

BTC白皮书

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

October 31, 2008

www.cryptovest.co.uk

Abstract

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

1. W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998. ↵
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999. ↵ ↵
3. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991. ↵
4. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital timestamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993. ↵
5. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997. ↵ ↵
6. A. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002. ↵
7. R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980. ↵
8. W. Feller, "An introduction to probability theory and its applications," 1957. ↵

2009年的比特币白皮书《BTC：一种点对点的电子现金系统》中大量引用了密码朋克邮件列表成员所著的论文。

BTC白皮书引注概况

姓名	技术概况	引注	是否是密码朋克
戴伟	分布式记账技术	B-money白皮书	是
H·Massias	时间戳服务器技术	《在最小化信任的基础上设计一种时间戳服务器》	存疑
D. Bayer	时间戳服务器技术	《在最小化信任的基础上设计一种时间戳服务器》	存疑
S·Haber	时间戳服务器技术	《提升电子时间戳的效率和可靠性》、《比特币字串的安全命名》	存疑
W·S·Stornetta	时间戳服务器技术	《如何为电子文件添加时间戳》、	存疑
A. Back	哈希现金技术	《哈希现金——拒绝服务式攻击的 克制方法》	是
R.C. Merkle	Merkle树	《公钥密码系统的协议》	是
W. Feller	比特币安全性的概率学 论证	《概率学理论与应用导论》	否

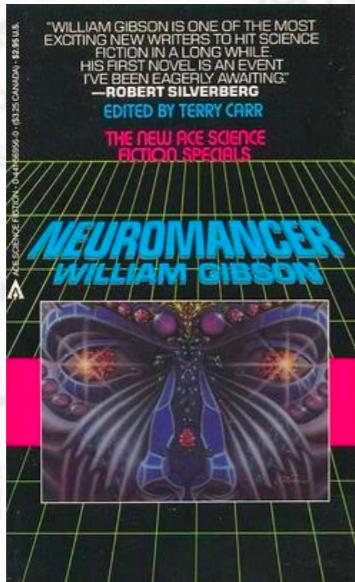
资料来源：bitcoin.org 通证研究院

比特币的初心：密码朋克

“在电子时代，对于开放的社会来说，隐私必不可少。隐私不同于秘密。隐私是某人不想公之于众的东西。而秘密，是他不想让任何人知道的东西。**隐私是一种权力**。它让某人有权决定公开什么，不公开什么。”

——节选自《加密朋克宣言》（1993）

赛博朋克 (cyberpunk) : 当时的科幻文化



神经漫游者 (William, 1984)

赛博朋克，将“cyber”（计算机的）和“punk”（朋克）组合，形成了以“计算机网络控制”为绝对核心，带有“反乌托邦精神和悲剧色彩”的全新流派。它涵盖了黑客、虚拟实境、人工智能（AI）、都市扩张、贫富差距等话题。



银翼杀手

黑客帝国

升级

阿丽塔：战斗天使 攻壳机动队

密码朋克宣言 (1)

在电子时代，对于开放的社会来说，隐私必不可少。隐私不同于秘密。隐私是某人不想公之于众的东西。而秘密，是他不想让任何人知道的东西。**隐私是一种权力。**它让某人有权决定公开什么，不公开什么。

如果双方进行某种交易，那么他们各自拥有这一互动的记忆。双方都有权陈述各自关于此次交易的记忆。谁能够禁止他们发言呢？或许有人能够通过立法来禁止，但相比于隐私，言论自由对于开放社会来说甚至更加重要。我们不会试图限制任何言论。如果许多人够在同一个论坛上发言，那么每个人相当于对所有人发言，这样就可以同时积累个人和众人的知识。电子化的交流让这一小组得以实现，即使有人想要禁止小组产生，他也不可能成功。

因为我们渴望隐私，所以我们必须确保交易双方仅获得交易所需的信息。因为任何信息都可能在交易中提及，所以我们必须保证暴露最少的信息。在大多数情况下，个人信息并非必不可少。当我在商店里购买一本杂志，付钱给店员的时候，他没有必要知道我是谁。当我要求我的电子邮件服务商发送和接受消息时，他没有必要知道我在给谁发送信息，我发送了什么，或者别人对我说了什么；他只需要知道如何从这里获得消息，我欠他多少服务费。当我的身份在交易中被服务商暗中获取了，我就没有了隐私。我无法再选择性的披露我的信息；我只能被迫一直处于暴露的状态。

由此可见，**保护开放社会中的隐私需要匿名的交易系统。**迄今为止，现金交易系统是最好的匿名交易系统。匿名交易系统并非秘密交易系统。当且仅当他们想要这么做时，匿名系统允许个体披露他们的身份，这是隐私的实质。

开放社会中的隐私同样需要密码学。当我发言时，我只想让我指定的听众听到它。当我发言的内容全世界都可以听到时，我就丧失了隐私。加密象征了意味着对隐私的要求，用弱密码加密意味着对隐私要求不高。再者，当披露默认情况下为匿名的个人身份时，为了保证这个披露真实可靠，我们需要密码学的数字签名。

我们不能奢望政府、企业、或者其他庞大、匿名的组织出于他们的仁慈来授予我们隐私权。评价我们会对他们有利，并且我们应该认为他们确实会这么做。要抵抗他们的言论就是要对抗信息的性质。信息不止想要免费，而且渴望免费。信息会扩展到所有可能的储存空间。信息是谣言的兄弟，它更年轻，更强壮；与流言相比，信息传播得更快，有更多的角度，包含更多的知识，然而给出的结论更少。

如果想要获得隐私权，我们必须捍卫它。我们必须联合起来，创造可以处理匿名交易的系统。几个世纪以来，人们已经通过低语、夜幕、信封、紧密的房门、秘密的手语，以及邮递员来保护自己的隐私。过去的技术无法支持可靠的隐私，但电子技术可以。

密码朋克宣言 (2)

我们，密码朋克，致力于构建匿名系统。为了捍卫我们的隐私，我们用密码学，用匿名邮件转发系统，用数字签名，用电子货币。

密码朋克写代码。我们认识到，需要有人编写软件来保护隐私，而且我们无法在有人没有隐私的情况下获得隐私，所以我们将开发这些软件。届时，我们将开源我们的代码，让我们的密码朋克战友们可以使用它。我们的代码对全球，任何使用它的人免费。如果你要封杀我们写的软件，我们不在乎。我们清楚，**软件是无法被销毁的，彻底的分布式系统永不停机。**

密码朋克们谴责对于密码学的控制，因为**加密从根本上是一种私人行为**。加密实际上是从公共领域抹掉我们的信息。即使是禁止密码学的法律也只能在一国的疆界内生效，在国家暴力机器所能控制的范围内肆虐。**密码学将不可避免地扩散到全球，同样，它创造的匿名交易系统也将如此。**

要使隐私权的意识广为传播，它必须成为社会契约的一部分。人们必须联合起来，为了共同的利益，合力去部署这些系统。隐私权的未来，取决于人们在社会中的合作。我们，密码朋克，思你所思，忧你所忧，并且希望与你携手，不再自我欺骗。我们绝不会因为有谁反对，放弃我们的事业。

密码朋克致力于使网络对隐私更加安全。让我们一起加速向前迈进。

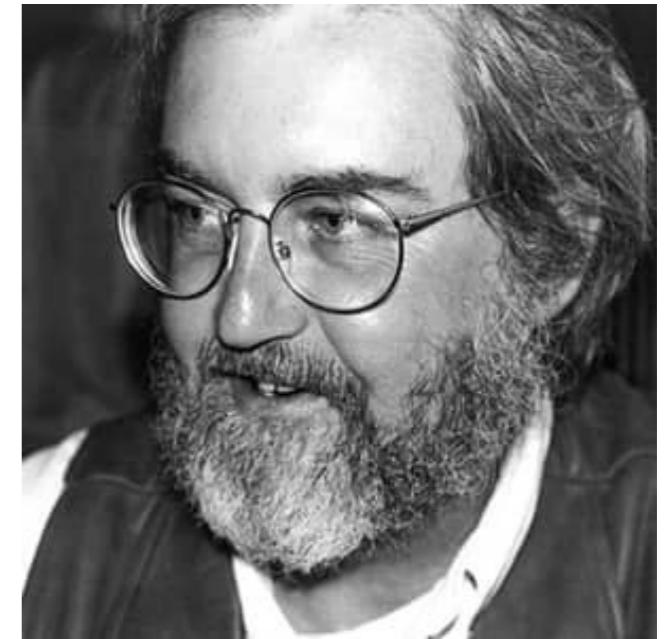
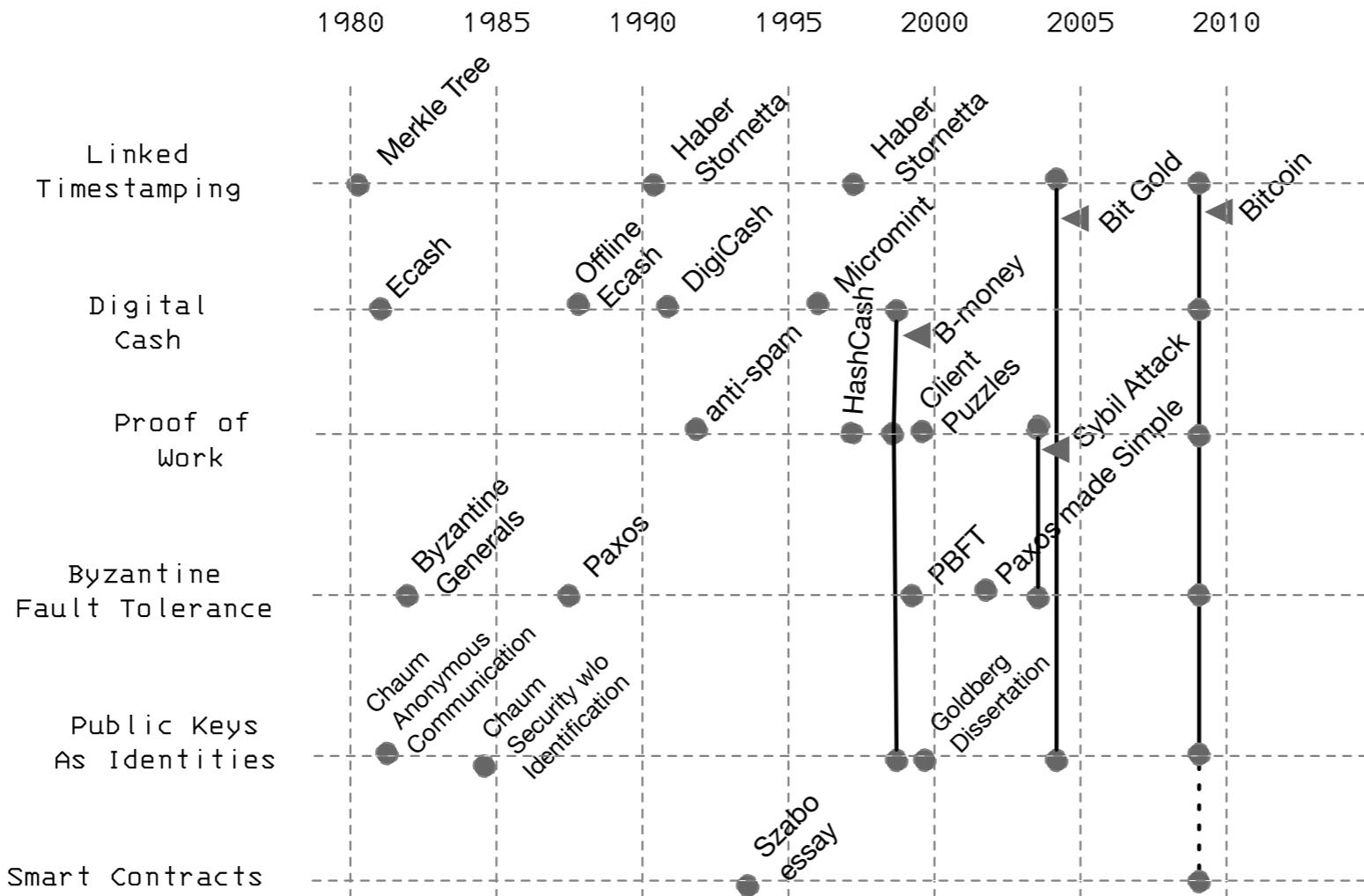
前进。

埃里克·休斯

<hughes@soda.berkeley.edu>

1993年3月9日

Bitcoin学术图谱 (1)

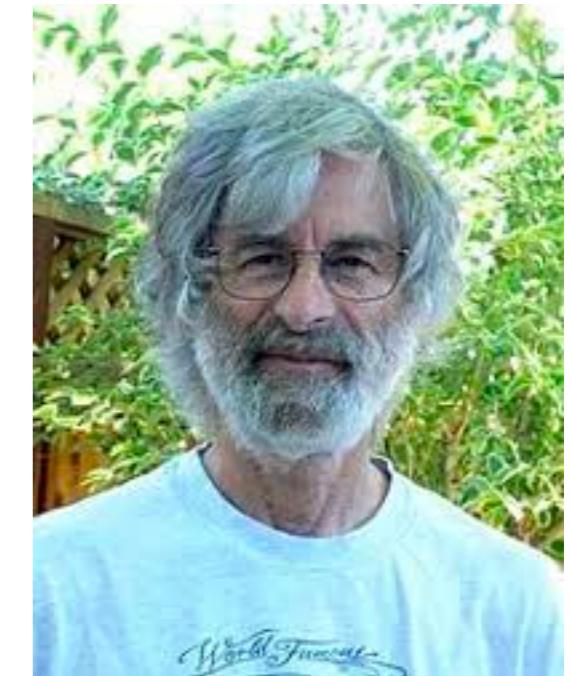
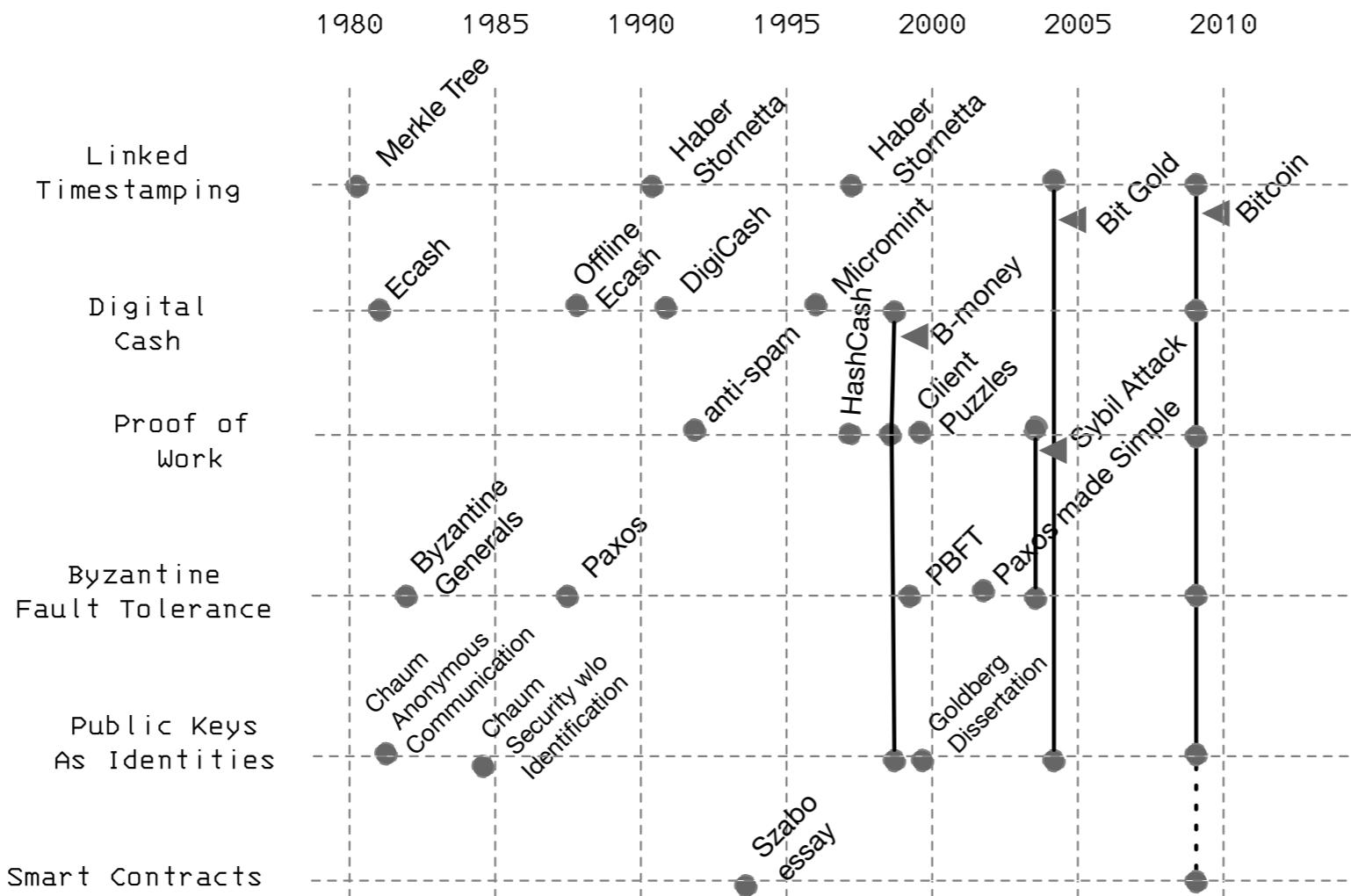


蒂姆西·梅 (Timothy May)

加密信用 (Crypto Credits) :

20世纪80年代，加密货币的始祖，用于奖励那些致力于保护公民隐私的黑客们。

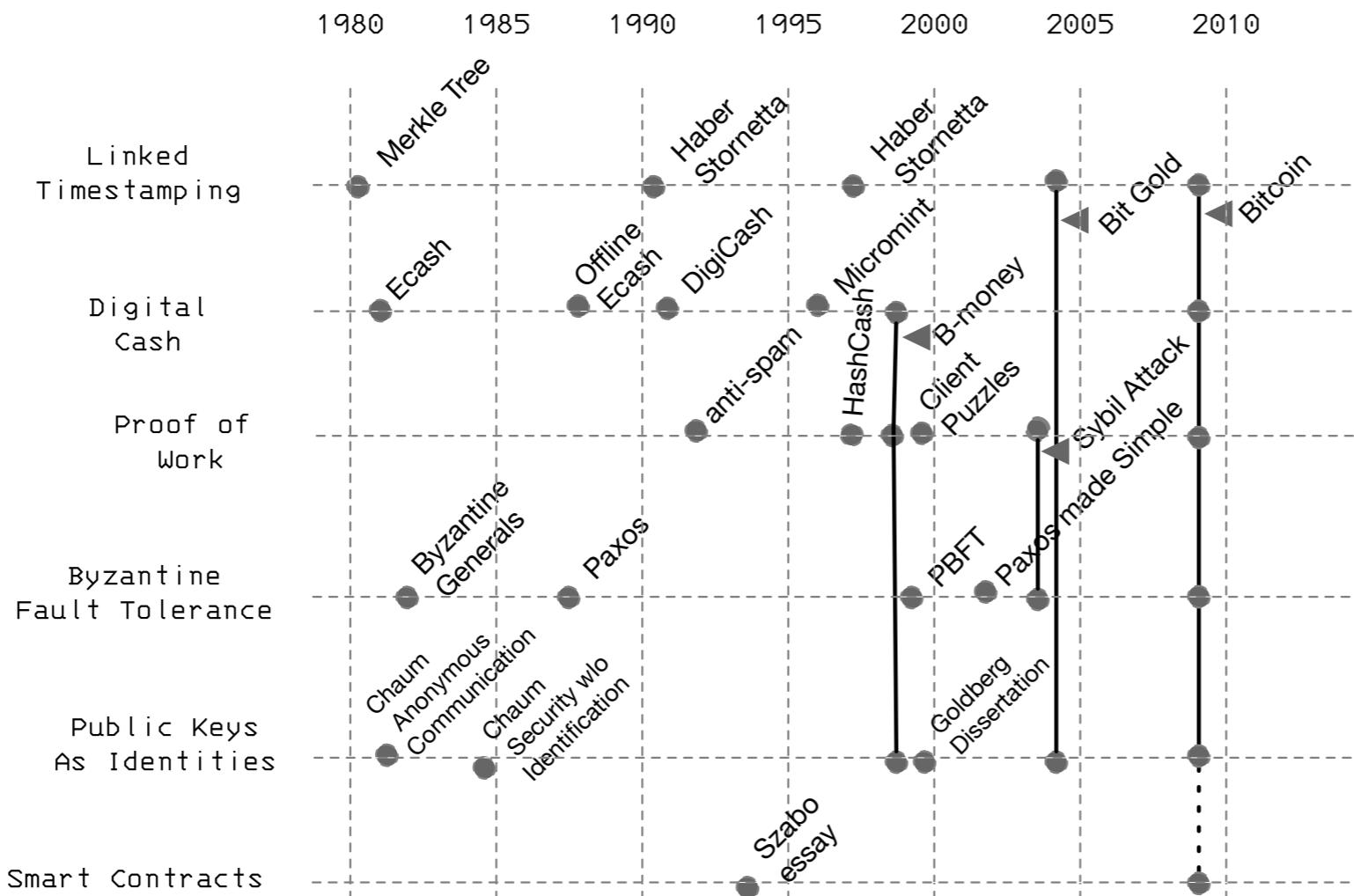
Bitcoin学术图谱 (2)



莱斯利·兰伯特 ((Leslie Lamport)

拜占庭将军问题 (Byzantine Generals Problem) : (区块链分布式系统课时讲)
加密货币的难点在于如何创建分布式共识，因此莱斯利·兰伯特等人1982年提出了拜占庭将军问题。

Bitcoin学术图谱 (3)

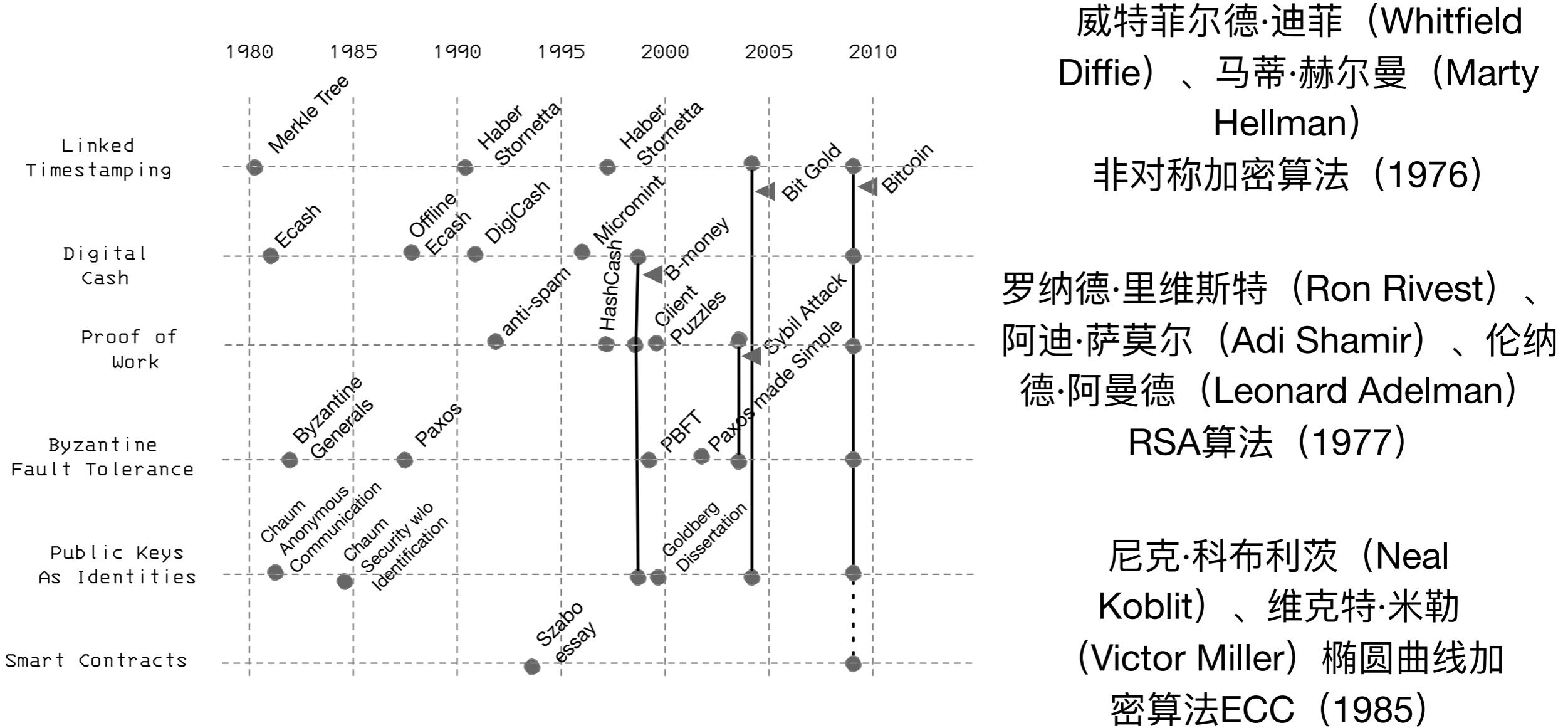


大卫·乔姆 (David Chaum)

Ecash:

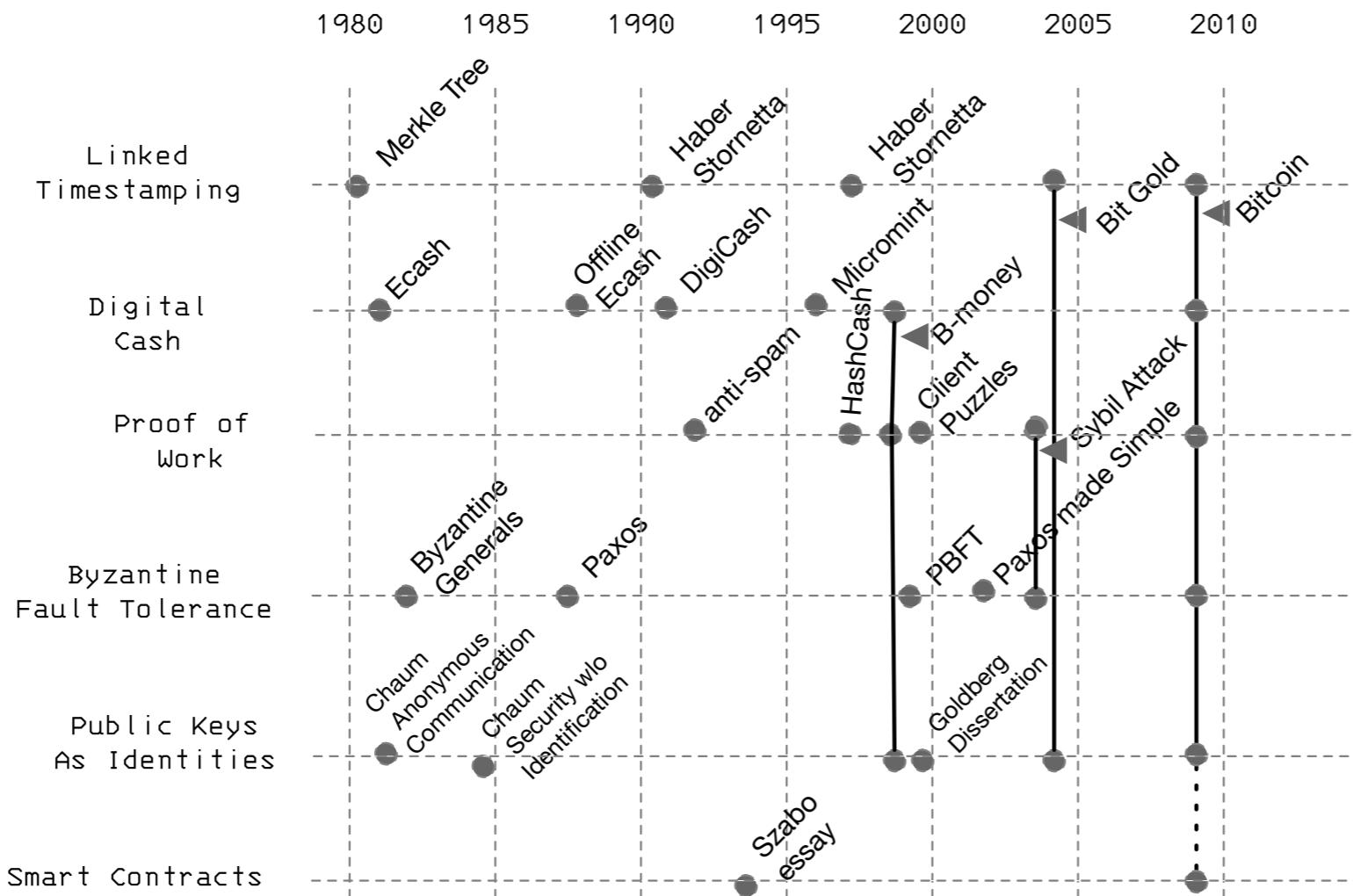
1990年，大卫·乔姆 (David Chaum) 提出注重隐私安全的密码学网络支付系统，具有不可追踪的特性，就是后来的电子货币Ecash，不过Ecash并非去中心化系统，后来大多数电子加密货币都继承了Ecash重视隐私安全的特性，以盲签名技术 (Chaumian blinding) 为基础，但都没有流行起来，因为他们都依赖一个中心化的中介机构。

Bitcoin学术图谱 (4)



非对称加密的创新 (第2小节讲)

Bitcoin学术图谱 (3)



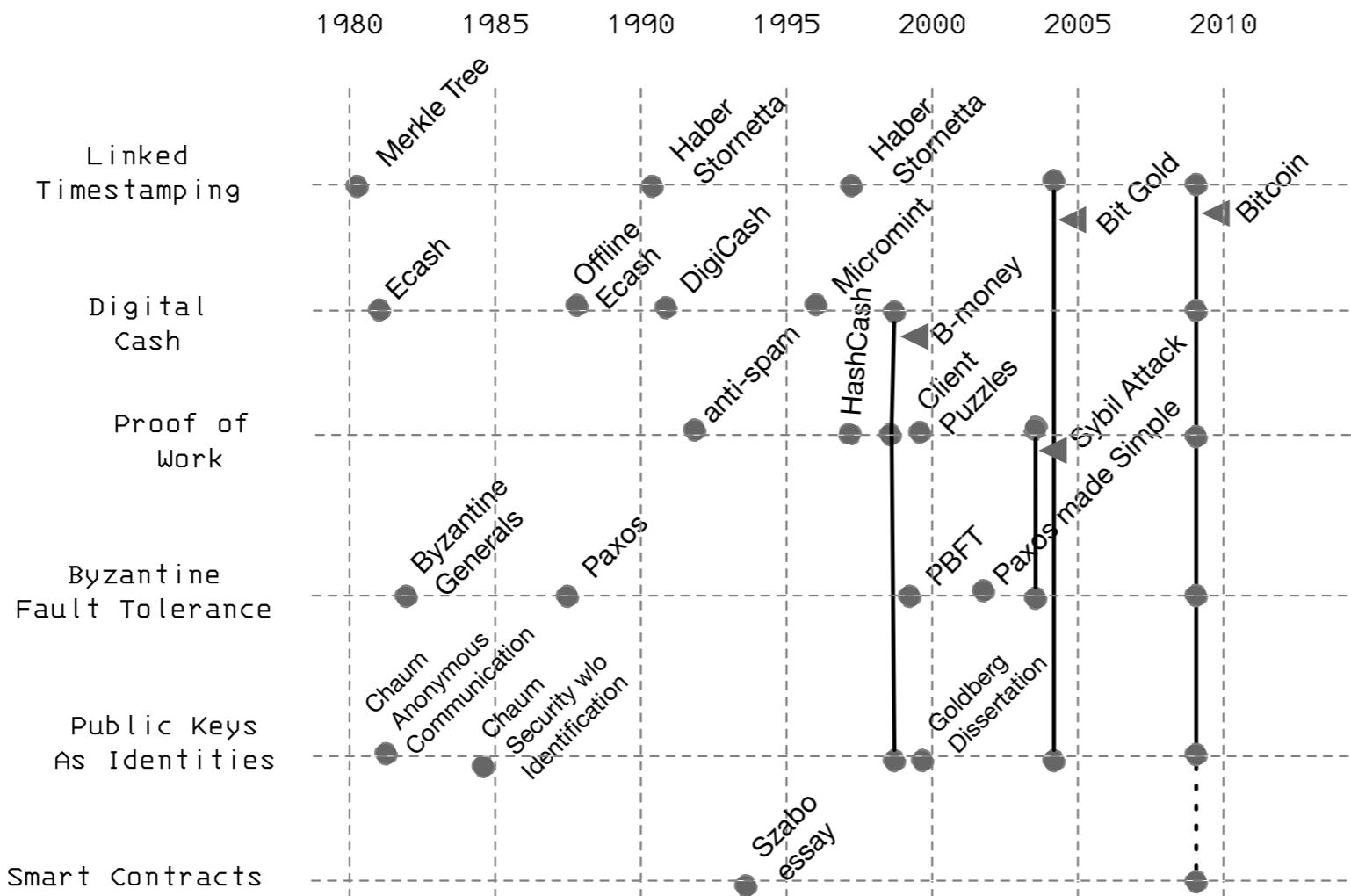
戴·伟 (Dai Wei)

B-money:

B-money的设计在很多技术特质上与比特币非常相似，但是不能否认的是，B-money有些不切实际，其最大的现实困难在于货币的创造环节。

主要问题：计算量成本计算无法计算。

Bitcoin学术图谱 (5)

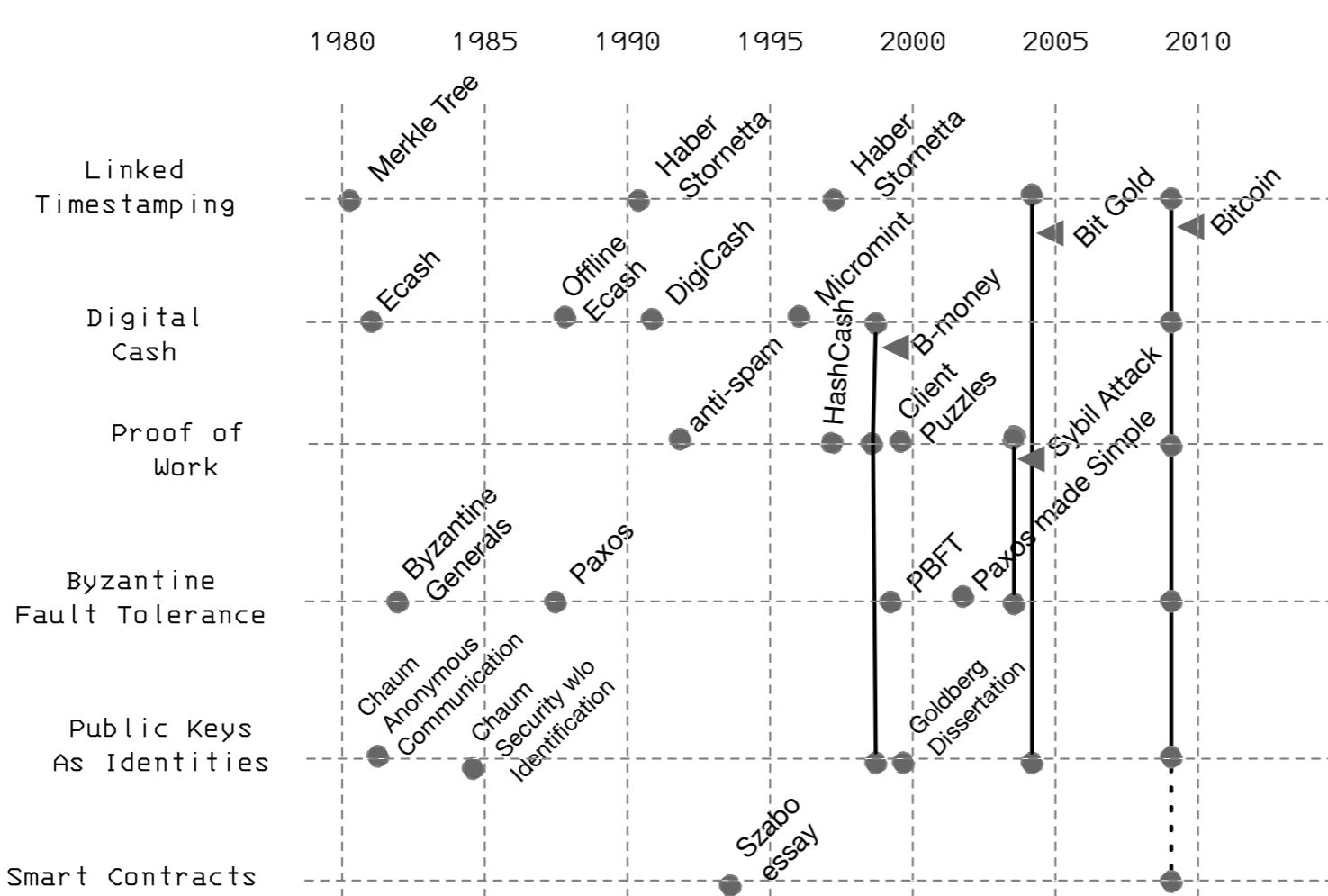


尼克·萨博 (Nick Szabo)

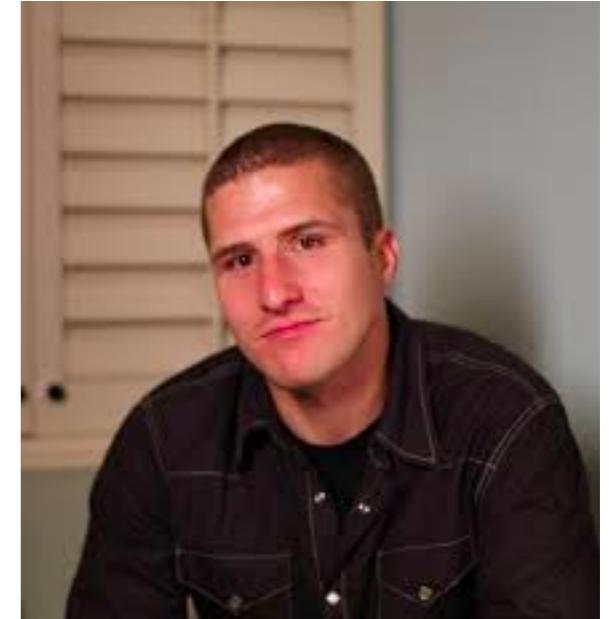
BitGold:

2005年，BitGold提出用户通过竞争解决数学难题，再将解答的结果用加密算法串联在一起公开发布，构建出一个产权认证系统。这个系统和比特币系统已经非常接近。

Bitcoin学术图谱 (6)



P2P技术（区块链分布式系统课时讲）

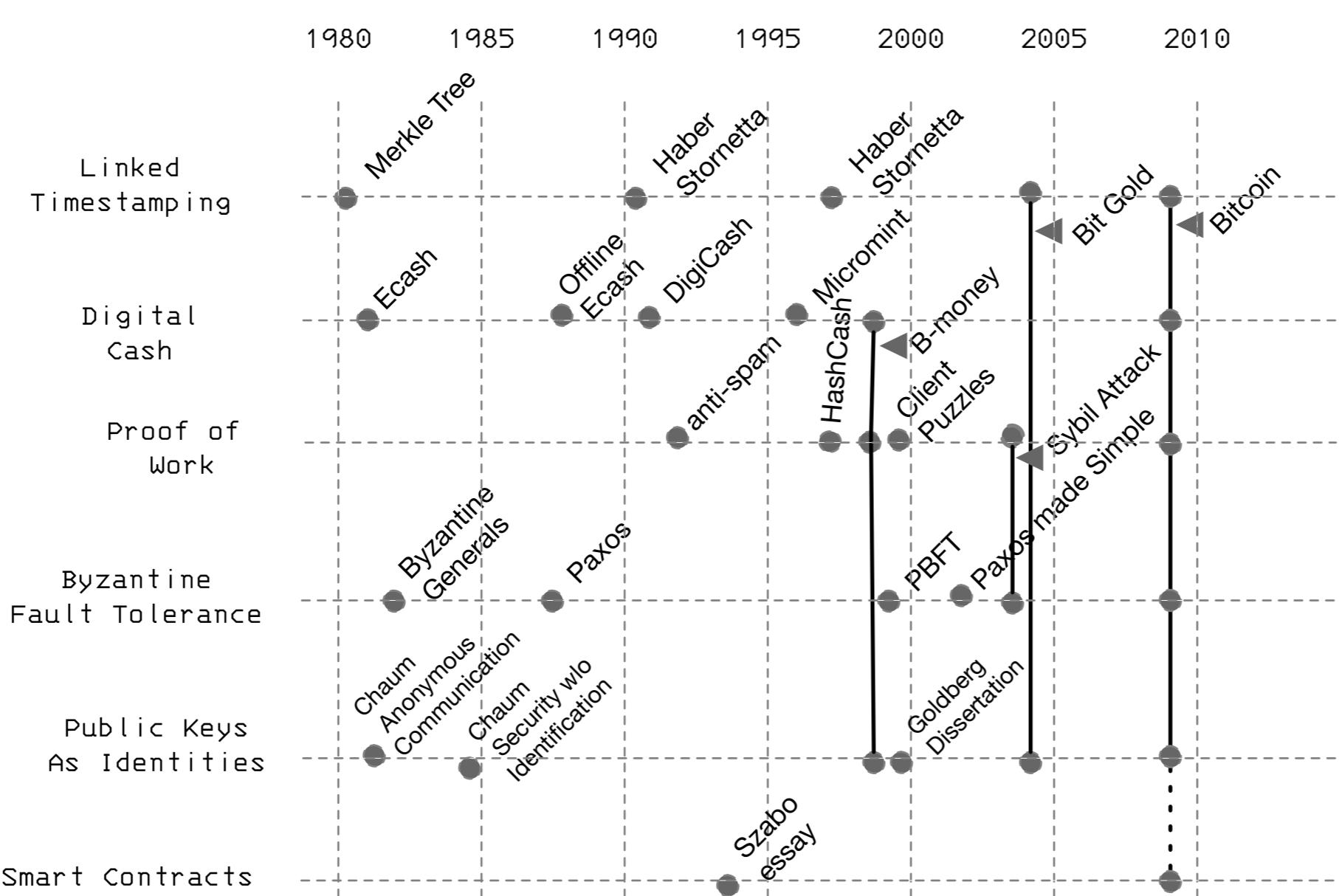


肖恩·范宁 (Shawn Fanning)



肖恩·帕克 (Shawn Parker)

Bitcoin学术图谱 (7)

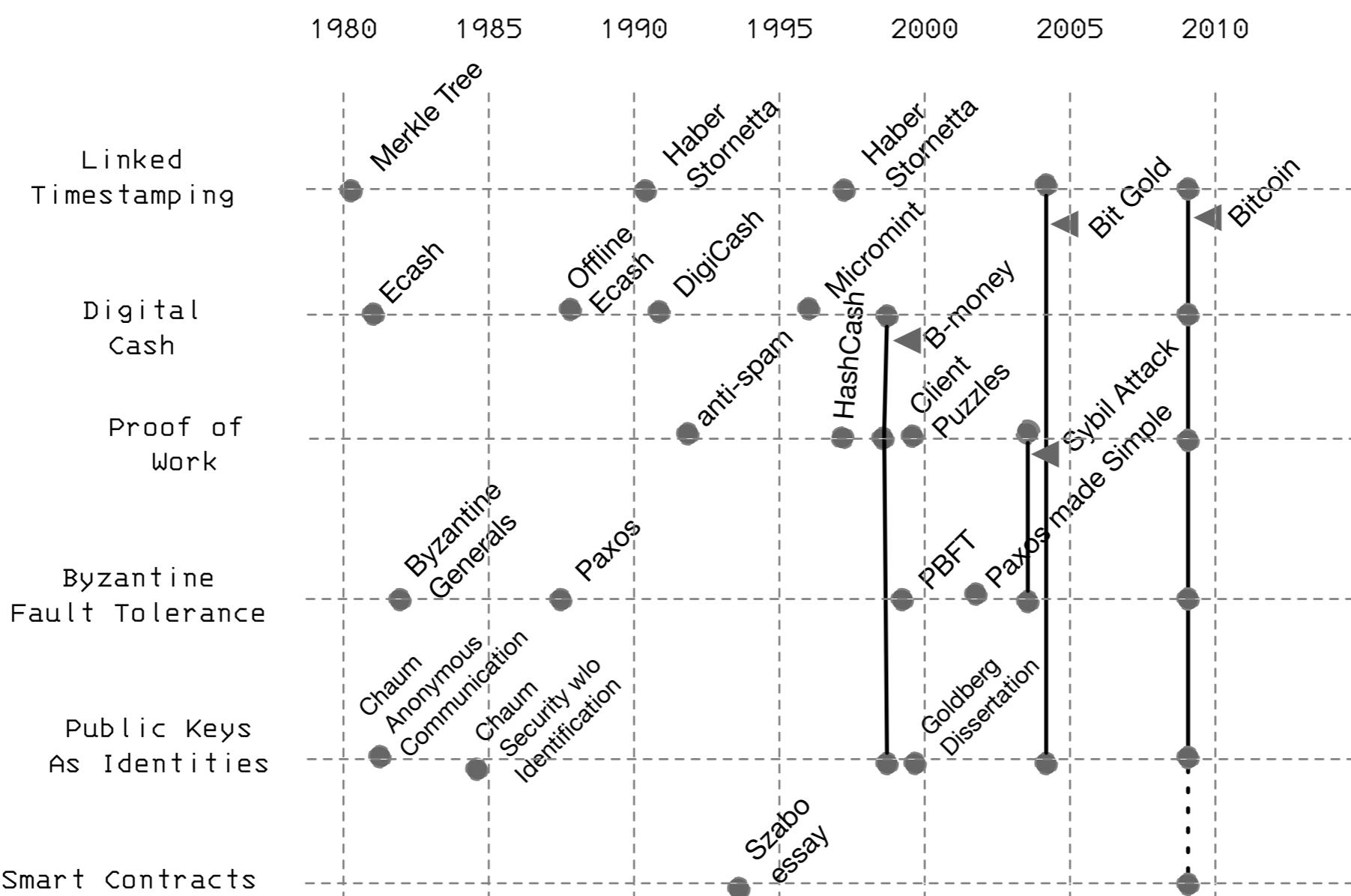


亚当·拜克 (Adam Back)

哈希现金 (Hash Cash) :

解决双重支付问题,起初用于限制垃圾邮件发送与拒绝服务攻击。

Bitcoin学术图谱 (8)



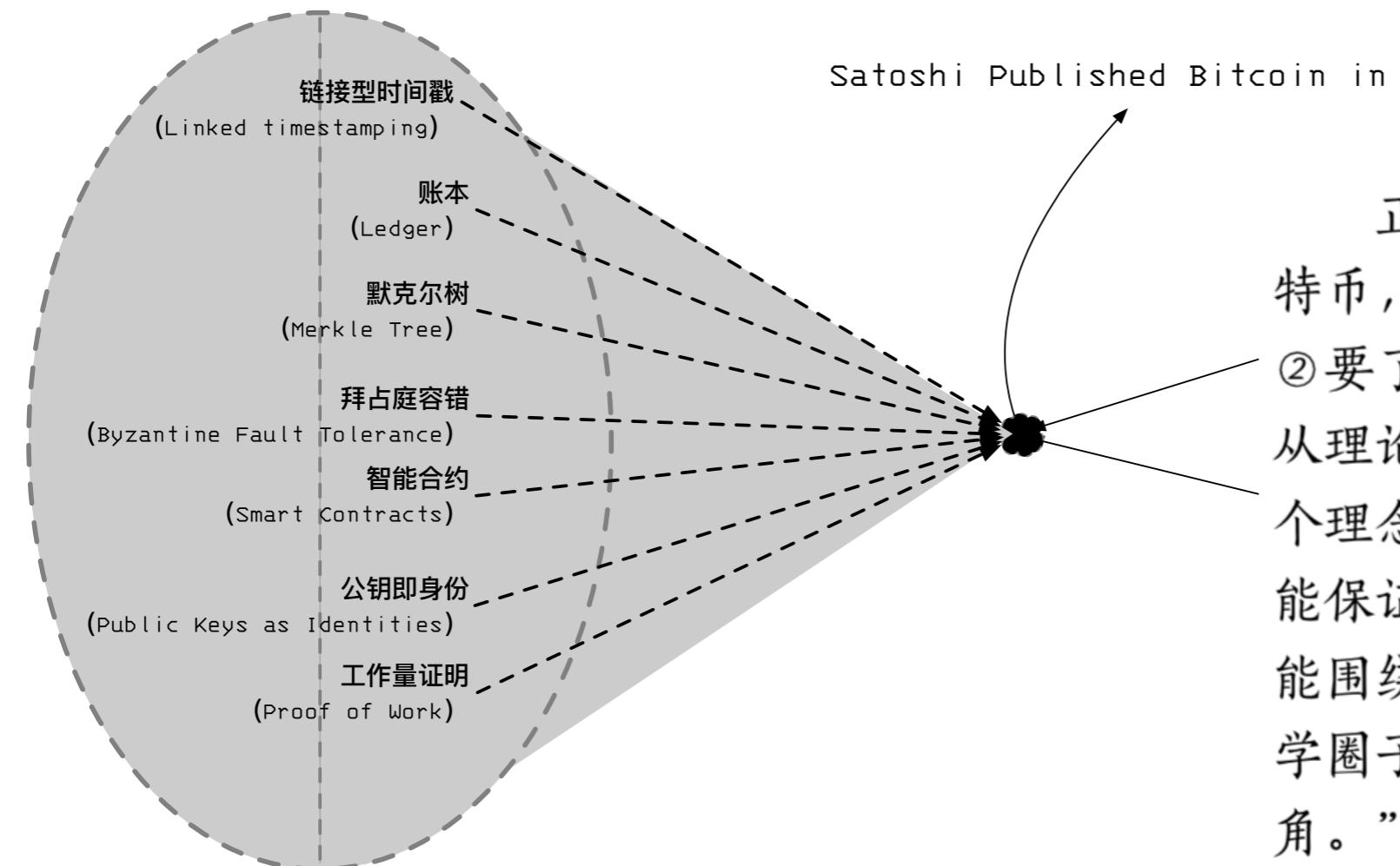
亚当·拜克 (Adam Back)



哈尼·芬尼 (Hal Finney)

亚当·拜克 (Adam Back) 哈希现金 (Hash Cash) → 哈尼·芬尼 (Hal Finney) 可复用工作量证明
Based on 达利亚·马凯的拜占庭容错机制 (Byzantine Quorum Systems)

Bitcoin学术图谱 (9)



正如戴伟事后评价说：“要想开发出比特币，必须：①对货币有非常深入的思考；②要了解密码学；③认为比特币这样的系统从理论上是可行的；④要有足够的动力将这个理念开发成实际产品；⑤编程能力出色，能保证产品安全；⑥有足够的社交技巧，才能围绕这个产品创建一个成功的社区。密码学圈子能符合前三个条件的人就已是凤毛麟角。”

2008年，区块链诞生

密码朋克：从未远去

成员

发明

Bram Cohen

BitTorrent, 又称BT下载

Sarah Harrison

维基解密

Taher Elgamal

SSL协议

Sir Timothy John
Berners-Lee

万维网 (WorldWide Web)

Shawn Parker

脸书 (Facebook)