陀螺研究院 X SECBIT X 金融壹账通 ONECONNECT

零知识证明技术发展报告

2020年5月

联合发布

陀螺研究院 Tuoluo Research　金融壹账通 ONECONNECT　SECBIT　成都链安 BEOSIN

Shenzhen University
Blockchain Technology Research Center

深圳市信息服务业区块链协会

版权声明

指导单位： 深圳市信息服务业区块链协会
协撰单位： 深圳大学区块链技术研究中心
编委会成员
指　　导：余文锋　杨达豪 郭宇 张胜利 贾牧
主 笔 人：余维仁
编写人员：卢艺文　余维仁

前言

4月初，从在会议中播放色情内容的“Zoom轰炸”，到偷偷向Facebook发送用户数据，视频会议软件Zoom的隐私丑闻持续引发大家的关注。联想之前炒得沸沸扬扬的脸书公司隐私泄露事件，隐私问题已经成为制约互联网产业发展的最大绊脚石之一。

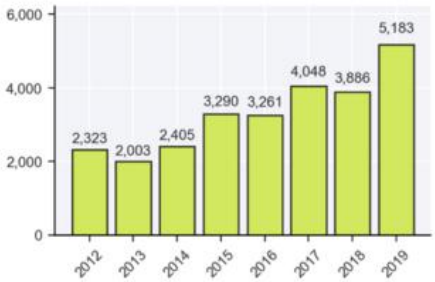

Figure 1: Number of breaches reported by 9/30 each year

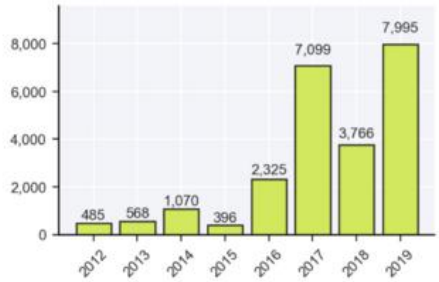

Figure 2: Number of records lost (in millions) by 9/30 each year

资料来源：Risk Based Security

回顾2019即将过去的一年，大规模的数据泄露事件频频发生，呈现爆发递增的趋势。据安全情报供应商Risk Based Security（RBS）的2019年Q3季度的报告，2019年1月1日至2019年9月30日，全球披露的数据泄露事件有5183起，泄露的数据量达到了79.95亿条记录！随着以人工智能、大数据和物联网为代表的信息技术革命的推进，数据的价值进一步凸显，数据成为了企业的重要资产和持续创新的推动力。因此，保障数据在采集、传输、利用和共享等各个环节安全的重要性不言而喻。

区块链作为一种底层技术和基础架构，将它与其他新兴信息技术，如人工智能，大数据分析，零知识证明技术，物联网，数据存储等，相互结合将创造极大的价值。它能够在金融服务、政务管理、能源管理、知识产权、公益、监管、数据共享、供应链管理、保险和存储等领域发挥重要的作用，甚至是颠覆性地变革。

零知识证明技术做为现代密码学的重要组成部分，它能够在不泄漏任何秘密信息的前提下完成对此秘密信息的验证。零知识证明技术对于解决当前信息安全中的诸多问题，如数据安全、隐私安全、监管检查等都能够发挥重要的作用。零知识证明与区块链的完美结合很好的解决了区块链当前面临的困局。一方面，区块链公开透明的天然特性，使其在在隐私和数据安全问题上存在诸多局限；另一方面如何解决性能问题，提高吞吐量和响应速度是当前区块链大规模落地所面临的最大问题。

目录
Table of Contents

一、区块链与零知识证明技术综述

自 2008年中本聪白皮书发布以来，区块链技术至今已经历了 12 年的发展，期间不乏许多戏剧化的演变。从早期在密码学圈子里兴起，到中间经历了资本疯狂泡沫的时代，再到如今逐渐回归理性，区块链真正服务于社会的价值也慢慢凸显。如今区块链在信息技术已经明显占据了一席之地，也是各国争相角逐地新的技术竞技场。

而在过去十多年的技术和应用演进中，区块链已经不仅只是中本聪白皮书中所描绘的一种点对点支付协议，而是在它原生支持支付和弱化第三方的基础上，结合更多技术和应用需求，逐步发展成为“世界计算机”。但随着区块链应用的不断探索，近两年数据隐私和性能扩展成为社区最广泛讨论的问题。根据目前的实践来看，零知识证明正是解决这些问题的最有力武器，随着技术的落地，零知识证明如今已经成为区块链技术中不可缺少的一环。

互联网与大数据技术的快速发展，为社会生活带来了翻天覆地的变换。信息数据时代，每天产生海量的数据，小到个人信息，大到国家数据信息，这些数据既在当下拥有不可估量的力量，对预测未来的发展趋势也尤为重要。新华社 11 月 5 日发布了《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》，正式将数据列为生成要素。数据资产化已经成为不可阻挡的趋势。而区块链作为重塑生产关系的关键因素，也将在数据生产，数据共享，数据确权和数据保护中发挥了重要作用。

其中值得一提的是隐私数据泄漏的问题和数据所有权的矛盾已经变得尤为突出，这对个人人身安全和财产安全带来的威胁都是致命的。所以如

何数据隐私安全问题和数据所有权问题是当下技术研究的一个重要方向。研究人员渐渐将目光转向区块链领域，尤其是结合以零知识证明为代表的密码学方案去解决这类问题，是具备极好的优势的。

区块链由于本身的限制，导致其无法在性能和交易处理速度上达到传统应用的要求，这一点严重制约了区块链的大规模落地应用。因此如何提高区块链的性能及其吞吐量尤为关键。零知识证明技术在压缩数据量提高性能方面可以发挥很大的作用，这一点很好的弥补了区块链的这一约束。

二、零知识证明技术发展

2.1 零知识证明的概念

零知识证明技术是现代密码学的一个重要组成部分。它是指证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。

一个零知识证明必须满足三个性质：

1.完备性（Completeness）：当证明者和验证者都表现诚实，遵循协议来执行验证步骤时，如果证明者的陈述是真的，那么一定可以被验证者接受。

2.可靠性（Soundness）：如果证明者的陈述是假的，那么任何一个作弊的证明者不可能使一个诚实的验证者相信他的陈述。

3.零知识（Zero-knowledge）：证明执行完成后，验证者仅能知道证明者的陈述是否为真，除此以外，他在证明过程中获取不到其它任何信息。零知识证明技术的背后依赖于强大的理论基础，如计算复杂性理论和信息论。包括图灵机，概率可检查证明，P/NP 问题等等都在其研究范围内。

2.2 理论发展

零知识证明技术的理论研究已经过了三十几年的发展历程，目前也已取得了非常显著的成果，但直到近十年来，其巨大潜力才逐渐突显出来。如今，零知识证明理论研究正呈现一种百花待放的态势。

2.2.1 诞生

零知识证明思想由来已久，早在16世纪的文艺复兴时期，意大利有两位数学家为竞争一元三次方程求根公式发现者的桂冠，就采用了零知识证明的方法。

但“零知识证明“这个概念真正在学术界被提出是在 20 世纪 80 年代中期，由 S.Goldwasser、S.Micali 及 C.Rackoff 三人在一篇名为「交互式证明系统的知识复杂性」[GMR85]的论文中提出。这篇论文在 NP 的证明系统中引入了”交互”和”随机性”，构造了交互式证明系统。同时这篇论文中还提出了零知识证明的这个名词，并给出了其性质的定义。零知识证明逐步成为密码学领域的一个理论研究分支。

2.2.2 奠基时期

随后的十几年里，密码学家们提出了一系列的概念，这些巨大的突破为后来的零知识证明发展奠定了基础。比如1986年，Amos Fiat 和 Adi Shamir提出了 Fiat-Shamir 变换，是一种将交互式证明系统变成非交互的通用方法。此外，为了实现非交互式零知识（NIZK）证明系统。M. Blum, P. Feldman, and S. Micali指出了”交互”与“隐藏随机性”并不是必要的，继而提出基于 公共参考串 CRS Common Reference String）模型的非交互式零知识证明系统。1992年， J. Kilian 提出了简洁非交互零知识证明的概念，并基于概率可检查证明（PCP）提出了一种证明系统。1990 年，德国数学家和密码学家 Claus-Peter Schnorr 提出一种基于离散对数难题的知识证明机制，它实现的签名机制（称为 Schnorr 签名）。1996 年，Cramer在博士论文中推广了 Schnorr 签名，正式提出了 Sigma 协议的概

念，这成为一种被广泛采用的零知识证明构造框架。1998 年，Ronald Cramer 和 Ivan Damg°ard提出了基于算术电路可满足性（NPC问题）的零知识证明系统，可以把通用的计算转换成抽象的算术电路，然后即可以用零知识证明来验证输入与给定的输出对应。

2.2.3 理论发展时期

经过 20 年的理论发展，零知识证明最底层的理论根基已经逐渐清晰，开始逐渐走向成型，并出现了不同的零知识证明技术分支。

2005 年，Dan Boneh, Eu-Jin Goh 和 Kobbi Nissim提出了一种基于双线性映射的单次乘法的同态公钥加密方案，于是在2006 年，J. Groth, R. Ostrovsky 和 A. Sahai. N基于这个工作提出了基于双线性映射的非交互式零知识证明技术，这也是第一个适用于所有 NP 问题的 达到“完美零知识”的论证系统（Argument）。该系统还有一个非常重要的优化就是它第一次通过采用椭圆曲线的双线性映射，大大缩短了 CRS 的长度以及证明长度。从此，椭圆曲线双线性映射成为零知识证明构造技术中相当重要的一环。

2007 年，Yuval Ishai，Eyal Kushilevitz，Rafail Ostrovsky 和 Amit Sahai提出了利用安全多方计算（ MPC，Secure multiparty computation)，产生零知识证明的技术新思路，被称为 MPC-in-the-head，它也建立了零知识证明的一个重要研究分支。

2008 年，Shafi Goldwasser、Yael Tauman Kalai和Guy N. Rothblum 提出了一种交互式的证明系统——GKR协议，这是一种实现可验证计算的美妙方案。这个协议也成为实现通用零知识证明的一个重要技术分支，比如后续的 zkVSQL、Hyrax、Libra等协议。

2009 年，Jens Groth提出了一种实用的实现常见矩阵运算零知识证明系统。证明系统无需 Trusted-Setup，基于标准的离散对数难题假设。这个证明系统奠定了一个重要的零知识分支，其中的向量内积证明、向量Hadamard证明是“防弹证明”（Bulletproofs）的重要理论基础，也形成了基于椭圆曲线的通用零知识证明技术的一个重要分支。

2010 年，Jens Groth 提出了一种在当时颇具争议性的安全假设——指数知识假设（Knowledge of Exponent Assumption，KEA），通过采取这个争议性假设，可以将零知识证明的长度缩短到常数级别。Groth 的这个大胆工作直接将零知识证明朝着实用性方向发展推进了一大步。但是，这个方案也引入了一个技术问题，并且在后来区块链领域应用中成为一个关注的焦点，这就是可信预设置（Trusted-Setup）。Groth 通过把一些秘密随机值隐藏到 CRS 中，实现了证明长度的大幅缩减，但是也带来了一些安全风险。无论如何，这一方案确立了未来十年最重要的零知识证明技术分支。

同时2006年前后，Eli Ben-Sasson 等人改进了 PCP 理论构造，将概率可检查证明的长度压缩到了准线性级别。这些学者的工作推动了基于 PCP 理论的通用零知识证明构造技术，成为后续 zkSTARK，Aurora 等证明系统的关键理论基础。成为无可信预设置，并且可以抗量子的零知识证明技术重要分支之一。

2.2.4 工程落地序幕

进入到21世纪的第二个十年，随着不同的零知识证明分支理论的发展，一些零知识证明技术已经初现工程实用的曙光。密码学家们开始在工程化方向上深入研究，也正式拉开了零知识证明工程化的序幕。其中在2012 年，Nir Bitansky, Ran Canetti, Alessandro Chiesa 和 Eran Tromer 发表

论文正式提出了 zk-SNARK （Zero-knowledge Succinct Non-interactive Argument of Knowledge）这个名词。大家意识到，证明长度必须要足够小，才能降低证明的验证时间，并且非交互性对实际应用极具诱惑力。

接下里，2013 年 Rosario Gennaro，Craig Gentry，Bryan Parno 和 Mariana Raykova的研究成果（GGPR13）意义重大。他们在 J. Groth 2010 年工作的基础上，提出了一种漂亮的改进方案，利用 QSP（Quadratic Span Programs）或QAP（Quadratic Arithmetic Program）技术，大大缩短了证明时间，并且把证明长度压缩到了很小的常数级别，几百个字节大小。随后，Parno 等人在此基础上实现了一个叫做 Pinocchio 的可验证计算协议，并且继续做了优化和改进，最重要的是，Pinocchio 协议不满足于停留在纸面理论阶段，而是做了完整的工程化实现，并且有力证明了零知识证明的工程可行性。Pinocchio 协议可以将庞大的计算压缩到不足300字节，并且证明时间接近线性。

2014年，Eli Ben-Sasson, Alessandro Chiesa等人稍稍改进了 Pinocchio 协议，并且提出了一个名为 ZeroCash 的匿名币协议，这是著名的 区块链匿名加密货币 ZCash 的前身。随后 ZCash 团队在零知识证明工程化方面做出了比较大的贡献。

2.2.5 应用驱动的繁荣时期

最近几年，随着区块链技术的蓬勃发展，零知识证明的应用场景也在不断增多，也不断对零知识证明的理论与技术提出了新的挑战。

区块链项目中以 ZCash 为代表的团队需要性能表现更加出色的方案，Groth16在 Pinocchio 协议上做了一步极致优化，在略微加强安全性假设的情况下，把证明尺寸压缩了将近一半，成为目前区块链领域中最广泛使用的零知识证明技术方案。

随着匿名加密货币的发展，更轻量级的金额范围证明有较大的需求空间。B. Bunz 等人在论文 [BCGP16]的基础上改进得到了一个可以聚合的范围零知识证明，该方案就是著名的“防弹证明”。它一经提出就迅速被 Monero 项目采纳并实现。当然防弹证明不仅仅可以用作范围证明，也是一个无需可信预设置的通用零知识证明技术，也逐步被一些团队采纳并应用。

Groth16 方案的使用不方便之处在于备受争议的可信预设置。Eli Ben-Sasson 等人在PCP 理论的基础上逐步发展出了“透明” zkSNARK，也被成为 zkSTARK。所谓透明，正是指预设置过程可以一种更加透明的方式来完成。并且 zkSTARK 主要基于 Hash 算法，不再依赖椭圆曲线，是一种目前可以对抗量子计算机的方案。随后的Aurora 等工作进一步改进了 zkSTARK 技术，目前已经成为极具竞争力的主流零知识证明技术之一。

2018年，Jens Groth 等人提出了一种可更新的全局CRS 方案——Sonic，所谓可更新是指，可信预设置可以随时进行更新，只要大家怀疑秘密已被泄露。所谓全局，是指计算过程不再与 CRS 绑定，一个应用只需要完成一次可信预设置即可实现不同的零知识证明电路计算。

此外，基于 GKR 协议的零知识证明方案，比如Hyrax 也可以实现透明预设置，但会牺牲一部分性能，而 Yupeng Zhang 等人通过加入全局可信预设置的折中方案，可以大大提高效率，这也是 Libra 方案一个优势。折中方案兼顾安全性与性能，获得了不少团队的青睐，新的证明系统 PLONK，Marlin 等都在这个全局可更新CRS基础上进行各种优化，并且取得了一些成果。

值得一提的是Jiaheng Zhang，Tiancheng Xie, Yupeng Zhang 与 Dawn Song 提出的Virgo 方案，这是基于 GKR 协议，透明预设置的高效证明系统，并且具有较好的证明生成性能。

区块链应用中有大量数据不断更新的应用场景，这需要可以递归组合的零知识证明，也催生了 Halo 与 Fractal 等递归零知识证明。
这些零知识证明方案各有千秋，需要根据应用场景来选择甚至改造，这无疑阻碍了零知识证明的标准化和落地应用。但斯坦福大学的 Dan Boneh 教授在近期一次访谈中，预言在几年内可能会有统一的零知识证明协议出现，进而可能会大大促进零知识证明的工程化，标准制定，以及落地应用。

2.3 工程实现

当前零知识证明技术的工程实现自 2013 年算起至今，尚处于早期阶段，还有很长的路要走。但零知识证明技术在近两年引起关注，越来越多的团队正在投入到这一领域，因此零知识证明技术的工程实现成果也在快速增长。 而随着区块链产业的进一步扩大和隐私问题的越发突显，相信未来对零知识证明技术的投入也将进一步提高。

本文整理了当前零知识证明技术在工程上的实现，并从技术结构，实现语言，开源库三个方面分析发展现状。

2.3.1 技术架构

当前零知识证明的技术实现架构大致可以分为五层结构：

1. 底层基础

底层基础算法库是实现零知识证明系统的前提，因为零知识证明技术依赖于大量的数学基础原理来完成计算，如有限域计算，矩阵运算，椭圆曲线运算等等。

如基于椭圆曲线的零知识证明协议中，就需要依赖大量的椭圆曲线实现。secp256k1，BN254 和 BLS12-381 是工程实现中大量使用的几条曲线。

在《中华人民共和国密码法》颁布后，国内一系列的应用也开始基于SM2、SM9等国密算法的曲线标准构建零知识证明系统。

2. 证明系统（proof system）

证明系统也就是零知识证明协议，拥有证明系统才能完成证明。零知识证明协议有很多，每一种协议的实现步骤也不尽相同，因此每一种协议都需要对应一个证明系统。目前应用最为广泛的当属Groth16，Bulletproofs。

3. 电路约束（circuit）

为了完成一次零知识证明，需要先将待证明的实际问题转换成证明协议可以验证的约束关系。这种约束关系是以电路的形式表示出来的。因此构造电路约束关系是零知识证明工程实现中一个非常核心的部分，它是建立在实际问题和证明之间的桥梁。

电路的构造是难度很大。一方面，由于不同问题所对应的约束关系不同，电路也有所不同；另一方面，构造电路的正确性难以保证，一旦构造的电路不正确，证明结果的可靠性就难以保证，并且尤其对于复杂的问题，约束关系若不完整或者不正确也很难被发现。

因此在实际的应用中，如何保证电路实现的正确性，完整性和高效率是尤为关键的一环。

4. 电路组件（gadget）

在实际的复杂约束关系中包含了很多复用的简单约束关系，如布尔值证明、范围证明和哈希证明等等，而这些约束关系经常被作为一个 gadget 集成在开源库中，这样即开发人员仅需直接调用接口即可正确得完成这部分的电路构造，这既简化了开发人员的工作量，也减少了开发过程中的错误。

5. 上层应用

上层主要分为两大类：

1. 在应用中直接通过调用零知识证明库完成电路构造和证明

2. 为了简化区块链上层 DAPP 开发零知识证明应用的难度，开发人员在区块链底层构建工具包集成零知识证明开源工具，如以太坊上的 SNARK 工具箱 ZoKrates

2.3.2 实现语言

出于不同实现场景的考量，零知识证明实现的语言也有很多种。

一方面，由于零知识证明中涉及大量的运算，对计算机计算速度的要求较高，因此大部分的零知识证明都选择使用系统级编程语言实现，如C++，Rust。

值得一提的是，Rust 语言作为一门同时兼具安全、并发和性能的现代系统级编程语言最近几年迅速蹿红，由于安全性和高性能又是零知识证明实现中非常重要的考量因素，因此基于 Rust 语言在零知识证明开源库非常多。

另一方面，很多开源库选择使用应用级编程语言，如Java，JavaScript。由于实际的应用场景非常复杂，而系统级语言相较于应用级编程语言功能比较匮乏，而复杂的使用环境可能会导致系统级语言的速度优势并不能完全凸显出来，因此在一些使用场景，开发人员会选择使用应用级编程语言完成零知识证明的开发。

2.3.3 开源库

据不完全统计，与零知识证明相关的开源库包括数十个，本小节仅介绍部分比较有代表性的开源库。

1. libsnark

C++语言实现的零知识证明开源库，由 SCIPR Lab 开发并维护。它是目前实现最完整，应用最广泛的零知识证明开源库。毫不夸张地说，libsnark 支撑并促进了 zk-SNARKs 技术的首次大规模应用，填补了零知识证明技术从最新理论到工程实现间的空缺。它实现了包括GGPR13，PGHR13，BCGTV13，BCIOP13，BCTV14，Groth16和GM17等等在内的多种主流协议。同时它实现了多个常用的Gadget电路。

2. bellman

是使用rust实现的零知识证明开源库。bellman是一个用于构建zk-SNARK电路的工具箱。它提供了电路特性和基本结构，以及基本的小工具实现，如布尔值和数字抽象。bellman实现了Groth16 协议算法。

3. dalek bulletproofs

是一个rust版本的 BulletProofs 实现，也是最快的 BulletProofs 实现。它提供了单一范围证明和聚合范围证明，强类型多方计算，和可编程约束系统 API。

4. snarkjs

这是一个基于 JavaScript 语言实现的 zkSNARKs 开源库。

5. ZEXE

这是一个基于 Rust 语言实现的 ZEXE 协议的开源库，它实现一个了账本系统，使得用户能够执行脱机计算产生产生可公开验证这些脱机执行的正确性的交易。该仓库实现的零知识证明协议有 Groth16 和 GM17。

6. ZoKrates

该仓库将零知识证明开源库（libsnark 和 bellman ）包装成统一的工具箱，以完成在以太坊上的zkSNARKs 调用。

7. ZkVM

零知识证明虚拟机（ the zero-knowledge virtual machine），它基于 rust 语言在虚拟机层面实现了对智能合约的 Bulletproofs 证明。

8. libiop

libiop 仓库使用C++语言实现的，它仅依赖轻量级对称密码学（哈希函数），提供透明和后量子的zkSNARK结构。该仓库实现了三种证明协议：Ligero，Aurora 和 Fractal。

三、零知识证明在区块链领域的应用

3.1 隐私保护

3.2 扩容

2020年 3 月 19 日，以太坊创始人 Vitalik Buterin 发布推文表达了自己对 ETH 2.0 未来约 5-10 年及以后发展的看法。Vitalik Buterin 表示，过去两年以太坊团队已经从“blue sky”研究阶段转向了具体的研究和开发，尤其指出 zkSNARK 技术也从最初的遥不可及变得越来越实际。

零知识证明技术的两个重要特点是使其能在区块链领域得到应用的主要因素：1）零知识证明能够保护数据的隐私性，在不泄漏数据的条件下对其进行证明；2）零知识证明仅需要生成很小数据量的证明就可以完成对大批量数据的证明。

3.1 隐私保护

区块链作为一种公开账本，一旦上链所有的数据全部公开，不免涉及到隐私数据，如个人身份信息，高安全级别的合规数据检查，资产信息等。而零知识证明在保护数据隐私上有着不可比拟的优势，因此零知识证明在保护链上数据隐私方面发挥着很大的作用。

3.1.1 链上资产交易

资产信息是一个人或者一个机构的隐私信息中非常重要的一部分，账户的资产信息及资产交易信息暴露在公开场合这对于资产管理无疑是很大的风险和威胁。而区块链的一个主要特征就是公开的账本，所有的交易信息都公开可追溯，虽然这在一定的程度上解决了信息不对称和欺诈的问题，但也确实对账户资产隐私造成了很大的危害。一旦用户与区块链上的某个钱包地址关联，那么这个用户的所有资产信息和交易信息都将暴露无遗。

为此，区块链从业者提出了多个解决该问题的方案。如更换新地址，混币技术，Cryptonote 和环签，以及零知识证明。其中零知识证明的优势

最为明显，它通过提交完全不泄漏任何信息的证明来完成交易的方案，是实现了交易信息完全匿名，同时有能够支持大规模的交易，因此它被广泛采纳用于实现区块链上的资产交易隐私保护。

不仅仅是区块链本身的底层货币，以智能合约为基础的 Token 资产（如 ERC20 Token，ERC721 Token）的资产转移也同样可以使用零知识证明技术来保护交易隐私。

3.1.2 数字身份认证

据 PingWest 品玩 2020 年 3 月 19 日报告，有用户发现 5.38 亿条微博用户信息在暗网出售，涉及到的账号信息包括用户 ID、账号发布的微博数、粉丝数、关注数、性别、地理位置等。据不完全统计，仅 2019 年，公开渠道发布的用户数据泄露事件就有 43 起，涉及全球 16 个国家，11 个行业。用户个人信息数据的高价值属性让数据泄露带来的损失不断升级，同时也带来非常不好的社会影响，甚至危害国家安全。

由此可见，传统的身份信息认证手段——将用户的个人信息完成认证并保存在服务器后台的方式已经很难保障用户的个人身份信息和隐私安全了，尤其是对于以去中心化为核心特征的区块链领域来说，如何通过技术手段实现在不泄漏用户身份信息前提下完成身份信息认证变得尤为重要。在最初区块链上，仅存在钱包地址账户，这与现实生活中的个人身份并没有直接的关联关系，用户仅依靠持有的私钥来获取账户的所有权。但随着区块链进一步落地应用，基于区块链的应用不免与实际生活和现实个人身份的联系越发密切。

在用户数字身份的认证问题上，零知识证明能够在完成身份认证中的交互的同时，保证用户信息的隐私性和认证结果的正确性。提供证明的一

方只需要将里有用户身份信息计算出来的数字上链，验证方即可验证用户身份，并且依赖数学手段，可以完全保证身份信息为真实可信的，同时任何人也无法从证明中提取用户个人信息的数据。

3.1.3 监管检查

除了用户的个人身份信息，在如航空，能源，金融，保险等领域，很多的应用场景下都存在着大量的隐私数据，这些数据不能暴露于公众但又必须受到某些机构的监管。当这些领域与区块链相结合时，如何在保护数据隐私的前提下实现对数据的检查和监管变为尤为重要。

零知识证明的隐私保护能力和验证能力完美得解决了这个问题。通过零知识证明技术，这些隐私数据无需直接上链，隐私数据由第三方提供，再由证明者生成合规证明提交上链，而监管方仅需要验证链上提交的证明即可完成监管检查。例如在信用凭证的场景下，由银行提供某用户是否正确支付了税款，再由用户生成数据证明提交上链，监管方完成验证：1）用户提交的证明是否是根据银行提供的数据生成的证明；2）用户数据是否达到信用凭证要求。

监管检查对于公链的用处并不大，但对于联盟链，尤其是对安全性要求较高，监管力度较大的领域，零知识证明的该项应用非常重要。

3.2 扩容

随着越来越被大众所熟知和认可，区块链本身的性能问题已经难以满足当下的需求。一方面，由于去中心化网络数据传输和节点同步的约束，致使区块大小非常有限，因此每个区块能够容纳的交易数量很有限，而区

块链能存储的数据也很有限；另一方面，由于区块同步机制的存在，导致交易不能及时处理，这严重阻碍了对响应速度有极高要求的传统应用场景向区块链迁移。

零知识证明仅需要生成很小数据量的证明就可以完成对大批量数据的证明。很多技术专家们一早就注意到零知识证明的这一特性对于解决区块链性能瓶颈所具备的潜力。早在2018 年 10 月，以太坊创始人 Vitalik 就曾表示，通过使用zk-SNARK大规模验证交易，就可以在以太坊上扩展资产交易规模。利用zk-SNARK，Ethereum上每秒可处理的数量达到 500 笔。这是当时 Ethereum 网络每秒所能处理的交易数量的30倍以上。目前很多基于零知识证明的扩容解决方案有很多，主要以链下扩容，链上区块压缩和轻量级客户端三个方向为主。

3.2.1 链下扩容

链下扩容是指在加密货币的主链之外，建立外围或第二层交易网络的分层结构，即将绝大部分的计算转移到链下或侧链来完成，而主链仅提交极小数据量的计算结果。迄今为止，技术专家们在区块链扩容方面的尝试有很多，并且已经有一些较为成熟的分层方案已经开始落地使用。

实现分层方案的一个最核心的问题就是如何保证从二层网络提交到主链数据的真实性，零知识证明正是解决这一问题的一个重要方案。首先，零知识证明的重要特性 —— 仅需要生成很小数据量的证明就可以完成对大批量数据的证明，这一点非常契合分层方案中在二层完成数据计算而仅向主链提交很小的数据量的需求；其次，零知识证明的数学特性保障了只要提交到主链的数据能够通过验证，那么数据就是正确的，二层网络完成的计算就是可信的。因此，零知识证明技术它在不牺牲原有区块链安全性的前提下实现更高的并发量，并且由于提交到链上的数据变小，而完成一笔交易或执行合约的成本也变得更小。

zkRollup 方案就是基于零知识证明实现的二次扩容方案。每一次的状态转变都需要提供零知识证明，由主链上的合约进行验证，只有验证通过才能更改状态，即每一次状态转变都严格依赖密码学证明。相比较于与之类似的方案 Optimistic Rollup，ZK Rollup 在安全性方面具备压倒性的优势。

据估计，Ethereum 在完成伊斯坦布尔升级之后，zkRollup 可以使以太坊的吞吐量提高到大约每秒 3000 笔交易(tps)。目前基于zkRollup 的扩容解决方案和应用有很多，如 ZK Sync、Loopring 3.0协议等。

3.2.2 链上区块压缩

在区块链上，区块的大小是有限的，每个区块所能容纳的交易数量也是有限的，因此如果能够使每笔交易的数据量缩小，那么区块所能承载的交易数也会增加。所以除了向链下扩展，区块数据压缩也是提高区块链吞吐量的一种重要思路。

使用零知识证明实现的压缩为应用上链也提供了诸多的好处：1）解决了很多实际业务中处理的数据量很大，根本无法上链的难题。2）降低了成本，压缩后的数据提交的上链后，所消耗的手续费也将下降。因而区块压缩技术为更多的应用上链增加了可能性。

与链下扩容类似，实现区块压缩的关键就是如何在验证压缩后的数据的真伪。同样零知识证明在这里依然可以发挥很大的用处。并非要将完整的数据都要提交上链才能保证业务的正确执行，因此可以把链下的许多个业务处理过程压缩成一个很小的证明，然后智能合约验证提交的证明就能保证服务节点没办法作弊。

Filecoin 是一个去中心化存储项目，它的业务中涉及海量的数据，这些数据不可能全部上链，因此压缩提交到区块的数据非常重要。而它所采用的方式就是利用零知识证明实现”数据的压缩“。除了Filecoin 以外，使用零知识证明手段来实现数据压缩的项目还有很多，如 Coda，Mir。

3.2.3 轻量级客户端

随着区块的不停累加和业务的增长，全节点的数据量也在不断增加，因此区块链全节点将变得巨大，这使得节点的网络同步以及存储都变得很难。因为一方面，下载几百 G 甚至几 T 的全节点数据需要耗费很长时间；另一方面，全节点需要对下载的数据完全校验来确保数据的正确性，在大部分的区块链上校验过程需要将全节点所有的交易按照顺序执行一遍再和下载的状态作比较，每个全节点都要做一次校验，因此这个过程非常消耗时间。

受制于硬件设备的要求和运行全节点的复杂性，使得同步全节点对于大部分普通用户来说非常困难，这严重阻碍了区块链的大规模应用。因此如果通过技术手段解决以上问题构建出轻量级客户端是区块链应用可以大规模商业的必备要素。

因此零知识证明的压缩能力再一次发挥作用。同时利用零知识证明的验证能力，可是在不牺牲安全性的前提下很好的解决区块同步期间每个全节点都要重复执行验证交易区块数据的问题。所以说零知识证明为构建轻量级客户端提供了很好的方案。

上文所提到的 Coda 项目，通过零知识证明的不断递归能力，将目前几十 GB 的区块链账本压缩到 20k，而这个数据量使得哪怕是移动端设备都可以轻而易举地完成区块同步。

零知识证明在解决区块链上的隐私问题和性能扩展方面发挥了极大的作用。零知识证明在区块链领域的使用最近两年才渐渐取得较为广泛的关注，还有大量的应用场景有待发掘。Vitalik 曾表示，零知识证明能够被应用于以太坊区块链上几乎所有的场景。这项黑科技将带来的巨大威力非常值得业内期待。

四、应用案例分析

4.1 公链基础

4.2 底层扩展

零知识证明在区块链领域的应用大致可以分为三层：公链基础，底层扩展和上层应用。

4.1 公链基础

零知识证明的隐私保护能力和数据压缩能力是其成为公链基础组成技术的主要原因。

4.1.1 Zcash

ZCash 是在原始的比特币代码库基础上结合零知识证明技术开发的一种保护交易隐私的区块链。它的构想来自于麻省理工大学、约翰·霍普金斯大学等多个科研机构。Zcash 除了保证了交易的隐私性以外，还具备高效、安全且低手续费的优势。

ZCash 钱包地址分为隐蔽地址和透明地址两种。透明地址之间的交易则与比特币交易没有区别：发送者、接收者以及交易金额都是公开可见的；隐蔽地址之间的交易也会出现在公有区块链上，但交易的地址、资金的数额以及备注字段都是被加密过，再由 zk-SNARK 证明在网络共识规则下验证交易的有效性；另外，隐蔽地址和透明地址之间也是可以进行交易的。Zcash 在保护交易隐私的同时还是保持了对审计及监管的友好，隐蔽地址交易的发送者和接收者都可以公开交易细节给第三方，用于满足见证、合规或审计需求。

ZCash 最早采用了2013年提出的零知识证明 zkSNARK 协议 Pinocchio。2019年，Zcash 切换到了 Groth16 证明系统，这是一个在 Pinocchio 协议上进一步极致优化的零知识证明协议，证明的尺寸被压缩到了原来的一半。Groth16 有一个明显问题就是，需要对每一个计算过程进行 Trusted

Setup，一旦代码有一点点修改，那么就需要重新来完成 Trusted Setup。Zcash 开发者正在试图使用 zk-STARK 来代替现有的零知识证明方案，但目前尚处于研究阶段，还未实际使用。

4.1.2 Monero

Monero 同样是一种实现了交易匿名的区块链。诞生于2014年，使用的算法是基于 Crypto Note协议的Crypto Night算法，最初是为了抵抗类似比特币的矿机而设计的。

Monero 的匿名交易是三种机制结合来实现的——隐形地址（Stealth Address）、环签名（Ring Signature）和环机密交易（Ring Confidential Transaction/ringCT）。Stealth Address 是指在 Monero 的交易中，允许并要求付款者代表收款者为每笔交易随机创建的一次性地址，通过使用隐身地址，只有付款者和收款者才能确定付款的地址；环形签名是一种数字签名，它是用于在在 Monero 的交易中，交易签名者使用他的私钥及其他人的公钥来生成一个签名，当其他人想要验证时，利用环成员公钥验证一个环签名是否由环成员之一生成，但无法确定具体的哪个成员；环机密交易用于混淆交易中发送金额的方式。

早期的 ringCT 实现方式存在很大的弊端就是其导致交易的规模巨大。2018年10月，门罗币每六个月一次的硬分叉升级上引入了零知识证明协议 BulletProofs（防弹）加密，用来代替原来的 ringCT 实现方式。BulletProofs 协议对保密交易使用范围证明，以此进一步确保交易的有效性的。BulletProofs 技术将交易证明的大小从 10 KB 缩小到 1-2 KB，压缩比率达到80%以上，同时降低80%的交易费用。BulletProofs 设计精妙，创建了一种更简短、更快和更强大的非交互式零知识证明，在一定程度上缓解了Monero 账本太大，扩容难，交易手续费贵的问题。

4.1.3 Filecoin

Filecoin 项目是 2019 年的一个重要的明星项目，旨在打造一个基于区块链系统的数据存储和检索方案。Filecoin 基于IPFS 协议，并在其基础上增加了奖励协议层。IPFS（The InterPlanetary File System）又称“星际文件系统”，是由Protocol Labs（协议实验室）发布的一种点到点的分布式文件系统，通过底层协议，可以让存储在IPFS系统上的文件，在全世界任何一个地方快速获取，且不受防火墙的影响，可以让我们访问数据的速度更快，更加安全，并且更加开放。

Filecoin协议的设计主要涉及四个部分：去中心化的存储网络、存储证明、可验证市场和工作量证明。其中存储证明是为了防止攻击和存储提供商作假。Filecoin 的存储证明的主明包括 PoRep（Proof of Replication，复制证明）和 PoSt（Proof of Spacetime，时空证明）。复制证明是指证明人要提供存储证明给用户，用以证明用户的数据 已经被存在到了证明人专用的物理存储设备上；时空证明是用来验证证明人在一定时间内真实得将用户的数据存储在了他的设备上，这个证明本质上就是要求证明人不断的生成证明，并在一个提交周期内提交存储证明。这两种证明都是使用零知识证明协议 Groth16实现的。

另一方面，Filecoin 的研究人员也同时看到了零知识证明在区块链扩容和保护链上交易隐私的巨大潜力，并着力于使用 SNARK 聚合技术来改进和优化 SNARK 的实现方案，因此未来零知识证明将会在 Filecoin 项目上发挥更大的作用。

4.1.4 Coda

Coda项目第一个具有简洁区块链特点的加密货币协议，被称为 "A

wallet that fits in your pocket"（一个能塞进口袋的钱包）。它利用零知识证明技术对区块进行压缩，从而大大降低了运行全节点的成本。 该项目是2019年的明星项目，目前测试网已经上线。

Coda 节点生成一个新区块时，它还会生成一个 zkSNARK 的证明，以验证该块是否有效，这样网络中的所有节点都可以存储证明，而不是原始的区块。同时，Coda 还利用了零知识证明能够不断递归证明的特征，将区块数据不断压缩，最终将目前几十 GB 的区块链账本压缩到 22KB，从而使得区块数据变得很小。

由于区块压缩，用户不必再考虑区块的大小，使得即便是移动端也可以即时同步区块链数据，这大大的提高了区块链网络的吞吐量，并可以实现大规模分散的区块链。

4.2 底层扩展

将零知识证明技术做为底层扩展技术的组成部分，以此支撑上层应用来使用零知识证明技术也是一个重要的方向。

4.2.1 ZK Rollup

ZK Rollup 基于零知识证明技术实现的以太坊二层扩容方案。随着以太坊生态的日益成熟，基于以太坊应用的尝试也越来越多，而以太坊系统存在的诸多限制也日益凸显——目前的系统无法支撑高并发量和数据响应速度要求极高的传统业务。Ethereum 社区提出了很多二层扩容方案，如 Plasma、Optimistic Rollup 和 ZK Rollup 以提高以太坊的可扩展性，提

升以太坊的速度和总交易吞吐量。Plasma 项目目前已经终止，Rollup 方案是目前最火热的方案，而这其中ZK Rollup 又以在安全方面的绝对压倒性优势被社区认可。

在 ZK Rollup 方案中，用户不再直接将交易数据提交上链，而是将带有签名的交易信息发送给协调者（Coordinator），协调者收集所有交易并构建电路证明这批交易全部有效，并将有效性证明和简单的交易数据提交上链，由智能合约完整证明的验证，最后更新链上帐户状态的默克尔树。由于上链的数据量远小于原始的交易数据，因此，达到了扩展的效果。

尤其在 2019年 12 月 7 日以太坊网络实施的伊斯坦布尔硬分叉升级中，包含了两个以太坊改进提案可以降低zkSNARK 证明的 Gas 消耗。在这次升级过后，理论上 zkRollup 能够促使以太坊的吞吐量大约达到每秒3000笔交易(TPS)，而目前以太坊的吞吐量仅约 30 TPS；另一方面，由于数据的压缩，使得每笔交易的 Gas 费用也有所下降，伊斯坦布尔升级前一笔需要耗费 21000 Gas 的原始交易，在升级后使用 ZK Rollup 来提交交易仅需要花费 300 Gas 的手续费。所以说 ZK Rollup 扩容方式为以太坊网络支撑大规模商业提供了可能性。

目前 Ethereum 上已经出现了很多基于 ZK Rollup 的项目，如 ZK Sync、Loopring3.0 协议。其中ZK Sync 旨在为以太坊带来 Visa 级别的数千笔交易 / 秒（TPS）的吞吐量，并同时保证资金如同底层 Layer 1 账户般安全并维持高度的抗审计性。协议的另一个重要方面是它的超低延迟：ZK Sync 中的交易会提供即时经济终结性（instant economic finality)。同时用户体验也是 zkSync 关注的一个重要方面。

4.2.2 ZEXE

ZEXE 是一套基于零知识证明的验证链下交易计算的系统。该方案由自于 ZCash、伯克利大学、约翰霍普金斯大学等的研究人员联合在 2018 年提出。

ZEXE 系统使用户能够执行脱机计算并随后产生可公开验证的交易，并能够证明这些脱机计算的正确性。同时除了已消耗的输入和已创建的输出的数量，交易不会显示有关脱机计算的任何信息。这套系统实现了在保护数据隐私的前提下，实现高效的链下计算和链上验证，它解决了当前区块链网络上两个重要制约因素：

1）全节点为了验证提交上链的交易，需要重新执行它来完成验证，确保其状态装换的正确性，因此节点做了大量的重复计算。

2）全节点执行交易时不仅暴露了状态转换相关的合约，还显示了合约的内部状态变换，使得合约的执行过程和内部数据毫无隐私性可言。
ZEXE 是基于零知识证明协议及递归证明的，与 2019 年 4 月正式在Github上建立代码库，标志着其工程实现的开始。

4.2.3 ZoKrates

ZoKrates 是一个 Remix 插件，Remix 是 Ethereum 官方推荐的智能合约开发IDE，可以在浏览器中快速部署测试智能合约。ZoKrates 作为以太坊上的一个 zkSNARKs 的工具链，它的作用是帮助开发人员比较容易地实现链下生成零知识证明，再提交到以太坊链上用智能合约对其进行验证。

ZoKrates 本身是使用 Rust 实现的，底层集成了现有的零知识证明开源库 bellman 和 libsnark。

零知识证明作为一项门槛极高的技术，其开发和使用难度严重的制约了该项技术的推广，而 ZoKrates 的工具链极大的降低了以太坊上智能合约开发人员的门槛，对于推动零知识证明技术在以太坊平台的应用发挥了巨大的作用。

4.2.4 ZkVM

Stellar 是一个由前瑞波币（Ripple）创始人 Jed McCaleb 发起的数字货币项目，用于搭建一个数字货币与法定货币之间传输的去中心化网关。为了提高 Stellar 网络的可扩展性，高效性和灵活性，Stellar 做了很多的研究。ZkVM 就是其发布的一项研究成果，旨在帮助 Stellar 为用户提供更多的隐私性和灵活性。

ZkVM，也就是（zero-knowledge virtual machine），是一个实验性的多资产区块链架构，用于实现可伸缩和加密的智能合约。每笔交易中包含两个部分的内容组成：智能合约程序和零知识的证明。当虚拟机执行交易的时候，不仅需要执行智能合约程序，还有验证交易中提交的证明，而且为合约的执行提供了强大的安全保证。

4.2.5 FiMAX

FiMAX是由平安集团联营公司金融壹账通推出，采用了3D零知识算法体系的，零知识、零延迟区块链基础设施平台，为企业、金融机构和政府组织等提供标准化、可快速接入的联盟链底层服务。

该底层为了根除区块链商业应用中普遍存在的隐私问题，采用了全加密形式的区块链框架——所有上链的数据均由数据提供方自行加密后上传，加密私钥由提供方自行保管。同时，该底层通过3D零知识算法体系，实现

了所有逻辑计算、运算和验证均能够在链上信息不解密的密文状态下完成。在加密环境下，FiMAX所采用的3D零知识证明能够完成零知识全同态（加、减、乘、除）计算和验证，单次密文验证时间约在1毫秒左右，在验证的灵活性和验证效率方面满足了当前绝大多数区块链商用场景对底层技术的要求。FiMAX底层及其3D零知识算法体系，目前已被应用于解决多个传统行业内因为“数据孤岛”造成的信息不对称、协同效率低下等问题。通过在密文状态下的灵活运算与交叉验证，区块链上各个参与方能够在不共享数据的情况下，共享数据间验证带来的价值。在其近期推出的3D零知识算式和跨链方案中，不同区块链系统间甚至无需共享加密后的信息，在仅共享零知识验证加密系数的情况下，便能实现灵活的数据计算交互和交叉验证。

这一系列方案为数据高度敏感、监管要求严格的行业和机构（例如金融机构、政府部门等），提供了一种可行的，数据无需流出系统的区块链数据交互方案。目前该系列方案已应用于中国海关总署天津口岸、中国广东省中小融平台等大型项目。

4.3 上层应用

4.3.1 Loopring

Loopring 3.0 协议是以太坊主网上首个采用 ZK Rollup 进行扩容的 DEX 协议。 于2020 年 2 月 27 日上线公测 版本 Beta1。此版本中所有的撮合逻辑都在链下完成。撮合（Settlement）生成的证明将提交上链，在链上证明其链下的撮合正确。Loopring 3.0的交易继承了以太坊主网一致的安全性，同时又能够提供高出目前其他去中心化交易所百倍的吞吐量。在足够多的交易的情况下，Loopring 3.0 在君士坦丁堡升级后，TPS 能达到 1400，每笔交易平均下来的费用大约在 1 美分。

4.3.2 zkPoD

零信任公平交易是很多行业中普遍存在的需求，也是电子商务技术的未来。zkPoD由SECBIT Labs提出的一个实用的交换可数字化商品（数据）的零信任公平交易系统。简单来说，zkPoD 是基于零知识证明和智能合约实现的可验证的数据交付协议。zkPoD 协议充分利用了区块链天然的支付功能，并应用了零知识证明的两大优势：（1）隐私性；（2）仅生成很小的证明就能够验证非常大数据量的数据的优势，将链下数据传输和链上验证支付结合，使得其既能够实现交付动作的原子性，又同时支持大数据文件的交易 。

4.3.2 AZTEC

AZTEC 项目是基于以太坊系统的匿名交易协议，基于此能够实现对以太坊上任何通用的资产的快速匿名转换。AZTEC隐私网络目前已在以太坊区块链上正式启动。

AZTEC 提供了一种名为 ZKAsset 的资产，我们称它为「票据(note)」，可以将以太坊网络上的任意数量的 ERC20 Token 转换票据，这些票据仅所有者信息是公开可见的，而票据上存储的金额数量和代币类型都是隐藏的。AZTEC 的隐私性同样是利用零知识证明实现的。为了实现互操作性，AZTEC 上的所有资产共享一个零知识证明 Trust Steup，所有的票据状态都是由同一个智能合约——Aztec Cryptography Engine (ACE)来管理。AZTEC 团队将会把新一代的零知识证明协议 PLONK 部署到 ACE 上。AZTEC 的整个设计是为了给 DApp 开发者提供各种隐私模块，目前共提供 7 个模块，开发人员可以将这些模块结合起来搭建自己的 DApp 合约，而不需要掌握底层的加密原理。

五、零知识证明技术发展趋势

零知识证明技术诚然已经是区块链领域一项非常重要的底层技术，它对于提高区块链领域的隐私安全，提升区块链系统的并发处理能力和实现链上链下相结合来说，都发挥了重要的作用。但时至今日，零知识证明技术尚未完全发展成熟，理论和工程实现都处于快速发展当中，四个较为明显的趋势—— 技术标准化，后量子零知识证明，性能优化和公链集成正在迅速增长。

5.1 后量子零知识证明

区块链上的公私钥机制以及大量的零知识证明协议都是基于椭圆曲线离散对数难题而设计的，目前计算机的计算能力来说破解离散对数难题几乎的不可能，但对于具备的指数级的计算能力的量子计算机来说，却可以轻易做到的。庆幸的是，要瓦解区块链，需要具有 4000 量子比特的量子计算机才可以做到，目前的量子计算机距离 4000 量子比特还有很大的距离。不过量子计算机给现代密码学带来的隐患已经无法忽视，研究抗量子的密码学方案势在必行。

抗量子的零知识证明研究同意也是当下密码学家们研究的一个重要方向，并且已经发布的零知识证明协议中就有不少基于基于散列的方案，具备后量子安全的特性。

1. zk-STARKs 协议是首个实现既可以不依赖任何信任设置来完成区块链验证，同时计算速度随着计算数据量的增加而指数级加速的零知识证明协议。它不依赖公钥密码系统，仅依赖散列函数和信息论，因此能够抵御量子攻击。

2. Virgo：这一方案只使用了轻量级的密码学原语，例如抗碰撞的散列函数，因此可能是抗量子计算的。

3. Ligero：基于一个叫做 MPC-in-the-head 的零知识证明协议设计理念，依赖于公开的随机性以及散列函数的可用性，因此同样具有后量子安全。

同样基于格的零知识证明也是目前研究的一个重要方向，早在 2016 年就有密码学家提出的一个新的诚实验证者零知识证明协议就是基于格密码体制的。

5.2 性能优化

性能问题是阻碍零知识证明大规模落地的一个重要因素。零知识证明技术实现在性能上的考量主要有三个方面：证明尺寸，生成证明的时间和验证证明的时间。

零知识证明的一个重要优势就是它仅需要生成很小尺寸的证明就可以完成对大批量数据进行验证，这是其能够在区块链上实现性能扩展的主要原因。但是由于零知识证明技术本身中涉及大量的计算，其在执行时间和空间上的销耗都比较大，因而其本身存在性能瓶颈。
其实自零知识证明诞生以来，密码学家们在其性能优化问题上的探索就一直深耕不缀，并且这两年随着零知识证明应用的推广，这个方向的研究也在逐步加强。零知识证明技术的性能优化主要可以分为两大类—— 证明协议优化和硬件加速。

5.2.1 证明协议优化

零知识证明协议性能的提升一直都是密码学家们考量的一个重要部分，不同的协议期在证明尺寸，证明时间和验证时间上都各有优势，有所不同。图 5-1 为 zkSNARKs、zkSTARKs 和 Bulletproofs 的性能对比图。总体来说，这三种证明协议中 zkSNARKs（Groth16）的优势比较明显。

	SNARKs	STARKs	Bulletproofs
Algorithmic complexity: prover	O(N * log(N))	O(N * poly-log(N))	O(N * log(N))
Algorithmic complexity: verifier	~O(1)	O(poly-log(N))	O(N)
Communication complexity (proof size)	~O(1)	O(poly-log(N))	O(log(N))
- size estimate for 1 TX	Tx: 200 bytes, Key: 50 MB	45 kB	1.5 kb
- size estimate for 10.000 TX	Tx: 200 bytes, Key: 500 GB	135 kb	2.5 kb
Ethereum/EVM verification gas cost	~600k (Groth16)	~2.5M (estimate, no impl.)	N/A
Trusted setup required?	YES 😒	NO 😄	NO 😄
Post-quantum secure	NO 😒	YES 😄	NO 😒
Crypto assumptions	Strong 😒	Collision resistant hashes 😄	Discrete log 😒

图 5-1 零知识证明性能对比图

（图片来源：https://github.com/matter-labs/awesome-zero-knowledge-proofs）

零知识证明协议的理论研究很快，尤其最近两年不断有新的协议诞生，这些协议如 Sonic、PLONK、Marlin、Libra等都在提升性能上取得了很大的进步。但目前为止，Groth 16 在性能方面依然具备较明显的优势。

5.2.2 硬件加速

除了在软件方面优化协议本身，加快硬件的计算速度也是提高零知识证明性能的一个重要方向。

硬件加速是指在计算机中通过把计算量非常大的工作分配给专门的硬件来处理以减轻中央处理器的工作量之技术。硬件加速一直是计算机领域优化性能提高处理速度的重要方式，在图像处理，人工智能，挖矿等方向都有广泛的应用。因此通过提高硬件响应速度来加快零知识证明的处理速度也是一个极其重要的手段。

2019年，ZCash 基金会宣布了 FPGA 加速项目——The Zcash FPGA acceleration engine（Zcash FPGA 加速引擎）的成果。这个项目的第二阶段就着重于zk-SNARK和所需的椭圆曲线操作的加速。

不止是Zcash FPGA 加速引擎项目，还有很多研究团队都在参与研究针对零知识证明的硬件加速方法，以试图更广泛得提升零知识证明的处理速度。

5.3 零知识全同态加持

零知识与全同态都集中在对密文数据的处理上，但现有的零知识和全同态方案均存在一定的不足：

在协议的安全性上，许多零知识协议的理论基础还存在疑问，安全假设并没有得到严格的证明，这无形中给数据安全增加了风险。而全同态解决方案，安全强度只在2^80左右，与公认的2^128的安全强度还存在一定的差距。

在工程层面上，无论零知识还是全同态的处理能力都不够理想：零知识处理速度太慢，全同态的运算性能退化又不可避免。此外，针对关键的密文除法运算，两种方案都未能很好得支持。同时，全同态加密后的数据膨胀问题不可忽视，动辄一万倍的数据量增加，会对区块链系统产生灾难性的影响。

随着基于区块链技术的项目越来越多，使用方对数据隐私保护的需求日益增加，对密文数据的处理成为了关键的一环，如何解决零知识与全同态这两个密码学分支的不足成为了一个迫切的需求。零知识与全同态的整合应用成为了一个可行的发展方向。

针对上述问题，2018年，金融壹账通FiMAX开发团队在解决方案中提出了3D零知识证明，将零知识证明和同态加密技术实现了有机的结合，对加密数据的加、减、乘、除四则运算原生支持。通过在密文状态下，对数据进行按照清晰的算式进行运算和验证，大大简化了零知识开发应用的困难

度，对零知识技术在生产环境中大范围推广应用创造了条件。首先，该方案能够确保数据的安全强度达到2^110以上；其次，该方案基于对加密数据进行四则运算的模型，并原生支持除法运算，不仅应用开发起来更加友好，处理能力也能满足金融系统中的要求，在优化后可以将同态运算时间缩小到1ms以内；最后，基于3D零知识证明技术进行的数据加密，在处理效率和密文大小上与传统加密方式相比并不会有显著的变化。

5.4 标准化

零知识证明技术尚未形成标准化，理论与工程实现方案较为分散，这在一定程度上加大了零知识证明技术推广和使用的难度，因此零知识证明技术的标准化是非常有必要的。

一方面，零知识证明技术的标准化可以使其从处理特定问题，发展到处理更大范围的相关问题和场景；另一方面，由于零知识证明背后复杂的理论基础，在工程实践中其安全性通常难以得到业界的信任，而技术标准化后，零知识证明协议的安全性无需再依赖单个研究团队。同时，尽管零知识证明协议和工程实现各有不同，但每种方案都有相似的地方，所以实现技术的标准化是有可能的。

目前已经有很多组织或机构正致力于此项工作，如ZKProof 是一项开放式学术研究计划，旨在通过一个包容的、社区驱动的标准化过程来寻求主流零知识证明密码学。ZKProof认为，通过建立一个被广泛接受的框架，可以最好地实现ZKP加密技术的更广泛采用，该框架将为数据隐私产品和应用程序带来更好的安全保证和更大的互操作性。

5.5 公链集成

公链集成同样也是零知识证明技术发展的一项重要趋势。公链集成零知识证明的必要性主要包括以下三个因素：

1. 零知识证明开发难度，目前零知识证明技术的应用和实现门槛很高，且尚未形成标准化，因此在区块链上实现零知识证明应用的开发对技术人员来说无疑是极大的挑战。而如果公链本身能够在底层集成零知识证明，将大大降低开发难度。

2. 零知识证明系统的理论和工程实现都各不相同，背后的原理也极为复杂，零知识证明协议的实现其安全性能以保证。因此如果公链本身能够在底层统一集成零知识证明库，其安全性也就一定程度上得到了保证。

3. 公链上的 DApp 应用数量是无限的，一旦零知识证明进入大规模落地，基于零知识证明的 DApp 数量也是不计其数的。如果实现各不相同将严重制约 DApp 的互操作性，也非常不利于基于这类 DApp 的衍生应用的发展。

因此集成零知识证明是非常有必要的。作为 DApp 应用最为活跃的公链，Ethereum 社区一直对零知识证明技术抱有极大地热情，如 ZoKrates 项目就是以太坊上的一个 zkSNARKs 的工具链，它集成了libsnark 和 bellman，极大地提高了 DApp 开发人员的效率。除了以太坊之外，很多著名公链项目，如 Nervos、PlatON等都在着力于研究集成零知识证明的方案。

六、总结

零知识证明的底层理论基础是计算复杂性理论加上信息论，比如图灵机、P、NP问题、纸带、算法这些概念都被数学化，这是可以一路回溯到罗素、哥德尔、图灵等先驱的贡献，伴随着计算机互联网一路成长起来的理论技术。零知识证明理论领域有很多的传奇密码学家，正是由于他们不懈的耕耘，才研究出了这么神奇的黑科技。零知识证明技术的发展时间并不长，但无论是理论研究还是工程实践都取得了较好的发展。在理论方面已经有了较为成熟的方案，且依旧处在快速进步的阶段；在工程实现方面，零知识证明源码实现在快速迭代完善中，这是使得零知识证明技术能够实现落地应用的基础保障。

零知识证明技术的引入为区块链领域的诸多问题都提供了非常好的思路，尤其在隐私保护和扩容方面。值得一提的是，区块链领域所面临的这些问题，零知识证明并不是唯一的解决方案，但零知识证明最大的优势就是其解决方案是建立在不破坏原有区块链安全性的前提下实现的。

零知识证明技术在区块链领域的应用尚处于起步阶段。但零知识证明技术充满了潜力和对区块链的发展也带来了无限的可能性，因此这个领域正在以一种惊人的速度快速发展着。至此我们已经看到了零知识证明在后量子零知识证明、性能优化、标准化和公链集成上的发展趋势。量子密码对当前的诸多零知识证明协议都带来了很大的安全风险，因此为了摆脱量子密码的威胁，后量子零知识证明的研究也逐渐成为密码学家们的研究重点；在性能优化方面，技术专家们正在着力从协议实现，软件和硬件等多个方面开展研究；目前零知识证明协议繁多，实现方法各有不同，再加上零知识证明技术本身的难度极高，零知识证明的使用面临着很大的挑战，因此技术标准化意义重大；将零知识证明协议集成到公链底层技术中，这为基于公链的零知识证明应用的实现提供了极大的便利。

在经历了几年的发展变化后，到2020年区块链应用步伐将加快，而同时随着数据隐私矛盾的进一步激化，业内已经逐步意识到包括零知识证明在内的现在密码学技术的威力。相信在政府的大力支持下，随着商业投入的不断加大，密码学专家的深耕不倦以及专业技术团队的快速成长，零知识证明技术也将为区块链的发展创造更大的价值。

参考资料：

[1] https://baike.baidu.com/item/零知识证明

[2] https://en.wikipedia.org/wiki/Zero-knowledge_proof

[3] http://www.xinhuanet.com/politics/2019-11/05/c_1125195786.htm

[4] https://mp.weixin.qq.com/s/FPHkqwiHX8UVIlbu_PXSQw

[5] https://mp.weixin.qq.com/s/n47aNMIlfibETBzB1taqsg

[7] https://zkp.science/

[8] https://zkproof.org/

[9] https://z.cash/zh/

[10] https://www.getmonero.org/

[11] https://filecoin.io/

[12] https://www.chainnews.com/articles/841710280413.htm

[13] https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups/

[14] https://github.com/matter-labs/zksync

[15] https://www.chainnews.com/articles/482098173691.htm

[16] https://github.com/ZcashFoundation/zcash-fpga

[17] http://www.wlmqwlw.com/45405/1270.html

[18] http://crad.ict.ac.cn/CN/article/downloadArticleFile.do?attachType=PDF&id=3532

[19] https://www.jianshu.com/p/bbd72df695e2

陀螺研究院
Tuoluo Research

陀螺研究院：隶属于陀螺财经，研究院团队拥有专业的金融、计算机领域知识，以及丰富项目、行业分析经验。定位于研究数字经济特别是区块链如何重构生产和生活方式，助力产业转型升级，赋能实体经济。依托陀螺财经丰富的媒体资讯资源，研究院已经开设了技术专栏、陀螺公开课和专访等栏目，为推动技术应用落地搭建起沟通的桥梁。在客观事实、市场数据等基础上，我们构建了科学、严谨的数据分析与价值分析体系，致力于为区块链业内人士、区块链创业者以及所有关注区块链的人们提供最全面和有深度的分析内容。目前已经联合腾讯研究院发布过《2019中国区块链产业发展报告》，在行业内收获较大的关注度。同时研究院积极开展对外交流合作，已经和清华大学经管学院、浙江大学软件学院、深圳网络空间科学与技术省实验室（鹏程实验室）、深圳大学区块链技术研究中心、腾讯区块链、微众银行、趣链科技等知名高校（研究机构）及企业建立了紧密的合作关系。未来研究院将围绕区块链技术创新应用落地，赋能实体经济为主线，输出一系列报告或者分析文章供读者参考。

关注“**陀螺财经**”公众号

产业咨询