IEEE ICC®
IEEE International Conference on Communications
16–20 May 2022 // Seoul, South Korea // Hybrid: In-Person and Virtual Conference
Intelligent Connectivity for Smart World

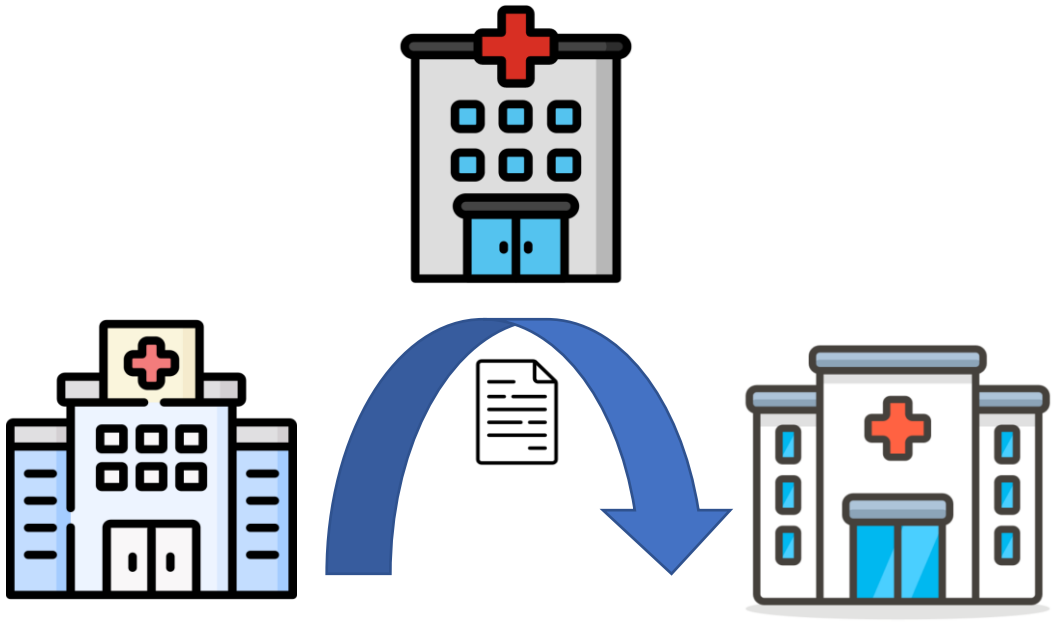
# BBS: A Blockchain Big-Data Sharing System



**Shan Wang, Ming Yang,** Southeast University, China
**Tingjian Ge, Yan Luo, Xinwen Fu,** UMass Lowell, US

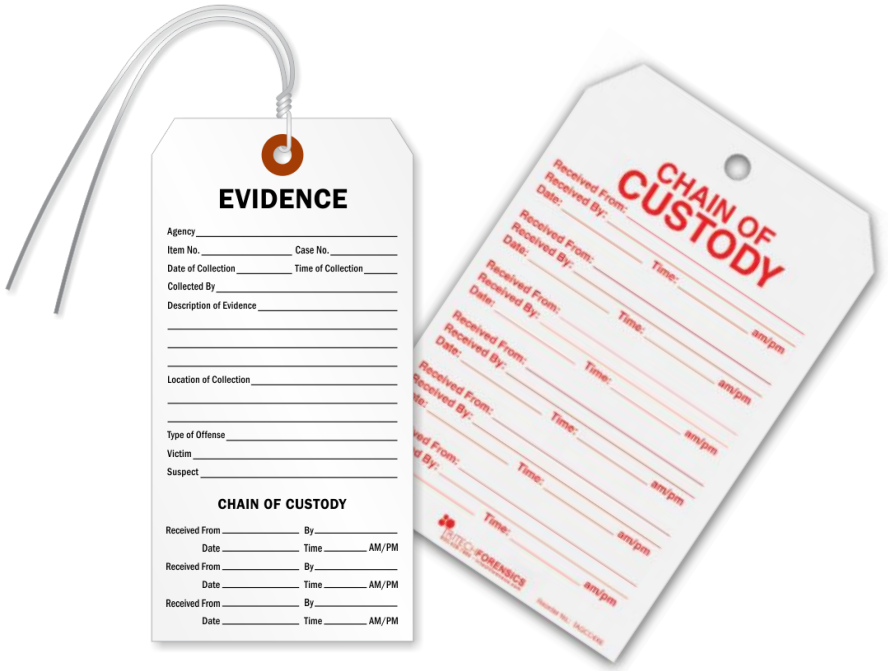
# Background

- Sharing data benefits cooperation and production
- Sharing sensitive data raises concerns of intellectual property (IP) theft and industrial espionage



# Chain of Custody

- Establishing chain of custody to document the trail of sensitive data
  - **Blockchain**: decentralized & non-repudiable ledger




# Related Work

- Sharing data in ledgers: storage and privacy issues
- Sharing data off-chain:
  - Big data selling: is not free; is not autonomous
  - Data access token management: fail to consider dishonest users

- **We propose a blockchain big-data sharing system (BBS) based on the permissioned blockchain**
  - Freely share sensitive big data with authenticated and authorized users
  - Establish the chain of custody within the ledger

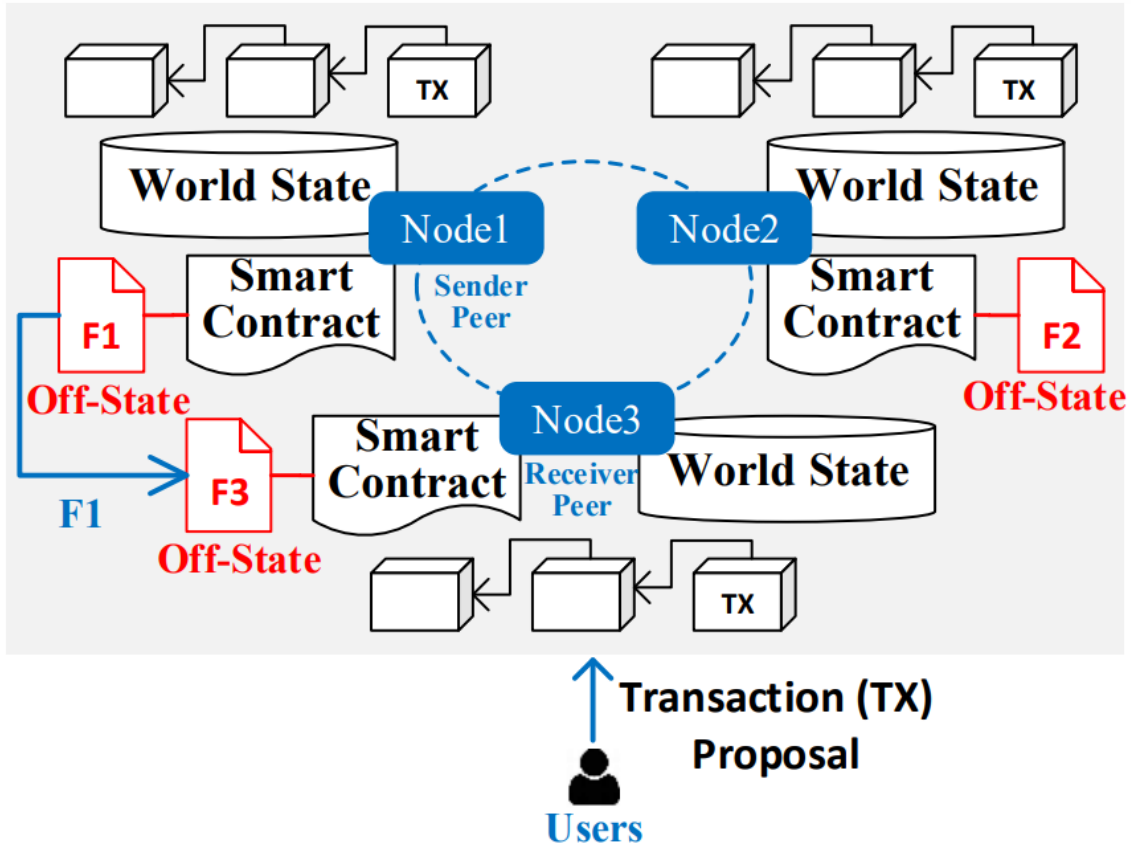
# Permissioned Blockchain

- **Hyperledger Fabric** is a popular permissioned blockchain framework
  - Multiple built-in permission mechanisms: **membership service**, **private data collection (PDC)** and **endorsement policy**
  - No built-in cryptocurrency: transactions are free


Half of Top 50 Blockchain enterprises choose Fabric

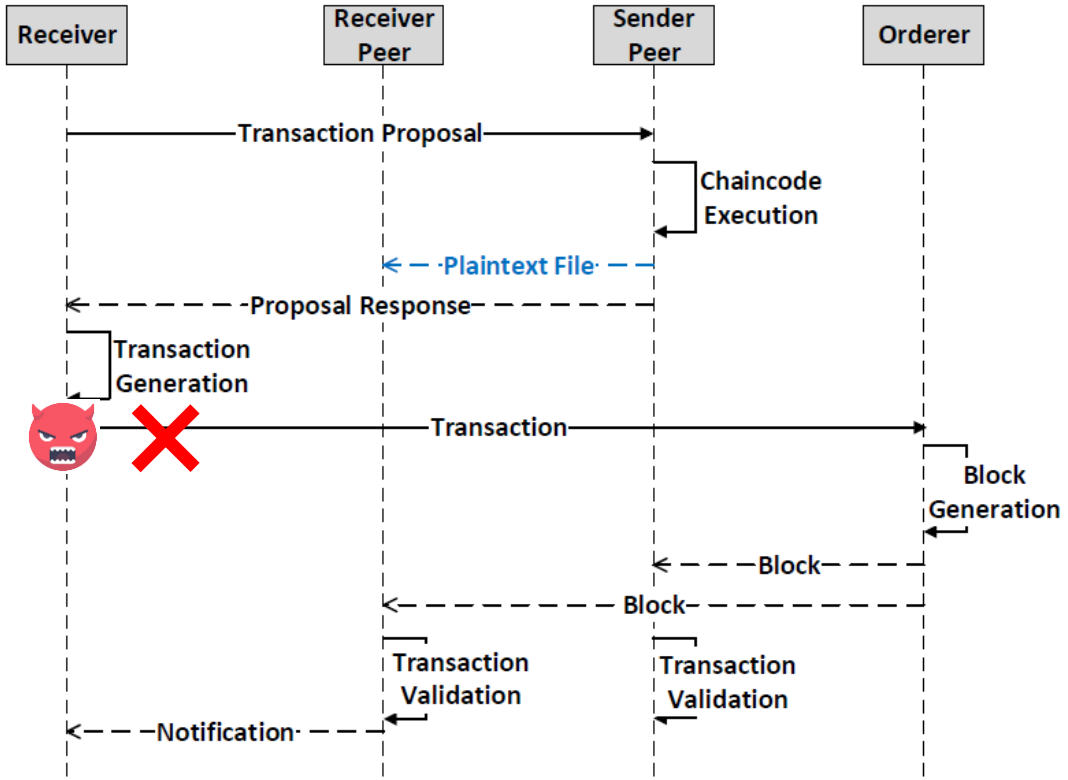
# System Model

- We propose the off-state sharing blockchain system model
  - ➢ "Off-state" is data stored at a storage space separate from the ledger at blockchain nodes
  - ➢ Users have to propose transactions to interact with the blockchain system so as to share data



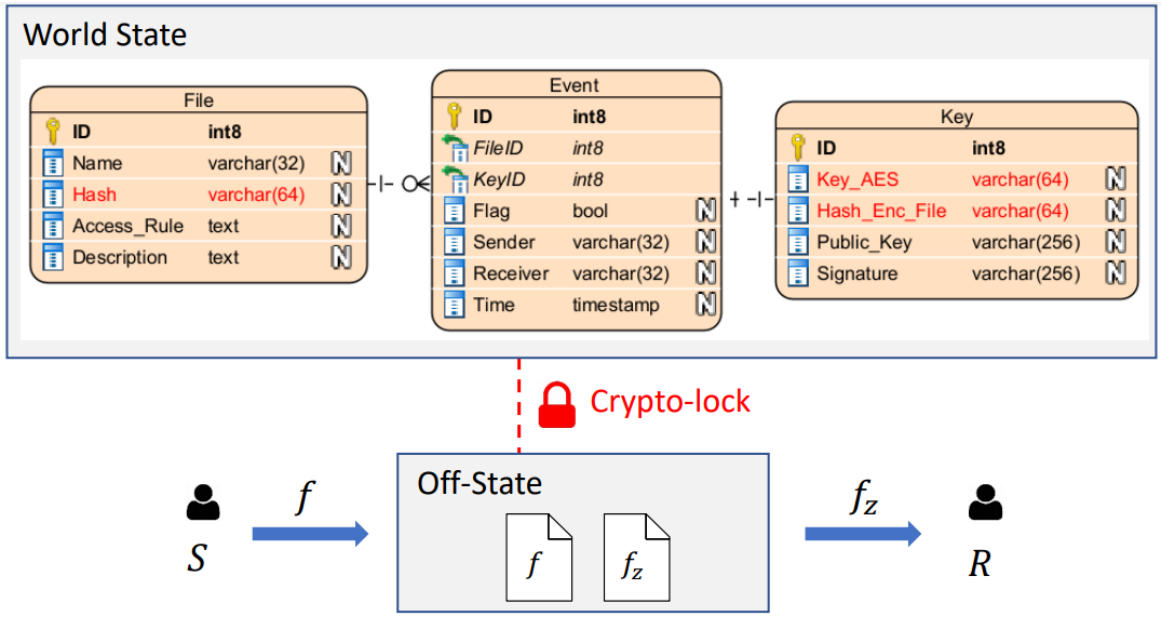
# Threat Model

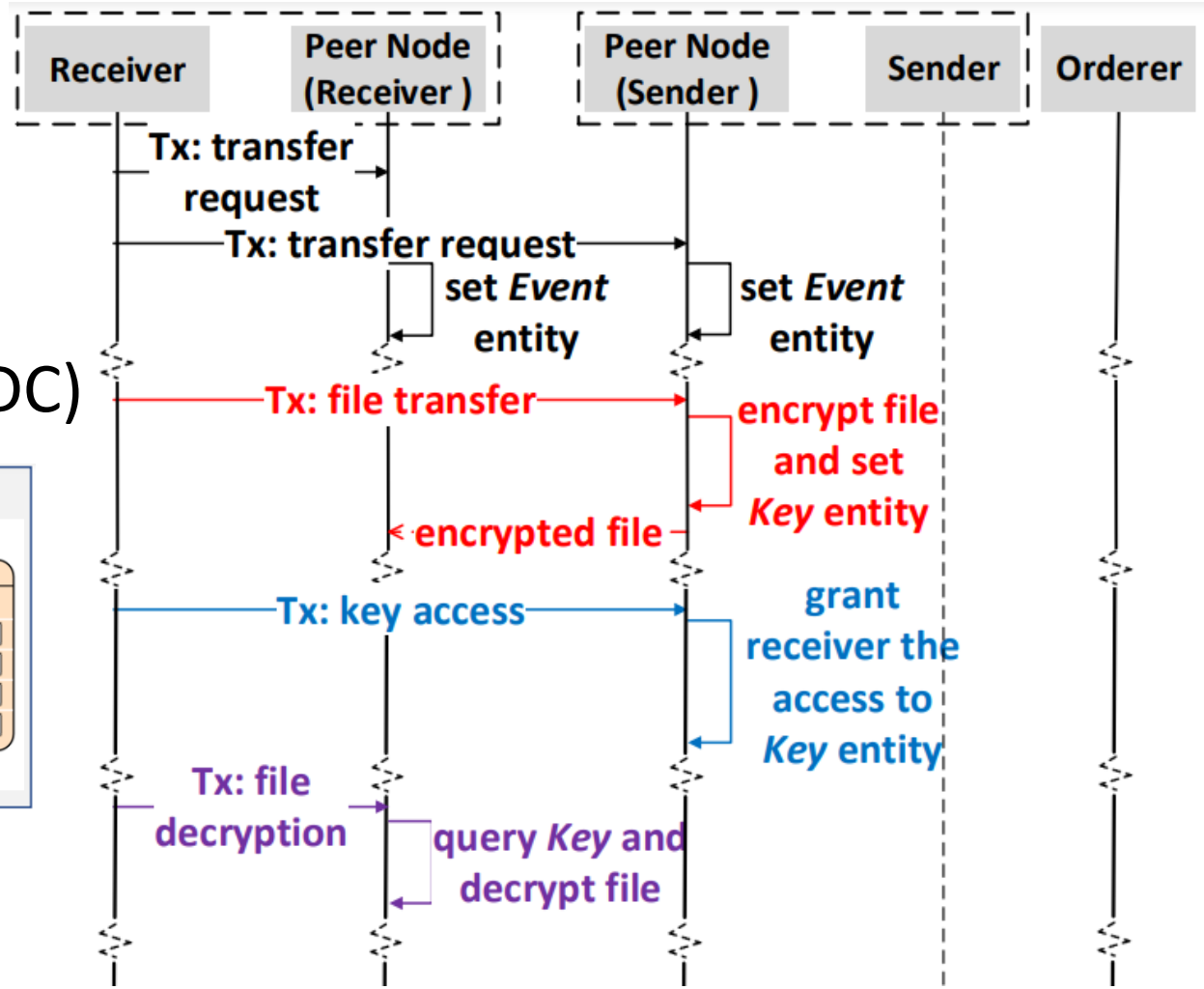
- Assumptions
  - ➢The underlying blockchain infrastructure is secure
  - ➢Users may be dishonest



# Off-State Sharing Protocol

- Stage 1: preparing off-state data
- Stage 2: sharing off-state data
  - ➢Involve four phases
  - ➢Utilize private data collection (PDC)



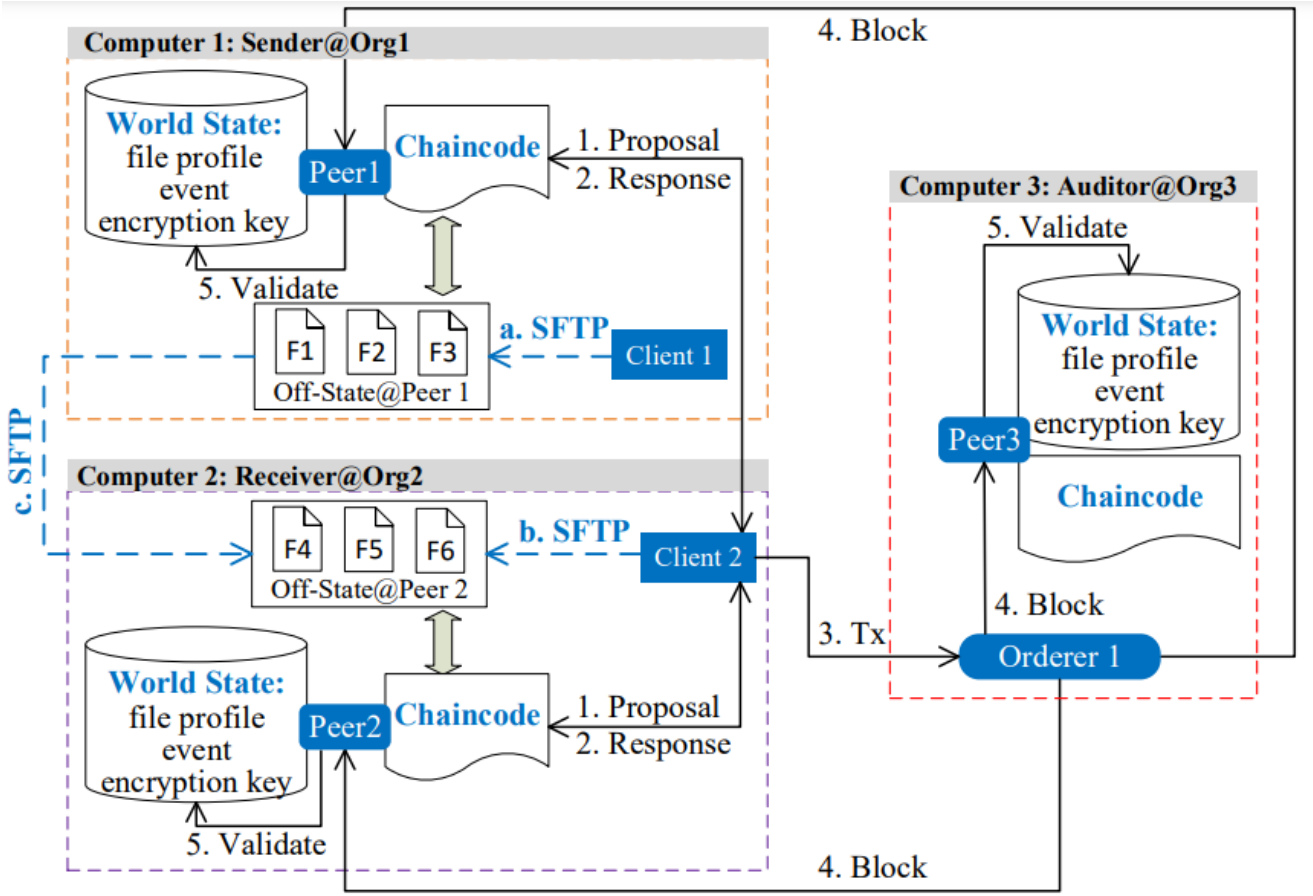



# Security Analysis

- **Sender cannot deny the sharing of data $f$ which may not be consistent with the description**
  - ➢The critical information such as hash $h$ of $f$ and hash $h_z$ of the encrypted file $f_z$ is recorded in ledger
- **Receiver cannot deny he/she has received the shared data $f$**
  - ➢The built-in PDC mechanism can guarantee that the Receiver has to propose and submit ``Tx: key access" to get the encryption key $k$ to decrypt $f_z$
- The blockchain provides **non-repudiable evidences** in ledger

# Evaluation – Prototypical System

- Prototypical off-state sharing system based on Hyperledger Fabric



# Evaluation - Performance and Feasibility

- We use files of different types and various sizes
- We evaluate the latency of the four transactions and the latency of the whole session.

TABLE I
TEST FILE LIST

| Type | Size | Describtion |
|---|---|---|
| .pdf | 67MB | "C++ Primer Plus" eBook |
| .mp4 | 218MB | An over 5 hours song list video |
| .tif | 576MB | The image of Moon from NASA |
| .zip | 1.2GB | A collection of medical images |
| .rar | 2.6GB | The compressed file of one movie |
| .zip | 5.3GB | The compressed file of two movies |

# Evaluation – Impact of File Size

- For each test file, we conduct the file sharing session 32 times
- Each time only one file sharing session is performed

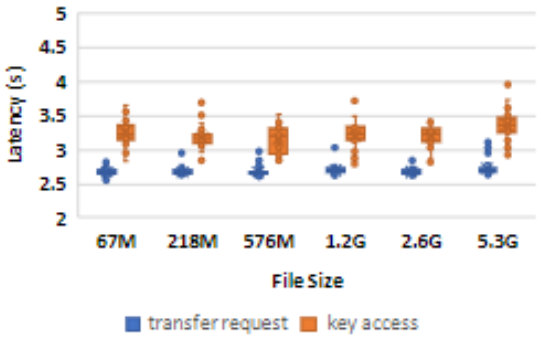



Fig. 7. Transaction latency of "Tx: transfer request" and "Tx: key access"

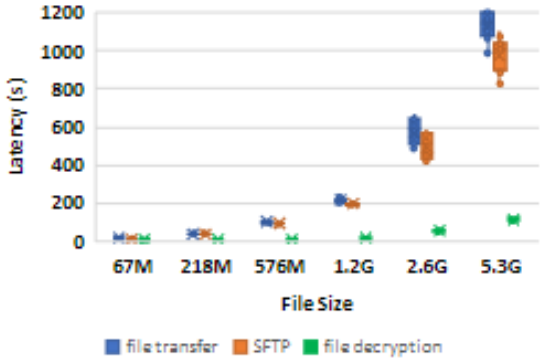



Fig. 8. SFTP latency and transaction Latency of "Tx: file transfer" and "Tx: file decryption"

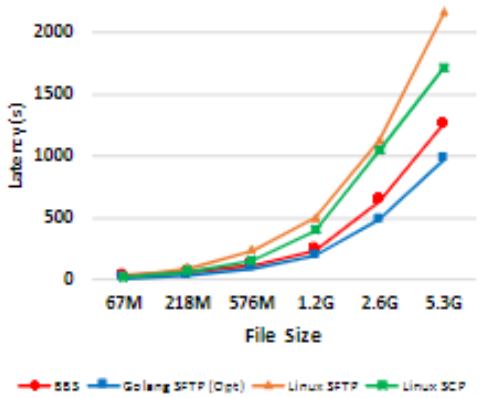



Fig. 9. File sharing session latency

# Summary

- "**Off-state**" is introduced to refer to data stored off the ledger, shared between pairs of nodes
  - ➢ Addressing storage and privacy issues
- Our **off-state sharing protocol** utilizes smart contracts and permission mechanisms and chain of custody evidences are maintained in the ledger
  - ➢ Achieving autonomy and security
- We implement **a prototypical BBS with Fabric**
  - ➢ Evaluating BBS' feasibility and performance

IEEE ICC®
IEEE International Conference on Communications
16–20 May 2022 // Seoul, South Korea // Hybrid: In-Person and Virtual Conference
Intelligent Connectivity for Smart World

# BBS: A Blockchain Big-Data Sharing System



**Shan Wang, Ming Yang,**
**Tingjian Ge, Yan Luo, Xinwen Fu**

# THANK YOU!

# Q&A