海联金汇 HYUNION HOLDINGS
股票代码：002537

UMF 联动优势 UNION MOBILE FINANCIAL TECHNOLOGY
海联金汇旗下企业

科技赋能普惠金融

UMID去中心化身份认证平台预研

王宇

MAKE FINTECH EVERYWHERE

核心问题

1、我们说的 DID 是指什么？
2、DID 能解决什么问题？
3、DID 不能解决什么问题？
4、我们怎么解决 DID 解决不了的问题？

目录

背景与现状

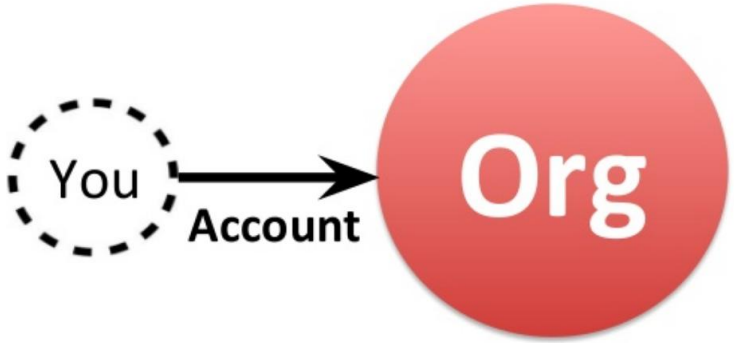
身份　　数字身份

背景与现状

数字身份的三种模型

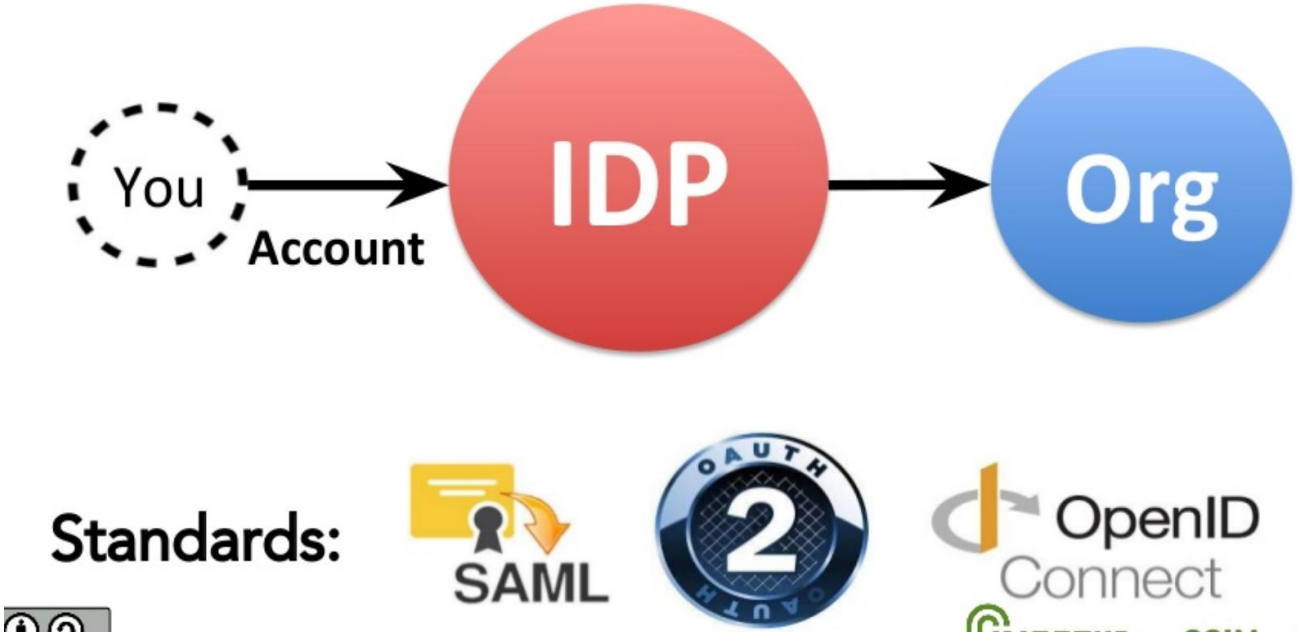
背景与现状

一、中心化的数字身份



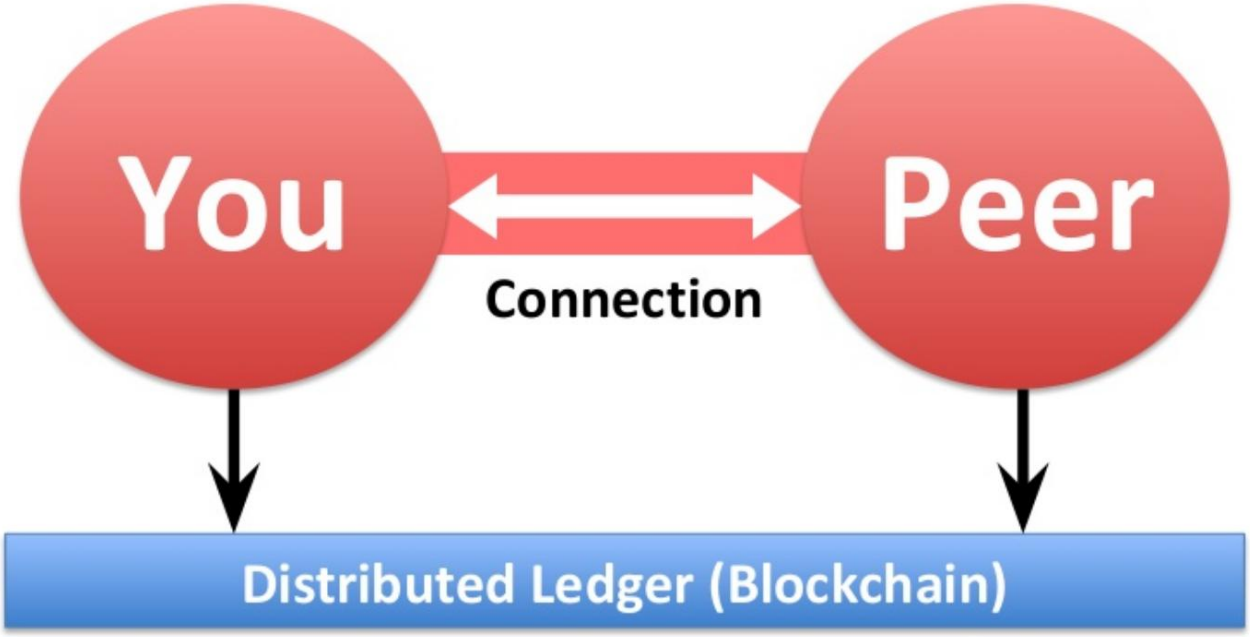
背景与现状

二、第三方数字身份服务（IDP）



背景与现状

三、自主主权的数字身份（SSI）



背景与现状

Self-sovereign identity (SSI)

小视频

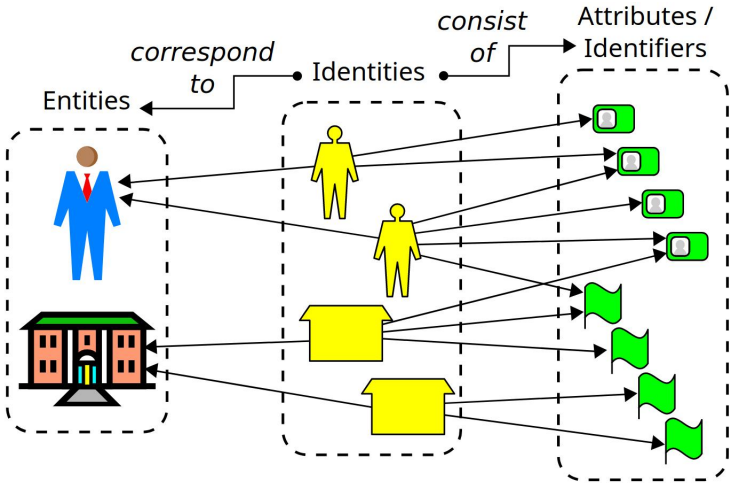
European Union SSI

The European Blockchain Services Infrastructure (EBSI)

背景与现状

SSI 是数字身份运动下的概念：

1. 只有自己拥有全部的数字身份信息
2. 自己可以完全控制数字身份下的可验证证明

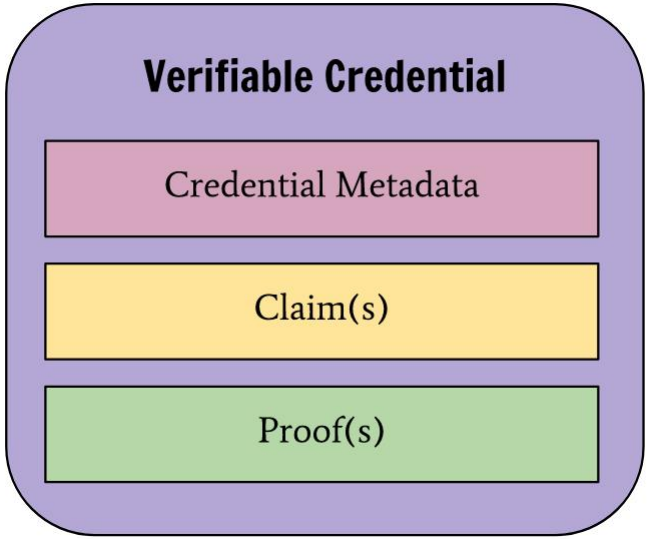


背景与现状

可验证的证明 和 去中心化的身份标识 结合使用，实现了 SSI 的理念。

目录

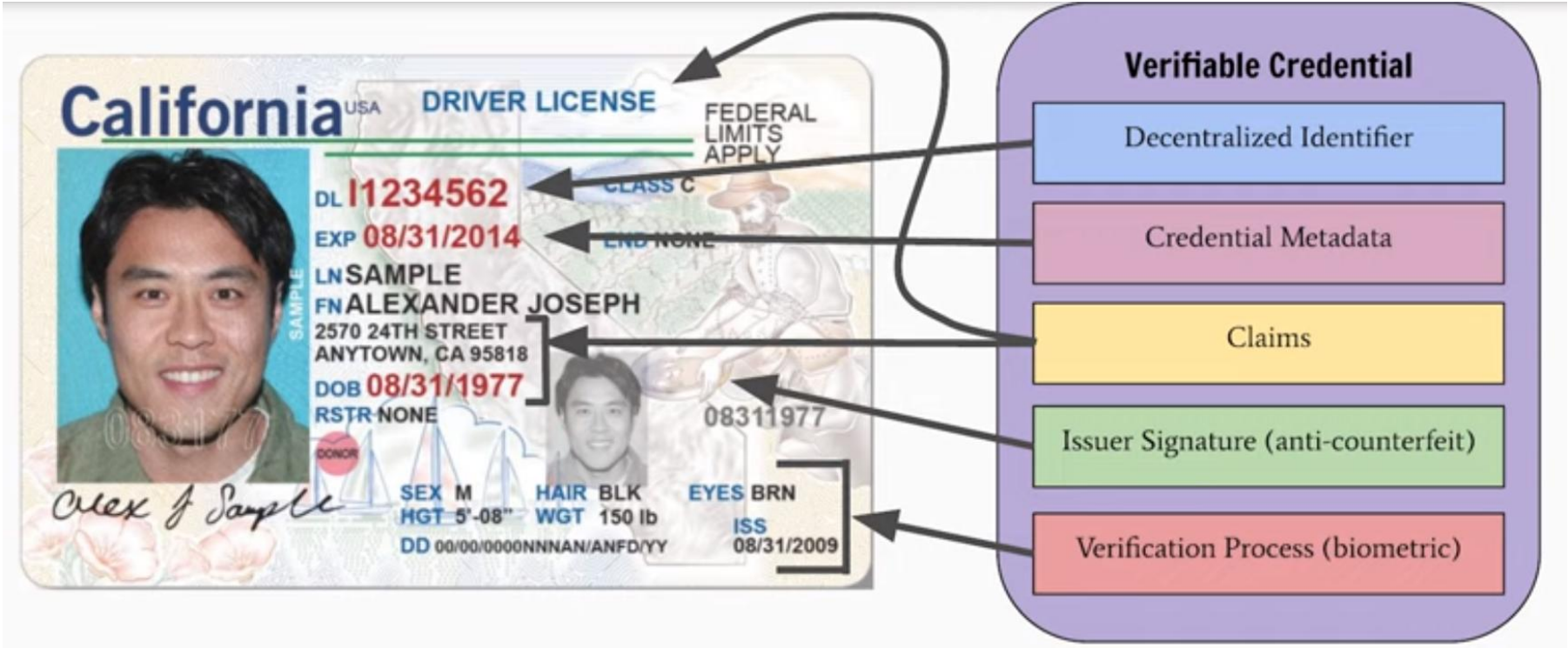
可验证的证明



Veriable Credentils 可验证的证明

Veriable Claims 可验证的声明

可验证的证明


California USA DRIVER LICENSE
FEDERAL LIMITS APPLY
DL I1234562
CLASS C
EXP 08/31/2014
END NONE
LN SAMPLE
FN ALEXANDER JOSEPH
2570 24TH STREET
ANYTOWN, CA 95818
DOB 08/31/1977
RSTR NONE
DONOR
SEX M
HGT 5'-08"
HAIR BLK
WGT 150 lb
EYES BRN
DD 00/00/0000NNNAN/ANFD/YY
ISS 08/31/2009
SAMPLE
08311977
Verifiable Credential
Decentralized Identifier
Credential Metadata
Claims
Issuer Signature (anti-counterfeit)
Verification Process (biometric)

可验证的证明

Baas 怎么使用可验证的证明

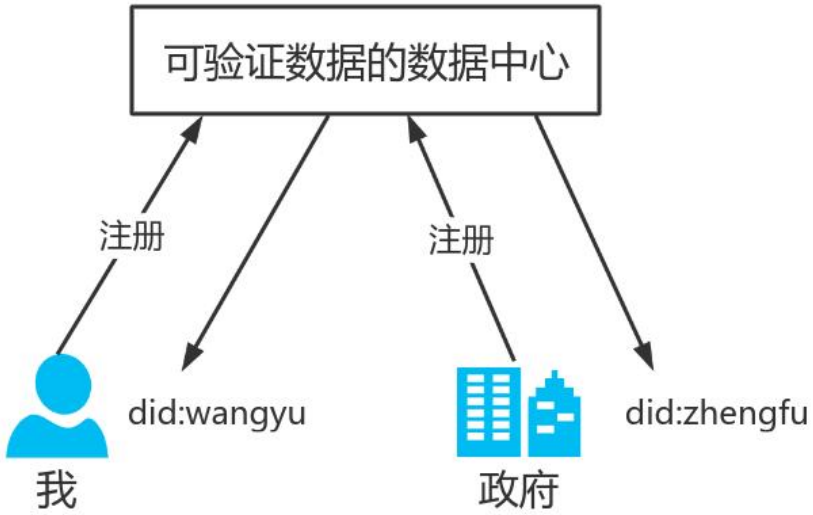
可验证的证明

Baas 目前的数字身份机制：

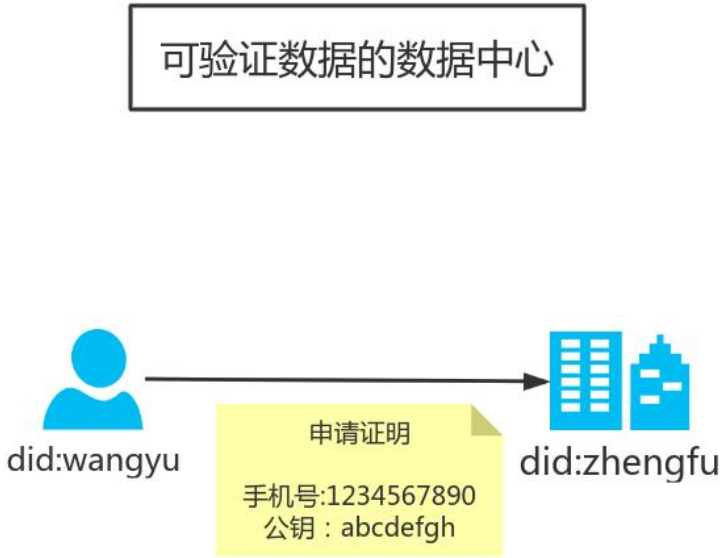
手机号码 + 密码

可验证的证明

注册


可验证数据的数据中心
注册
注册
did:wangyu
did:zhengfu
我
政府

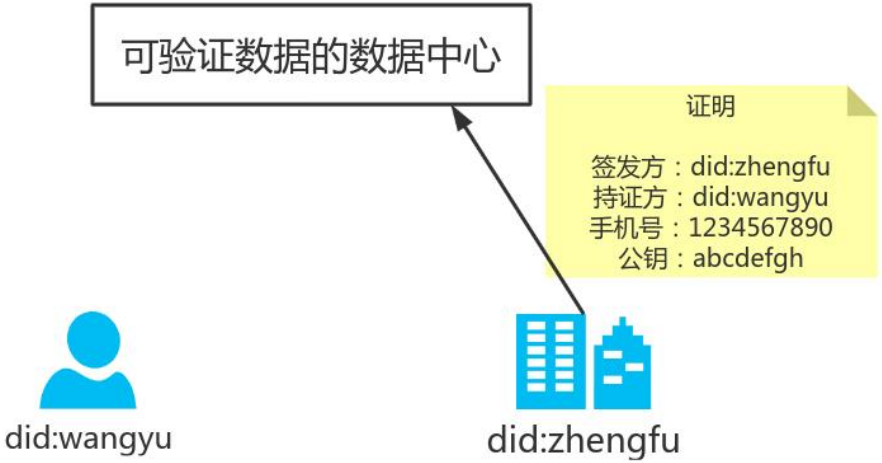
（1）


可验证数据的数据中心
did:wangyu
申请证明
手机号:1234567890
公钥：abcdefgh
did:zhengfu

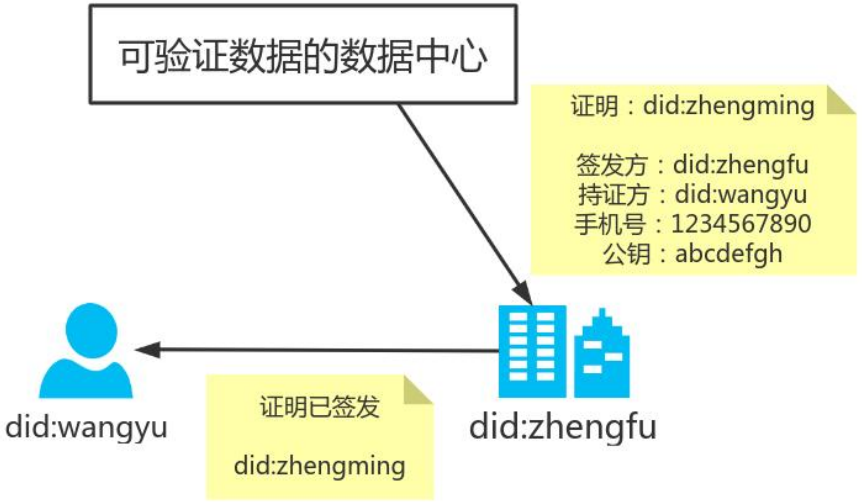
（2）

可验证的证明

签发证书



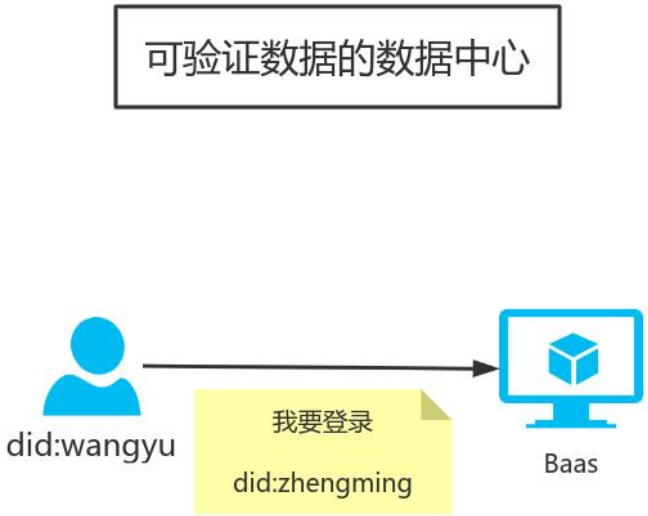
（3）



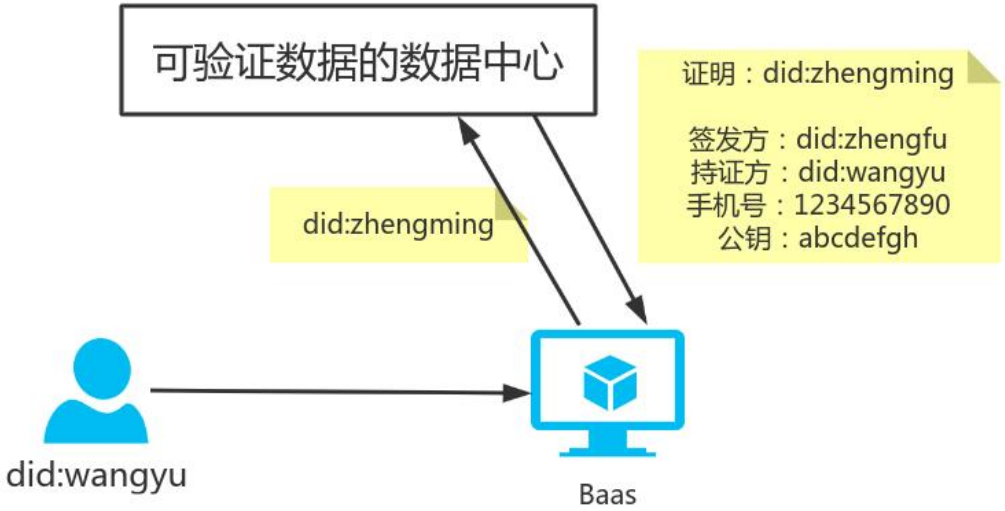
（4）

可验证的证明

申请登录



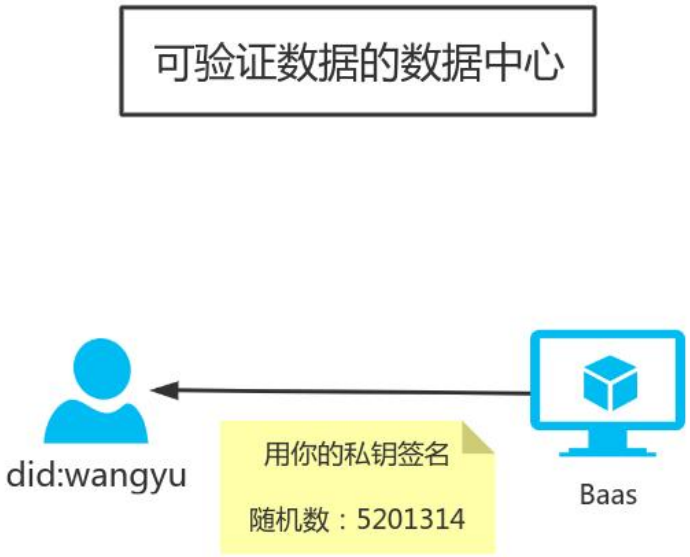
（5）



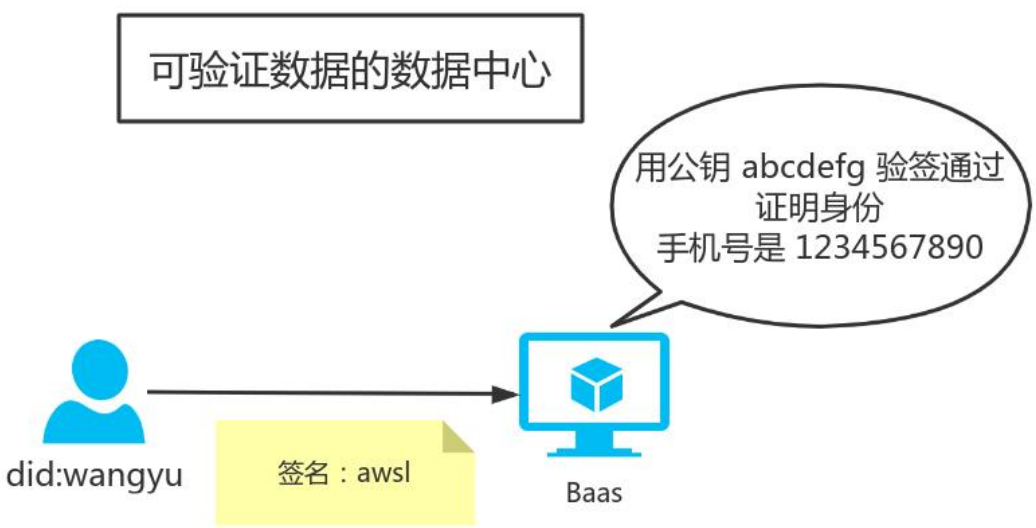
（6）

可验证的证明

验证 DID 所有权（DID Auth）



（7）



（8）

可验证的证明

为什么用户不直接告诉 Baas 手机号是多少？

可验证的证明

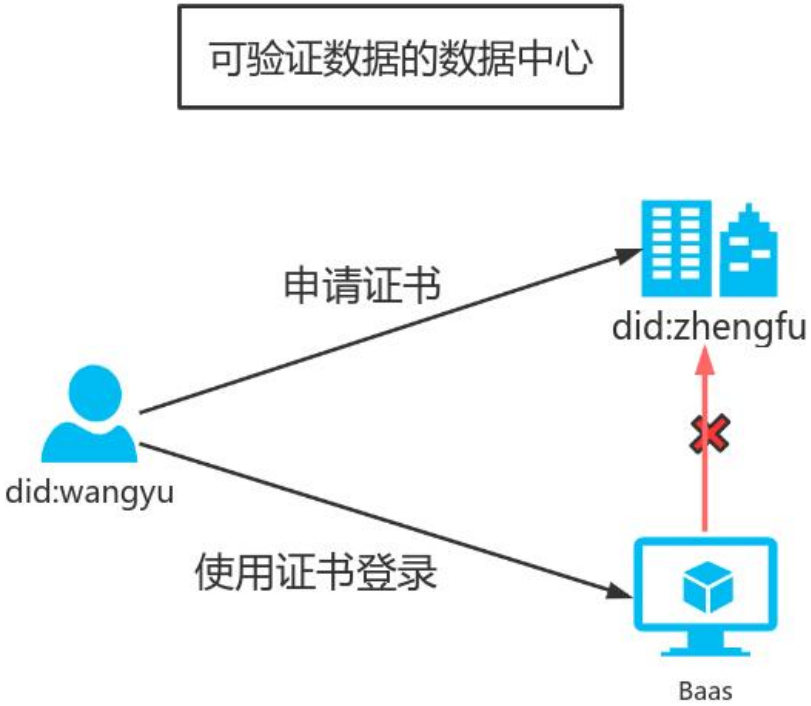
公钥/私钥 机制是必要的吗？

为什么不再用账号密码？

可验证的证明

可验证数据的数据中心（Verifiable Data Registry）使用区块链，区块链起到了什么作用？

可验证的证明



Baas 需要和政府直接通信，验证证明有效性吗？

可验证的证明

私钥丢了怎么办？

Decentralied Key Management System （DKMS）

去中心化的密钥管理系统

可验证的证明

可验证的证明解决了什么问题：

1、权威机构背书，签发了数字证明
2、数字证明是机器可读、机器可验证的

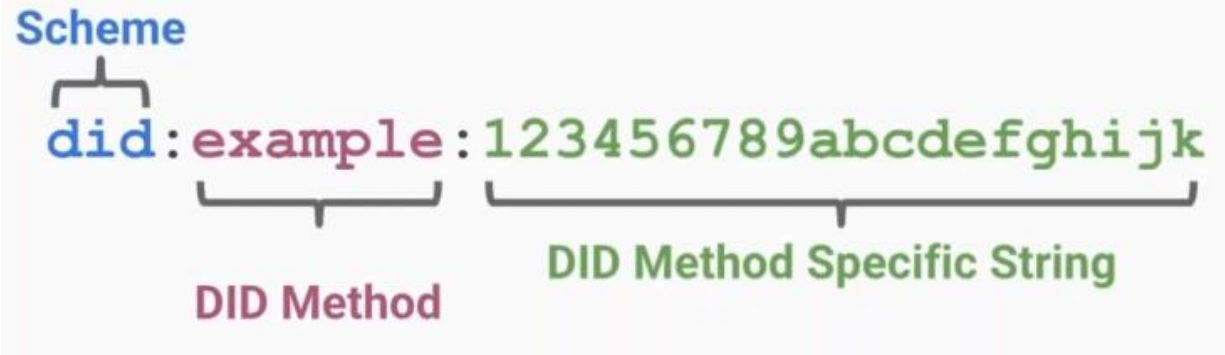
目录

去中心化的身份标识

Decentralized Identifiers (DIDs)	去中心化的标识
Digital Identity	数字身份

去中心化的身份标识

DID



去中心化的身份标识

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

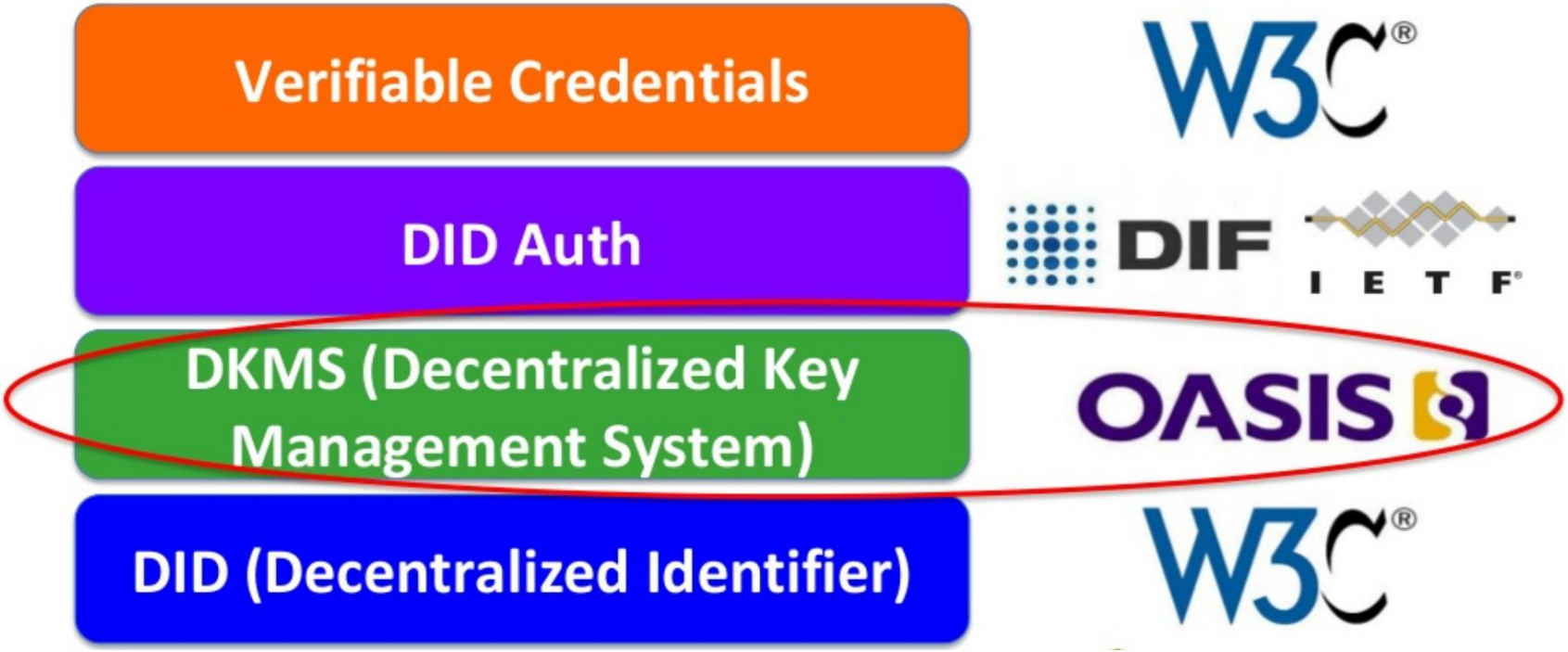
DID 文档

去中心化的身份标识

Linded Data　　有连接的数据

JSON-LD（JSON for Linking Data）　　DIDs默认选用

SSI的相关规范


Verifiable Credentials
W3C
DID Auth
DIF
IETF
DKMS (Decentralized Key Management System)
OASIS
DID (Decentralized Identifier)
W3C

目录

接下来的计划

2020年四季度目标（10月1日 ~ 12月31日）

1. 完成解决方案文档的 1.0 正式版本。
2. （可选）以白皮书为目标改善解决方案文档。
3. 开发 DIDs 实现，通过 test suite。
4. 沟通 w3c，了解加入 DIDs 案例列表问题。
5. （可选）加入 DIDs 案例可能需要写完整的 specification。
6. 规划 Verifiable Credentrails 实现开发计划。

2021年一季度目标（1月1日 ~ 3月31日）

1. 开发 Verifiable Credentrails 实现，通过 test suite。
2. 规划 agent 开发计划。

2021年二季度目标（4月1日 ~ 6月31日）

1. 去中心化身份认证平台具备演示和接入应用的能力。

要点：

文档大于代码

方案大于实现

感谢聆听　敬请指正