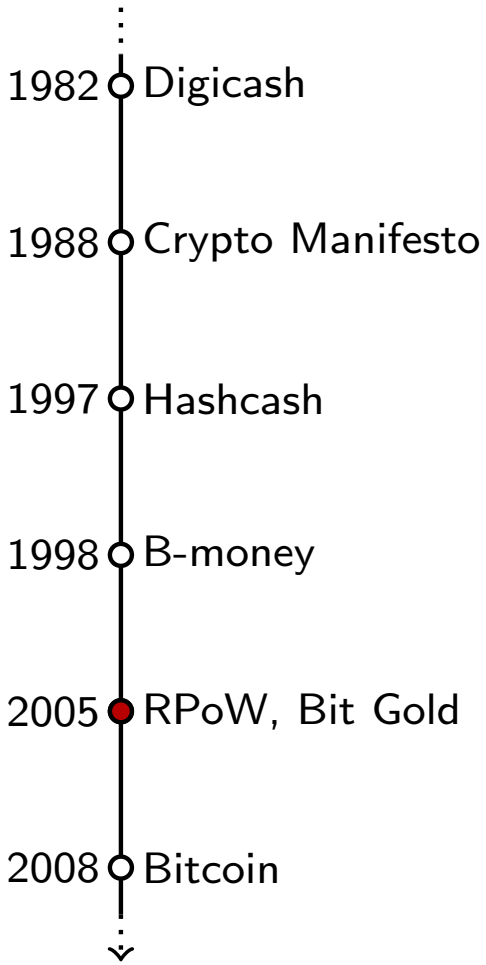
Before Bitcoin



Reusable Proofs of Work - Hal Finney [2]

- Combines ideas of Wei Dai and Adam Back.
- A RPoW client can create a RPoW token by providing a proof-of-work string and signing with his private key.
- Server can map that token to the signing key.
- Client can give the token to another key by signing a transfer order to a public key.
- Server registers the token as belonging to the corresponding private key.

Before Bitcoin



Bit Gold - Nick Szabo

- Describes the combination of the proof-of-work algorithm for competitive money creation.
- Computing power is used to collateralise a public ledger, which grows into a chain of blocks through a reflexive reference.
- "Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold." [3]

References and Recommended Reading

[1] Adam Back, *Hashcash - a denial of service counter-measure*, Tech Report (2002).

[2] Hal Finney, *Reusable proofs of work*, 2005.

[3] Nick Szabo, *Bit gold*, December 2005.