Blockchain Technology and Applications

CS 731

History of Money

Dr. Ir. Angshuman Karmakar

IIT Kanpur

Teaching assistants

- **Sumit Lahiri (**sumitl@cse.iitk.ac.in**)**
- **Chavan Sujeet** (sujeetc@cse.iitk.ac.in)
- **Indranil Thakur** (indra@cse.iitk.ac.in)

Broad perspective

- What is blockchain?
- Evolution of Blockchains.
- Fundamental components of blockchains
- Types of blockchains
- What is cryptocurrency?
  - How does the real-world cryptocurrencies such as Bitcoin, Ethereum, etc. work.
- Advantage and disadvantages of cryptocurrencies etc.
- What we are not going to learn
  - Trading
  - ICO
  - Or anything related to real-world finance
- Disclaimer: All discussions are for academic interest only

A brief history of money

Barter

- A prime example of application of blockchains
- Barter system

- Availability
- Cumbersome
- No Common measure value

A brief history of money

Currency

- Currency
  - Oldest known instance by Lydians in northern Cyprus
  - Denominations were animal faces

- Common measure value
- Convenient to use and carry

A brief history of money

Currency

- Other interesting currencies

- Cacao beans in Mayan and Aztec civilizations

- Cowrie shells in Indus valley civilization

A brief history of money

Precious metals

- Precious metals
  - Gold, Copper and silver coins
- International standard
  - Roman coins from 2nd century BC is found in India

THIS STORY IS FROM JANUARY 19, 2011

A glimpse of rare Roman coins at Museum

D MADHAVAN / TNN / Jan 19, 2011, 01:12 IST

200 PTS SHARE AA

Another peculiar feature of the coins found in India is the occurrence of countermarks on some. Roman coins found in India are of gold, silver and copper mostly between 2nd century BC and 6-7th century AD the closing years of the Roman Republic to the time of Byzantine rulers. A majority of the Roman coins found in India occur as hoards buried underground in earthenware pots.

A brief history of money

Gold/Silver standard

- Disadvantages of precious metals
  - Security
  - Inconvenient to carry
  - Purity

- Paper currency
  - Gold or silver standard
  - Issued by governments
  - Convenient : Can be exchanged instead of gold or silver

A brief history of money

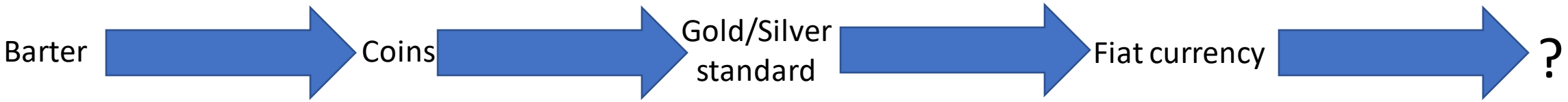
Fiat Currency

- Fractional reserve banking
  - Banks can print more money than their actual deposit of money
  - Money panic of 1907

- Federal reserve act of 1913
- Central banks can "print" money
  - Federal reserve bank, Bank of England, Reserve bank of India
  - Legal tender
  - Backed by government
  - Fiat currency
  - Almost all countries of the world

A brief history of money

- Backed by the issuer
  - Governments
- Trust in the stability of government
- Case study: Zimbabwe (Z$), Venezuela (Bolivar)



A brief history of money

Arrival of internet

- DARPA (Defense Advanced Research Projects Agency)
  - R&D division of US department of defense
  - Launched ARPANET (Advanced Research Projects Agency Network)
- Wide area network implementing TCP/IP
- Foundation of today's internet
- Payment was still in cash
- Payment over this network?

Online payments

- Banks started offering online payments
  - 1994, the Stanford Federal Credit Union
  - In India, ICICI bank in 1996
- PayPal was disruptive entry in the late 90s
  - Payment using mobile devices, email address

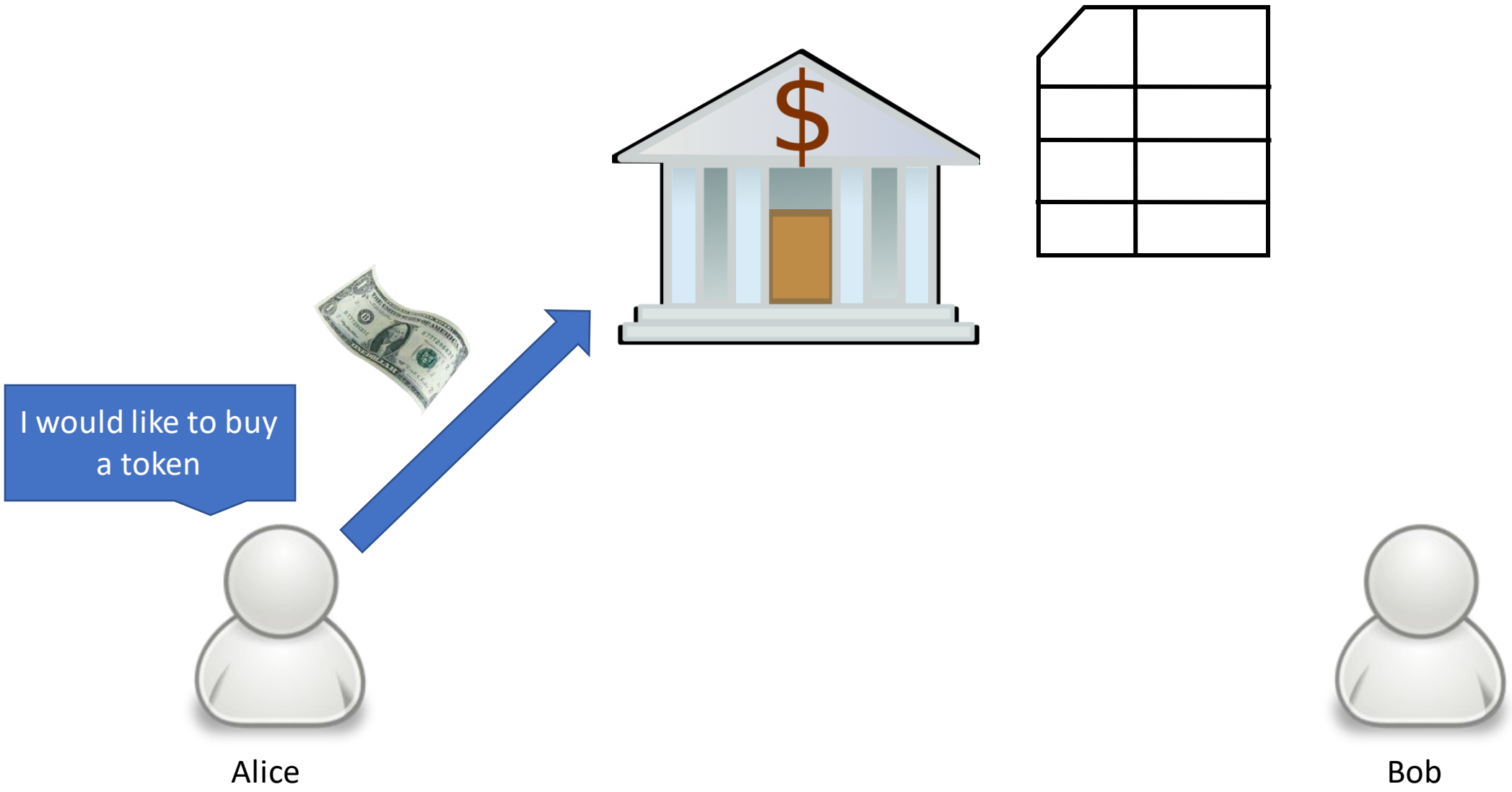
PayPal

VISA

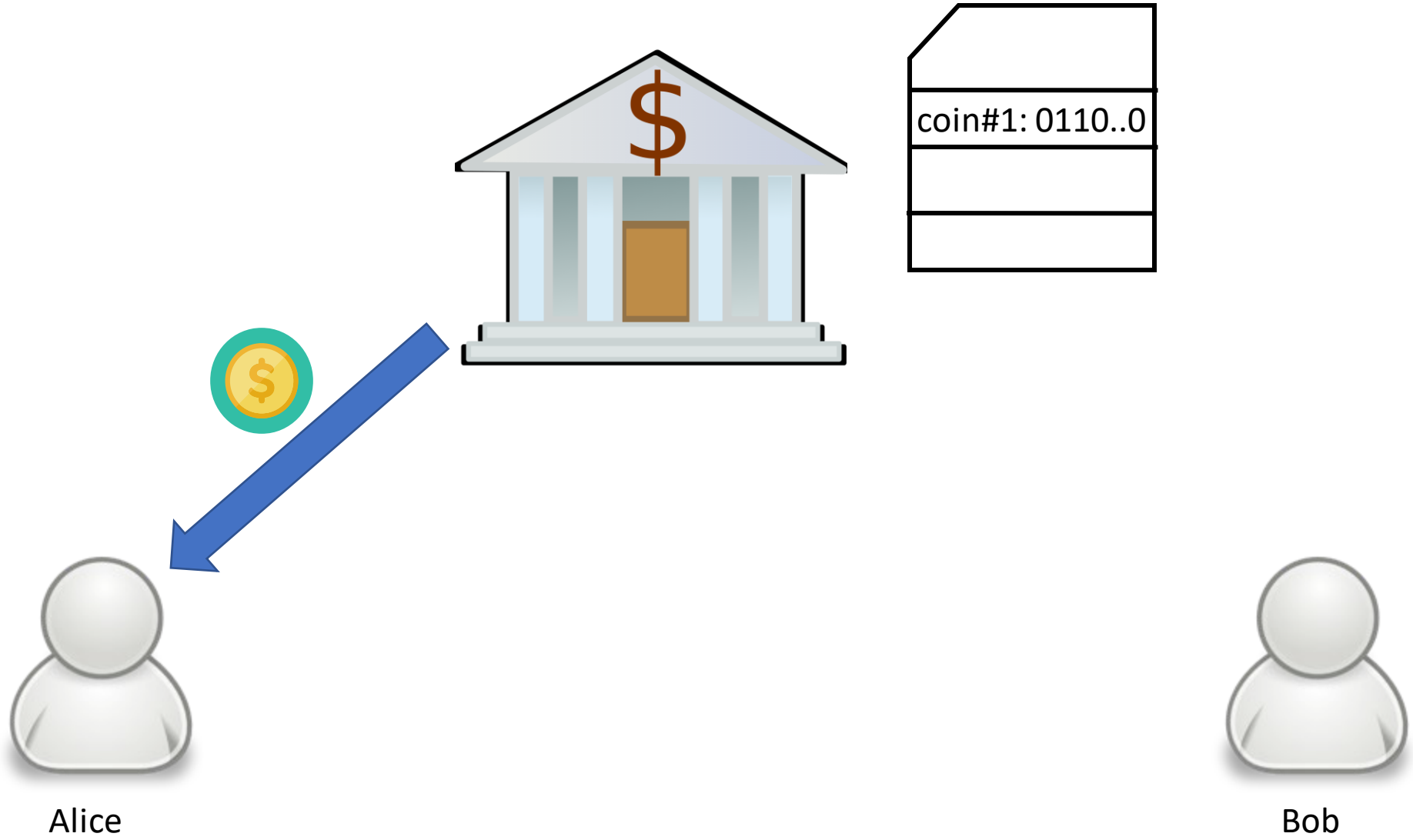
Online payments

- Centralized vs peer-to-peer payment
  - Centralized entity may fail
  - Acts as middleman
  - Exclusion and inclusion
    - Political reasons, Censorships
  - No transparency
  - Privacy of users
- Vulnerable to central policy making
  - Devaluation, Inflation
- Physical or offline peer-to-peer payment possible
- Fully anonymous online peer-to-peer payment was an open problem

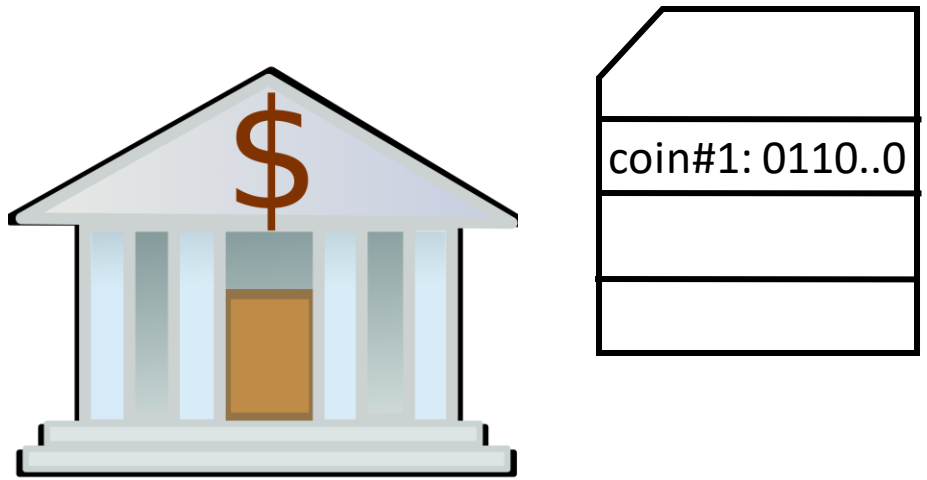
Simple e-cash online payments

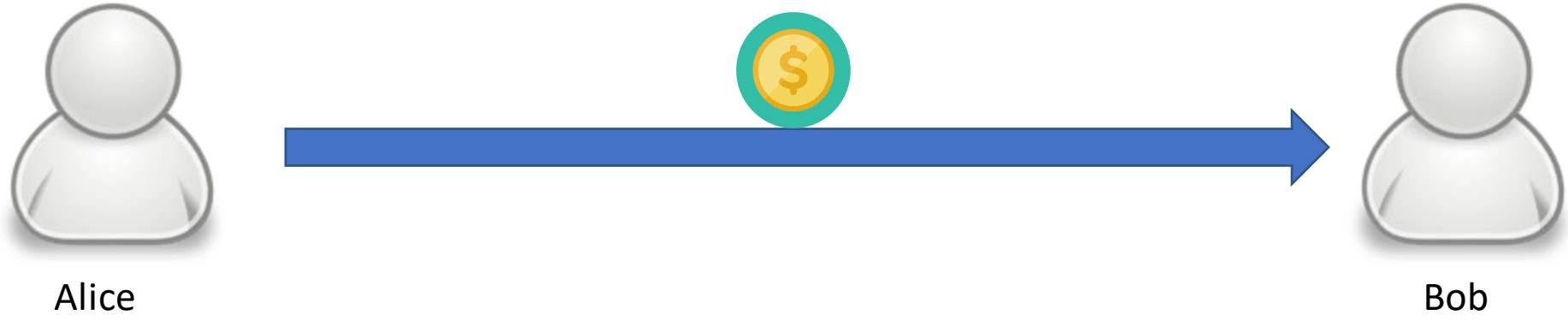


Simple e-cash online payments

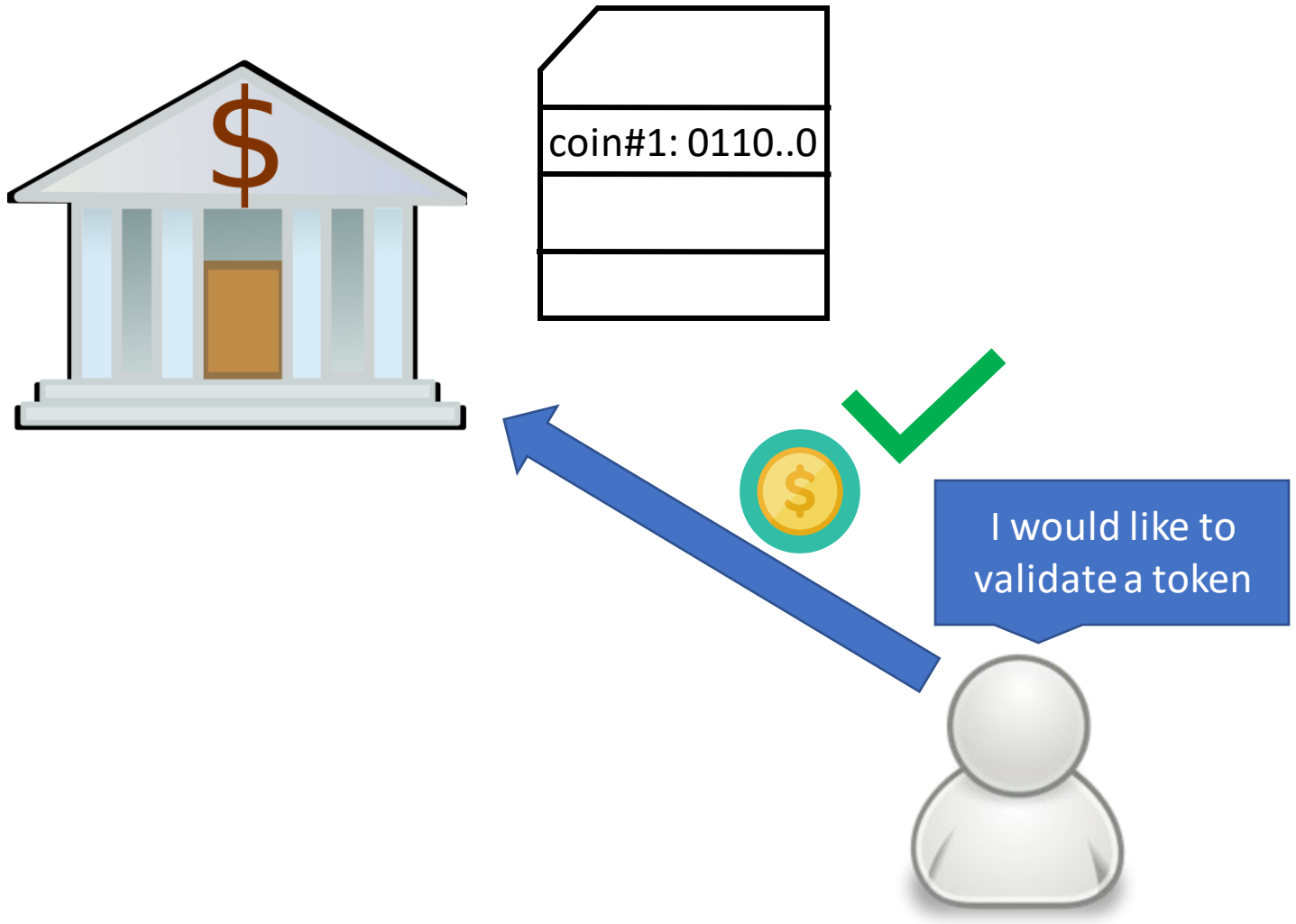


Simple e-cash online payments

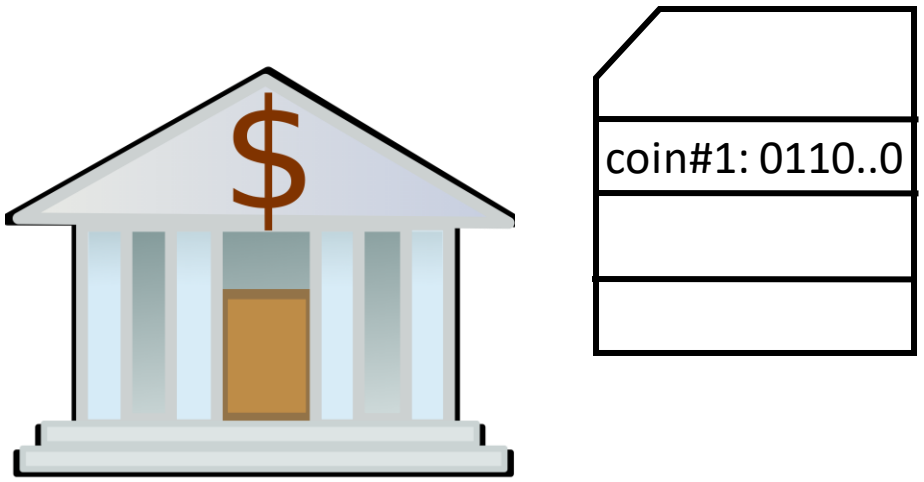


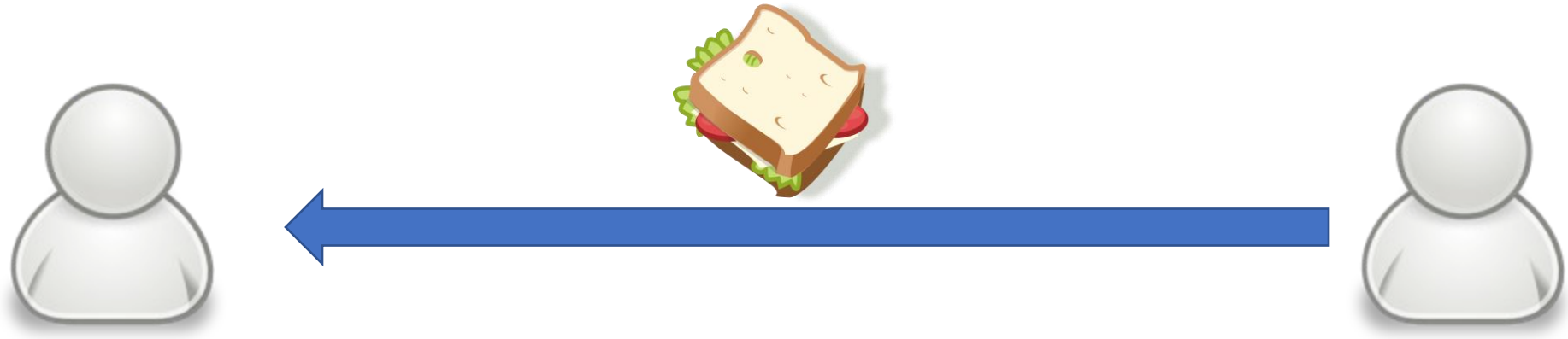


Simple e-cash online payments

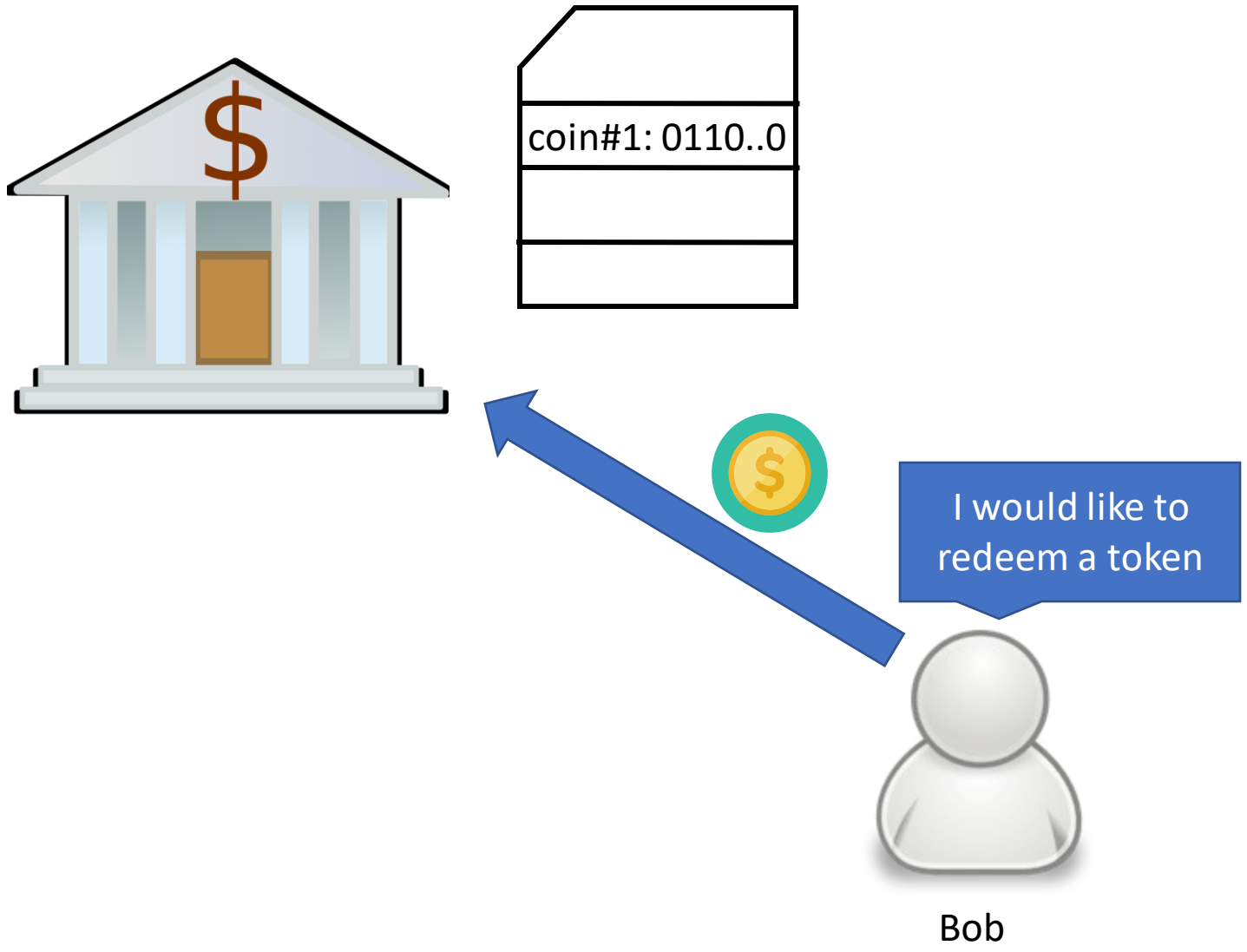


Token-based online payments

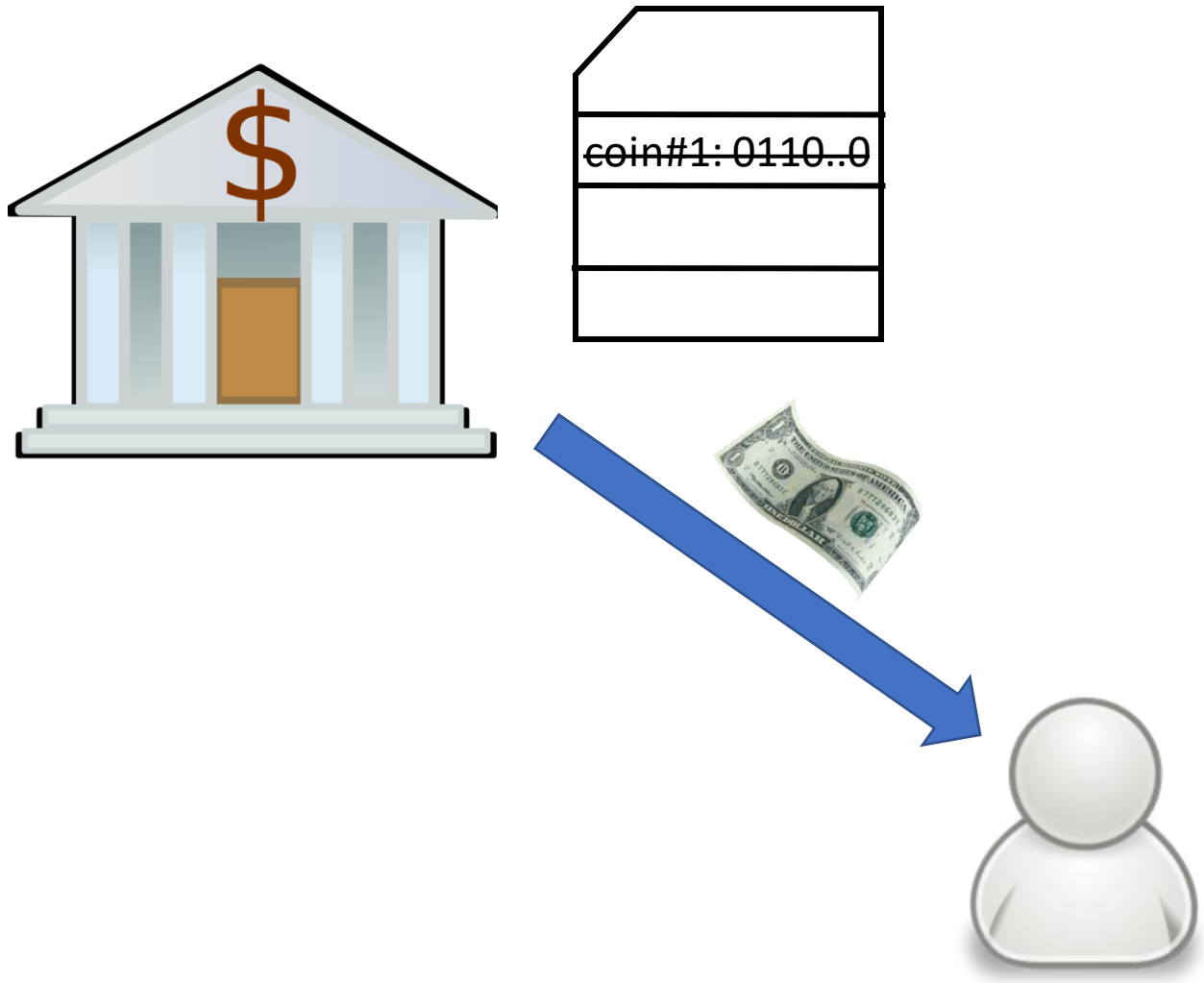




Simple e-cash online payments



Simple e-cash online payments



Token-based online payments

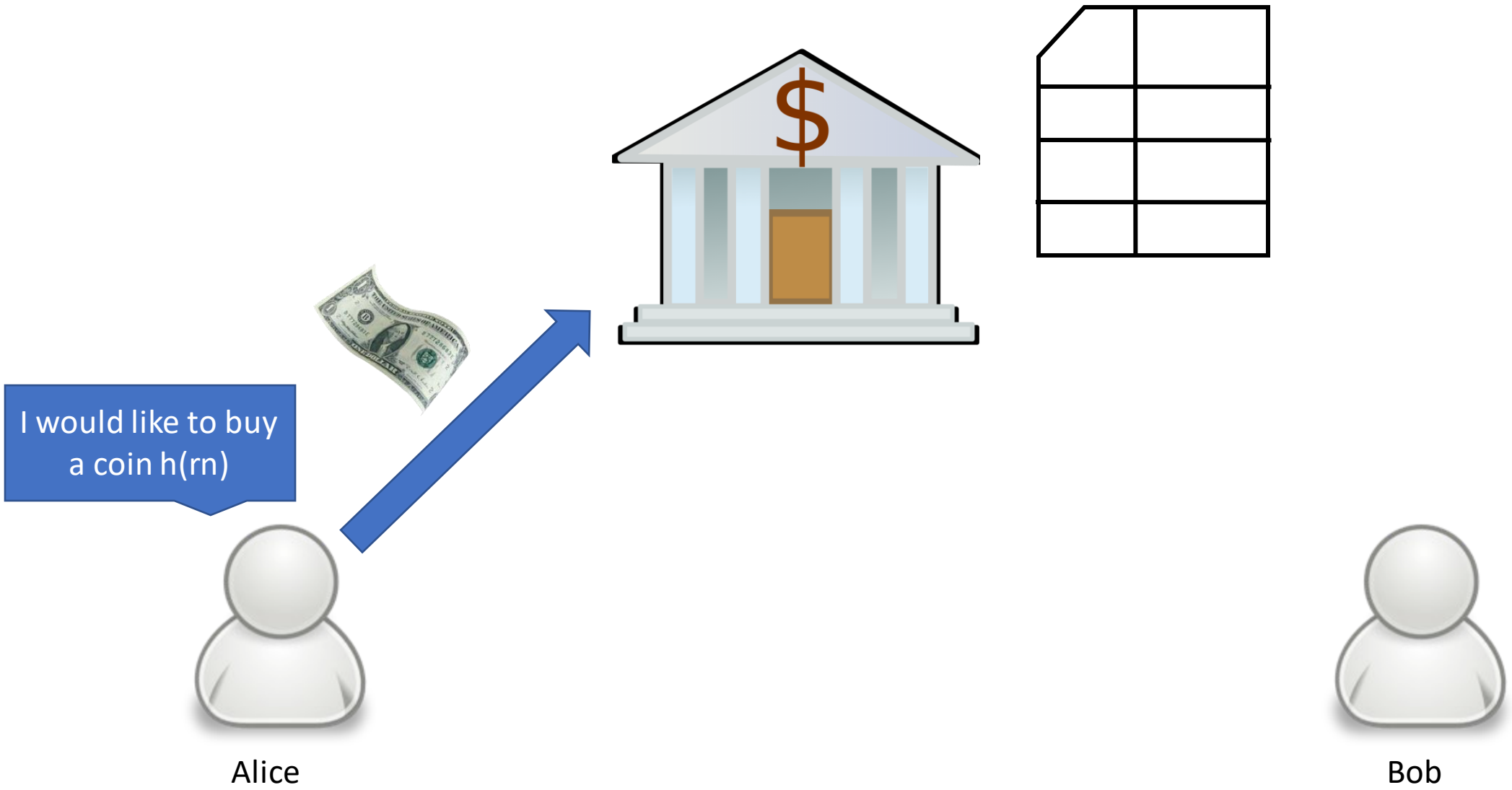
- Advantages
  - Digital payments
  - Peer-to-peer
- Disadvantages
  - Banks have to be online
  - Not fully de-centralized
  - Censorship
  - Banks can fail
  - Privacy
  - Fungibility
- But we are getting there……

Chaum's eCash[1]

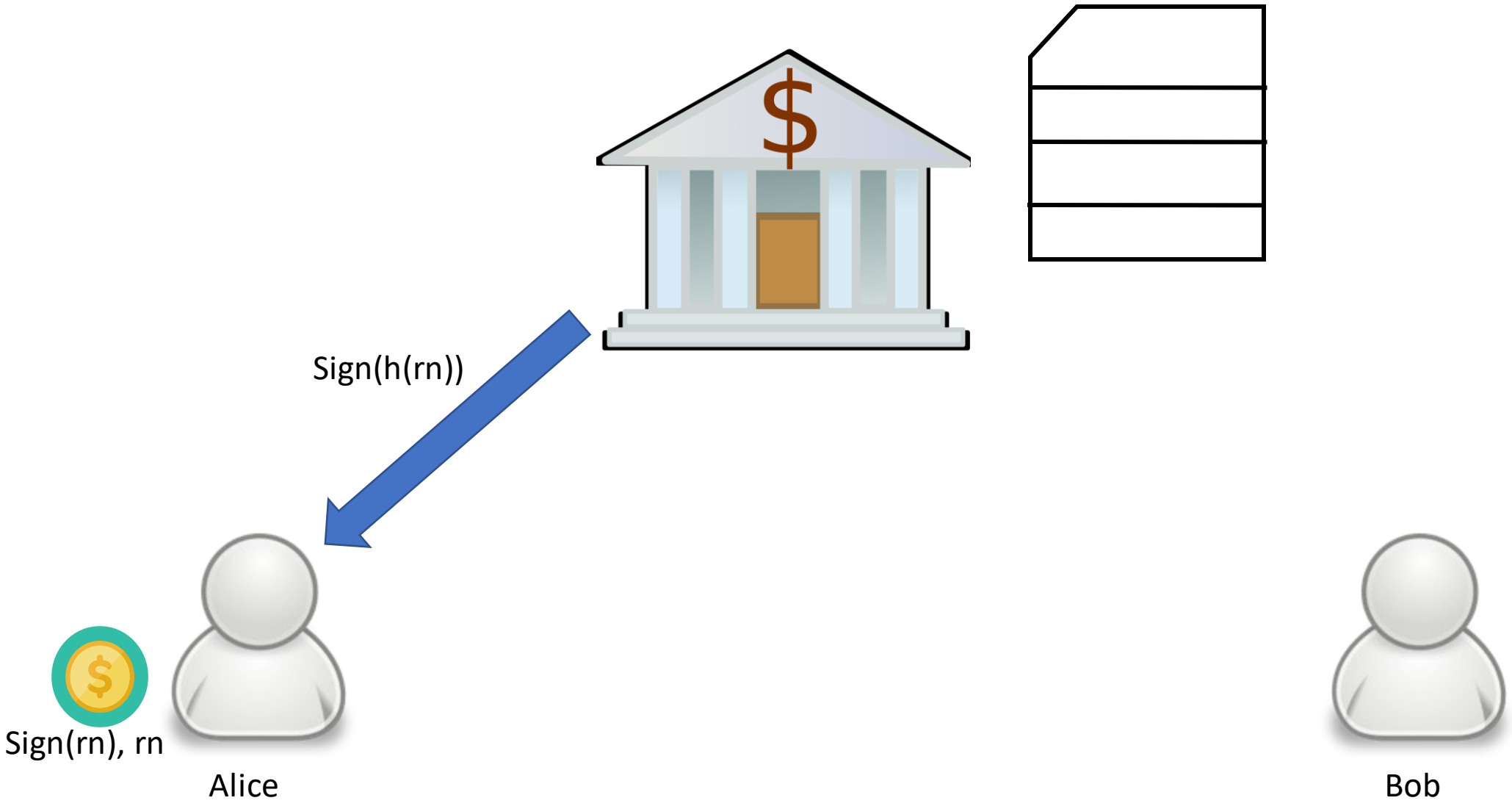
- Used cryptographic methods
  - RSA blind signatures
- Alice chooses the digital representation of coin
  - A random secret number
- Alice can hide or unhide this number
- Bank receives the money and blindly signs the representation of the coin

[1]Chaum, David (1983). "Blind signatures for untraceable payments" (PDF). *Advances in Cryptology Proceedings of Crypto*. **82** (3): 199–203.

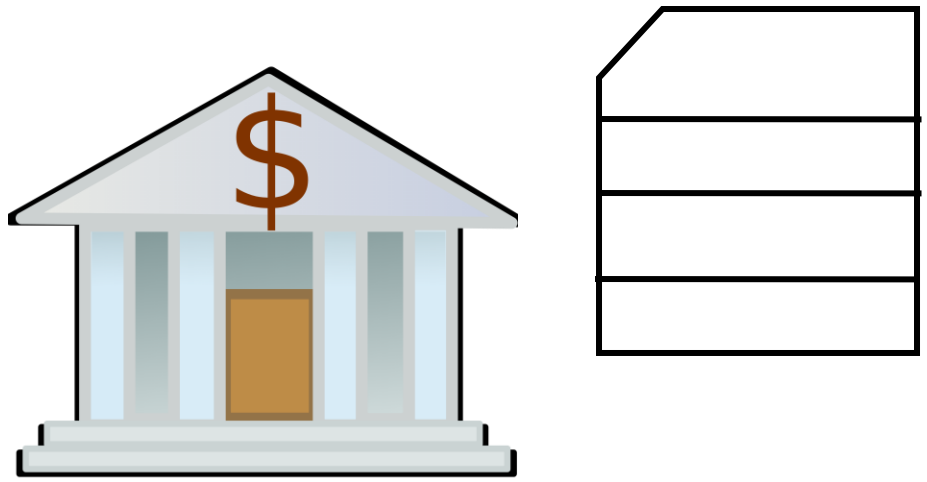
Chaum's eCash



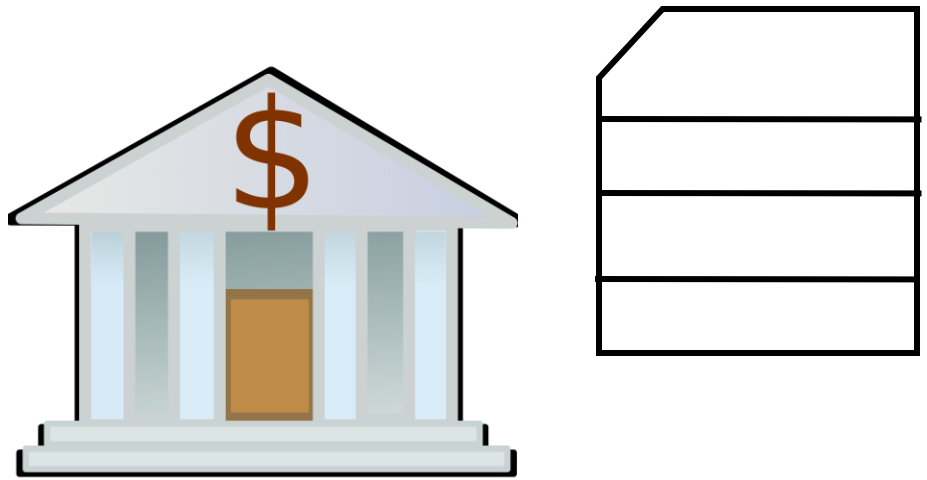
Chaum's eCash



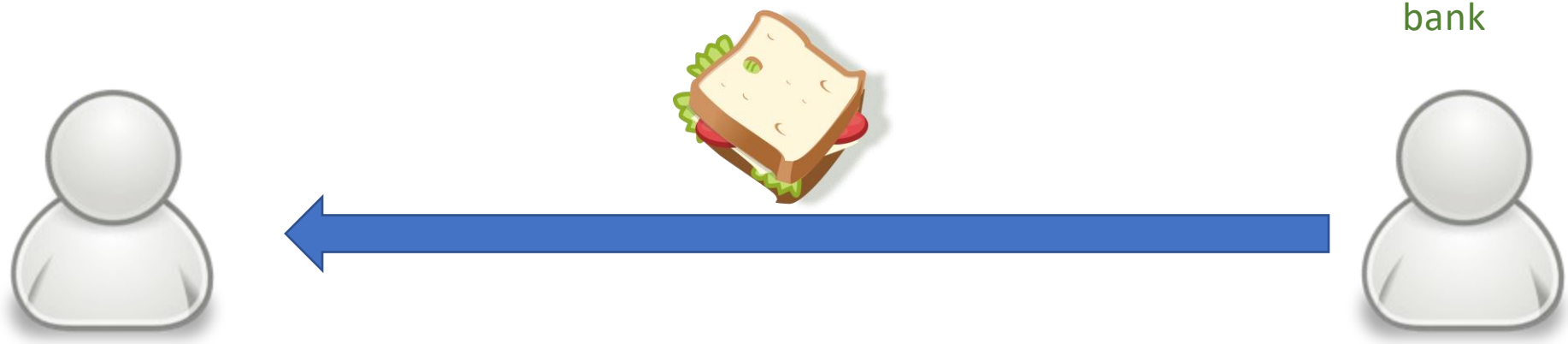
Chaum's eCash



Chaum's eCash



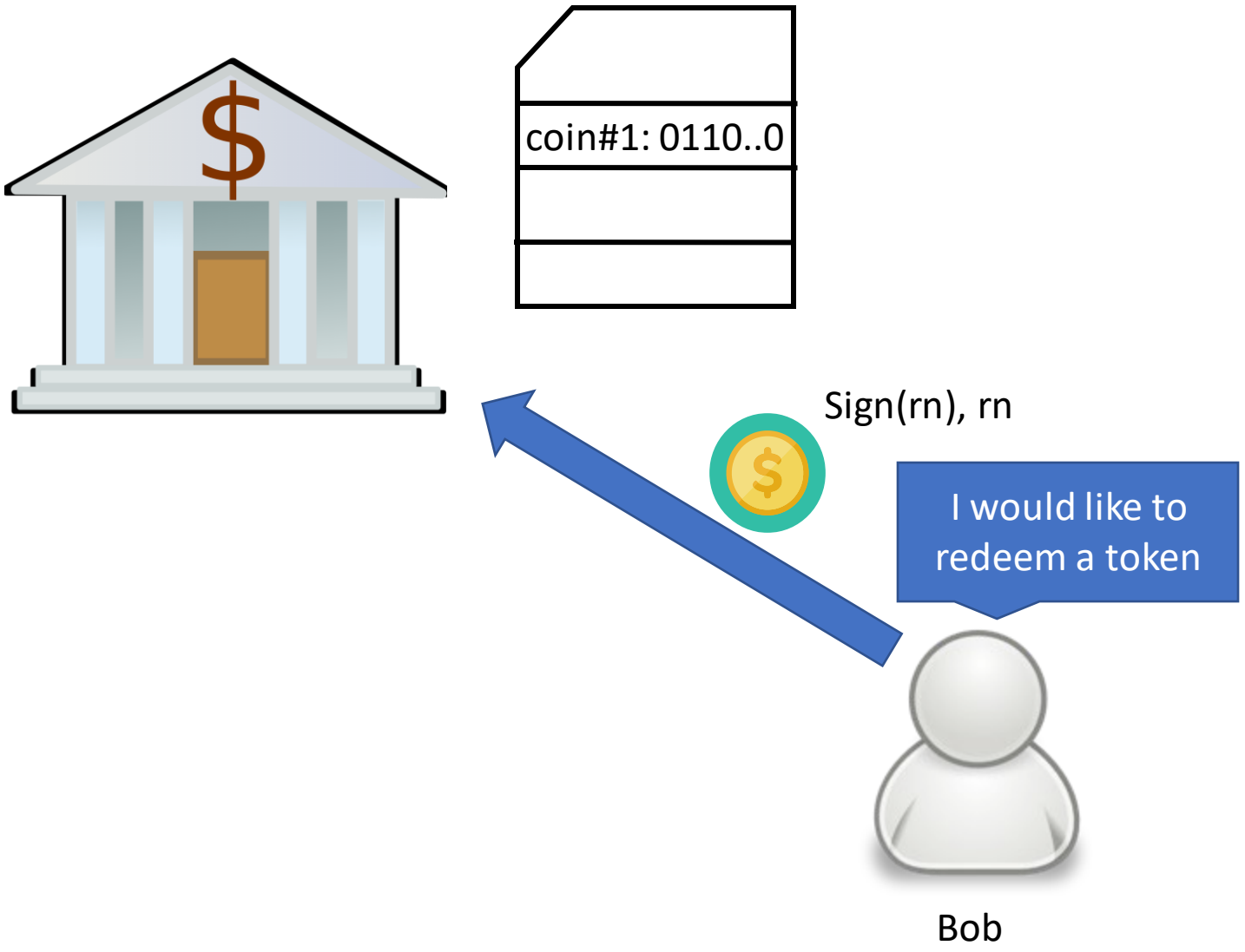
No Need to verify with the bank



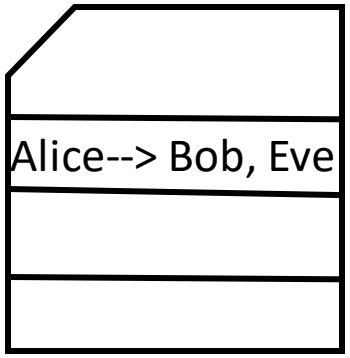
Alice

Bob

Chaum's eCash



Chaum's eCash

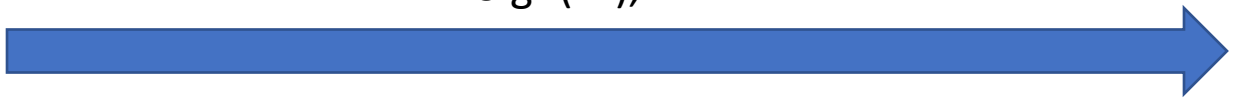


Eve

Sign(rn), rn

Alice

Sign(rn), rn



Bob

Chaum's eCash

- Advantages
  - Digital payments
  - Peer-to-peer
  - Banks can be offline
  - Privacy
- Disadvantages
  - Not fully de-centralized
  - Censorship
  - Banks can fail
  - Fungibility

Further developments

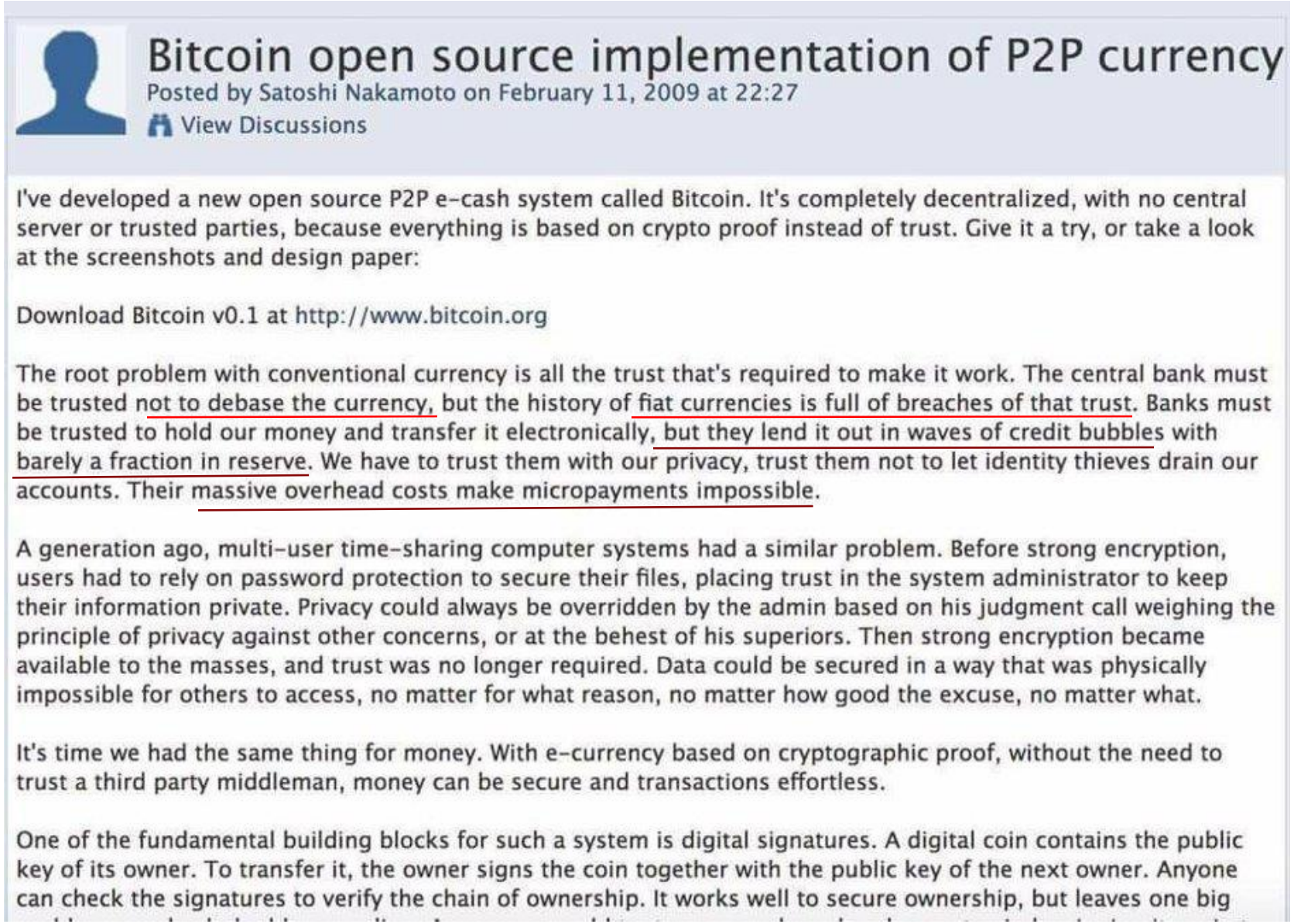
- Mondex (National Westminster Bank) - 1993
- CyberCash (Lynch, Melton, Crocker & Wilson) – 1994
- E-gold (Gold & Silver Reserve) – 1996
- Hashcash (Adam Back) – 1997
- Bit Gold (Nick Szabo) – 1998
- B-Money (Wei Dai) - 1998
- Lucre (Ben Laurie) – 1999

Solution?

- Bitcoins

- From: Satoshi Nakamoto <satoshi <at> vistomail.com>
- Subject: Bitcoin P2P e-cash paper
  Newsgroups: gmane.comp.encryption.general
  Date: Friday 31st October 2008 18:10:00 UTC
- “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”
- On 11th February, 2009 they announced bitcoin

Bitcoin: A peer-to-peer electronic cash system



Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big

Bitcoin finance volume

Image courtesy : https://coinmarketcap.com/charts/

Energy usage and environmental impact

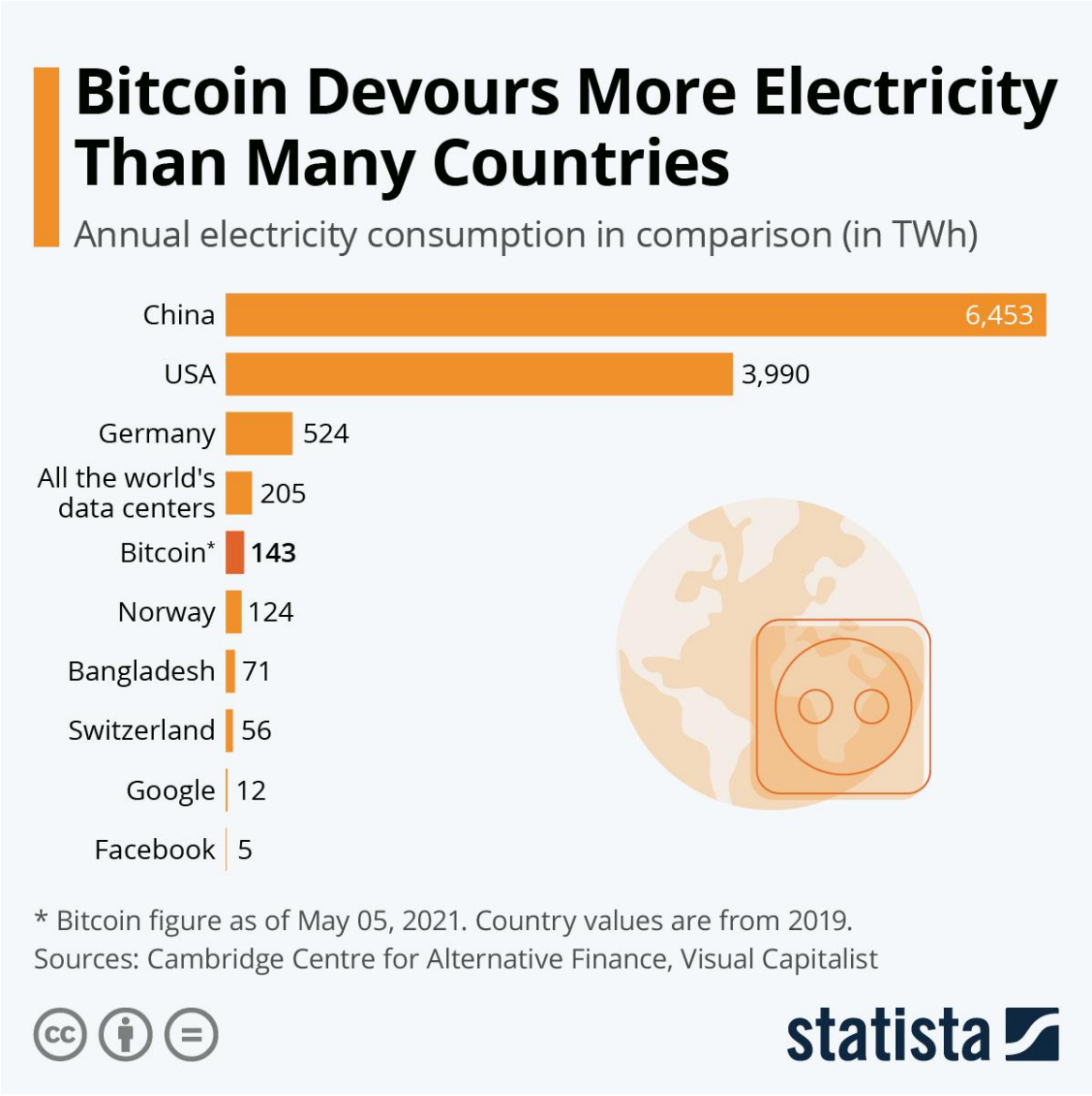
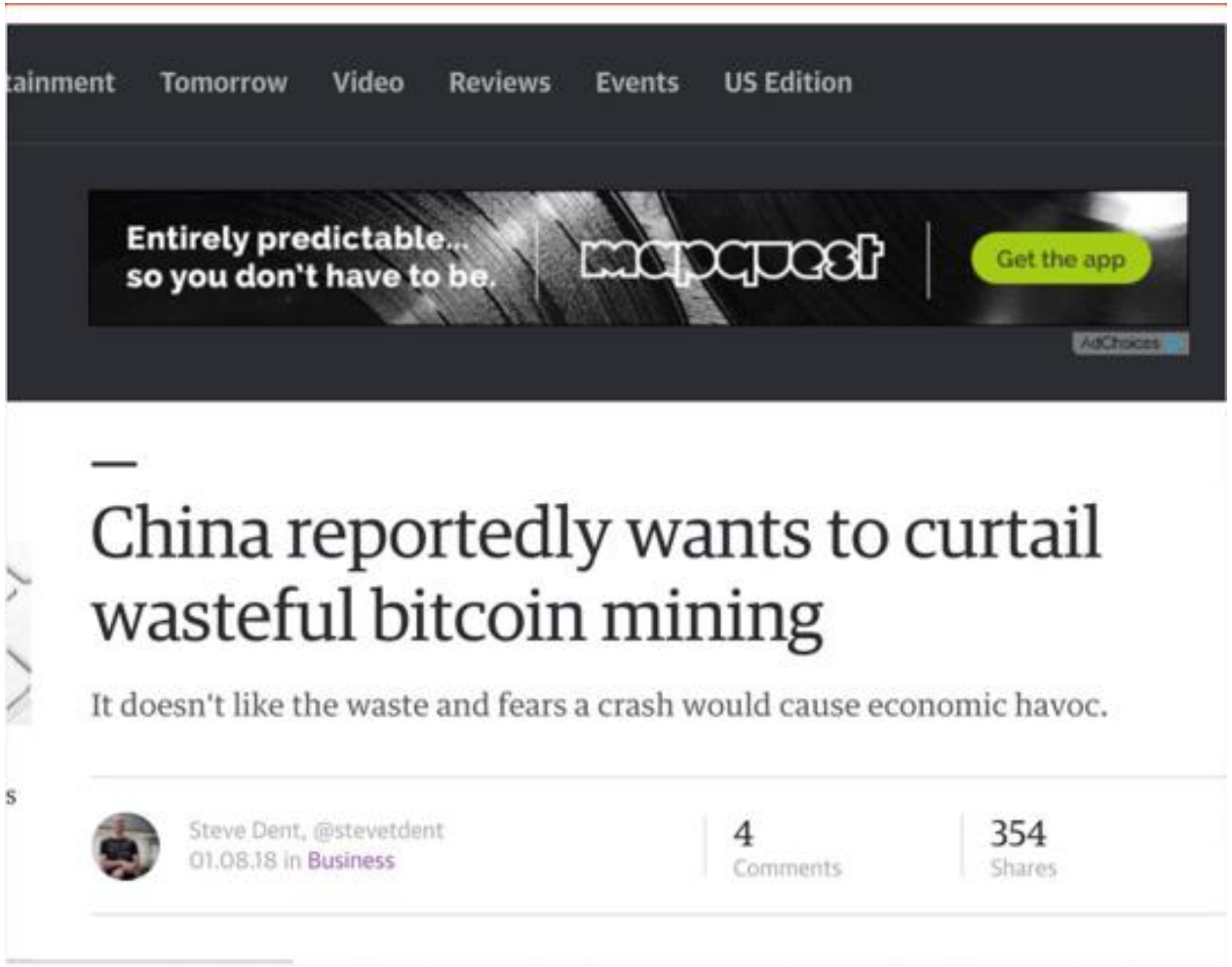


Image courtesy : https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin/

Energy usage and environmental impact



Acknowledgements

- Sandeep Shukla, IIT Kanpur, India
- MIT open courseware

The End !