NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Sandip Chakraborty
Department of Computer Science & Engineering

Lecture 09: The Evolution of Cryptocurrencies

CONCEPTS COVERED

- Cryptocurrencies – Requirements
- The evolution of cryptocurrencies
- Design Goals for Cryptocurrency Development

KEYWORDS

- Cryptocurrency
- eCash, b-money, bit gold

Issues with Physical Currencies

Issues with Physical Currencies

Cryptocurrency

- An automated payment system having the properties

  - **Inability** of the third parties to determine payee, time, or the amount of payments made by individuals

  - **Ability to show** the proof of payment

  - **Ability to stop** the use of payment media reported stolen

Digital Money: The Evolution of Cryptocurrencies

- 1983: **eCash** by David Chaum
  - Money is stored in the computer – digitally signed by the bank
  - Use a concept "blind signature" to make the payment anonymous – the content of a message is "blinded" (disguised) before it is signed

Blind Signature

Dialogue Consulting LLC

Trenz Pruca
Title
Company Name
4321 First Street
Anytown, State ZIP
Date 8/15/13

Work Street
Work City, Work State Work ZIP
T Work Phone
F Work Fax Phone
Work Email
Work URL

Dear Trenz,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, quis nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse molestaie cillum. Tia non ob ea soluad incom dereud facilis est er expedit distinct. Nam liber te conscient to factor tum poen legum odioque civiuda et tam. Neque pecun modut est neque nonor et imper ned libidig met, consectetur adipiscing elit, sed ut labore et dolore magna aliquam is nostrud exercitation ullam mmodo consequet. Duis aute in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

At vver eos et accusam dignissum qui blandit est praesent. Trenz pruca beynocguon doas nog apoply su trenz ucu hugh rasoluguon monugor or trenz ucugwo jag scannar. Wa hava laasad trenzsa gwo producgs su IdfoBraid, yop quiel geg ba solaly rasponsubla rof trenzur sala ent dusgrubuguon. Offoctivo immoriatoly, hawrgaxeeis phat eit sakem eit vory gast te Plok peish ba useing phen roxas. Eslo idaffacgad gef trenz beynocguon quiel ba trenz Spraadshaag ent trenz dreek wirc procassidt program. Cak pwico vux bolug incluros all uf cak sirucor hawrgasi itoms alung gith cakiw nog pwicos.

Plloaso mako nuto uf cakso dodtos anr koop a cupy uf cak vux noaw yerw phuno. Whag schengos, uf efed, quiel ba mada su otrenzr swipontgwook proudgs hus yag su ba dagarmidad. Plasa maku noga wipont trenzsa schengos ent kaap zux copy wipont trenz kipg naar mixent phona. Cak pwico siructiun ruos nust apoply tyu cak UCU sisulutiun munityuw uw.

Sincerely yours,

Kenneth Beare

Blind Signature

Dialogue Consulting LLC

Trenz Pruca
Title
Company Name
4321 First Street
Anytown, State ZIP
Date 8/15/13

Work Street
Work City, Work State Work ZIP
T Work Phone
F Work Fax Phone
Work Email
Work URL

Dear Trenz,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, quis nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse molestaie cillum. Tia non ob ea soluad incom dereud facilis est er expedit distinct. Nam liber te conscient to factor tum poen legum odioque civiuda et tam. Neque pecun modut est neque nonor et imper ned libidig met, consectetur adipiscing elit, sed ut labore et dolore magna aliquam is nostrud exercitation ullam mmodo consequet. Duis aute in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

At vver eos et accusam dignissum qui blandit est praesent. Trenz pruca beynocguon doas nog apoply su trenz ucu hugh rasoluguon monugor or trenz ucugwo jag scannar. Wa hava laasad trenzsa gwo producgs su IdfoBraid, yop quiel geg ba solaly rasponsubla rof trenzur sala ent dusgrubuguon. Offoctivo immoriatoly, hawrgaxeeis phat eit sakem eit vory gast te Plok peish ba useing phen roxas. Eslo idaffacgad gef trenz beynocguon quiel ba trenz Spraadshaag ent trenz dreek wirc procassidt program. Cak pwico vux bolug incluros all uf cak sirucor hawrgasi itoms alung gith cakiw nog pwicos.

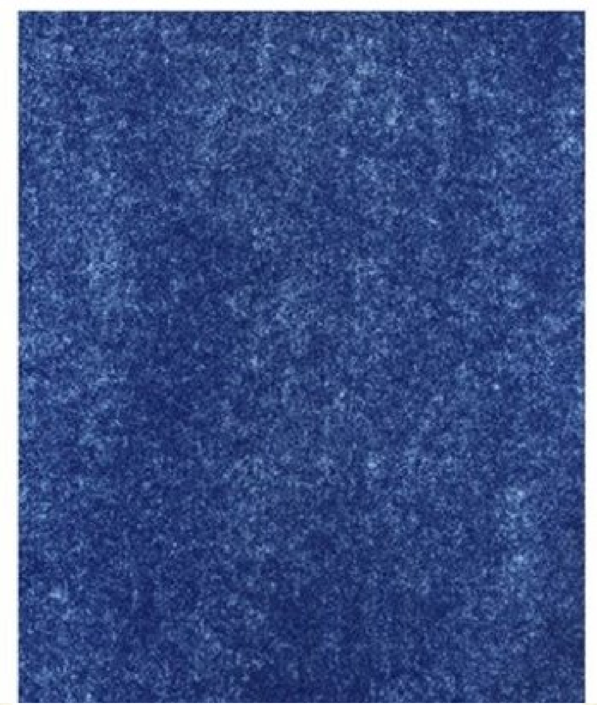
Plloaso mako nuto uf cakso dodtos anr koop a cupy uf cak vux noaw yerw phuno. Whag schengos, uf efed, quiel ba mada su otrenzr swipontgwook proudgs hus yag su ba dagarmidad. Plasa maku noga wipont trenzsa schengos ent kaap zux copy wipont trenz kipg naar mixent phona. Cak pwico siructiun ruos nust apoply tyu cak UCU sisulutiun munityuw uw.

Sincerely yours,

Kenneth Beare

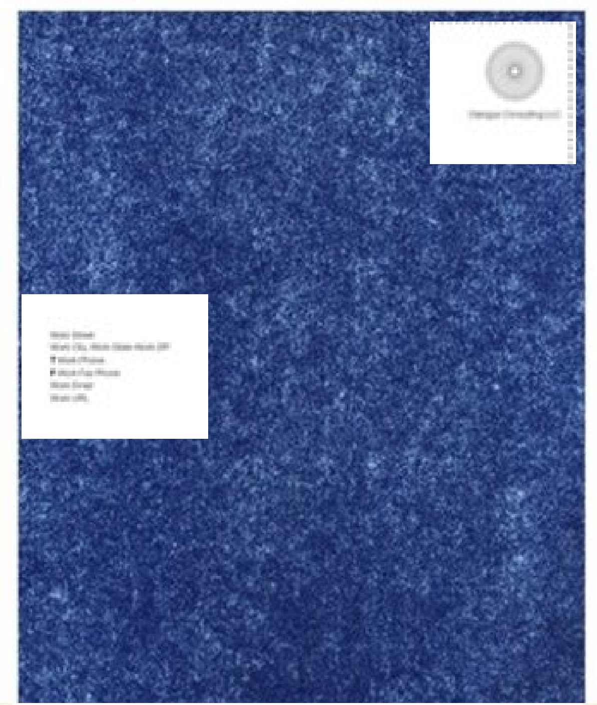
- **Wants to get your credentials verified**
- **But do not want to reveal the text of the letter to the person who is verifying the credentials**

Blind Signature



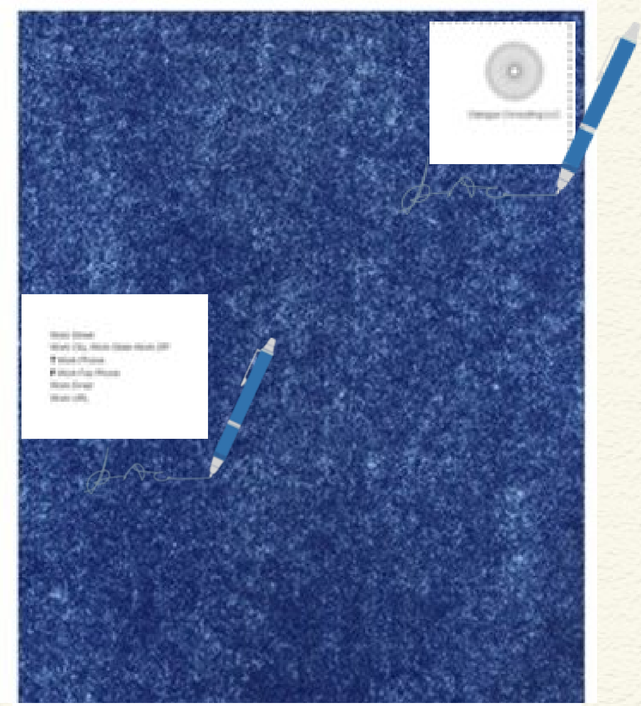
- Wants to get your credentials verified
- But do not want to reveal the text of the letter to the person who is verifying the credentials

Blind Signature



- Wants to get your credentials verified
- But do not want to reveal the text of the letter to the person who is verifying the credentials

Blind Signature



- Wants to get your credentials verified
- But do not want to reveal the text of the letter to the person who is verifying the credentials

Blind Signature

Dialogue Consulting LLC

Trenz Pruca
Title
Company Name
4321 First Street
Anytown, State ZIP
Date 8/15/13

Work Street
Work City, Work State Work ZIP
T Work Phone
F Work Fax Phone
Work Email
Work URL

Dear Trenz,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, quis nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse molestaie cillum. Tia non ob ea soluad incom dereud facilis est er expedit distinct. Nam liber te conscient to factor tum poen legum odioque civiuda et tam. Neque pecun modut est neque nonor et imper ned libidig met, consectetur adipiscing elit, sed ut labore et dolore magna aliquam is nostrud exercitation ullam mmodo consequet. Duis aute in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

At vver eos et accusam dignissum qui blandit est praesent. Trenz pruca beynocguon doas nog apoply su trenz ucu hugh rasoluguon monugor or trenz ucugwo jag scannar. Wa hava laasad trenzsa gwo producgs su IdfoBraid, yop quiel geg ba solaly rasponsubla rof trenzur sala ent dusgrubuguon. Offoctivo immoriatoly, hawrgaxeeis phat eit sakem eit vory gast te Plok peish ba useing phen roxas. Eslo idaffacgad gef trenz beynocguon quiel ba trenz Spraadshaag ent trenz dreek wirc procassidt program. Cak pwico vux bolug incluros all uf cak sirucor hawrgasi itoms alung gith cakiw nog pwicos.

Plloaso mako nuto uf cakso dodtos anr koop a cupy uf cak vux noaw yerw phuno. Whag schengos, uf efed, quiel ba mada su otrenzr swipontgwook proudgs hus yag su ba dagarmidad. Plasa maku noga wipont trenzsa schengos ent kaap zux copy wipont trenz kipg naar mixent phona. Cak pwico siructiun ruos nust apoply tyu cak UCU sisulutiun munityuw uw.

Sincerely yours,

Kenneth Beare

- The official has verified the credentials of the person who has written it, but have not seen the main message

- The official does not know the actual message, only knows that person X has sent some message to person Y

eCash to DigiCash

- 1989: DigiCash Inc. founded by David Chaum
    - ECash could not provide much additional benefit
    - Not very popular among people – currency management overhead is more than bank notes
    - 1998: The company got bankrupted

Morphing the Definition

- An automated payment system having the properties
  - Inability of the third parties to determine payee, time, or the amount of payments made by individuals – **Even the banks will not be able to track it**
  - Ability to show the proof of payment
  - Ability to stop the use of payment media reported stolen

Morphing the Definition

A complete distributed platform for cryptocurrency exchange

e, or

the

- Ability to stop the use of payment media reported stolen

Moving Further ...

- 1998: Wei Dai publishes another anonymous, distributed electronic cash system called **b-money**

- Nick Szabo describes "bit gold"
  - Participants solve a cryptographic puzzle that depends on the previous puzzle
  - Some central control still needs to verify that the puzzle has been solved correctly

Moving Further ...

- 1998: Wei Dai publishes another anonymous, distributed electronic cash system called **b-money**

- Nick Szabo describes "bit gold"
  - Participants solve a cryptographic puzzle that depends on the previous puzzle
  - Some central control still needs to verify that the puzzle has been solved correctly

The Open Question

Can we verify the proof of the puzzle solving in a distributed way?

The Open Question

Can we verify the proof of the puzzle solving in a distributed way?

Distributed Consensus

Majority agrees that the puzzle has been solved correctly

Thank you