E-Cash and Cypherpunks

Murat Osmanoglu

E-Cash

E-Cash

E-Cash

1 *C* = 0101000…11100011

E-Cash

1 *C* = 0101000…11100011

E-Cash

1 *C* = 0101000…11100011

E-Cash

1 C = 0101000…11100011

E-Cash

1 C = 0101000…11100011

- check the signature

E-Cash

Double-spending

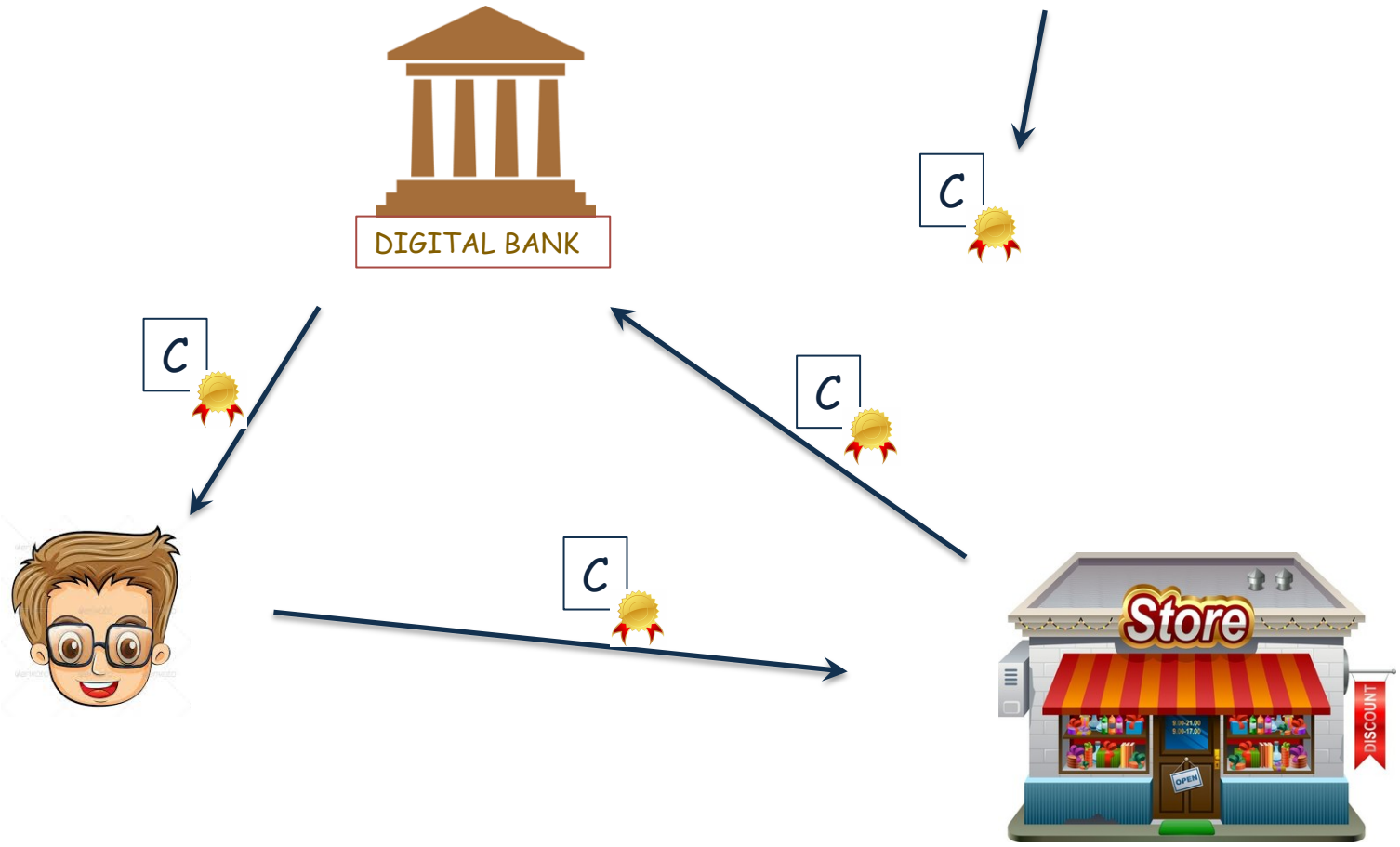
1 C = 0101000…11100011

- check the signature

E-Cash

Double-spending

1 C = 0101000…11100011



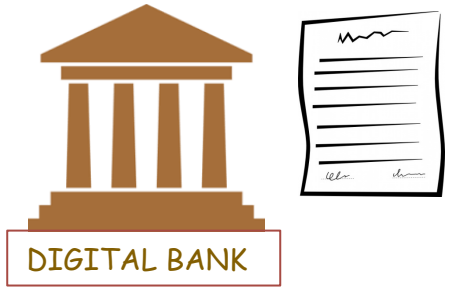
- check the signature
- send it to the bank for double-spending

E-Cash

Double-spending

- check the list

1 C = 0101000…11100011



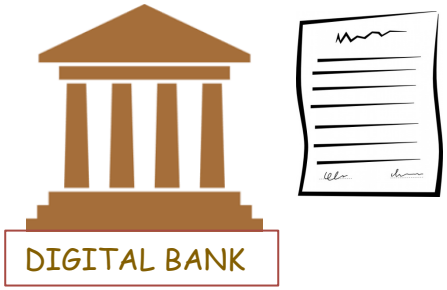
- check the signature
- send it to the bank for double-spending

E-Cash

✓ Double-spending

- check the list

1 C = 0101000…11100011



- check the signature
- send it to the bank for double-spending

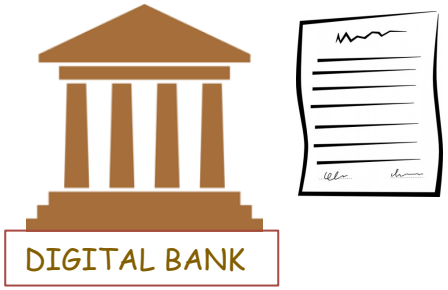
E-Cash

✓ Double-spending

? Privacy

- check the list

1 C = 0101000…11100011



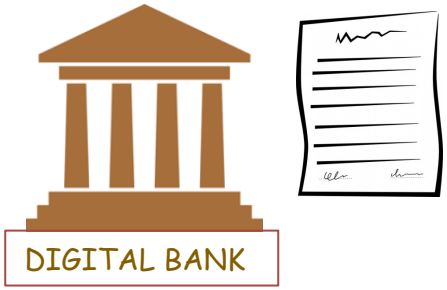
- check the signature
- send it to the bank for double-spending

E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982

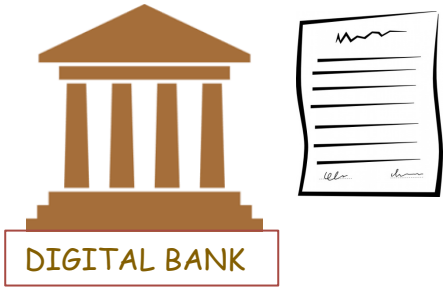


E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982



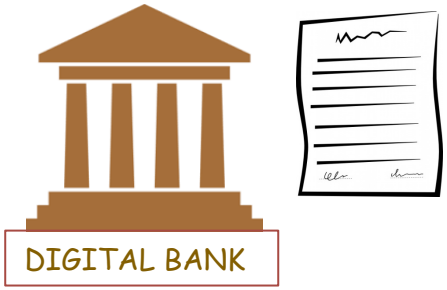
- generate a random C
- encrypt it; E(C)

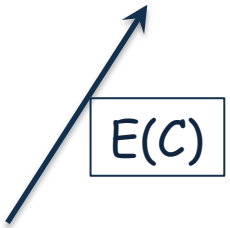
E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982





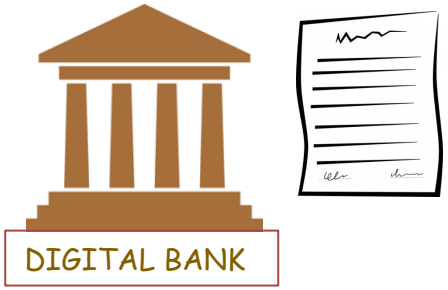
- generate a random C
- encrypt it; E(C)

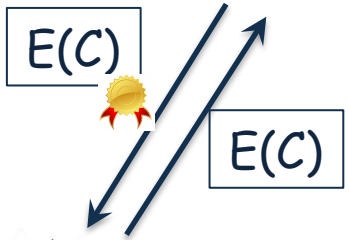
E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982





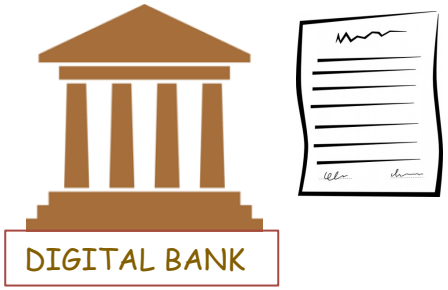
- generate a random C
- encrypt it; E(C)

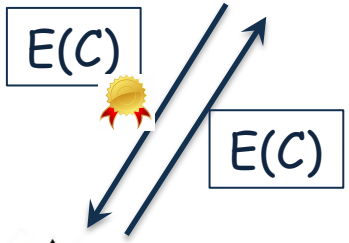
E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982





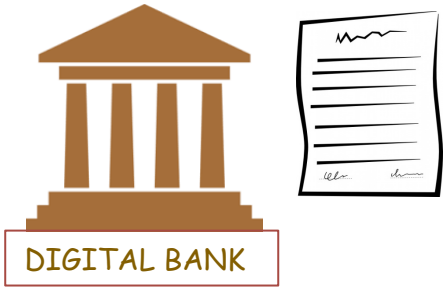
- generate a random *C*
- encrypt it; *E*(*C*)
- decrypt *S*(*E*(*C*)) as *S*(*C*)

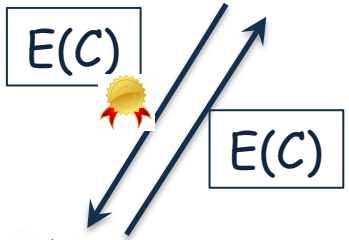
E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982





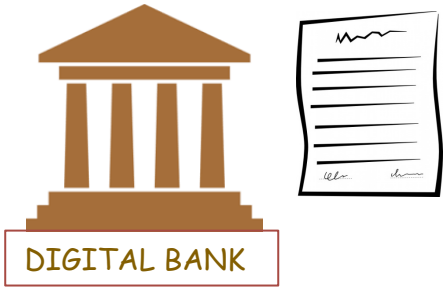
- generate a random C
- encrypt it; E(C)
- decrypt S(E(C)) as S(C)

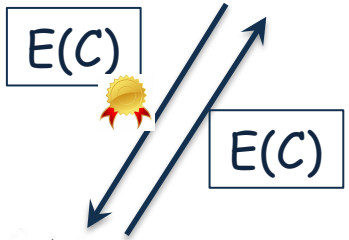
E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982





- generate a random C
- encrypt it; E(C)
- decrypt S(E(C)) as S(C)

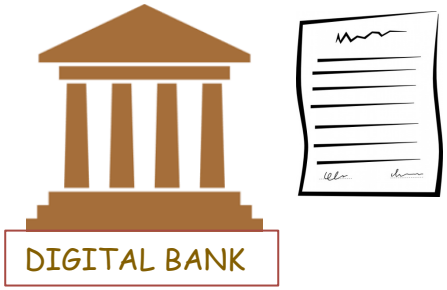
- check the signature

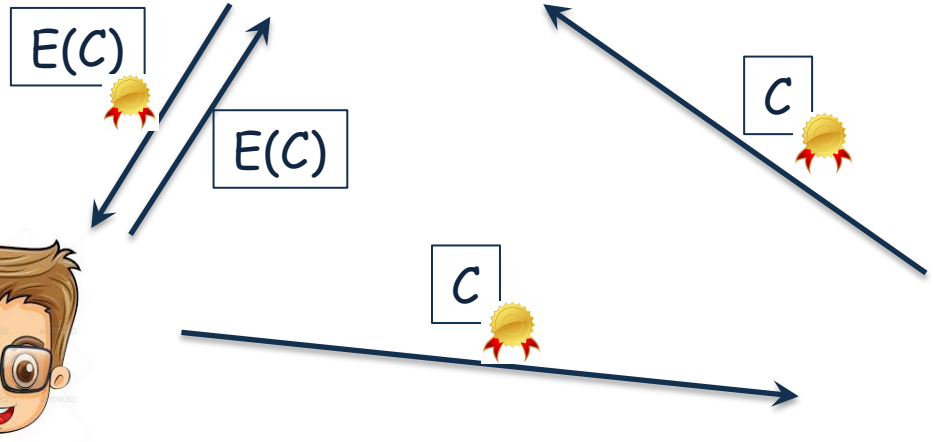
E-Cash

✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982





- generate a random C
- encrypt it; E(C)
- decrypt S(E(C)) as S(C)

- check the signature
- send it to the bank for double-spending

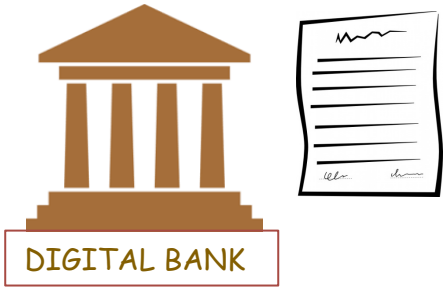
E-Cash

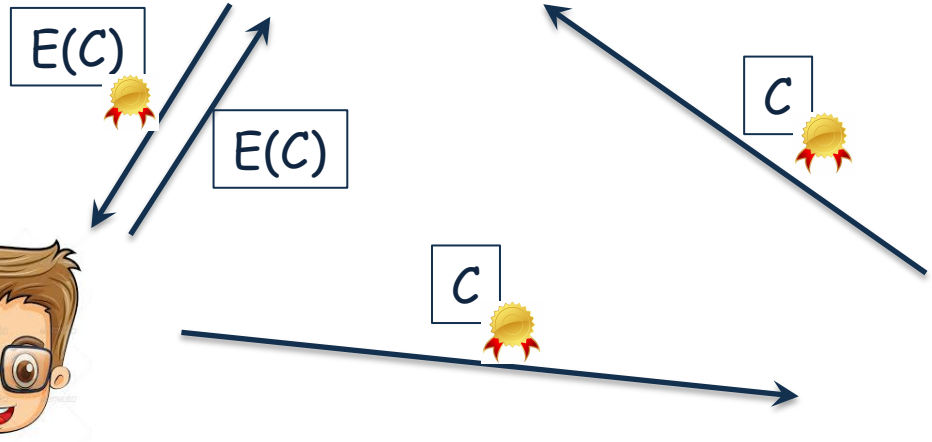
✓ Double-spending

? Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982

- check the list





- generate a random C
- encrypt it; E(C)
- decrypt S(E(C)) as S(C)

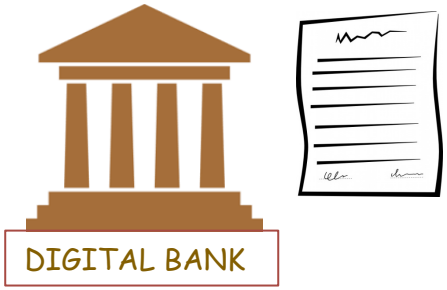
- check the signature
- send it to the bank for double-spending

E-Cash

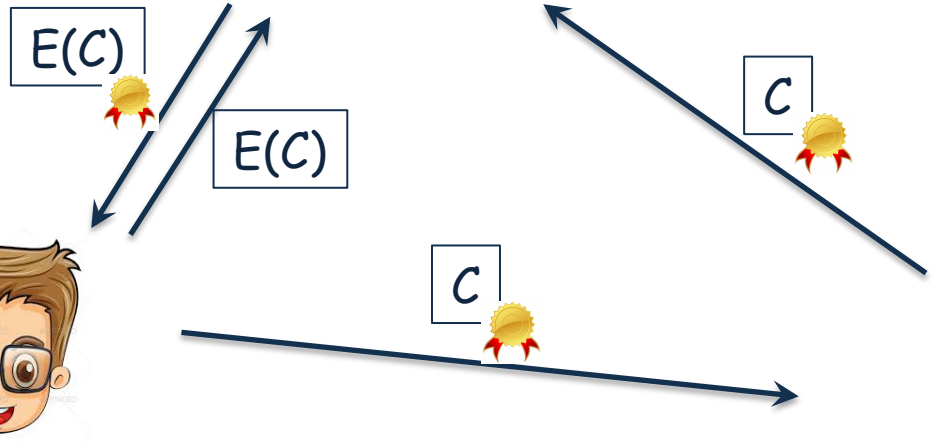
✓ Double-spending

✓ Privacy

David Chaum, *Blind Signatures for Untreceable Payments*, 1982



- check the list



- generate a random C
- encrypt it; E(C)
- decrypt S(E(C)) as S(C)

- check the signature
- send it to the bank for double-spending

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'
- Chaum extended the idea with Fiat and Naor to allow offline payments that enables detection of double-spending
- Chaum founded DigiCash in 1990
- The company negotiated deals with VISA, Netscape, Microsoft (all of them fell through)
- He talked with Bill Gates about integrating ecash in every copy of Windows 95. But he refused to sell it for less than 1 or 2 dollars per sold copy. This attitude killed the agreement

Cypherpunk Manifesto

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk'

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash and pseudonymous reputation systems

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash and pseudonymous reputation systems

  'Security without Identification : Transaction Systems to Make Big Brother Obsolete', 1985

Cypherpunk Manifesto

- 'cypherpunk' created from the words 'cipher' (or cypher) and 'cyberpunk' (a genre of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

- an activist promoting wide use of strong crypto and privacy-enhancing technologies as a route to social and political change.

- its roots traced back to the study of David Chaum on anonymous digital cash and pseudonymous reputation systems

  'Security without Identification : Transaction Systems to Make Big Brother Obsolete', 1985

- In late 1992, three people: Eric Hughes (mathematicians from Berkeley), Tim May (businissman retired from Intel), and John Gilmore (computer scientist) were gathering to discuss some cryptographic and programing issues

Cypherpunk Manifesto

- They later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

Cypherpunk Manifesto

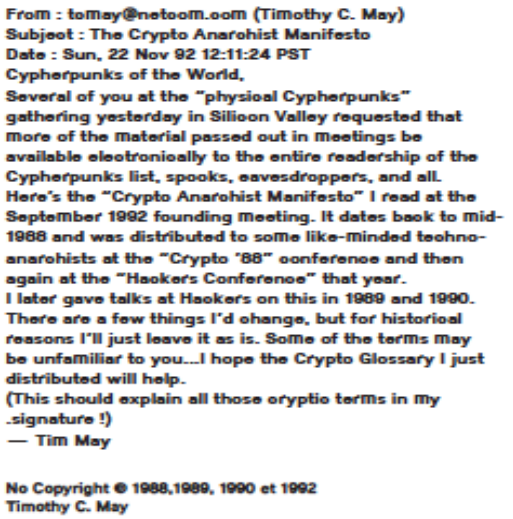
- They later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

- Timothy May published 'the Crypto Anarchist Manifesto' in 1992

Cypherpunk Manifesto

- They later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

- Timothy May published 'the Crypto Anarchist Manifesto' in 1992



From : tcmay@netcom.com (Timothy C. May)
Subject : The Crypto Anarchist Manifesto
Date : Sun, 22 Nov 92 12:11:24 PST
Cypherpunks of the World,
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all.
Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year.
I later gave talks at Hackers on this in 1989 and 1990. There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.
(This should explain all those cryptic terms in my .signature !)
— Tim May

No Copyright © 1988,1989, 1990 et 1992
Timothy C. May

THE CRYPTO-ANARCHIST MANIFESTO

Thimothy C.May

MANIFESTE CRYPTO-ANARCHISTE

Cypherpunk Manifesto

- They later initiated a mailing list (the number of subscribers reached 2000 in 1997) to reach out some other cypherpunks outside of Bay Area.

- Timothy May published 'the Crypto Anarchist Manifesto' in 1992

> "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."

Cypherpunk Manifesto

- Eric Hughes published *'A Cypherpunk's Manifesto'* in 1993, which can be considered as holy text of this movement.

Cypherpunk Manifesto

- Eric Hughes published *'A Cypherpunk's Manifesto'* in 1993, which can be considered as holy text of this movement.

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

Cypherpunk Manifesto

- Eric Hughes published *'A Cypherpunk's Manifesto'* in 1993, which can be considered as holy text of this movement.

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

"When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. Therefore, privacy in an open society requires anonymous transaction systems."

Cypherpunk Manifesto

- Adam Back, inventor of Hashcash

Cypherpunk Manifesto

- Adam Back, inventor of Hashcash
- Nick Szabo, inventor of smart contracts, designer of bit gold

Cypherpunk Manifesto

- Adam Back, inventor of Hashcash
- Nick Szabo, inventor of smart contracts, designer of bit gold
- Hal Finney, the receiver of the first transaction made in Bitcoin

Cypherpunk Manifesto

- Adam Back, inventor of Hashcash
- Nick Szabo, inventor of smart contracts, designer of bit gold
- Hal Finney, the receiver of the first transaction made in Bitcoin
- Satoshi Nakamoto, inventor of Bitcoin

Cypherpunk Manifesto

- Adam Back, inventor of Hashcash
- Nick Szabo, inventor of smart contracts, designer of bit gold
- Hal Finney, the receiver of the first transaction made in Bitcoin
- Satoshi Nakamoto, inventor of Bitcoin
- Julian Assange, founder of wikileaks, author of 'Cypherpunks : Freedom and the Future of the Internet'

B-Money

B-Money

- introduced by Wei Dai, computer engineer graduated from University of Washington.

B-Money

- introduced by Wei Dai, computer engineer graduated from University of Washington.

- In May 2011, in an article Nick Szabo stated that

> "Myself, Wei Dai, and Hal Finney were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai)"

B-Money

- introduced by Wei Dai, computer engineer graduated from University of Washington.

- In May 2011, in an article Nick Szabo stated that

> "Myself, Wei Dai, and Hal Finney were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai)"

- Wei Dai stated that

> "...my understanding is that the creator of Bitcoin, who goes by the name Satoshi Nakamoto, didn't even read my article before reinventing the idea himself. He learned about it afterward and credited me in his paper. So my connection with the project is quite limited"

B-Money

- introduced by Wei Dai, computer engineer graduated from University of Washington.

I am fascinated by Tim May's crypto-anarchy. In a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.

B-Money

- introduced by Wei Dai, computer engineer graduated from University of Washington.

I am fascinated by Tim May's crypto-anarchy. In a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.

Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.