Digicash

Murat Osmanoglu

MONEY

Money is the award of succes
Sakıp Sabancı

Money money money!
Napoleon Bonaparte

For a man is rich in proportion to the number of things which he can afford to let alone.
Henry David Thoreau

MONEY

- any item or verifiable record that is generally accepted as payment for goods and services

Its Functions

Its Functions

- measure of value

Its Functions

- measure of value
- store of value

Its Functions

- measure of value
- store of value
- medium of exchange

Its Properties

Its Properties

- fungible

Its Properties

- fungible
- durable

Its Properties

- fungible
- durable
- portable

Its Properties

- fungible
- durable
- portable
- divisible

Its Properties

- fungible
- durable
- portable
- divisible
- easy to produce

Its Properties

- fungible
- durable
- portable
- divisible
- easy to produce
- uniform

Its Properties

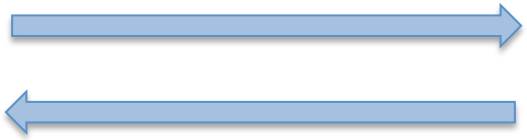
- fungible
- durable
- portable
- divisible
- easy to produce
- uniform
- limited in supply

Its Properties

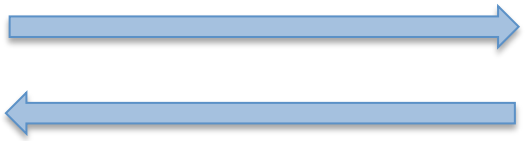
- fungible
- durable
- portable
- divisible
- easy to produce
- uniform
- limited in supply
- hard to forge

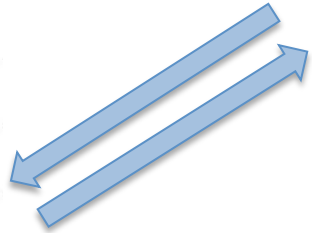
Barter

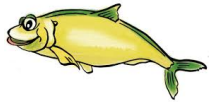
Barter



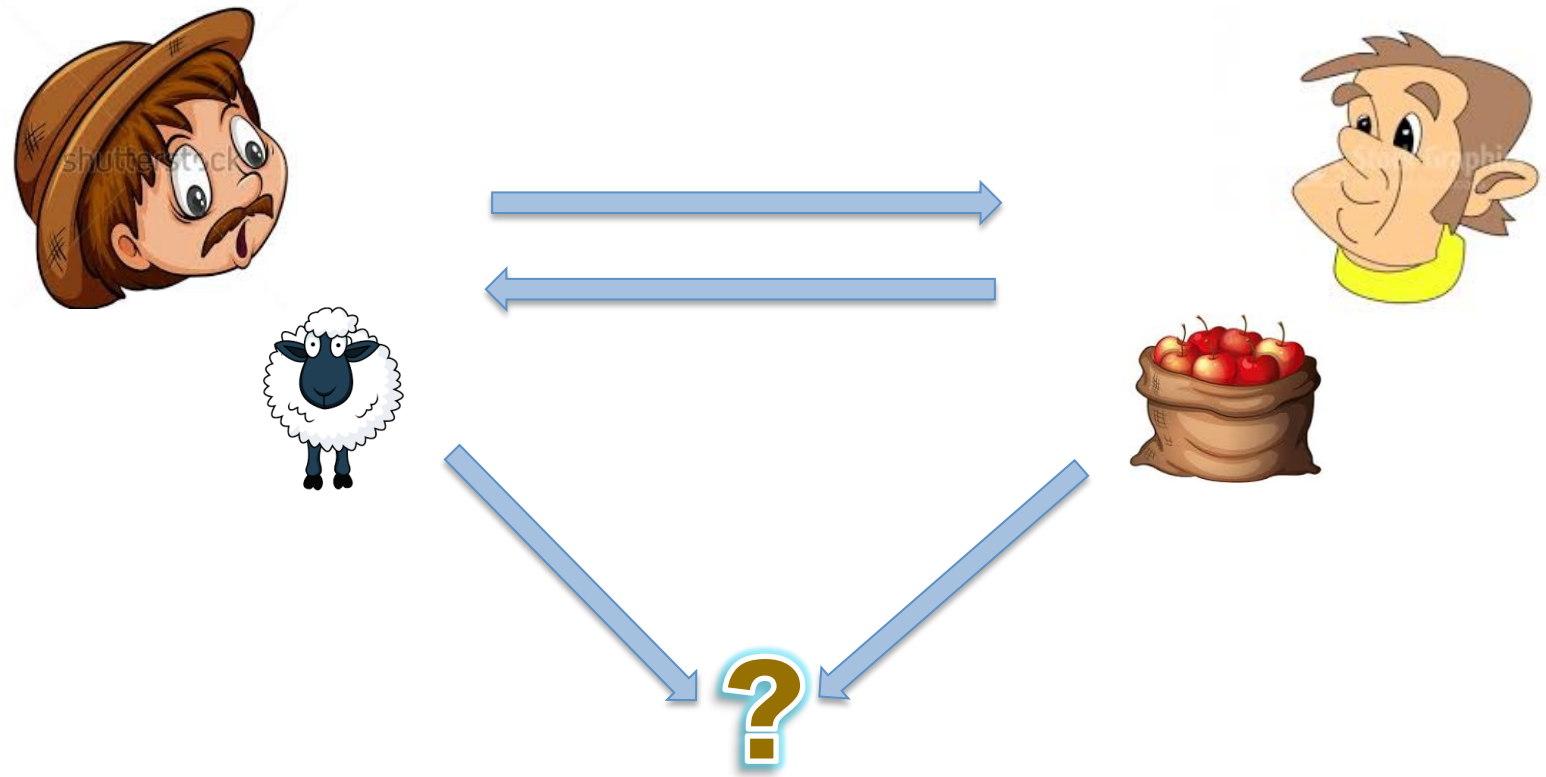
Barter







Barter



History of Money

History of Money

- cattle such as cow, sheep, and goat between B.C. 9000-6000

History of Money

- cattle such as cow, sheep, and goat between B.C. 9000-6000

- sea shells in China around B.C. 1200

History of Money

- cattle such as cow, sheep, and goat between B.C. 9000-6000

- sea shells in China around B.C. 1200

- Rai stones in Yap island till the beginning of 20th century

History of Money

- cattle such as cow, sheep, and goat between B.C. 9000-6000

  durable ? portable ? uniform ?

- sea shells in China around B.C. 1200

- Rai stones in Yap island till the beginning of 20th century

History of Money

- cattle such as cow, sheep, and goat between B.C. 9000-6000

  durable ? portable ? uniform ?

- sea shells in China around B.C. 1200

  divisible ? uniform ? limited in supply ?

- Rai stones in Yap island till the beginning of 20th century

History of Money

- cattle such as cow, sheep, and goat between B.C. 9000-6000

  durable ? portable ? uniform ?

- sea shells in China around B.C. 1200

  divisible ? uniform ? limited in supply ?

- Rai stones in Yap island till the beginning of 20th century

  divisible ? portable ? easy to produce ?

History of Money

- Chinese using money made from mixture of copper and bronze around B.C 1000

History of Money

- Chinese using money made from mixture of copper and bronze around B.C 1000

portable ? hard to forge ?

History of Money

- Chinese using money made from mixture of copper and bronze around B.C 1000

  portable ? hard to forge ?

- first time in the history precious metals such as gold and silver used as money around B.C. 600 by Lydians

History of Money

- Chinese using money made from mixture of copper and bronze around B.C 1000

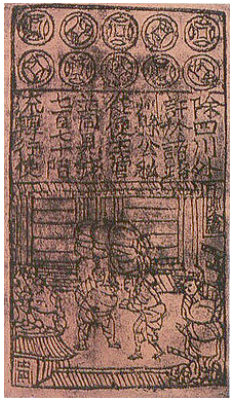
  portable ? hard to forge ?

- first time in the history precious metals such as gold and silver used as money around B.C. 600 by Lydians

  portable ? easy to produce ?

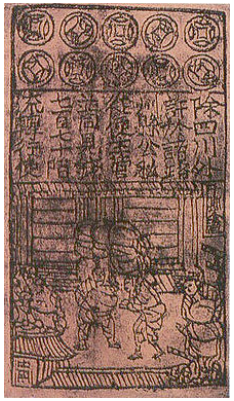
History of Money

- first paper money used in A.D 806

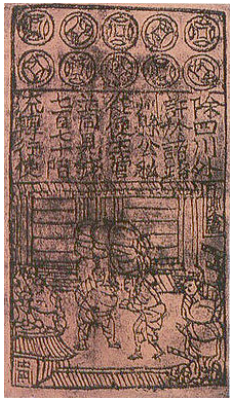


History of Money

- first paper money used in A.D 806
- paper money introduced to Europe in 13th century

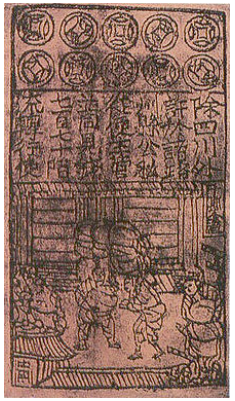


History of Money



- first paper money used in A.D 806
- paper money introduced to Europe in 13th century
- first paper money in Europe produced by Swiss bank Stockholm Banco in A.D. 1661

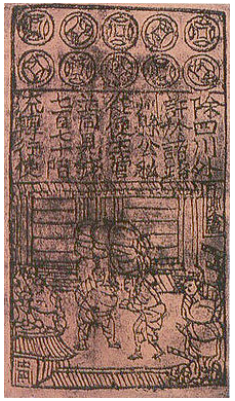
History of Money



- first paper money used in A.D 806
- paper money introduced to Europe in 13th century
- first paper money in Europe produced by Swiss bank Stockholm Banco in A.D. 1661

- fungible ✔
- durable ✔
- portable ✔
- divisible ✔
- easy to produce ✔

History of Money



- first paper money used in A.D 806
- paper money introduced to Europe in 13th century
- first paper money in Europe produced by Swiss bank Stockholm Banco in A.D. 1661

- fungible ✔
- durable ✔
- portable ✔
- divisible ✔
- easy to produce ✔
- uniform ✔
- limited in supply ✔
- hard to make false ✔

History of Money

- 1950 de Diner's Club issued the first credit card in 1950

History of Money

- 1950 de Diner's Club issued the first credit card in 1950

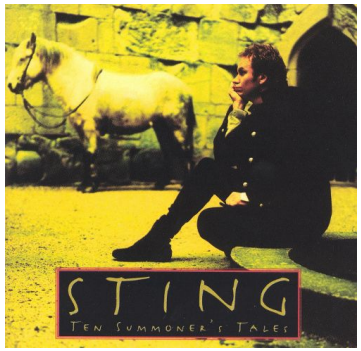
- British bank Barclays installed the first ATM machine in London in 1967

History of Money

- 1950 de Diner's Club issued the first credit card in 1950

- British bank Barclays installed the first ATM machine in London in 1967

- first secure e-commerce transaction made through NetMarket by Khan in August 1994



Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

On the one hand, knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle. For example, consider payments for such things as transportation, hotels, restaurants, movies, theater, lectures, food, pharmaceuticals, alcohol, books, periodicals, dues, religious and political contributions.

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'
- the intuition for blind signature

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'
- the intuition for blind signature

BLIND SIGNATURE CRYPTOSYSTEMS

The new kind of cryptography will be introduced first in terms of an analogy and then by description of its parts, their use, and the resulting security properties. No actual example cryptosystem is presented.

Basic Idea

The concept of a blind signature can be illustrated by an example taken from the familiar world of paper documents. The paper analog of a blind signature can be implemented with carbon paper lined envelopes. Writing a signature on the outside of such an envelope leaves a carbon copy of the signature on a slip of paper within the envelope.

Consider the problem faced by a trustee who wishes to hold an election by secret ballot, but the electors are unable to meet to drop their ballots into a single hat. Each elector is very concerned about keeping his or her vote secret from the trustee, and each

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

  - Payer chooses a random x and forms c(x)
  - Payer gives note c(x) to bank

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

  - Payer chooses a random x and forms c(x)
  - Payer gives note c(x) to bank
  - Bank signs the note c(x) as s''(c(x)), debits payer's account
  - Bank returns s''(c(x)) to payer

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

  - Payer chooses a random x and forms c(x)
  - Payer gives note c(x) to bank
  - Bank signs the note c(x) as s''(c(x)), debits payer's account
  - Bank returns s''(c(x)) to payer
  - Payer strips as c''(s''(c(x))) = s''(x)

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

  - Payer chooses a random x and forms c(x)
  - Payer gives note c(x) to bank
  - Bank signs the note c(x) as s''(c(x)), debits payer's account
  - Bank returns s''(c(x)) to payer
  - Payer strips as c''(s''(c(x))) = s''(x)
  - Payer checks whether s(s''(x)) = x or not and stops if not.
  - Payer provides s''(x) to a payee to make a payment

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

  - Payer chooses a random x and forms c(x)
  - Payer gives note c(x) to bank
  - Bank signs the note c(x) as s''(c(x)), debits payer's account
  - Bank returns s''(c(x)) to payer
  - Payer strips as c''(s''(c(x))) = s''(x)
  - Payer checks whether s(s''(x)) = x or not and stops if not.
  - Payer provides s''(x) to a payee to make a payment
  - Payee checks whether s(s''(x)) = x or not and stops if not
  - Payee sends s''(x) to bank

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

- Payer chooses a random x and forms c(x)
- Payer gives note c(x) to bank
- Bank signs the note c(x) as s''(c(x)), debits payer's account
- Bank returns s''(c(x)) to payer
- Payer strips as c''(s''(c(x))) = s''(x)
- Payer checks whether s(s''(x)) = x or not and stops if not.
- Payer provides s''(x) to a payee to make a payment
- Payee checks whether s(s''(x)) = x or not and stops if not
- Payee sends s''(x) to bank
- Bank checks whether s(s''(x)) = x or not and stops if not

Digicash

- introduced by Chaum in 1982,
  'Blind Signatures for Untraceable Payments'

- Payer chooses a random x and forms c(x)
- Payer gives note c(x) to bank
- Bank signs the note c(x) as s''(c(x)), debits payer's account
- Bank returns s''(c(x)) to payer
- Payer strips as c''(s''(c(x))) = s''(x)
- Payer checks whether s(s''(x)) = x or not and stops if not.
- Payer provides s''(x) to a payee to make a payment
- Payee checks whether s(s''(x)) = x or not and stops if not
- Payee sends s''(x) to bank
- Bank checks whether s(s''(x)) = x or not and stops if not
- Bank checks whether x on the list or not and stops if it is
- Bank credits account to payee

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

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

Untraceable Electronic Cash †
(Extended Abstract)

David Chaum[1] *Amos Fiat*[2] *Moni Naor*[3]

[1] Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
[2] Tel-Aviv University
Tel-Aviv, Israel
[3] IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120

Introduction

The use of credit cards today is an act of faith on the part of all concerned. Each party is vulnerable to fraud by the others, and the cardholder in particular has no protection against surveillance.

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

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)

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

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

fungible ? practical ?