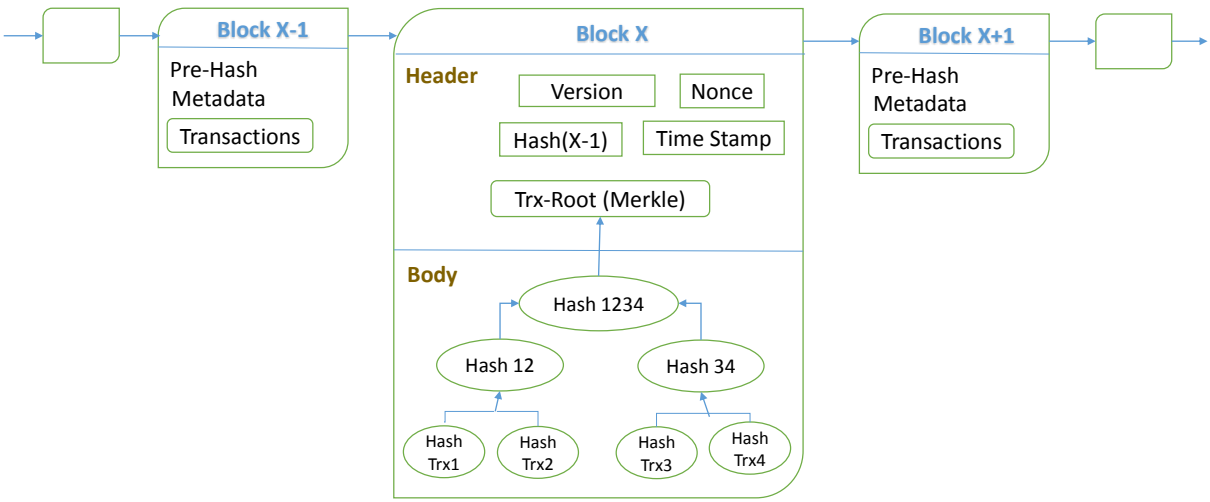
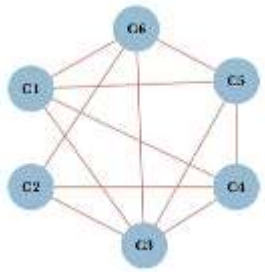
PASS using Blockchain Technology and its Risks and Challenging

zchen@mercy.edu
Z Chen
Dept. Math & CSs, Mercy College



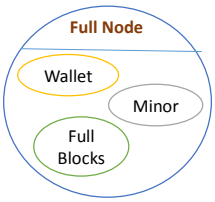
Network

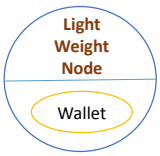


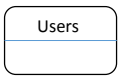
Models

- Permisionless
- Permissioned
- Hybrid

Roles







Consensus

POW	Proof of Work
POS	Proof of Stake
DPOS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PO.ET	Proof of Existence
ILP	InterLedger Protocol
VRF+BA	Verifiable Random funct - Byzantine Agreement

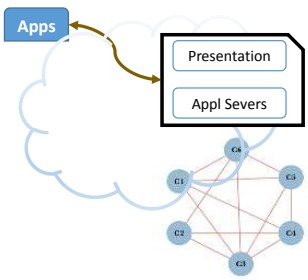
Smart Contract

Shared Ledge

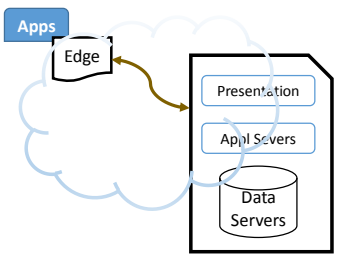
Zero Knowledge Proof
zero knowledge blockchains

Hyperledge
Etherium
EOS

DApps



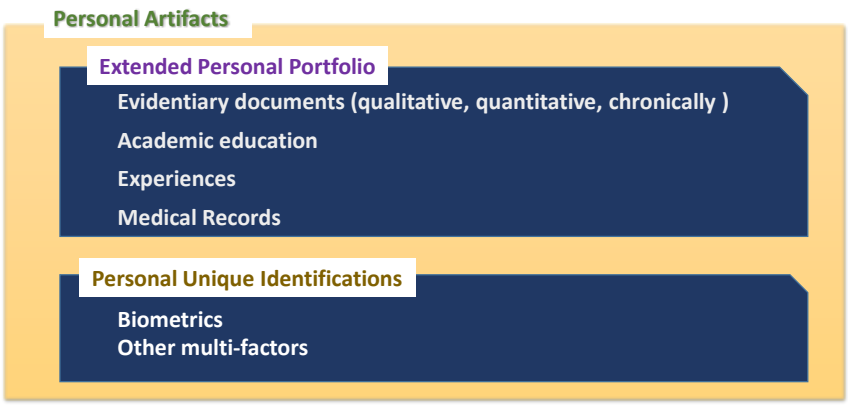
Cloud Apps

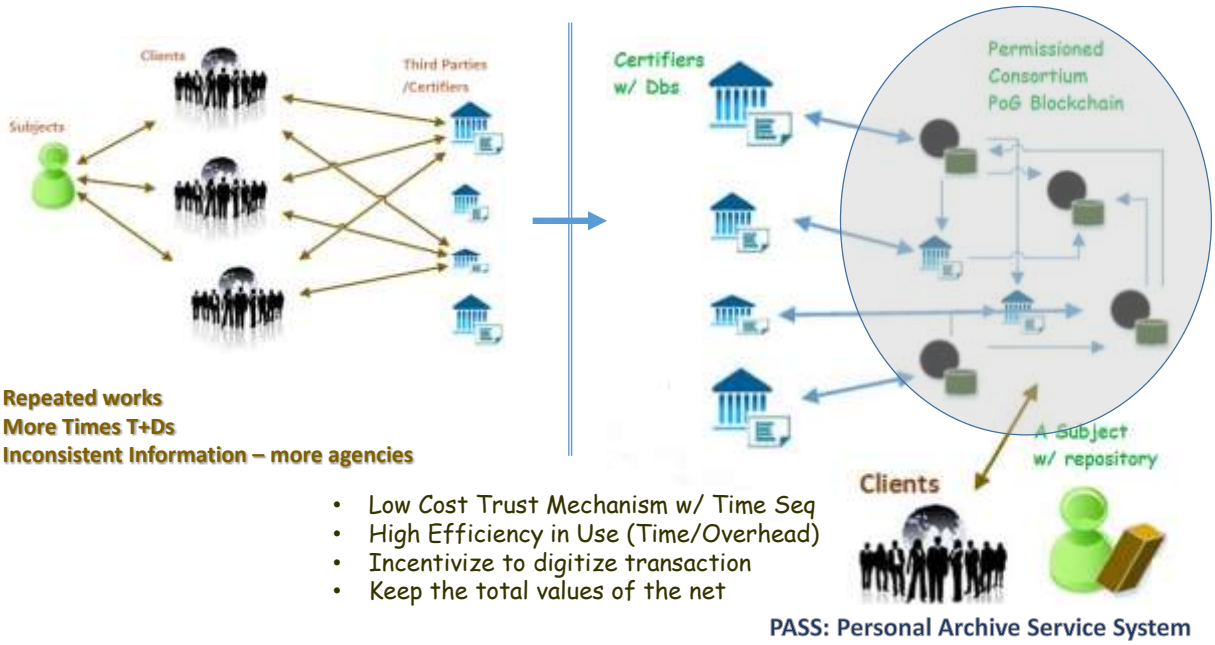


Personal Cryptography
Crowd Value Participation
Time Sequence

Immutable
Provenance
Transparency
Decentralization
Finality
Privacy
Security

1. To build trust from weak or no trust so to lower the cost of conducting business
2. To have records transparent, provenance, secure and immutable so fake tranx and false ledger impossible
3. To turn the world into value investors – good citizens to keep the value
4. To transform/renovate business process for established business
   - Clearing House, Audit, Risk Management
   - Financial services
   - supply chain finance (centralized, loan distribution, supply and demand, contract)
5. To create new business opportunities
   - Culture Heritage to be Greenish
   - Digital IDs and certifications
   - Supply Chain Trusted Environment
   - Healthcare IT (GDPR; Data Exchange)

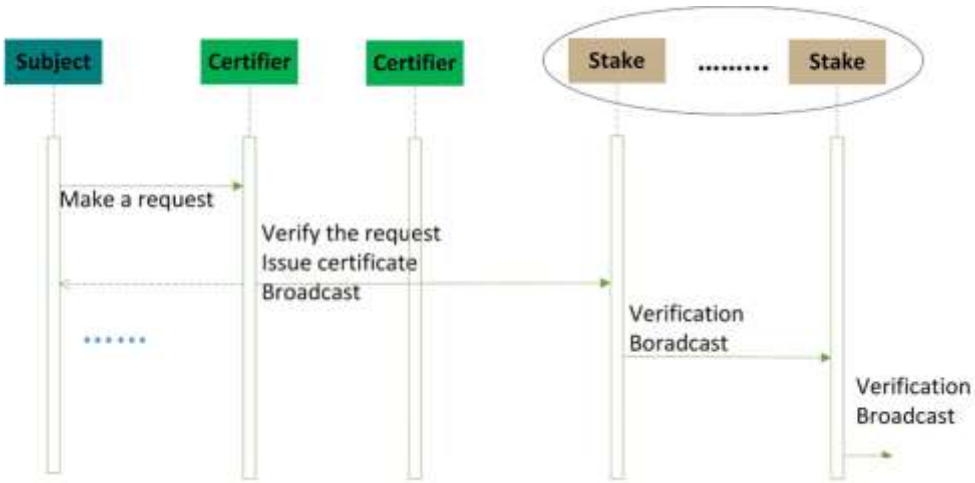


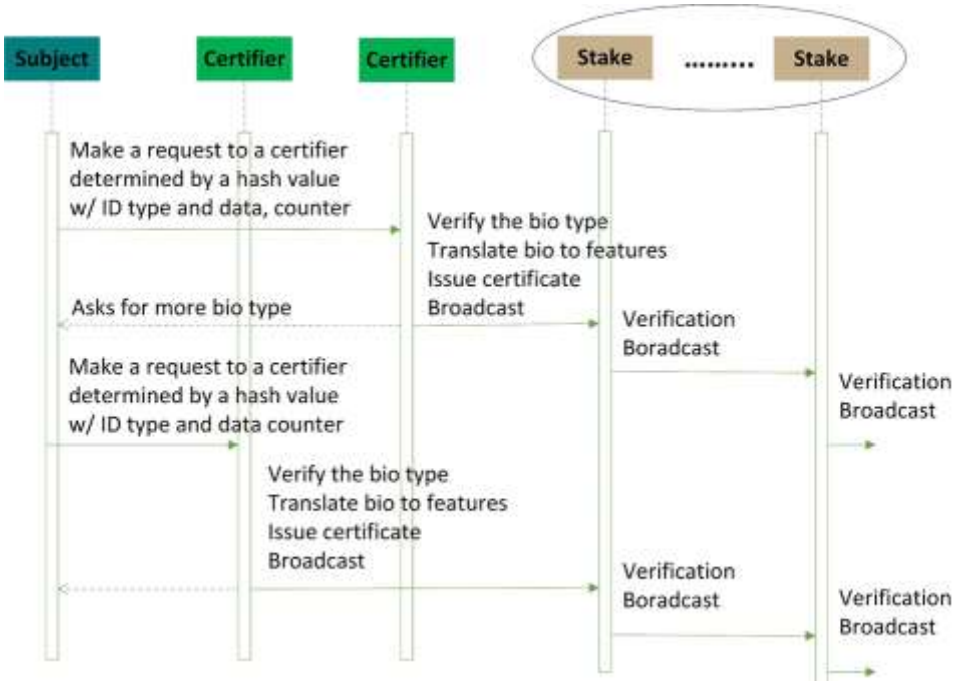


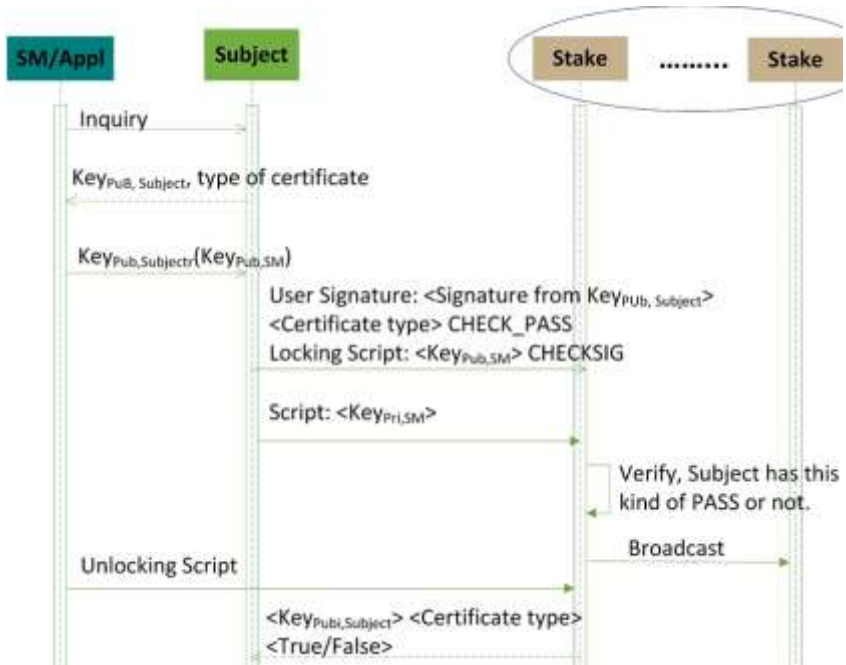
Repeated works
More Times T+Ds
Inconsistent Information – more agencies

- Low Cost Trust Mechanism w/ Time Seq
- High Efficiency in Use (Time/Overhead)
- Incentivize to digitize transaction
- Keep the total values of the net

PASS: Personal Archive Service System




Subject
Certifier
Certifier
Stake
.....
Stake
Make a request to a certifier determined by a hash value w/ ID type and data, counter
Verify the bio type
Translate bio to features
Issue certificate
Broadcast
Asks for more bio type
Verification Boradcast
Verification Broadcast
Make a request to a certifier determined by a hash value w/ ID type and data counter
Verify the bio type
Translate bio to features
Issue certificate
Broadcast
Verification Boradcast
Verification Broadcast


SM/Appl
Subject
Stake
.....
Stake
Inquiry
$Key_{PuB,\ Subject}$, type of certificate
$Key_{Pub,Subject}(Key_{Pub,SM})$
User Signature: <Signature from $Key_{PUb,\ Subject}$>
<Certificate type> CHECK_PASS
Locking Script: <$Key_{Pub,SM}$> CHECKSIG
Script: <$Key_{Pri,SM}$>
Verify, Subject has this kind of PASS or not.
Broadcast
Unlocking Script
<$Key_{Pubi,Subject}$> <Certificate type>
<True/False>

Ethereum PASS Implementation

Hyperledger Fabric Implementation

Date, Time	Entry Type	Participan	
2018-05-07, 12:35:26	DeauthorizeDiploma	2001 (User)	view record
2018-05-07, 12:26:19	ActivateCurrentIdentity	none	view record
2018-05-07, 12:25:56	ShowDiploma	2001 (User)	view record

Submit Transaction

Transaction Type DeauthorizeDiploma

```
{
  "$class": "org.z.pass.DeauthorizeDiploma",
  "diploma": "resource:org.z.pass.Diploma#1001",
  "newClient": "resource:org.z.pass.Client#0001"
}
```

Submit Transaction

Transaction Type ShowDiploma

```
{
  "$class": "org.z.pass.ShowDiploma",
  "diploma": "resource:org.z.pass.Diploma#1001",
  "newClient": "resource:org.z.pass.Client#0001"
}
```

Web pass-mercy | admin | org.z.pass.School

PARTICIPANTS
- Client
- School
- User

ASSETS
- Diploma

TRANSACTIONS
- All Transactions

1001

```
{
  "$class": "org.z.pass.School",
  "schoolID": "1001",
  "schoolName": "MercyCollege",
  "Introduction": ""
}
```

1002

```
{
  "$class": "org.z.pass.School",
  "schoolID": "1002",
  "schoolName": "ShanghaiUniv",
  "Introduction": ""
}
```

Blockchain Security as a Services

- Smart Contract Risk Assessment Services (Audit, Assessment, Scanning, Compliances)
- Data Security and Privacy Assessment
- Key Management
- Application Threat Modeling and Secure Coding
- Business Infrastructure Assessment (FIPS (140-2) and EAL Compliance)
- Incidents Response

Risks and Challenging

- Block Size Limitation
- Blockchain Storage Expansion
- Transaction Numbers per second Increasing
- Key Pair Protection and Security
- More Smart Contract Design, Development and Assessment
- Consensus Optimization
- Anonymity Improvement
- Use Case Scalability from POC to Deployment and Production
- Beyond Technology - Digital Currency, ICO and Tokens

Zhixiong Chen and Yixuan Zhu, Participant and Content Aware Social Webs, in the presentation SOFC, Dallas, June, 2018

Zhixiong Chen and Yixuan Zhu, Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging, in the proceeding of the 2017 IEEE 6th International Conference on AI & Mobile Services, Honolulu, Hawaii, June, 2017, PP93-99

Yixuan Zhu and Zhixiong Chen, RealID: Building A Secure Anonymous Yet Transparent Immutable ID Service, proceeding in the 2017 IEEE International Conference on Intelligent Data and Security, 26-28 May 2017, Beijing, China, PP:277-280