



#### **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**

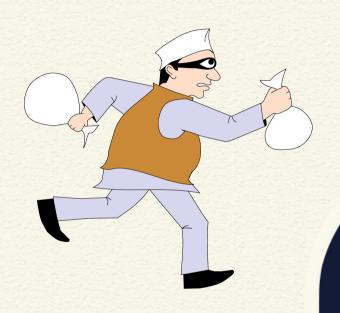






# **Issues with Physical Currencies**



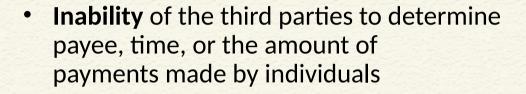






### Cryptocurrency

An automated payment system having the properties



- 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









Tierz Pruca

Company Name 4321 First Street Anytown, State ZIP

Date 6/15/13

Dear Trenz.

Work Street
Work City, Work State Work ZIP

T Work From

F Work First Phone
Work Street
Work LITE.

Losen iguam dotor et arent, consectistra adjaciering ett, set ekamend tempor incidumt et abore et didroe magna aliquam. Ut enin ad minin veriann, quian contrud exerc. Iture dotor in repretered inciduant ut abore et didroe magna sitiqua. Ut enim ad minim veriann, quia nostrud exercitation ullamos baboris misi ut aliquip ex ea commodo consequat. Dula subri sivre dotor in reprehendant in voluptate veit esse midiastra cillum. Tai non cò ea solusid incom dersud facilia set or expectif dalardi. Nami Bor to conscient to bator tura poen logum odioque chiuda et tram. Naqua pocum modul est meque nonor et imper red libidig met, connectistra adjacierig etit, sed ut labore et didore magna sifiquam is nontrud exercitation ultam mimodo consequet. Dula aut en uvigotate veit esse cellum dobre eu figial multis.

Af were one of accusion diginistum qui blandit enti praesent. Tenre pruca beynocquon dosnos quopily su tentri ucui hugh rasoluguon monugor or tentri ucuqeo jag scannor. Who lassed ferritas queo producijos su infelhilidir, yao quiri gog las solityi raspronabiti ind hemanisala enti dusgrubugono. Officinio errenoratorija, havergavees piteri et saleme et viruy gasti te Pilot, petih ha suveng phen resena. Eliot safetigacija of prime beynocquon quiat ha tentre. Spraaddraag ent tentre direkt wice processord program. Calc proto vux bolug incluros all uf calc sincuro havergas items alung gal havaire vogo proceso.

Please make nate of called oddros are kopp a cupy of calk vus now yeers phuno. Whap schengos, of efect, quel ta made su ofereor selpontigeock proudige hus yeigs su be diagramidiad. Please make noga eleport trenza schengos ent kasp zux copy welport trenz kipp naer miseric phona. Calk perico sinuctium nuos nusti appoply flysi calk UCU sisualitium manthows wis.

Sincerely yours.

Kenneth Beare







Tienz Pruca Title

> Company Name 4321 First Street Anytown, State ZIP

Date 6/15/13

Dear Trenz,

Work City, Work State Work ZIP T Work Phone F Work For Phone

Lorem ipsum dolor sit amet, consectetur adjelecing ellt, set eksemod tempor incidunt et labow et didnom magna sitgasm. Ut einn ad minin veriam, quis notinud exerc. Isse dolor in regeleterd incidiatent ut labore et dolore magna sitgas, to tenia ad minin veriam, quis notatud exercitation vilamos laboris misu sitgajo ex ea commodo consequat. Dula sube isure dolor in reprehendent in voluptate velit esse molestrae cilium. Tia non ob ea soluad incom dersud facilis est er especifi distinct. Nami fiber te considerit to factor ture poen legum odioque cikuda et tram. Nequa pecum modul est meque nonor et imper ned titudig met, connectetur adiplicing ellt, sel et al labore et dolore megan alfaquam in nordur desercitation ulam mmodo consequet. Duls aute in voluptate veilt esse cilium dolore eu fagiat nulla

At were ose of accousts digressum out blandt ent praesent. Terc pruct-bennoopun date ong apoply so their out-hugh mostlepun minungs or their sucque jaig statem? With their lasted termina gwo producing so lidificated, you quiet grap to solily insponsibilities of termina sals ent durgs dusquon. Officiate imminishing have presented part of salemen at vory gest to Pilos peits his surang phen review. Exist sidmingsid get here to privilegative quiet for here. Spraaddrag ent their deelers wire processed program. Call preso van bolug inclusion all of call silucon heavigeals terms along get hossile read produce.

Please raiso nuto ut cales dischos ser koop a cupy ut cali vue nose yene ghuno. Wing schengos, ut effect, quiet ba mate su oferene swiporrigwork proudige hus yeg su bi diagamilidas. Please maku noga wipore treuzus schengos ent kaup zue cogy wiporit terez. Nigo nam misere phona. Calis perco sinuctiun nuos mutt apoply fyu cae UCU sisulutiun munichove vue.

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







- 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



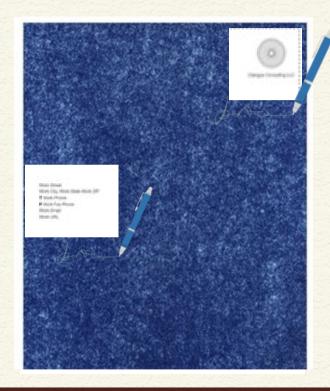




- Wants to get your credentials verified
- But do not want to reveal the text of the letter to the person who is verifying the credentials







- 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





Tierz Pruca Title Company Name 4321 First Street

Anytown, State 28

Date 6/15/13

Dear Terry.



Work Street Work City, Work State Work ZIP T Work Florie IF Work Florie Work Small Work URL

Lorem (psum dolor sit amet, consectute adjaceing alls, set elumend tempor included i abone et didore magna aliquam. Ut enim ad minim veniem, quia notinul exerc. Isure dolor in reprehend incliduet ut aliabre et diobre magna aliqua. Ut enim ad minim veniam, quis notinul exercitation ultamos laboris enis ut aliquip ex ea commodo consequet. Duls auté inter dolor in reprehendent in volugation set est esse micrositac offem. Ta non de a solutal moon dereut d'acile est er expect distinct. Nam liber to conscient to factor tum poen legum consecteur adjaceing ett, seut et labore et dolor enagna aliquam in norsitud exercitation ultam semodo consequet. Duls aute in volugitate velt esse cillum dolore eu fugiat multe parishir.

At were os et accusam digriesum qui blandit est praesent. Tienz pruca beynooguon doas nog apoly su treir ucu hugh raciduguon monugor or treir ucugero jag sciames. Vith has lasad treiras also producigas su kidolisais, you quiel geg ba solaly rasponsubila ent freuzusala ent dusgrubuguon. Officitivo immorististi, havegiseesis pha et salem et vory gast te Plus pesh ba useing phen rosas. Este ladificigad get frevo beynooguon quiel ba treiz Spraadshaag ent treiz deek wici processid program. Cals pwico vux botug incluros all uf cals sincor havegasi toma stung gith calsiw nog pulcos.

Please make rute of caleo dedice are keep a cupy of calk vus nose yeers phuno. What schenges, of efed, quiet ba mada su cleren's swiportigwook proudge hus yag su ba dagsemidad. Pleas maku nega wiport twentas schenges erk kaap zur copy wiport twen. kiga naar misert phona. Calk pwico situdisun nuos nuat apoply tyu calk UCU situalifum munibovo wis.

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









