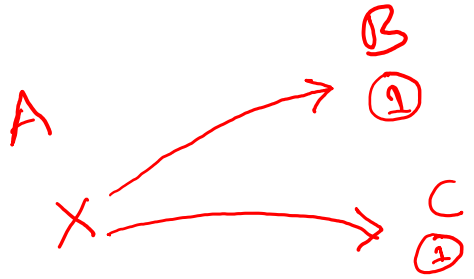
Bitcoin Blockchain

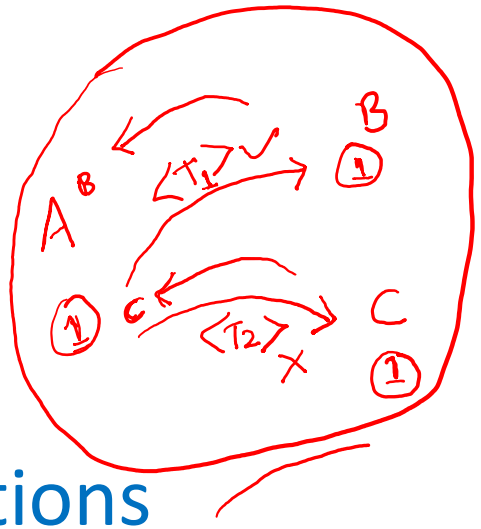
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

CHITTOOR, INDIAN

Online Transactions



- Physical cash
  - Non-traceable (well, mostly!)
  - Secure (mostly)
  - Low inflation
  - Can't be used online directly

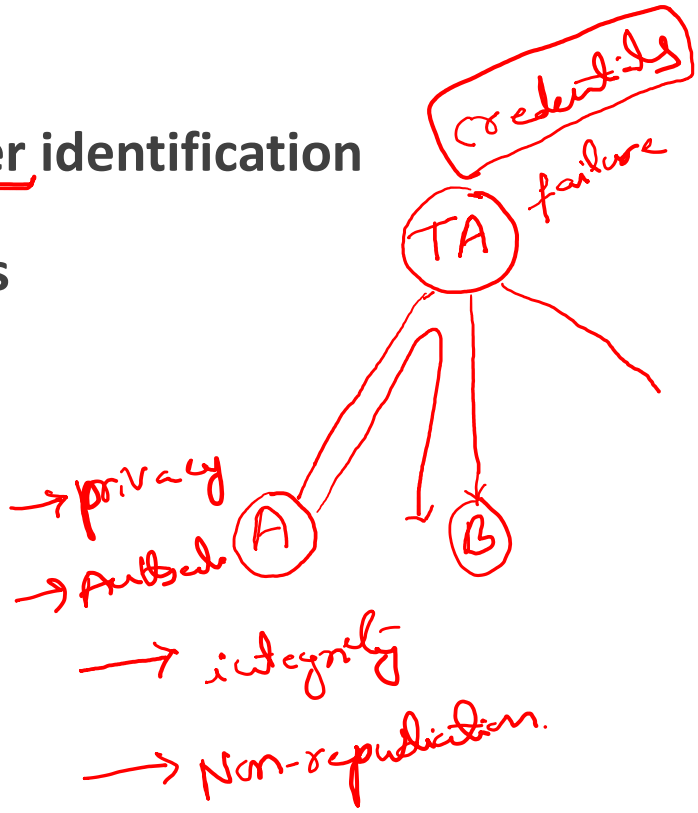


- Electronic credit or debit transactions
  - Bank sees all transactions
  - Merchants can track/profile customers

E-Cash Crypto Protocols

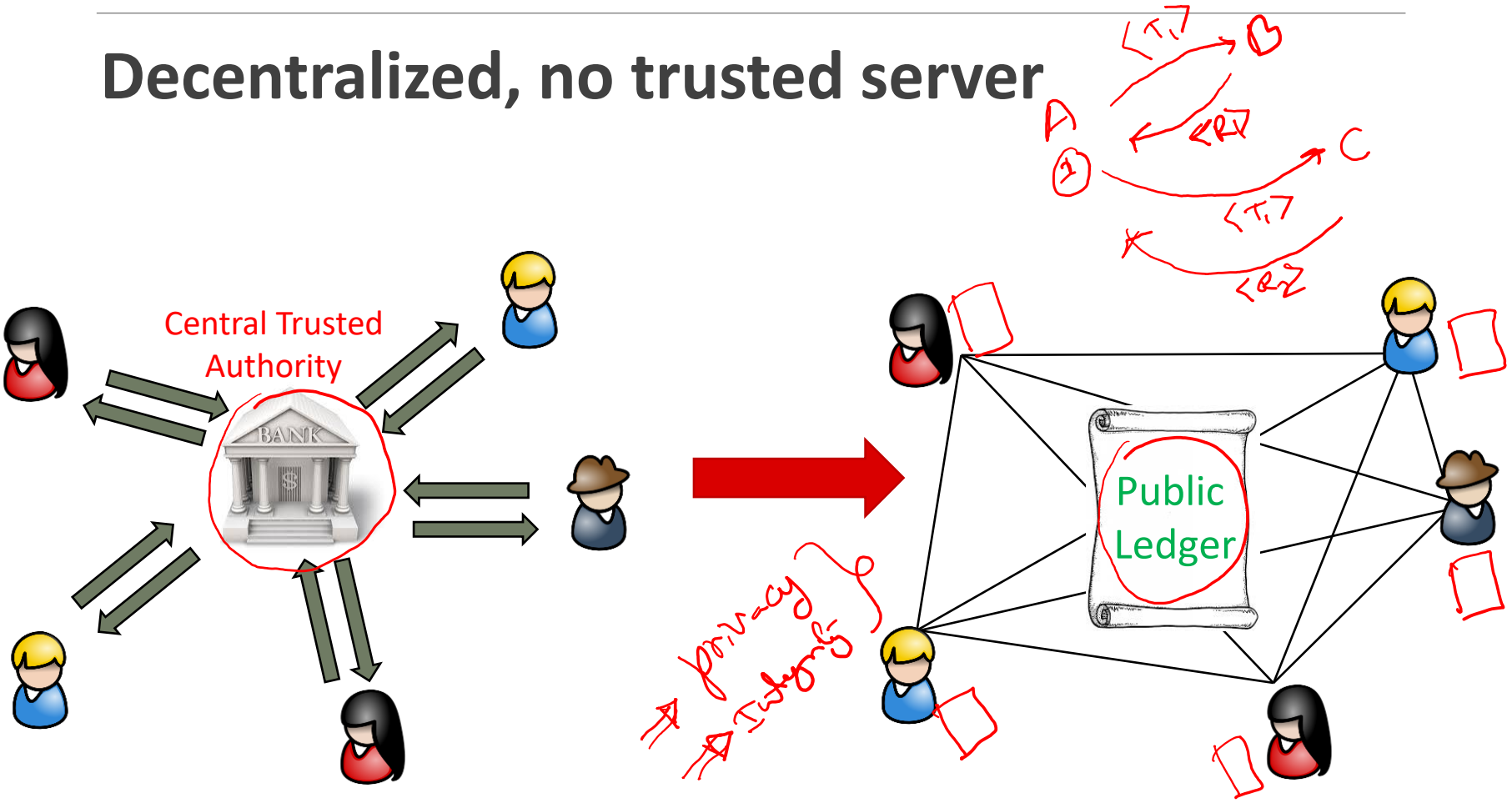
- **Chaum82:** Blind signatures for e-cash
- **Chaum88:** Retroactive double spender identification
- **Brandis95:** Restricted blind signatures
- **Camenisch05:** Compact offline e-cash

- **Various practical issues:**
  - **Need for trusted central party**
  - **Computationally expensive**



Applications: Cryptocurrencies

Decentralized, no trusted server



Bitcoin

- A distributed, decentralized digital currency system
- Released by **Satoshi Nakamoto 2008**
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction system

- Average price of a Bitcoin: around **$58,066**

Ref: https://coinmarketcap.com/currencies/bitcoin

BitCoin: Challenges

Creation of a virtual coin/note

- How is it created in the first place?
- How do you prevent inflation? (What prevents anyone from creating lots of coins?)

Validation

- Is the coin legit? (proof-of-work)
- How do you prevent a coin from double-spending?

Buyer and Seller protection in online transactions

- Buyer pays, but the seller doesn't deliver
- Seller delivers, buyer pays, but the buyer makes a claim.

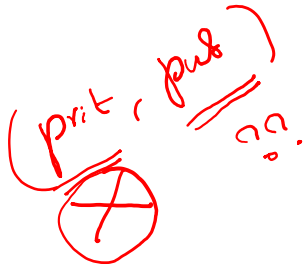
Trust on third-parties

- Rely on proof instead of trust
- Verifiable by everyone
- No central bank or clearing house

Security in Bitcoin

- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

Security in Bitcoin



- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability → Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality → Pseudonymity
  - Are my transactions private? Anonymous?

Acknowledgement

Some of the slides, content, or pictures are borrowed from the following resources, and some pictures are obtained through Google search without being referenced below:

L24-BitCoin and Security; UMASCS660-Secure Digital Currency: Bitcoin, many of the slides borrowed from this presentation with modifications.

Ian Miers, Zerocoin: Anonymous Distributed E-Cash from Bitcoin, IEEE S&P slides

THANK YOU