
Metaverse
元界
区块链如何解决用户隐私安全困境
Metaverse CTO 陈浩
Nov.30th.2017

# •目录

# Part 1

# 身份与数字身份

# 身份的概念

## *什么是身份*

个体或机构在自然时间序列上的发生的一切客观有序事件集合的的统称，该集合具备某种或多种特征，拥有可被验证、可被授权两大核心功能。

## *什么是数字身份*

是指上述概念发生在计算机系统和网络中的身份，被称为数字身份。

## *什么是区块链上的数字身份*

由不同角色组成的身份账本在区块链上的记录集合，且具有唯一标识（DID），可被元界区块链识别的身份。

# 身份终端与身份账本

## *身份终端*

是指用户进入元界区块链网络的代理，它可以是区块链钱包，也可以是硬件设备，该代理具有验证身份的功能，例如通过指纹验证，通过人脸验证，以及传统的账号密码验证，验证通过后即可使用区块链数字身份的数据和功能。

## *身份账本*

是指是指一个特定身份在区块链上的记录集。

Part 2

# 用户隐私与匿名

# 用户隐私与匿名

## *两种不同的事情*

- 用户隐私(Privacy)是一种概念(conception)，是由社会文化形成的对个人边界描述，是一种数据。
- 匿名(Anonymity)是用来表述主体的状态，是一种功能。

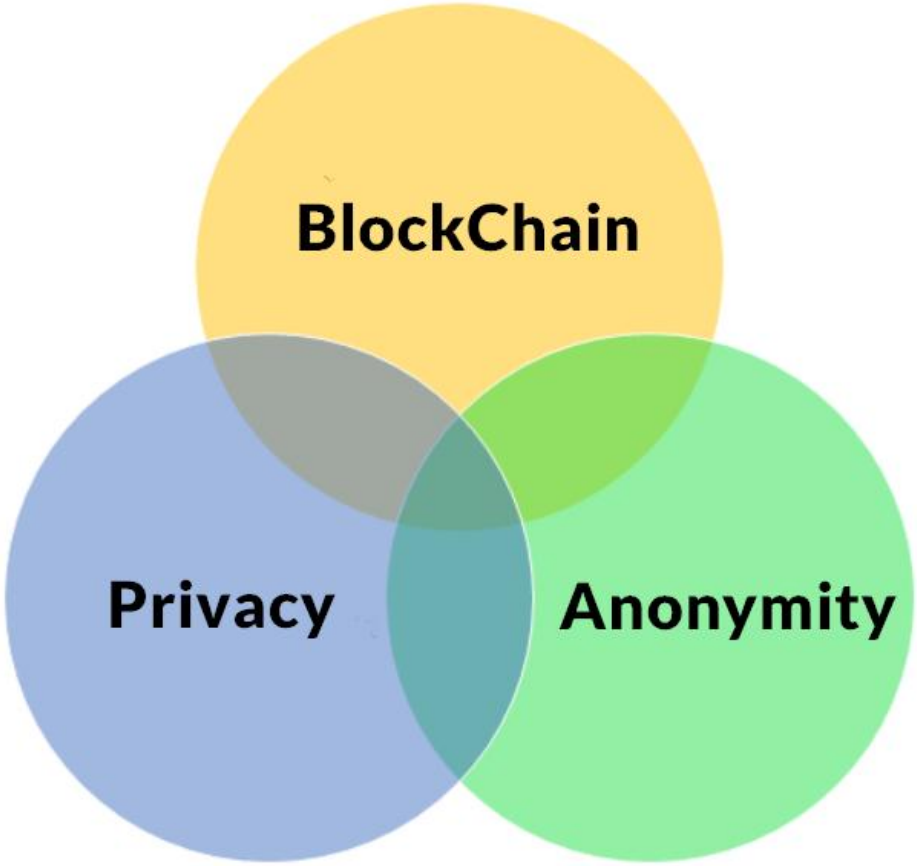
## *从匿名性到数字身份*

- 必要不充分条件。
- 没有身份的概念，无法形成边界。
- PII (Personally Identifiable Information)

# 用户隐私与匿名

- ***身份账本未必包含用户隐私***

- PII 驻留身份终端
- 身份账本提供匿名性操作



# 目前具有匿名性的币类

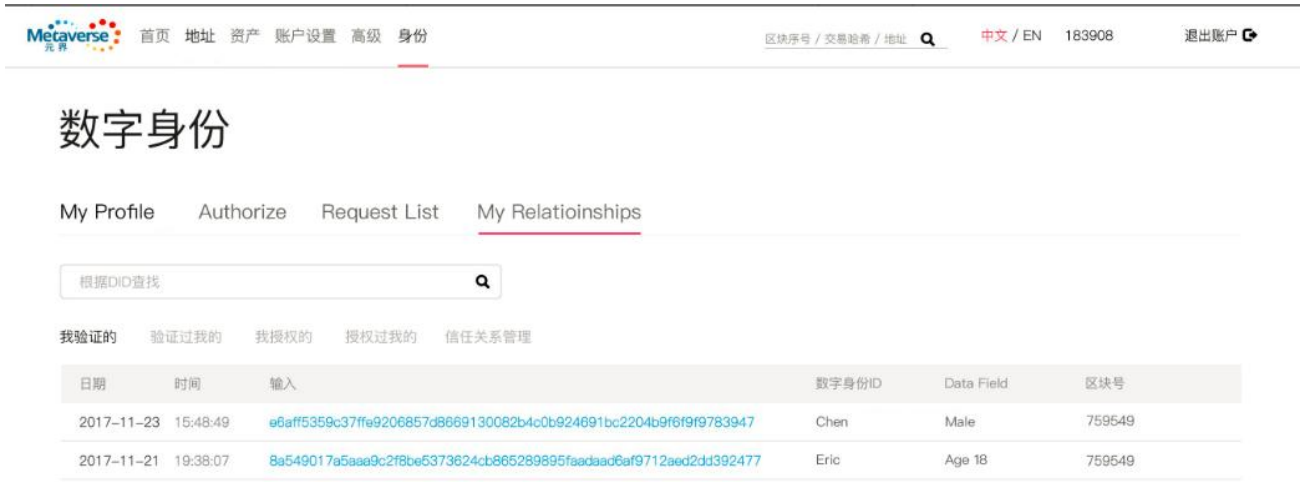
| 币种 | 主要技术 |
| --- | --- |
| **达世币(Dash)** | 混币（CoinJoin）<br>1.链式混合<br>2.盲化技术 |
| **门罗币(Monero)** | 隐蔽地址-stealth address<br>环签名-ring signature |
| **零币(Zcash)** | 零知识证明-Zero Knowledge Proof |

Part 3

# 数字身份与匿名性

# 数字身份的匿名性要求——高

- ***元界区块链内置数字身份***
- 支持隐蔽地址-stealth address
- 支持环签名-ring signature
- 支持零知识证明 - ZKPs




network.cpp (test\test-net) | Search Results | settings.cpp (src\lib\network) | stealth.cpp (src\lib\bitcoin\math) | validate_transaction.cpp (src\lib\

```
29: #include <metaverse/bitcoin/utility/data.hpp>
30: #include <metaverse/bitcoin/utility/endian.hpp>
31:
32: namespace libbitcoin {
33:
34: using namespace chain;
35:
36: bool is_stealth_script(const script& script)
37: {
38:     if (script.pattern() != chain::script_pattern::null_data)
39:         return false;
40:
41:     BITCOIN_ASSERT(script.operations.size() == 2);
42:     const auto& data = script.operations[1].data;
43:     return (data.size() >= hash_size);
44: }
45:
46: bool to_stealth_prefix(uint32_t& out_prefix, const script& script)
47: {
48:     if (!is_stealth_script(script))
49:         return false;
50:
51:     // A stealth prefix is the full 32 bits (prefix to the hash).
52:     // A stealth filter is a leftmost substring of the stealth prefix.
53:     constexpr size_t size = binary::bits_per_block * sizeof(uint32_t);
54:
55:     const auto script_hash = bitcoin_hash(script.to_data(false));
56:     out_prefix = from_little_endian_unsafe<uint32_t>(script_hash.begin());
57:     return true;
58: }
```

# 数字身份与用户隐私

## *数字身份的Profile*

**Verifiable Profile – 用户隐私的关键点**

- Profile 不推荐包含PII；
- 如果作为机构Profile ， 需要公众监督， 需要绝对公开；
- 具有信任关系的数字身份之间可以完全或部分共享Profile；
- 基于信任关系构建新型BaaS应用。

# 数字身份的更多特性与功能

- 去中心化的个人声誉
- 个人信息授权/数据交易
- 结合BaaS 应用
- 人-人/机器-机器/人-机器交互记录

Part 4

# Q&A Time


Metaverse
元界
THANK YOU