

An Evaluation System Based on Blockchain and Linkable Ring Signature

Thesis Defense

Presenter: Yi Liu
Supervisor: Qi Wang

OUTLINE

1

Motivation

2

Contribution

3

Concepts

4

Solution



Motivation

Motivation



Motivation



Motivation



User



Server/Database

Motivation



User



Server/Database



一星去哪儿了？美国亚马逊大量删除希拉里新书差评

🕒 2017-09-16 14:39:00

🔑 澎湃新闻

🔗 分享

🔍 A⁺

6

参与

滴滴司机持刀要挟乘客删差评 滴滴封禁涉事司机

来源：界面新闻 作者：陈晓双

2018-05-08 18:57

0

网购删除差评成新行业 收费80元以下基本靠恐吓

🕒 2015-11-20 13:35:00

🔑 大洋网

🔗 分享

🔍 A⁺



Contribution



Anonymity



Anonymity

Evaluation **F**orgery **R**esistance



Anonymity

Evaluation **F**orgery **R**esistance

Double-evaluating **R**esistance



Anonymity

Evaluation **F**orgery **R**esistance

Double-evaluating **R**esistance

Evaluation **P**rotection

Contributions

3

Anonymity

4

Double-evaluating Resistance

5

Evaluation Forgery Resistance

6

Evaluation Protection

Contributions

1

Universal Verifiability

3

Anonymity

4

Double-evaluating Resistance

5

Evaluation Forgery Resistance

6

Evaluation Protection

Contributions

1

Universal Verifiability

2

Individual Verifiability

3

Anonymity

4

Double-evaluating Resistance

5

Evaluation Forgery Resistance

6

Evaluation Protection

Contributions



01

A definition of the secure evaluation system

Contributions

01

A definition of the secure evaluation system

02

A solution based on blockchain and linkable ring signature

Contributions

01

A definition of the secure evaluation system

02

A solution based on blockchain and linkable ring signature

03

An implementation for evaluating teaching quality



C Concepts

C Concepts

Hash Function

Hash Function

Plaintext	Hash Value sha256
sustech	45a02730eb37e5915b90e06eda424e76101aa8d97566a9786338986f21aefdc2
Sustech	fa3a0dd1f80b2ad77338aaf7a78aa2366904ccb8fa77e0ae5d43254dbd322bde
sus tech	820269699bc57f95ea6afd2df17ff5dc8d4bb49946b94059c123049382142ce6
sustec	098e09ef23b4940f6b64ac880594fbb11623753fbffc97fa97787c72687c7bec

Concepts

Digital Signature

Concepts



Digital Signature



Concepts

Digital Signature



Concepts

Digital Signature



Concepts



Digital Signature



Concepts

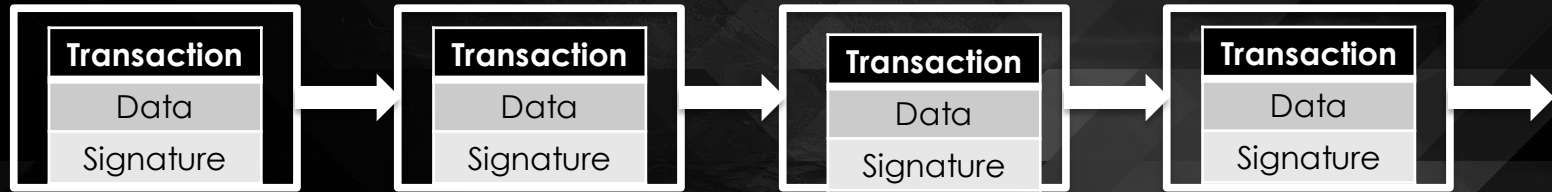


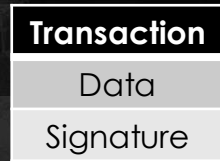
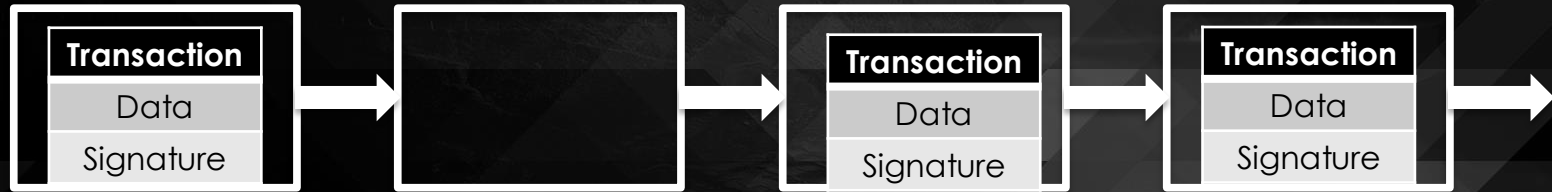
Digital Signature



C Concepts

B Blockchain





C Concepts

Ring Signature

Concepts



Ring Signature



Concepts



Ring Signature



Concepts



Ring Signature



Concepts



Ring Signature



Concepts



Ring Signature

Concepts



Ring Signature



Concepts



Ring Signature



Concepts



Linkable Ring Signature





Linkable Ring Signature



Linkable Ring Signature





Solution

Solution



Solution



Solution

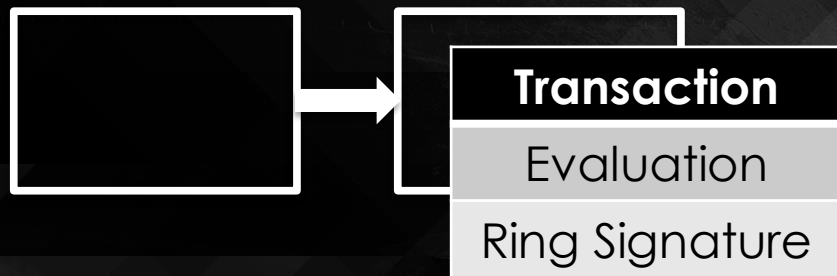


Transaction

Evaluation

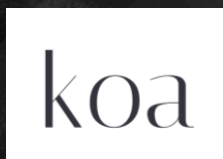
Ring Signature

Solution

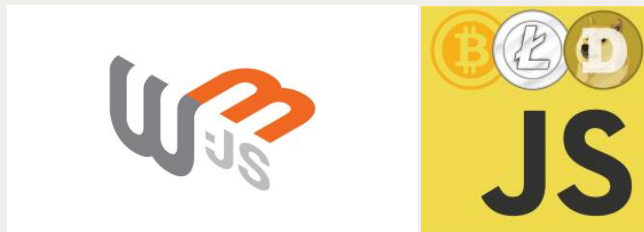


Solution

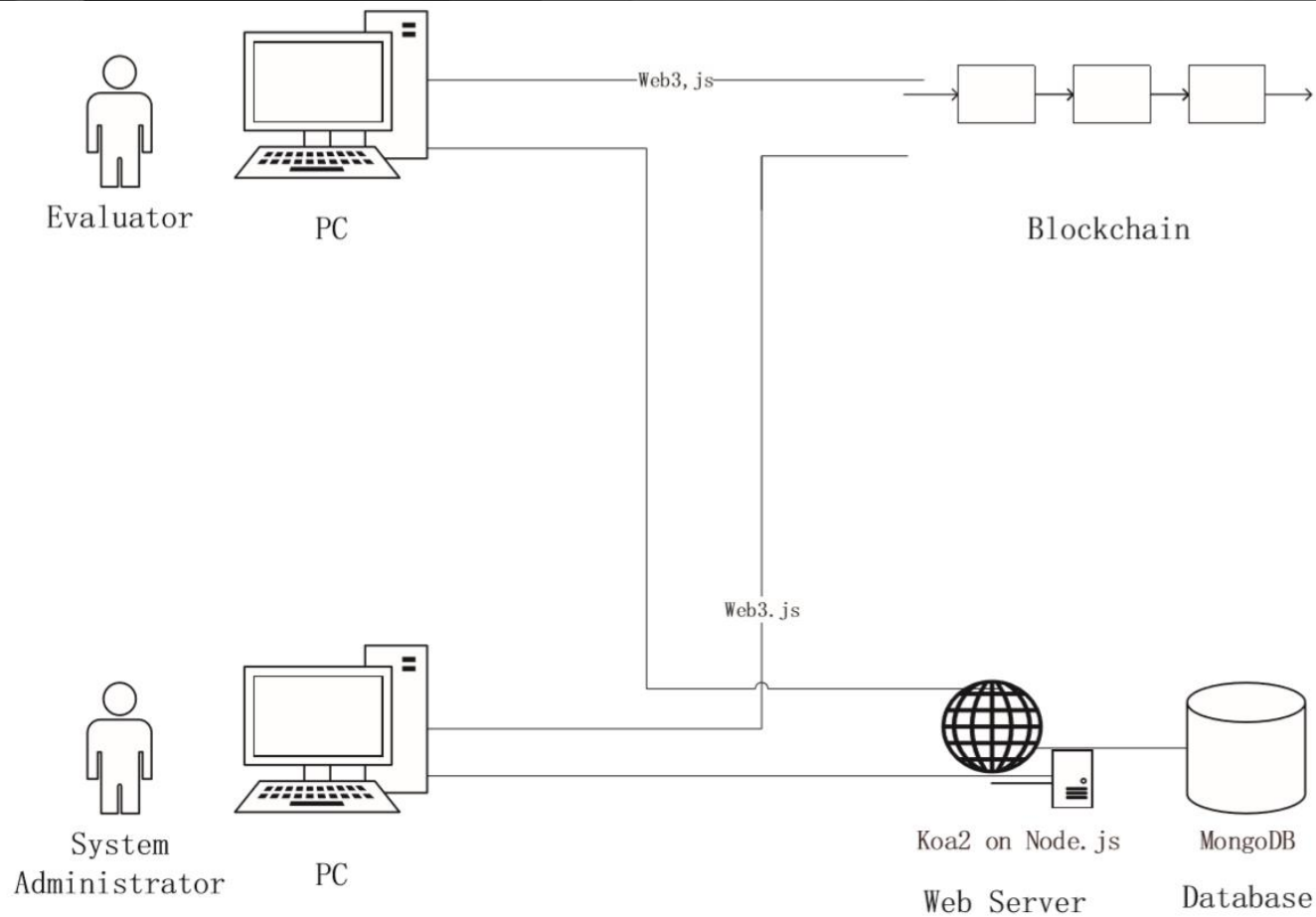




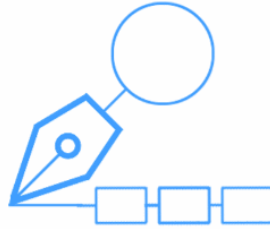
ethereum



Solution



Solution



[Log In](#)

[Sign Up](#)



Log In

Solution

* Course Name

Fall 2018 CS101 Discrete Mathematics

* Instructor

王琦

* Time

🕒

Start Time

-

End Time

☐ Candidates

3

🔍 Enter keyword

☐ 刘逸

☐ 吴腾

☐ 李舟

☐ Participants

0

🔍 Enter keyword

No data

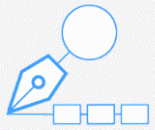
Choose an image

Publish

← → ↻

localhost:9528/#/courses/ongoing

||| Courses / Ongoing



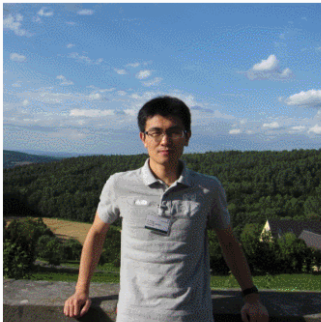
Home

Courses

Ongoing

Finished


Setup



Fall 2018 CS101 Discrete Mathematics
Instructor: 王琦
End Time: 2018/6/11 上午12:00:00

Start


Result



Fall 2018 CS101 Discrete Mathematics
Instructor: 王琦
End Time: 2018/6/11 上午12:00:00

Start

Result

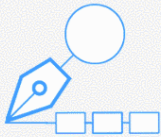


Fall 2018 CS101 Discrete Mathematics
Instructor: 王琦
End Time: 2018/6/11 上午12:00:00

Start

Result

Total 3 < 1 > Go to 1



Home

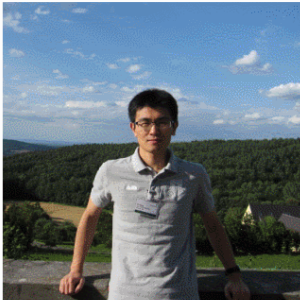
Courses

Ongoing

Finished

Setup

Courses / Ongoing




Fall 2018 CS101 Discrete Mathematics

Instructor: 王琦

End Time: 2018/6/11 上午12:00:00

Start

Result




Fall 2018 CS101 Discrete Mathematics

Instructor: 王琦

End Time: 2018/6/11 上午12:00:00

Start

Result



Fall 2018 CS101 Discrete Mathematics

Instructor: 王琦

End Time: 2018/6/11 上午12:00:00

Start

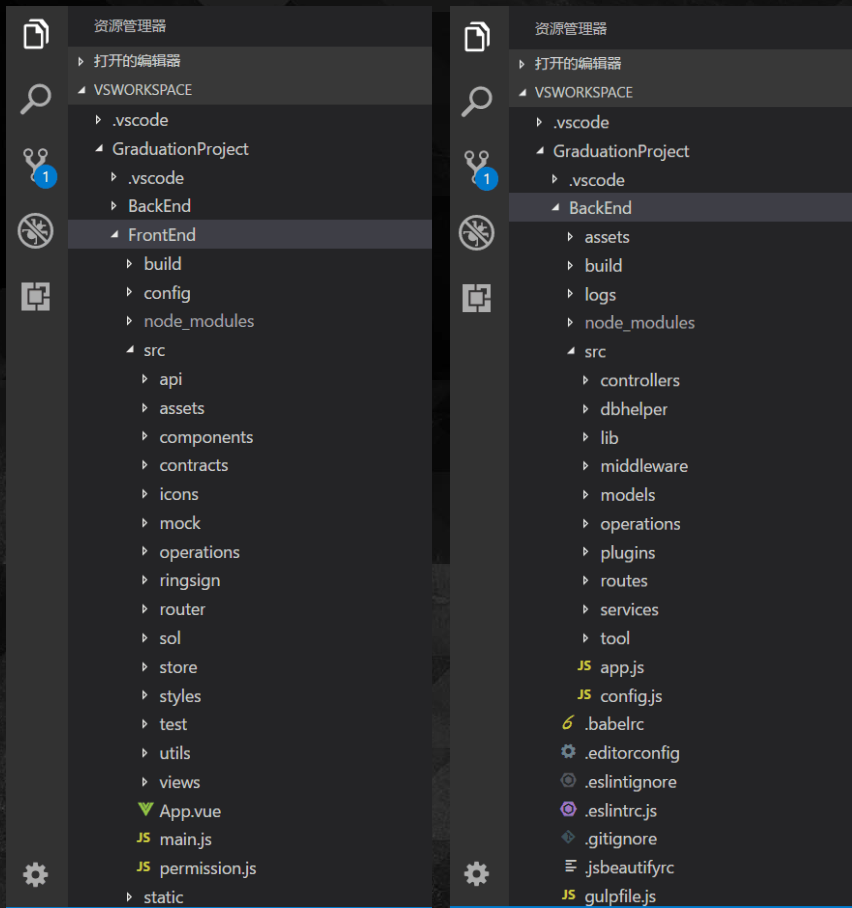
Result

Total 3

< 1 >

Go to 1

Solution



- Login and Logout
- Sign up (key generation)
- Users role control
- Smart contract
- Linkable ring signature using ECC
- Evaluation activity creation
- Evaluating
- Evaluation result visualization
- ...

Solution

Universal Verifiability

Individual Verifiability

Anonymity

Double-evaluating Resistance

Evaluation Forgery Resistance

Evaluation Protection

Solution

Unforgeability

Signer Ambiguity

Linkability

Culpability

Universal Verifiability

Individual Verifiability

Anonymity

Double-evaluating Resistance

Evaluation Forgery Resistance

Evaluation Protection

Solution

Unforgeability

Signer Ambiguity

Linkability

Culpability

Blockchain Reliability

Universal Verifiability

Individual Verifiability

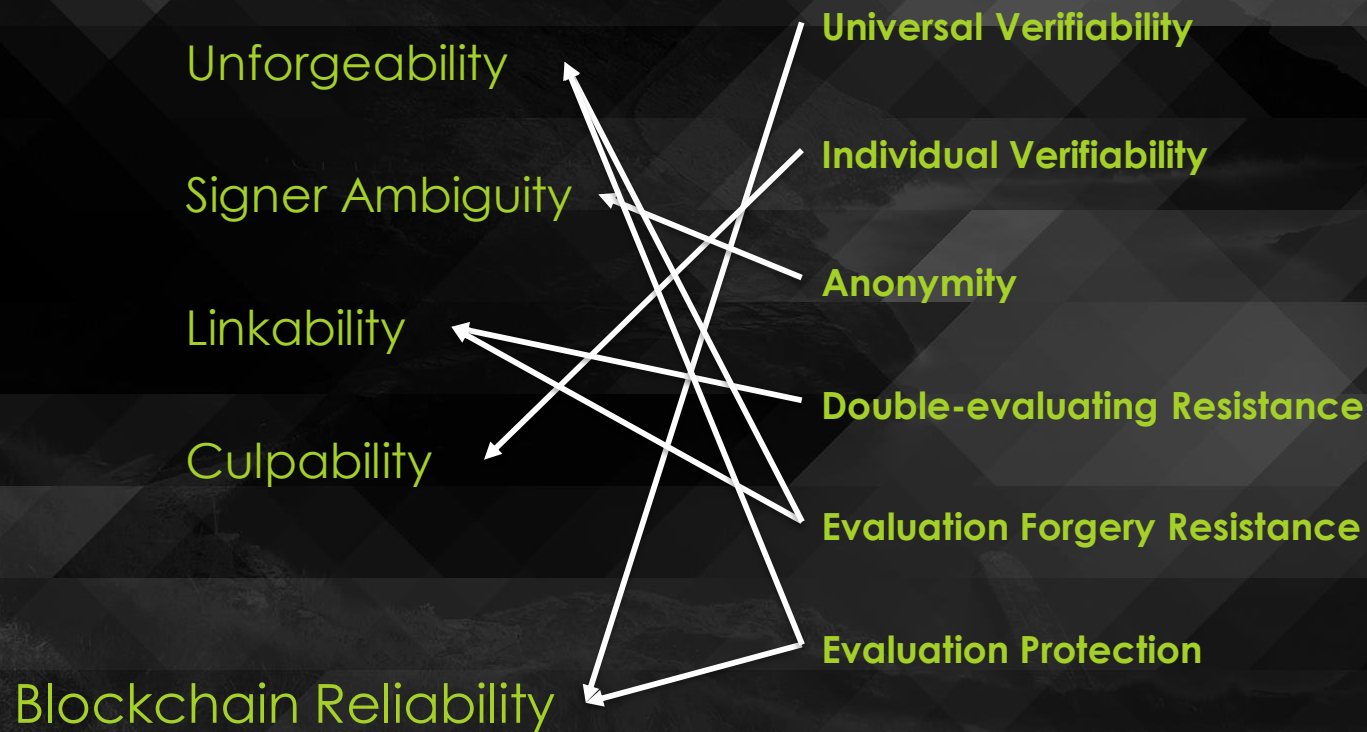
Anonymity

Double-evaluating Resistance

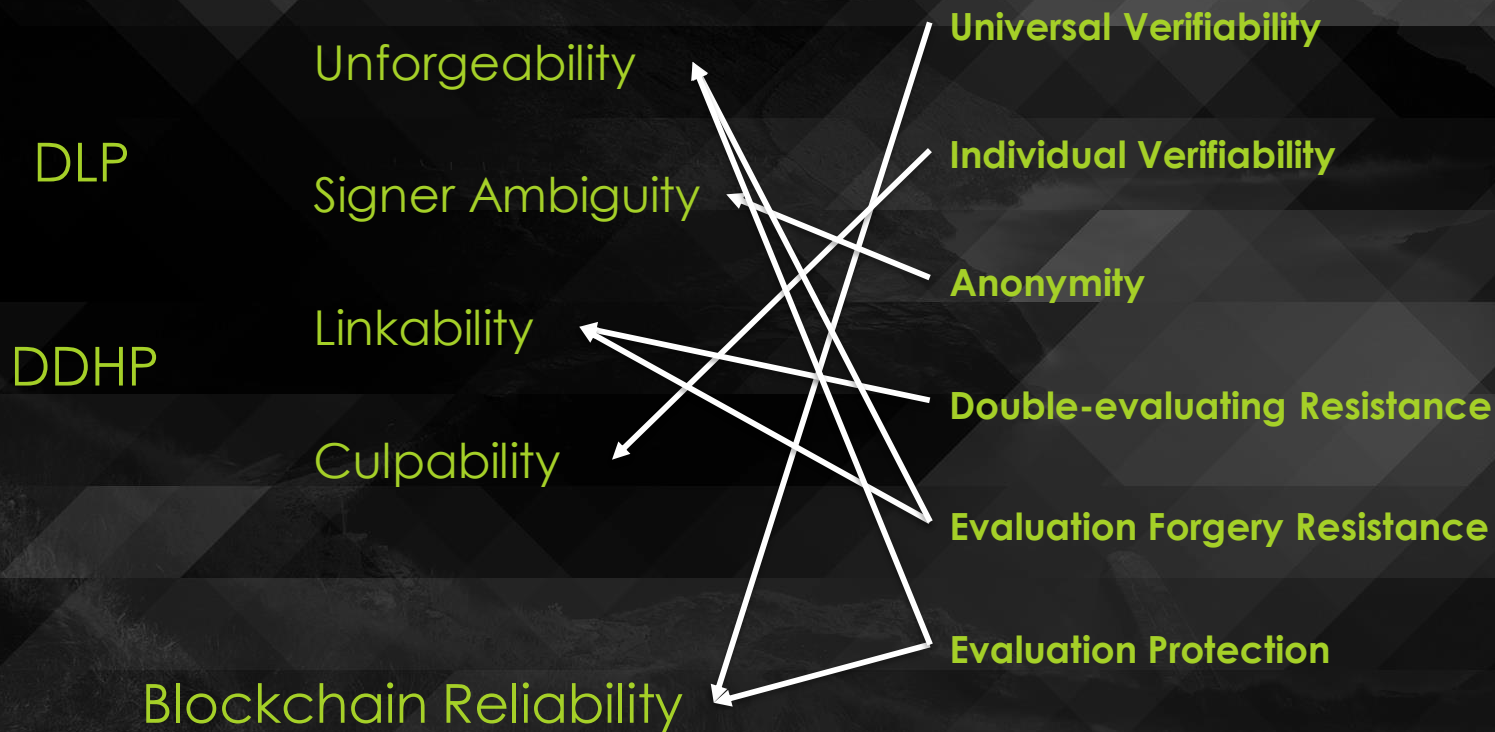
Evaluation Forgery Resistance

Evaluation Protection

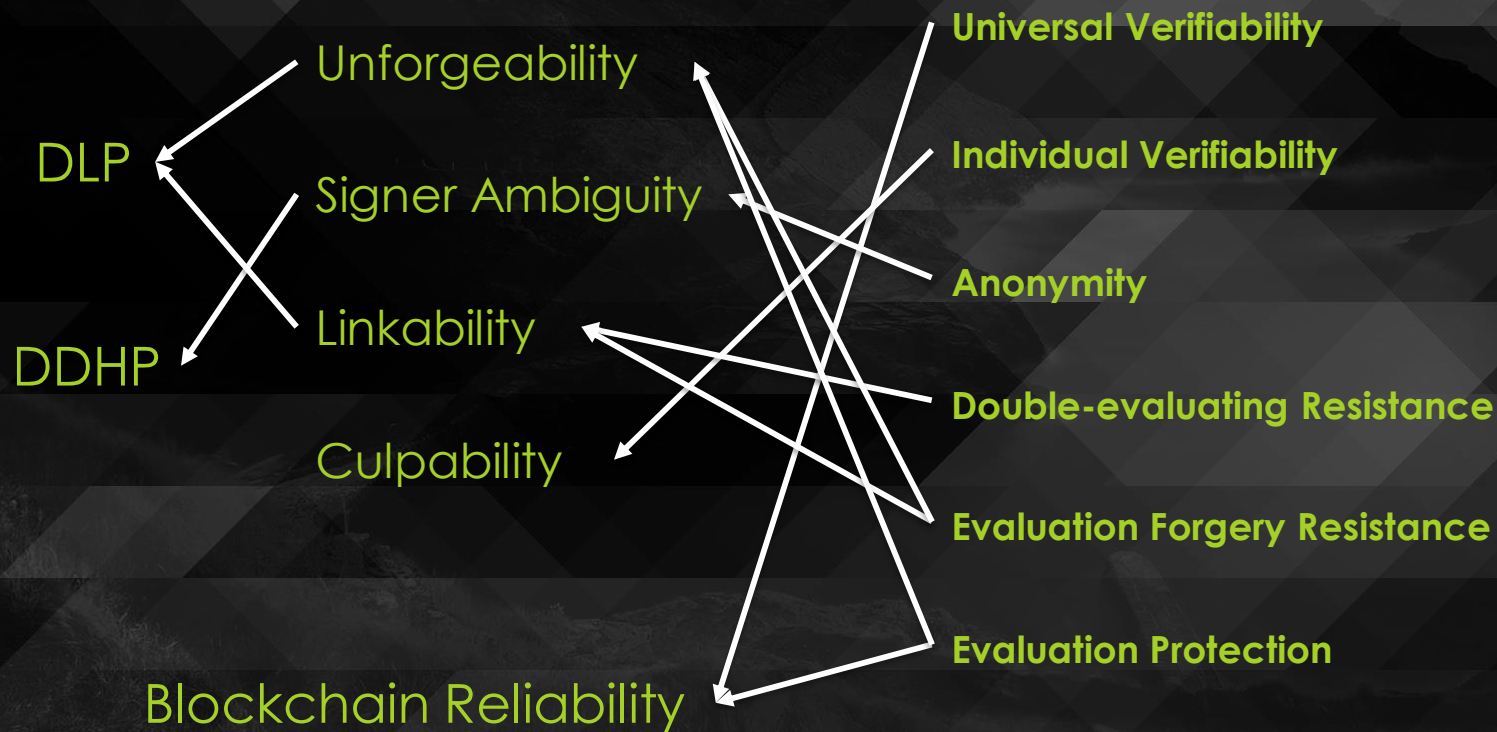
Solution



Solution



Solution



An Evaluation System Based on Blockchain and Linkable Ring Signature

Thesis Defense

Presenter: Yi Liu
Supervisor: Qi Wang