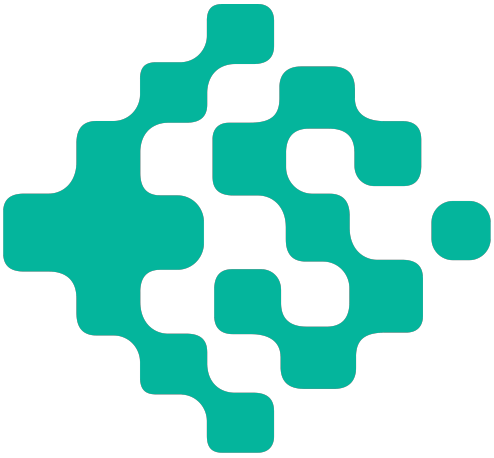

Litentry

Authorization and Data Exchange Infrastructure

分布式身份数据协议框架

Lite Paper

2019年10月

1 ，ð

ô力于创　一个ú于区W þ „分布式身份数据协议　协议包ì身份数据„授权　认证¡　　w S来说

1. 利(区W þ €术Š　ß Q Ü平台上„不　身份数据S　　一个(7不　•(　个平台上建Ë ê ñ „á o
2. Š身份á o I • Á数据„¡　权l û Ù(7　(7可以　ê ñ „身份数据　Ç加Æ ¨ X(本0　　ê ñ指š „Q Ü z ô
3. 协议包ì loT i T Q设　„身份认证　　i T Q时代' Ï „á o数据与人Œ Ä Ç ž °ù应
4. 协议M W „o件开发平台Œ l件认证设　•　业(协议之上可以{松„建Ë(于ê身F业：o „应(
5. 协议ú于â卡Q Ü „è þ y '　极' „ž强了i U '　不仅可以与当前ò有„Í区W þ Ô，Ô y币　以* J ø Þ　　时也可以与一些F业T ß之ô „T ß þ ø Þ Ô，IBM „… § &本[1].

2 Ì o介Í

• @ K机应(　'数据分析　5 P F务„A L　数据变得Š来Š Í •　F / •之　来„Ø有数据„^ Õ • (　个人• Á数据„Ä　　ù ê身身份I s . 数据„Ý ¤ ò　为新Q Ü时代Ï个人„' ¾ ˜

(诸　¿上¿下：o Ì ë无，制„á o授权请B　•　们Ä　了Ç　„数据　«(于È利' „(7 L为分析　(7 ; Ï　　þ Ï í á p ¸ „方式(Q Ü时代Ì变　了+)可Á „广J　　ó(Ù个万i互T „时代　　们@ - 买„@有IoT设　　v È ï上　„á o　ý首H去往了中心化„服务h　= ¡ Ï ' ß ò Ï ú台了‹ ，GDPR[2] Ù样严厉

[1] https://www.hyperledger.org/
[2] https://gdpr-info.eu/

„ • Á Ý ¤ 条 > F / (Ñ € l 司 … è 仍 6 (诸 „ € 术 K µ 来 ž ° ù 数据 „ 收 Æ € 术来取代 á 任 Litentry 提 › 了一个去中心化 „ 径来 ž ° 设 身份 „ ¡ Œ 授权也 (区 W þ „ Æ f € 术 ž 强 (7 • Á 数据 „ ‰ h

中 业 ù 互 T Q è 4 们收 Æ „ (7 身份 á o Š 来 Š • V (服务业分 å Š 来 Š ¾ Æ „ 今) 一方 b 中 业必 { Ç 中心化 Q Ü 平台来 Ç á o 授权来 Û L 服务 ù 平台产 了 • V 丧 1 v 他平台 ¢ 7 „ 不 ý ê 1 „ é 开发 „ å w 一些 c „ á o 服务 F 也 • 平台支付 9 (来 (7 „ 数据从事业务 另一方 b è 4 · 得 „ á o Š 来 Š Ã ¿ 不仅提 Ø 了身份 Ä „ û ß ' Î i 也 • 付 ú Ø „ ¡ 本去 • M 单 ¹ 故 œ Î i Œ 本 ý 最 È l 嫁到 (7 Litenty (去中心化 K µ ž ° 身份 á o „ A l 不仅 • 中 业 ž ° 与互 T Q è 4 ø Þ 争 „ È 利 ý 力 也可以 Ç € 术 • (7 ù 数据 „ • (中得到方 ¿ 并从 á o „ 授权中 · 利

一些 ‹ P Ô , 2016 年 Å 虎 „ (7 á o Ä 2 事件 Å 虎 ê ñ „ l J ð 有 « 影 Í „ (7 数 Ï Ø ¾ 5 亿 [3] v 中有数千万中 ý (7 d 庞 ' „ 0 下数据交 产 „ 数据 Ä 2 Œ Î i 也无可 0 Ï 2017 年 ù 果 „ ~ ¢ á o (中 ý m 到 ^ Õ . 卖 · 利 Ø ¾ 730 万 Ž C [4]

3 协议 y ¹

3.1 去中心化 , 念

Litentry 提 ú „ 去中心化 包 ì 以下 à 个方 b

身份 á o X ¨ „ 去中心化 个人身份 „ í 证 不 (¨ X (中心化 „ 服务 h / 可以 ¨ X (个人指 š „ 任 U 设 上

身份 á o 认证 „ 去中心化 Ï 一台 Œ 证设 只 • 可以 š 期 „ Œ 整个区 W þ Q Ü Û L á 1 可以 ì Ë „ 去 Œ 证身份 á o ó / » ¿ Û L

身份 á o s û „ 去中心化 以往 数据 Œ 个人 „ ù 应 s û • Ç l Á ¥ Û L 加 Æ Œ Ý X (一个中心化 „ 服务 h Ô , (互 T Q 中 Ï 一个 Q Ù „ 证书 ý ¨ X

[3] yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security
[4] cn.nytimes.com/business/20170612/china-apple-personal-data-sold/

(CA中 区Wþ中 Ù个áoÝX(整个去中心化QÜ利 本ôN 也ô‰h

身份áo来•„去中心化 Ï一个认证áo„来• ý可以有 个 Ô,f历„áo可以f校˜方提› 也可以1 f fb ž习å\„l司I机构来提› 并提›ù应 Gáo„Vé机制

3.2 QÜ互 '

Litentry ú于Polkadot[5] QÜ 得到了Web3 ú Ñ „yî支持[6] Web3 ú Ñ ô力于构建web3.0„ú@设施[7] S 一个去中心化„新互TQ¯ƒ Litentry„身份认证,念/web3.0,念中Í•„ Ä è分

,ÑWT@: (QÜ„vB/Polkadot协议 他(来Þ接不 „区Wþ Ï以*J[8] EOS[9] IBM…§&本ý可以 ÇPolkadot来调(Litentry中„ 个!W ¨Xû ß中Œ&号身份øs„¶ Ô, (以*J中 •X¨vÏ一个ÿå服务h„å有 Ù个列h可以¨X(Litentry中 v他@有„区Wþý可以从Litentry中来调(øsáo 并且•(们提›„一些方¿„接口功ý

(ÑWT底B/ 个wS应(:o„zý ¦ 他们可以

ô接调(Litentry ê身„Œ证授权„ý数

与v他„zý ¦ÛL á Ô,ÙÌ有一个e身?„zý ¦ Œ一个q享办l¤„zý ¦ (7(e身?ÛLŒ证时可以去检查(7/&(DÑ„q享办l¤èŒ ,果& 条件则可以不 •e身?授权即可Ûe

ÇLitentry ž°与v他区Wþ上zý ¦áo„互

Ç以上„BB互 ÏB之ôáo互享 cž°了èþè平台身份áo„互T

[5]https://polkadot.network/
[6]https://medium.com/web3foundation/web3-foundation-grants-wave-3-recipients-6426e77f1230
[7]https://web3.foundation/
[8]https://www.ethereum.org/
[9]https://eos.io/

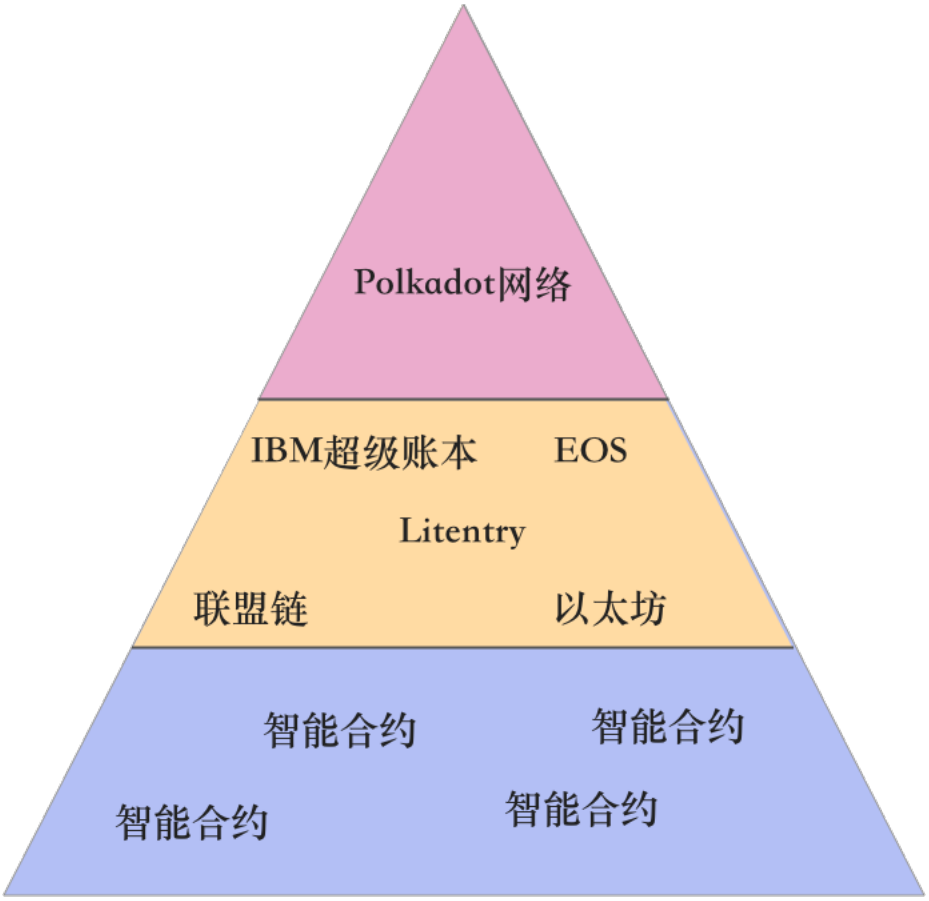

Figure 1: 区 W þ Q Ü B § 架构

3.3 协议 • 素

Litentry „ 协议中　　们主 • 包 ì Û 个 Í • „ C 素

D1 å 有权 P „ 人　Ä Ç （整个区 W þ Q Ü 中 ý 有 ù 应 „ Æ ¥ ù Œ l q 0 @　　们可以　ã 为　ß Q Ü 中 „ & 7　与 (7

D2 人 „ 身份　i T Q 设　„ 身份 / 一个广义 „ 身份 , 念　不仅包 ì 人 „ 身份　也包 ì i „ 身份　Ï 个 (7　ê 6 人　Ä Ç　可以 å 有　个　ó 不　„ 身份　Ô , (北京市 è Œ „ 身份　(1 ™ < 亚 è Œ „ 数 W l　　(l ‰ è　案 „ 身份 I　Ï 个

（7也可以　时å有不　设　„身份　h：ù某一台设　„@^权

D3 授予„权P　/ù应„身份授予„　可以证　w有ø应ý力„权P„一串数据　Ô，某个人ùvyšáoÔ，年龄临时„读取权利　　ù某个q享设　Ô，q享3DS印机一µ时ô„•（权II

D4　è数据　/权P（AlÇ　中产　„ù应„áo　Ô，（读取年龄áo/产　„Œ证/&á18•„请B时ô　0¹Œ：o　　/3DS印机（以上‹P中„S印参数　Ù些ý　Z为　è数据发　Ùù应授权身份„人Œ•（授权„人　双方　方　　也1/仅仅包ìÙ个;动„参与

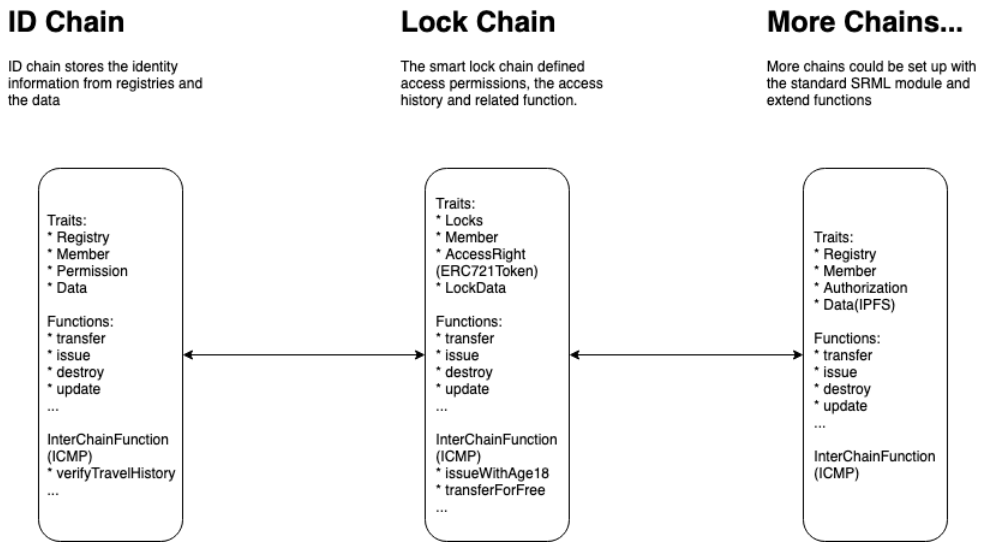

Figure 2: 协议：‹

下b　们以è　为‹　某个　¿„　板Ç（了　们„协议　他1/D1权P„å有（êñ„　¿中‰Å了一个zýè　（区Wþ中èŒ了ù应身份áoD2　也1（整个QÜ中l：了êñùè　设　„å有权　d　　Ç区Wþ授权10月1日当）„•（口令D3Ù了？¢A　？¢A　Ç　权PÝX（K机app　Litentry Signer　中　当）eO时　è　Œ证设　　时检查了？¢A„口令D3以及v（区WþQÜ上„á（记录　n认无误　Œ证　功　　O¿„áoD4　Ù个áo　ÔØÙ？东Œ？¢　ÇÙÍ方式可以　ú　　们以去中心Œ‰h„方式q享人　IoT设　„身份　整个Ç　Z到Œh¡有，三方平台„参与

3.4 Ï N ！ ‹

3.4.1 Œ证

＼为整个 „开/ Œ建设 们 •不 „Œ证：o „接e （Ï一个Œ证：o中 ý •有Œ证设 有时 /K机 ô „：o下/一个IoT设 他们ý •š期与区W þ Û L á （Ï一！ á „Ç 中 1 时w到了ô ¤区W þ Q Ü „＼（£么1可以 时·得Q Ü上 证„V励 £么‰Å Ù样一个Œ证„设 1可以š期收到token „V励 Ù样1可以À励早期„参与 加e Litentry

3.4.2 á o提›

时为了À励ô „身份á o提› 参与到Q Ü中来 们ù，三方提›„可`数据á o Ô，上b‹ P提到„教²Ì o á o Œ证 功之 3请Œ证 支付一š„token Ù á o提› à为提› e h了@：„á o Ù样也 •整个Q Ü „á o提›方Š来Š'

3.4.3 Q Ü提›方

ù于 杂„F业：o来说 1 •建Ë z ý ¦ Ï一！z ý ¦„g L ý ^极 Ï „gas 9（ Ù个9（1 提› Ù Q Ü „ÿ å 来支付Ù他们ô ¤Ù个Q Ü „9（

3.4.4 Litentry y î本身

ù与Litentry 们（Ï一！è Œ3请身份„时 以及授权„时 收取^常 „9（ 得Ê与可 „区W þ Q Ü Ù个9（（早期时 （7 „时 ^常N （y î Ÿ之 可以收取^常 „9（来支持y î „Ð营

时＼为一¶„€术l司 们也制＼了o件„开发框架 Œù应标Æ化„l件Œ证设 们 Ç€术支持 以及l件„ .来提Ø ê身„利¦

3.5 l件框架

们î前„ l件ž °了ú于树“ > „ ~ Œ证 • @5G IoT l件Œ ¹ 计– „发U z ý l件未来 „ ž加 们l件 ' Ä ! Ç (Litentry协议Z了E ³ „ Æ

们ù与ú于ARM框架„区W þ l件有@ ƒ丰Ì „ Ï Œ 们c (开发

区W þ { ¢ 7 ï Œ证设 设 „ Á ¥ ¨ X (设 „ l件TEE(可á g L ¯ ƒ)[10]中 • 得设 Á ¥无Õ Ç任U K µ ü ú Ù样得到Ü Ø于o件„ Ý ¤ • 得Œ证设 „ ‰ h ' ' ' 提Ø

ú于加Æ ¯ G „ N功 5 P身份卡 Ç接æ › 5 … n ~ ! W • 得Œ证„ • (, á (卡Œ身份证一样方¿ 时 Ç ö å识证 (Zero Knowledge Proof) ã ³了á o读取时„ Ä î ˜

â X有@ 年加Æ D产± 包„开发Ï Œ 们开发了ú于iOSŒ ‰卓l件加Æ „ K机o件 Ç (了î前业…最Ø „加Æ方Õ

3.6 o件€术

整个û ß „ o件框架主 • 分为以下à个 ! W

区W þruntime代 [11] Ù Ì / Litentry „核心 ; ‘ 提 › 了与不 区W þ之ô „ 接口

前ïweb交互app[12] Ç (rust语 开发 ô接 译区W þ上„ ¢ 7 ï文件 不仅提 › 了ô „功ý 也可以极 ' „方¿身份以及数据á o „查询Œ ¡ @有„ F业 : o ý可以 • (也支持ù应„ š制

ú于Rust语 ŒGraphQL中台数据查询服务h[13] Ç š期„ 区W þ Q Ü查询Œ证历史á o 并 Ç ' 数据来ž °数据„ X ¨ Œ提 › X Œ证设 提 › 一

[10]https://en.wikipedia.org/wiki/Trusted_execution_environment
[11]https://github.com/litentry/litentry-runtime
[12]https://github.com/litentry/litentry-web-app
[13]https://github.com/litentry/litentry-juniper-api