Trust Models in Blockchain Systems
Cathie Yun, Software Engineer at Chain
What is a blockchain?

- A blockchain = a **distributed ledger** implementation
- Cryptocurrencies store **transactions** on a blockchain ledger
Systems design

• System design is just a series of tradeoffs - there is no “right” design

• In what cases is using a blockchain a better system design?

• Blockchains tend to improve the trust model of systems
Agenda

1. What is a trust model?
2. Administration
3. Identity
4. Confidentiality
5. Recap
“Generally an entity can be said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects.”

ITU-T X.509, Section 3.3.54
+ auto-locking front door
Trust model changes from blockchain

- Administration: Who controls changes to the ledger?
- Identity: Who controls actions from “your” account?
- Confidentiality: What can people learn from looking at the ledger?
Agenda

1. What is a trust model?
2. Administration
3. Identity
4. Confidentiality
5. Recap
Administration

• Who controls changes to the ledger?

• Existing systems’ trust model: some central administrator
  • Bank
  • Hospitals
  • Companies
Administration

• Public blockchain trust model:
  • Miners
  • Whoever has influence over the miners
Administration

• **Private** (permissioned) blockchain trust model:
  
  • **You choose** the administrators
  
  • One administrator - equivalent to a normal database?
Administration

• Potential improvements to the trust model:
  • You can validate the actions of the administrators
  • You can decrease the incentive or ability to alter information
    • Cryptographic signing
    • Encrypted transactions
Trust models for administration

- Existing system: central authority
- Public blockchain: decentralized miners
- Private blockchain: semi-centralized authority
  - Depends on your choice of administrators
  - Potential improvements: validation, signing, encryption
Agenda

1. What is a trust model?
2. Administration
3. Identity
4. Confidentiality
5. Recap
Identity

• Who **controls actions** from “your” account?

• Existing systems’ trust model: some **central** administrator
  • Present your ID / passport at a bank
  • Verify your identity with your hospital
  • Create an account with a company
Identity

- With blockchain:
  - Your identity is your **private & public key** pair

- Trust model:
  - Only you have access to your private key
  - You won’t lose your private key
Identity

• What can go wrong?
  • What if you lose your key - is your money / data lost?
  • What if your key gets stolen - can someone control your account?
Identity

• Potential **improvements** to the trust model:
  • **Hardware wallet** that can’t leak your key?
  • Allowing blockchain administrators to do **account management**?
Trust models for identity

• Existing system: central authority

• Blockchain system: private / public key pairs
  • User-managed keys: users won’t lose or leak keys
  • Hardware-managed keys: hardware behaves as expected
  • Admin-managed accounts: central authority
Agenda

1. What is a trust model?
2. Administration
3. Identity
4. Confidentiality
5. Recap
Confidentiality

• **What can people learn** from looking at the ledger?

• Existing systems’ trust model: **everything!**

  • Banks: armed security guards
  • Hospitals: secure internal networks
  • Companies: secure account setup
Confidentiality

- **Unencrypted** blockchains trust model:
  - Everyone in the network can see everything
  - This is not appealing to businesses who want to keep data **private**.
Confidentiality

- **Encrypted** blockchains trust model:
  - The *encryption algorithm*
  - Participants’ ability to check data validity
Trust models for confidentiality

- Existing system: central authority controls access to ledger
- Unencrypted blockchain: no confidentiality
- Encrypted blockchain: trust the encryption & validation procedures
Agenda

1. What is a trust model?
2. Administration
3. Identity
4. Confidentiality
5. Recap
Trust models

- Trust models are use- and context-specific
- Blockchains can provide a better trust model for some services, and a worse one for others
- Different kinds of blockchains have different trust models
Existing trust models

- Administration: centralized read/write access
- Identity: centralized identity verification
- Confidentiality: centralized authority restricts data access
Blockchain trust models

• Administration
  • Public blockchain: miners decide write access, all can read
  • Private blockchain: semi-centralized read/write access
• Identity: private/public keys
• Confidentiality
  • Unencrypted blockchain: no confidentiality
  • Encrypted blockchain: encryption & validation procedures
Cathie Yun
cathie@chain.com

Questions?