

1*,* 2

1*,* 3

[1]

[2]

第 42 卷 第 4 期

自 动 化 学 报

Vol. 42, No. 4

2016 年 4 月

ACTA AUTOMATICA SINICA April, 2016 区块链技术发展现状与展望

袁 勇

1*,* 2

王飞跃

1*,* 3

摘 要 区块链是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新的去中心化基础架构与分布式计算范式, 目 前已经引起政府部门 、金融机构 、科技企业和资本市场的高度重视与广泛关注. 区块链技术具有去中心化 、时序数据 、集体维 护 、可编程和安全可信等特点, 特别适合构建可编程的货币系统 、金融系统乃至宏观社会系统. 本文通过解构区块链的核心要 素, 提出了区块链系统的基础架构模型, 详细阐述了区块链及与之相关的比特币的基本原理 、技术 、方法与应用现状, 讨论了 智能合约的理念 、应用和意义, 介绍了基于区块链的平行社会发展趋势, 致力于为未来相关研究提供有益的指导与借鉴.

关键词

引用格式

区块链, 比特币, 共识机制, 智能合约, 平行社会

袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481*−*494

**DOI** 10.16383/j.aas.2016.c160158

**Blockchain: The State of the Art and Future Trends**

YUAN Yong

WANG Fei-Yue

**Abstract** Blockchain is an emerging decentralized architecture and distributed computing paradigm underlying Bitcoin and other cryptocurrencies, and has recently attracted intensive attention from governments, ﬁnancial institutions, high- tech enterprises, and the capital markets. Blockchain s key advantages include decentralization, time-series data, collective maintenance, programmability and security, and thus is particularly suitable for constructing a programmable monetary system, ﬁnancial system, and even the macroscopic societal system. In this paper, we proposed a basic model of the blockchain system, discussed the principles, technologies, methods and applications of blockchain and the related Bitcoin systems. We also discussed the smart contract and its applications, and presented the future trends of blockchain-enabled paralleled societies. This paper is aimed at providing helpful guidance and reference for future research eﬀorts.

**Key words** Blockchain, Bitcoin, consensus mechanism, smart contract, paralleled society

**Citation** Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. *Acta Automatica Sinica* , 2016, **42**(4): 481*−*494

区 块 链是以 比 特币为 代 表的 数 字加密 货 币体 系 的 核 心 支 撑 技 术. 区 块 链 技 术 的 核 心 优 势 是 去 中 心 化, 能够通过运用数据加密 、时间戳 、分布式共识和 经 济 激 励 等 手 段, 在 节 点 无需互 相 信 任 的 分 布 式 系 统 中 实 现 基 于 去 中 心 化 信 用 的 点 对 点 交 易 、协 调 与 协作, 从而为解决中心化机构普遍存在的高成本 、低 效 率 和 数据 存 储 不安 全等 问题 提供 了 解 决 方 案. 随 着 比 特 币 近 年 来 的 快 速 发 展 与 普 及, 区 块 链 技术 的

收稿日期 2016-02-22 录用日期 2016-03-02

Manuscript received February 22, 2016; accepted March 2, 2016 国 家 自 然 科 学 基 金 (71472174, 71102117, 61533019, 71232006, 61233001) 资助

Supported by National Natural Science Foundation of China (71472174, 71102117, 61533019, 71232006, 61233001)

本文责任编委 林宗利

Recommended by Associate Editor LIN Zong-Li

1. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 2. 青岛智能产业技术研究院 青岛 266109 3. 国防科技大 学军事计算实验与平行系统技术中心 长沙 410073

1. The State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. Qingdao Academy of Intelli- gent Industries, Qingdao 266109 3. Research Center of Mili- tary Computational Experiments and Parallel System, National University of Defense Technology, Changsha 410073

研 究 与 应 用 也 呈 现 出 爆 发 式 增 长 态 势, 被 认 为 是继 大 型 机 、个 人 电 脑、互 联 网 、移 动/社交 网 络 之 后计 算 范 式 的 第 五 次 颠 覆 式 创 新, 是 人 类 信用 进 化 史上 继 血 亲信 用、贵 金属 信用 、央 行 纸币 信用 之后 的第 四 个 里程碑 . 区 块 链技术 是 下一 代 云 计算 的 雏形, 有 望 像 互 联 网 一 样 彻 底 重 塑 人 类 社 会 活 动 形 态, 并 实现从目前的信息互联网向价值互联网的转变.

区 块 链 技 术 的 快 速 发 展 引 起 了 政 府 部 门 、金 融 机 构 、科 技 企 业 和 资 本 市 场 的 广 泛 关 注. 2016 年 1 月, 英国政府发布区块链专题研究报告 , 积极推行 区 块 链 在 金 融 和 政 府 事 务 中 的 应 用; 中 国 人 民 银 行 召 开数字 货币 研讨 会探 讨采用 区块 链技 术发 行虚拟 货币的可行性, 以提高金融活动的效率 、便利性和透 明 度. 美 国 纳斯达克于 2015 年 12 月 率 先推出 基 于 区 块 链技术 的 证 券交易 平 台 Linq, 成 为 金融证 券 市 场 去 中 心 化 趋 势 的 重 要 里 程 碑; 德 勤 和 安 永 等 专 业 审 计 服 务 公 司 相 继 组 建 区 块 链 研 发 团 队, 致 力 于 提 升其客户 审计服务质量. 截 止到 2016 年 初, 资 本市 场已经相继投入 10 亿美元以 加速区块链 领域的 发

[3]

[5*−*6]

[6*−*14]

[15]

[16]

[4]

[17]

[1]

482

自

动

化

学

报

42 卷

展. 初 创公 司 R3CEV 基 于微 软 云 服务 平台 Azure 推出的 BaaS (Blockchain as a service, 区块链即服 务) 服 务, 已 与 美 国 银 行 、花 旗 银 行 等 全 球 40 余 家 大 型 银 行 机 构 签 署 区 块 链 合 作 项 目, 致 力 于 制定银 行业的区块链行业标准与协议.

区 块 链 技 术 起 源 于 2008 年 由 化 名 为 “中本 聪” (Satoshi nakamoto) 的学者在密码学邮 件组发表的 奠基性论文《 比特币: 一种点对点电子现金系统 》 , 目前尚未形成行业公认的区块链定义. 狭义来讲, 区 块 链是一 种按 照时 间顺 序将 数据 区块 以链 条的 方式 组 合 成 特 定 数 据 结 构, 并 以 密 码学方 式 保 证 的 不 可 篡 改 和 不 可 伪 造 的 去 中 心 化 共 享 总 账 (Decentral- ized shared ledger), 能 够 安 全 存储简单 的 、有 先 后 关 系 的 、能 在 系 统 内 验 证 的 数 据. 广 义 的 区 块 链 技 术 则 是 利 用 加 密 链 式 区 块 结 构 来 验 证 与 存 储 数 据 、 利 用 分 布 式 节 点 共 识 算 法 来 生 成 和 更 新 数 据 、利 用 自动化脚本代码 (智能合约) 来编程和操作数据的一 种全新的去中心化基础架构与分布式计算范式.

区块链具有去中心化 、时序数据 、集体维护 、可 编 程 和 安 全 可 信 等 特 点. 首 先 是 去 中 心 化: 区 块 链 数据的验证 、记账 、存储 、维护和传输等过程均是基 于 分 布 式 系 统 结 构, 采 用 纯 数学 方法而 不是 中心机 构 来 建 立分 布 式 节 点 间 的 信 任 关系, 从 而 形 成 去中 心化的可信任的分布式系统; 其次是时序数据: 区块 链 采 用 带 有 时 间 戳 的 链 式 区 块 结 构 存 储 数 据, 从 而 为 数 据 增加 了 时 间 维 度, 具 有极 强 的可 验 证 性 和 可 追溯性; 第三是集体维护: 区块链系统采用特定的经 济 激励机 制来 保证 分布 式系 统中 所有 节点 均可 参与 数据区块的验证过程 (如比特币的 “挖矿” 过程), 并 通 过共 识算法来 选 择特 定的 节点将新区块添加到区 块链; 第四是可编程: 区块链技术可提供灵活的脚本 代码系统, 支持用户创建高级的智能合约 、货币或其 他去中心化应用. 例如, 以太坊 (Ethereum) 平台即 提 供了图 灵完 备的 脚本 语言 以供 用户 来构 建任 何可 以 精 确 定 义 的 智 能 合 约 或 交 易 类 型 ; 最 后是安 全 可 信: 区 块 链 技术 采 用 非 对 称 密 码 学 原 理 对 数 据 进 行 加 密, 同 时 借 助 分 布 式 系 统各 节 点 的 工 作 量 证明 等 共 识 算 法 形 成 的 强 大 算 力 来 抵 御 外 部 攻 击 、保 证 区 块 链 数据 不 可 篡 改 和 不 可 伪 造, 因 而具 有 较高 的 安全性.

区 块 链 技 术 是 具 有 普 适 性 的 底 层 技 术 框 架, 可 以 为 金融 、经 济 、科 技 甚至 政 治 等 各领 域带 来 深刻 变革. 按照目前区块链技术的发展脉络, 区块链技术 将 会经历 以可 编程 数字 加密 货币 体系 为主 要特 征的 区 块 链 1.0 模 式 、以 可 编 程 金 融 系 统 为 主 要 特 征 的 区 块 链 2.0 模 式 和 以可编程 社 会为主 要 特 征 的区 块 链 3.0 模 式 . 目 前, 一 般 认 为 区 块 链 技 术 正 处 于 2.0 模 式 的 初 期, 股 权 众 筹 和 P2P 借 贷 等 各 类 基 于

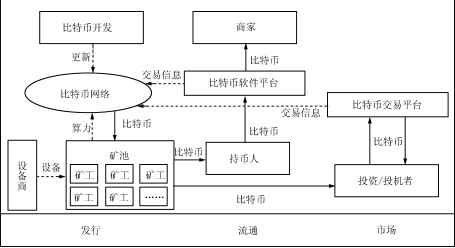
区 块链 技术 的 互联 网金 融应 用相继 涌现. 然 而, 上 述模式实际上是平行而非演进式发展的, 区块链 1.0 模 式 的 数字 加 密 货 币 体 系 仍 然远 未 成 熟, 距 离其 全 球货币 一 体化 的愿景 实际上 更远、更 困难. 目前, 区 块 链领域 已经 呈现 出明 显的 技术 和产 业创 新驱 动的 发展态势, 相关学术研究严重滞后、亟待跟进. 截止 到 2016 年 2 月, 以 万 方数据 知 识服务 平 台为 中 文 数据源 、以 Web of Science 和 EI Village 为英文数 据 源 的 文 献 检 索 显 示, 目 前 篇 名 包 含 关 键 词 “区块 链/blockchain”的仅有 2 篇中文 和 9 篇英文文 献 . 本 文系 统 性 地 梳 理 了区 块 链 的 基 本 原 理 、 核心技术 、典型应用和现存问题, 以期为未来研究提 供有益的启发与借鉴.

本 文 组 织 结 构 为: 第 1 节 概 述 区 块 链 与 比 特 币 的 发 展 史 及 二 者 的 关 系; 第 2 节 阐 述 区 块 链 的 基 础 架 构 模型及 其 关 键技 术; 第 3 节 和 第 4 节 分 别 概要 总 结 了 区 块 链技 术的 应用 场 景 与 现存 的问 题; 第 5 节介绍智能合约及其在区块链领域的应用现状; 第 6 节 展 望 了 区 块 链 驱 动 的 平 行 社 会 发 展 趋 势; 第 7 节 总结本文内容.

1 比特币与区块链概述

比特币是迄今为止最为成功的区块链应用场景. 据 区 块 链 实 时 监 控 网 站 Blockchain.info 统 计显示, 平 均 每 天 有 约 7 500 万 美元 的 120 000 笔 交 易 被写 入 比 特 币 区 块 链, 目 前 已 生 成 超 过 40 万 个 区 块 . 加 密 货 币 市 值 统 计 网 站 coinmarketcap.com 显 示, 截止到 2016 年 2 月, 全球共有 675 种加密货币, 总 市值超过 67 亿美元, 其中比特币市值约占 86 %, 瑞 波 币 和 以 太 币 分 别 居 二 、三 位 . 目 前 比 特 币 供 应 量 (即已经挖出的比特币数量) 已经超过 1 500 万枚, 按 照 每 枚 比 特 币 389.50 美 元 的 现 行 价格 估 算 其 总 市 值 已 超 过 59 亿 美 元, 在 世 界 各 国 2015 年 GDP 排 名中 占据第 144 位 (略 低于 欧洲 的摩 尔多 瓦). 换 言之, 在没有政府和中央银行信用背书的情况下, 去 中 心化的 比特 币已 经依 靠算 法信 用创 造出 与欧 洲小 国 体 量相当的全球性经济体. 预 计 到 2027 年, 全 球 10 % 的 GDP 将会通过区块链技术存储 .

比特币区块链的第一个区块 (称为创世区块) 诞 生于 2009 年 1 月 4 日, 由创始人中本聪持有. 一周 后, 中本聪发送了 10 个比特币给密码学专家哈尔芬 尼, 形成了比特币史上第一次交易; 2010 年 5 月, 佛 罗 里 达 程 序 员 用 1 万 比 特 币 购 买 价 值 为 25 美 元 的 披 萨 优 惠券, 从 而 诞生 了 比特币 的 第 一个公 允 汇 率. 此后, 比特币价格快速上涨, 并在 2013 年 11 月创下 每枚比特币兑换 1 242 美元的历史高值, 超过同期每 盎 司 1 241.98 美 元 的 黄金价 格. 据 CoinDesk 估 算, 目 前 全 球 约 有 6 万 商 家 接 受 比特 币 交 易, 其 中 中 国



[18]

[20]

[19]

4 期

袁勇等: 区块链技术发展现状与展望

483

是比特币交易增长最为迅速的国家 .

比 特 币本质 上 是由 分 布式网 络 系统生 成 的数 字 货币, 其发行过程不依赖特定的中心化机构, 而是依 赖 于分布 式网 络节 点共 同参 与一 种称 为工 作量 证明 (Proof of work, PoW) 的共识过程以完成比特币交 易 的 验 证 与 记 录. PoW 共 识 过 程 (俗 称 挖 矿, 每 个 节 点 称 为 矿 工) 通 常 是 各 节 点 贡 献 自 己 的 计 算 资 源 来 竞 争 解决 一 个 难 度 可 动 态 调 整的 数 学 问 题, 成 功 解 决 该 数 学 问 题 的 矿 工 将 获 得 区 块 的 记 账 权, 并 将 当 前时间 段的 所有比特币交易打包记入一 个 新的 区 块 、按 照 时 间 顺 序 链 接 到 比 特 币 主 链 上. 比 特 币 系 统 同 时 会 发 行 一 定 数 量 的 比 特 币 以 奖 励 该 矿 工, 并 激 励 其 他 矿 工 继 续 贡 献 算 力. 比 特 币 的 流 通 过 程 依 靠 密 码 学 方 法 保 障 安 全. 每 一 次 比 特 币 交 易 都 会 经 过 特 殊 算 法 处 理 和 全 体 矿 工 验 证 后 记 入 区 块 链, 同 时 可以 附带具 有一定 灵活性 的脚本 代码 (智 能合约) 以实现可编程的自动化货币流通. 由此可见, 比特币 和 区 块 链系 统 一 般 具 备 如 下 五 个关 键 要 素, 即 公 共 的 区 块链 账本 、分 布 式的 点 对点 网络 系 统 、去 中 心 化 的 共 识 算 法 、适 度 的 经 济 激 励 机 制 以 及 可 编 程 的 脚本代码.

区 块 链技术 为 比特币 系 统解 决 了数字 加 密货 币 领 域 长 期以 来 所 必 需 面 对 的 两 个重 要 问 题, 即 双 重 支 付问 题和拜占 庭 将 军问 题 . 双 重支付 问 题 又称 为 “双花”, 即 利 用 货 币的数 字 特 性两次 或 多 次使用 “同一 笔钱” 完 成 支 付. 传 统 金 融和 货币体 系中, 现 金 (法币) 因是物理实体, 能够自然地避免双重支付; 其 他数字 形式 的货 币则 需要 可信 的第三方中心 机 构 (如 银 行) 来 保 证. 区 块链 技 术的贡 献 是在没有第三 方 机 构 的 情 况 下, 通 过 分 布式 节 点 的 验 证 和 共 识机 制 解 决 了去 中心 化 系 统 的 双 重 支 付 问题, 在 信 息 传 输 的 过 程 同 时 完 成 了 价 值 转 移. 拜 占 庭 将 军 问 题 是

分 布 式 系统 交 互 过 程 普 遍 面临 的 难 题, 即 在 缺少 可 信 任 的 中 央 节 点 的 情 况 下, 分 布 式 节点如 何 达 成 共 识 和建 立互信 . 区 块链通过 数字加 密技术 和 分布 式 共 识 算 法, 实 现 了 在无 需 信 任单个 节 点 的 情况 下 构 建 一 个去 中 心 化 的 可 信 任系 统. 与 传 统 中心 机 构 (如 中 央 银行) 的 信 用 背 书 机 制 不 同 的 是, 比 特 币 区 块 链 形 成 的 是 软 件 定 义 的 信 用, 这 标 志 着中心 化 的 国家信用向去中心化的算法信用的根本性变革.

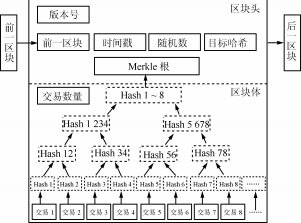
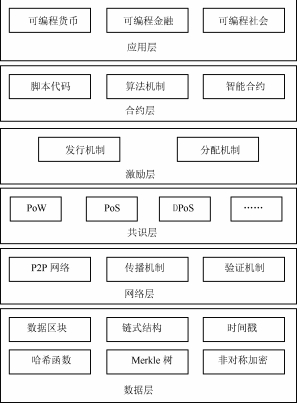
比 特 币 凭 借 其 先 发 优 势, 目 前已经 形 成 体 系 完 备 的 涵 盖 发 行 、流 通 和 金 融 衍 生 市 场 的 生 态 圈 与 产 业 链 (如 图 1 所 示), 这 也 是 其 长 期 占 据 绝 大 多 数 数 字 加 密 货币 市 场 份 额 的主 要原 因. 比 特币 的 开 源 特 性 吸 引 了 大 量 开 发 者 持 续 性 地 贡 献 其 创 新 技 术 、方 法 和机 制; 比 特币各网络节点 (矿 工) 提 供算力 以保 证 比 特 币 的 稳 定 共 识 和 安 全 性, 其 算 力 大多来 自 于 设 备 商 销 售 的 专 门 用 于 PoW 共 识 算 法 的 专 业 设 备 (矿机). 比特币网络为每个新发现的区块发行一定数 量 的 比 特 币 以 奖 励 矿 工, 部 分 矿 工可 能 会 相互合 作 建 立 收 益 共 享 的 矿 池, 以 便 汇 集算力 来 提 高 获 得 比 特币的概率. 比特币经发行进入流通环节后, 持币人 可以通过特定的软件平台 (如比特币钱包) 向商家支 付 比 特 币来 购 买 商 品 或 服 务, 这 体现 了 比 特 币 的 货 币 属 性; 同 时 由 于 比 特 币 价 格 的 涨 跌 机 制 使 其 完 全 具 备 金 融 衍 生 品 的 所 有 属 性, 因 此 出 现了 比 特 币交 易 平 台 以 方 便 持 币 人 投 资 或 者 投 机 比 特 币. 在 流 通 环 节 和 金 融 市 场 中, 每 一 笔 比特 币 交易 都 会 由比特 币网络的全体矿工验证并记入区块链.

比 特 币 是 区 块 链 技 术 赋 能 的 第 一 个 “杀手 级” 应 用, 迄 今 为 止 区 块 链 的 核 心 技 术 和 人 才 资 源 仍 大 多在比特币研发领域. 然而, 区块链作为未来新一代 的 底 层 基 础 技 术, 其 应 用 范畴势 必 会 超 越 数 字 加 密 货币而延伸到金融 、经济 、科技和政治等其他领域.

图 1

比特币生态圈

Fig. 1 The Bitcoin ecosystem



[21]

484

自

动

化

学

报

42 卷

比特币的现有技术 、模式和机制, 将会对区块链在新 应 用 领域 的发 展 提 供 有 益 的 借 鉴, 而 新领 域 的 区 块 链 创新也 势必 反过 来促 进解决比特币 系 统现存 的问 题. 因此, 比特币 和 区块 链技术 存在着 协同进 化 、和 谐共生而非相互竞争的良性反馈关系.

2 区块链的基础模型与关键技术

本 节将 结合 比特 币系 统的 技术 与应 用 现状, 阐 述区块链技术的基础模型 、基本原理和关键技术, 以 及 区 块 链 在 比 特 币 系 统 之 外 的 若 干 创 新 模 式. 现 存 的 其 他 区 块 链 应 用 大 多 都 与比 特币类 似, 仅 在 某 些 特定的环节或多或少地采用比特币模式的变种.

区 块 链 技术的基 础 架 构模 型 如 图 2 所 示. 一 般 说 来, 区块 链系统由数 据层、网 络层、共 识层、激 励 层 、合约层和应用层组成. 其中, 数据层封装了底层 数 据 区 块 以 及 相 关 的 数 据 加 密 和 时 间 戳 等 技 术; 网 络 层 则 包 括 分 布 式 组 网 机 制 、数 据 传 播 机 制 和 数 据 验 证 机 制 等; 共 识层主 要 封 装 网 络 节 点 的 各 类 共 识 算 法; 激 励 层 将 经 济 因 素 集 成 到 区 块 链 技 术 体 系 中 来, 主要包括经济激励的发行机制和分配机制等; 合 约层主要封装各类脚本 、算法和智能合约, 是区块链 可 编 程 特 性 的 基 础; 应 用 层 则 封 装 了 区 块 链 的 各 种 应用场景和案例. 该模型中, 基于时间戳的链式区块

图 2

区块链基础架构模型

结 构 、分 布 式节 点 的 共 识机 制、基 于共 识 算力 的 经 济 激励和 灵活 可编 程的 智能 合约 是区 块链 技术 最具 代表性的创新点.

2.1 数据层

狭 义 的区块 链 即是去 中 心化 系 统各节 点 共享 的 数 据 账 本. 每 个 分 布 式 节 点 都 可 以 通 过 特 定 的 哈 希 算法和 Merkle 树数据结构, 将一段时间内接收到的 交 易数据 和代 码封 装到 一个 带有 时间 戳的 数据 区块 中, 并链接到当前最长的主区块链上, 形成最新的区 块. 该过程涉及区块 、链式结构、哈希算法 、Merkle 树和时间戳等技术要素.

数 据区 块: 如 图 3 所 示, 每 个 数据 区块 一般 包 含 区 块 头 (Header) 和 区 块 体 (Body) 两 部 分. 区 块 头 封装了 当 前 版 本 号 (Version) 、前 一 区 块 地 址 (Prev-block) 、当前区 块的 目标哈希值 (Bits)、当前 区 块 PoW 共 识 过 程 的 解 随 机 数 (Nonce) 、Merkle 根 (Merkle-root) 以 及 时 间 戳 (Timestamp) 等 信 息 . 比 特 币 网 络 可 以 动 态 调 整 PoW 共 识 过 程 的 难 度值, 最 先 找到正确 的 解 随机 数 Nonce 并 经过 全 体 矿 工 验 证 的 矿 工 将 会 获 得 当 前 区 块 的 记 账 权. 区 块 体 则 包 括 当 前 区 块 的 交 易 数 量 以 及 经 过 验 证 的 、 区 块 创 建 过 程 中 生 成 的 所 有 交 易 记 录. 这 些 记 录 通 过 Merkle 树的哈希过程生成唯一的 Merkle 根并记 入区块头.

Fig. 2 A basic framework of blockchain

图 3 区块结构

Fig. 3 The structure of blocks

链 式 结 构: 取 得 记 账 权 的 矿 工 将 当 前 区 块 链 接 到前一区块, 形成最新的区块主链. 各个区块依次环 环 相 接, 形 成 从 创世 区 块 到 当 前区块 的一 条最长 主 链, 从而记录了区块链数据的完整历史, 能够提供区 块 链 数 据的 溯 源 和 定 位 功 能, 任 意数 据 都 可 以 通 过 此链式结构顺藤摸瓜 、追本溯源. 需要说明的是, 如 果 短时 间内 有两 个矿 工同 时 “挖出” 两 个新 的 区块 加 以 链 接的话, 区 块 主 链 可能会出 现 暂 时的 “分叉” 现 象, 其 解 决 方法 是约 定 矿 工 总 是选 择 延 长 累 计 工

[3]

[19]

256

256

[22]

[4]

[19]

4 期

袁勇等: 区块链技术发展现状与展望

485

作 量证 明 最 大 的 区 块 链. 因 此, 当主 链分叉 后, 后续 区 块 的 矿 工 将 通 过 计 算 和 比 较, 将 其 区 块链接 到 当 前 累 计 工 作 量 证 明 最 大 化 的 备 选 链 上, 形 成 更 长的 新主链, 从而解决分叉问题 .

时 间戳: 区 块链 技 术要 求获 得记 账权 的节 点必 须 在 当 前 数 据区 块 头 中 加 盖 时 间戳, 表 明区 块 数 据 的写入时间. 因此, 主链上各区块是按照时间顺序依 次 排列 的. 时 间 戳技 术本 身并 不复杂, 但 其在 区 块 链 技 术 中 的 应 用 是 具 有 重 要 意 义 的 创 新. 时 间 戳 可 以作为区块数据的存在性证明 (Proof of existence), 有 助 于 形 成 不 可 篡 改 和 不 可 伪 造 的 区 块 链 数 据 库, 从 而 为 区 块 链 应 用 于 公 证 、知 识 产 权 注 册 等 时 间 敏 感的领域奠定了基础. 更为重要的是, 时间戳为未来 基 于 区 块 链 的互 联 网 和 大 数 据 增加 了 时 间 维 度, 使 得通过区块数据和时间戳来重现历史成为可能.

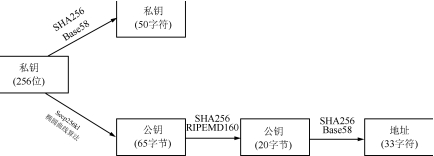
哈 希 函 数: 区 块 链 通 常 并 不 直 接 保 存 原 始 数 据 或交易记录, 而是保存其哈希函数值, 即将原始数据 编 码为特 定长 度的 由数字和字母组成的字符串 后 记 入区块链. 哈希函数 (也称散列函数) 具有诸多优良 特 点, 因而特 别 适 合 用 于存储区 块链数据. 例 如, 通 过 哈 希 输 出 几 乎 不 能 反 推 输 入 值 (单 向 性), 不 同 长 度输入的哈希过程消耗大约相同的时间 (定时性) 且 产 生 固 定 长 度 的 输 出 (定 长 性), 即 使 输 入 仅 相 差 一 个字节也会产生显著不同的输出值 (随机性) 等. 比 特 币 区 块 链 通 常 采 用 双 SHA256 哈 希 函 数, 即 将 任 意长度的原始数据经过两次 SHA256 哈希运算后转 换为长度为 256 位 (32 字节) 的二进制数字来统一 存储和识别. 除上述特点外, SHA256 算法还具有巨 大 的 散 列 空 间 (2 ) 和 抗 碰 撞 (避 免 不 同 输 入 值 产 生相同哈希值) 等特性, 可满足比特币的任何相关标 记需要而不会出现冲突.

Merkle 树: Merkle 树 是区块 链 的 重 要 数据结 构, 其 作 用 是 快 速归 纳 和 校 验 区 块 数 据 的 存 在性 和 完 整性. 如 图 3 所 示, Merkle 树 通 常 包 含 区 块 体 的 底 层 (交 易) 数 据 库, 区 块 头 的 根 哈希 值 (即 Merkle 根) 以及所有沿底层区块数据到根哈希的分 支. Merkle 树 运 算 过 程 一 般 是 将 区 块 体 的 数 据 进 行分组哈希, 并将生成的新哈希值插入到 Merkle 树 中, 如 此 递 归直 到只剩 最 后 一 个 根 哈 希 值 并 记 为 区 块 头的 Merkle 根. 最 常见的 Merkle 树 是 比特币采 用的二叉 Merkle 树, 其每个哈希节点总是包含两个 相 邻 的 数 据 块 或 其 哈 希 值 , 其 他 变 种 则 包 括 以 太 坊 的 Merkle patricia tree 等 . Merkle 树 有诸 多 优 点: 首 先 是 极大 地 提 高 了 区 块 链 的 运 行 效 率 和 可 扩 展 性, 使 得 区 块头 只 需 包含根 哈 希 值 而 不 必 封 装 所 有 底 层 数 据, 这 使 得 哈希运 算 可 以 高 效 地 运 行 在 智能手机甚至物联网设备上; 其次是 Merkle 树可支

持 “简化支付验证” 协议, 即在不运行完整区块链网 络节点的情况下, 也能够对 (交易) 数据进行检验 . 例如, 为验证图 3 中交易 6, 一个没有下载完整区块 链 数据的 客户 端可 以通 过向 其他 节点 索要 包括 从交 易 6 哈 希 值 沿 Merkle 树 上 溯 至 区 块 头 根 哈 希 处 的 哈希序列 (即哈希节点 6, 5, 56, 78, 5 678, 1 234) 来 快 速 确 认 交 易 的 存 在 性 和 正 确 性. 一 般 说 来, 在 *N* 个 交易组 成的 区块 体中 确认任一交易 的 算法复 杂度 仅 为 log2 *N* . 这 将 极 大 地 降 低 区 块 链 运 行 所 需 的 带 宽 和 验 证 时 间, 并 使 得 仅保存 部 分 相 关 区 块 链 数 据 的轻量级客户端成为可能.

非 对称 加密: 非 对称 加 密是 为满 足安 全性 需 求 和 所 有 权 验 证 需 求 而 集 成 到 区 块 链 中 的 加 密 技 术, 常 见 算法 包 括 RSA、Elgamal、Rabin、D-H 、ECC (即 椭 圆曲线 加 密算法) 等. 非 对 称 加密通 常 在加密 和 解 密 过 程 中 使 用 两 个 非 对 称 的 密 码, 分 别 称 为公 钥和私钥. 非对称密钥对具有两个特点, 首先是用其 中 一个密 钥 (公 钥或私 钥) 加 密信息后, 只 有另 一个 对应的密钥才能解开; 其次是公钥可向其他人公开 、 私 钥 则 保密, 其 他人 无 法 通 过 该公 钥 推 算 出 相 应 的 私 钥. 非 对 称 加 密 技 术 在 区 块 链 的 应 用 场 景 主 要 包 括信息加密 、数字签名和登录认证等, 其中信息加密 场景主要是由信息发送者 (记为 A) 使用接受者 (记 为 B) 的 公钥 对 信 息 加 密 后 再 发 送 给 B, B 利 用 自 己 的 私 钥对 信 息 解 密. 比 特币 交 易的 加 密 即 属 于 此 场 景; 数 字签名场景则 是由 发送 者 A 采用自 己的 私 钥加密信息后发送给 B, B 使 用 A 的公钥对信息解 密 、从 而 可 确 保 信 息 是 由 A 发 送 的; 登 录 认 证 场 景 则 是由客 户端 使用 私钥 加密 登录 信息 后发 送给 服务 器, 后 者 接 收后 采用该 客 户 端 的 公 钥 解 密 并 认 证 登 录信息.

以 比 特 币 系 统 为 例, 其 非 对 称 加 密 机 制 如 图 4 所 示: 比 特 币 系统 一 般 通 过 调 用 操 作 系 统 底 层 的 随 机 数 生 成 器 来 生 成 256 位 随 机 数 作 为 私 钥. 比 特 币 私 钥 的 总 量 可 达 2 , 极 难 通 过 遍 历 全 部 私 钥 空 间 来 获 得存 有 比 特币的私 钥, 因 而 是 密码 学 安全 的. 为 便于 识别, 256 位 二进 制 形式 的比 特币 私钥 将 通 过 SHA256 哈希算法和 Base58 转换, 形成 50 个字 符 长 度 的 易 识别和 书 写 的 私 钥 提 供 给 用 户; 比 特 币 的公钥是由私钥首先经过 Secp256k1 椭圆曲线算法 生 成 65 字 节长 度的 随 机 数. 该 公 钥 可用 于产 生比 特 币 交 易时 使 用 的 地 址, 其 生成 过 程为 首 先 将 公 钥 进 行 SHA256 和 RIPEMD160 双 哈 希运 算 并 生成 20 字节长度的摘要结果 (即 hash160 结果), 再经过 SHA256 哈希算法和 Base58 转换形成 33 字符长度 的 比 特 币 地 址 . 公 钥 生 成 过 程 是 不 可 逆 的, 即 不 能通过公钥反推出私钥. 比特币的公钥和私 钥 通 常



[4]

[3]

[19]

486

自

动

化

学

报

42 卷

图 4

比特币非对称加密机制

Fig. 4 The asymmetric cryptography of the Bitcoin system

保存于比特币钱包文件, 其中私钥最为重要. 丢失私 钥 就 意 味 着 丢 失 了 对 应 地 址 的 全 部 比 特 币 资 产. 现 有 的 比 特 币 和 区 块 链 系 统 中, 根 据 实 际应 用 需 求已 经 衍 生 出 多 私 钥 加 密 技 术, 以 满 足 多重签 名 等 更 为 灵活和复杂的场景.

2.2 网络层

网 络 层 封 装 了 区 块 链 系 统 的 组 网 方 式 、消 息 传 播 协 议 和数 据 验 证机 制 等 要素. 结 合 实 际应用 需 求, 通 过 设 计特 定 的 传播 协议 和数 据验 证 机 制, 可 使 得 区 块链系 统中 每一 个节 点都 能参与区块数据的校验 和 记 账 过 程, 仅 当 区 块数 据 通 过全网 大 部 分 节 点 验 证后, 才能记入区块链.

组网方式: 区块链系统的节点一般具有分布式 、 自治性 、开放可自由进出等特性, 因而一般采用对等 式 网络 (Peer-to-peer network, P2P 网 络) 来 组 织 散 布 全球的 参与数据验 证和记账的节点. P2P 网络 中 的每个 节点 均地 位对 等且以 扁平 式 拓扑 结构 相互 连 通 和 交 互, 不 存 在 任何 中 心 化的特 殊 节 点 和 层 级 结 构, 每 个 节点均 会 承 担网络 路 由、验 证 区块数 据 、 传播区块数据 、发现新节点等功能. 按照节点存储数 据量的不同, 可以分为全节点和轻量级节点. 前者保 存 有从创 世区块 到 当前最 新区块为 止 的完整 区块链 数 据, 并 通 过 实时参 与 区 块 数 据 的 校 验 和 记 账 来 动 态 更 新 主 链. 全 节 点 的 优 势 在 于 不 依 赖 任 何 其 他 节 点 而 能 够 独 立 地 实 现 任 意 区 块 数 据 的 校 验 、查 询 和 更新, 劣势则是维护全节点的空间成本较高; 以比特 币为例, 截 止到 2016 年 2 月, 创世区块至 当 前区块 的数据量已经超过 60 GB. 与之相比, 轻量级节点则 仅 保 存 一 部 分 区 块 链 数 据, 并 通过第 2.1 节 提 到 的 简 易支付 验证 方式 向其 相邻 节点 请求所需的数 据 来 完成数据校验.

数据传播协议: 任一区块数据生成后, 将由生成 该 数据的 节点 广播 到全 网其 他所 有的节点来加以验 证. 现 有 的 区 块 链 系 统 一 般 根 据 实 际 应 用 需 求 设 计 比 特 币 传 播 协 议 的 变 种, 例 如 以 太坊区 块 链 集 成 了 所 谓的 “幽灵 协议” 以 解决 因区 块 数据 确认 速度 快

而导致的高区块作废率和随之而来的安全性风险 . 根 据 中 本聪 的 设 计, 比 特币 系 统 的 交 易 数 据传 播 协 议包括如下步骤 :

1. 比特币交易节点将新生成的交易数据向全网 所有节点进行广播;
2. 每个节点都将收集到的交易数据存储到一个 区块中;
3. 每个节点基于自身算力在区块中找到一个具 有足够难度的工作量证明;
4. 当 节 点 找 到 区 块 的 工 作 量 证 明 后, 就 向 全 网 所有节点广播此区块;
5. 仅当包含在区块中的所有交易都是有效的且 之前未存在过的, 其他节点才认同该区块的有效性;
6. 其 他 节 点 接 受 该 数 据 区 块, 并 在 该 区 块 的 末 尾 制 造 新 的 区 块 以 延 长 该 链 条, 而 将 被 接受区 块 的 随机哈希值视为先于新区块的随机哈希值.

需 要 说 明 的 是, 如 果交易 节 点 是 与 其 他 节 点 无 连 接 的 新 节 点, 比 特 币 系统通 常 会 将 一 组 长 期 稳 定 运行的 “种子节点” 推荐给新节点建立连接, 或者推 荐至少一个节点连接到新节点. 此外, 交易数据广播 时, 并不需要全部节点均接收到, 而是只要足够多的 节 点 做 出 响 应 即 可 整 合 进 入 区 块 账 本 中. 未 接 收 到 特 定交易 数据 的节 点则 可向 邻近 节点请 求下载该缺 失的交易数据 .

数 据 验 证 机 制: P2P 网 络 中 的 每 个 节 点 都 时 刻 监 听 比 特 币 网 络 中 广 播 的 数 据 与 新 区 块. 节 点 接 收 到 邻 近 节 点 发 来 的 数 据 后, 将 首 先 验证该 数 据 的 有 效 性. 如 果 数据 有 效, 则 按照 接收 顺序 为新 数 据建 立 存 储 池 以 暂 存 尚 未 记 入 区 块 的 有 效 数 据, 同 时 继 续 向 邻 近 节 点 转 发; 如 果 数 据 无 效, 则 立 即 废 弃 该 数 据, 从 而 保 证无效 数 据 不 会 在 区 块 链 网 络 继 续 传 播. 以比特币为例, 比特币的矿工节点会收集和验证 P2P 网 络 中广 播 的 尚 未确 认 的 交 易 数 据, 并 对 照 预 定义的标准清单, 从数据结构 、语法规范性 、输入输 出 和 数 字 签 名 等 各 方 面 校 验 交 易 数 据 的 有 效 性, 并 将有效交易数据整合到当前区块中; 同理, 当某矿工

[23]

[24]

[19]

17

18

4 期

袁勇等: 区块链技术发展现状与展望

487

“挖”到新 区块 后, 其 他矿 工节 点也会按 照 预定义 标 准 来 校 验 该 区 块 是 否 包 含 足 够 工 作 量 证 明, 时 间 戳 是否有效等; 如确认有效, 其他矿工节点会将该区块 链接到主区块链上, 并开始竞争下一个新区块.

由 网络 层设 计机 理可 见, 区 块 链 是典 型 的分布 式 大 数 据 技 术. 全 网 数 据 同 时 存 储 于 去 中 心 化 系 统 的 所 有 节 点 上, 即 使 部 分 节 点 失 效, 只 要 仍 存 在 一 个 正 常 运 行 的 节 点, 区 块 链 主链数 据 就 可 完 全 恢 复 而 不 会 影 响 后 续 区 块 数 据 的 记 录 与 更 新. 这 种 高 度 分 散 化 的 区 块 存 储 模 式 与 云 存 储 模 式 的 区 别 在 于, 后 者是基 于中 心化 结构 基础 上的 多重存 储和多重数 据 备 份 模式, 即 “多中 心 化” 模式; 而 前 者 则是 完 全 “去中心化” 的存储模式, 具有更高的数据安全性.

2.3 共识层

如 何 在分布 式 系统中 高 效地 达 成共识 是 分布 式 计 算 领 域 的重 要 研 究 问题. 正 如 社 会 系统 中 “民主” 和 “集中” 的对立关系相似, 决策权越分散的系统达 成共识的效率越低 、但系统稳定性和满意度越高; 而 决 策 权 越 集 中 的 系 统 更 易 达 成 共 识, 但 同 时 更易出 现 专 制 和 独 裁. 区 块 链 技 术 的 核 心 优 势 之 一 就 是 能 够 在决策 权高 度分 散的 去中 心化 系统 中使 得各 节点 高效地针对区块数据的有效性达成共识.

早 期 的比特 币 区块链 采 用高 度 依赖节 点 算力 的 工作量证明 (Proof of work, PoW) 机制来保证比特 币 网 络 分 布 式 记 账 的 一 致 性. 随 着 区 块 链 技 术 的 发 展 和 各 种 竞 争 币 的 相 继 涌 现, 研 究 者 提出 多 种 不依 赖 算 力 而能 够 达 成 共 识 的 机 制, 例 如点 点 币首 创 的 权益证明 (Proof of stake, PoS) 共识 和比特股首 创 的 授 权 股 份 证 明 机 制 (Delegated proof of stake, DPOS) 共 识 机制 等. 区 块 链共识 层 即封装了这 些共识机制.

PoW 共识: 中本聪在其比特币奠基性论文中设 计了 PoW 共识机制, 其核心思想是通过引入分布式 节点的算力竞争来保证数据一致性和共识的安全性. 比 特币 系统 中, 各 节 点 (即 矿工) 基 于各自的计算机 算 力相互 竞争 来共 同解 决一个 求解 复杂 但验 证容 易 的 SHA256 数 学 难 题 (即 挖 矿), 最 快 解决该难 题 的 节 点将获 得区 块记 账权 和系 统自 动生 成的 比特 币奖 励. 该数学 难题 可表 述 为: 根 据当前难度值, 通 过 搜 索求解一个合适的随机数 (Nonce) 使得图 3 中区块 头各元数据的双 SHA256 哈希值小于或等于目标哈 希 值. 比 特 币系 统 通 过灵 活调 整 随 机 数 搜 索的 难 度 值来控制区块的平均生成时间为 10 分钟左右. 一般 说 来, PoW 共 识 的 随 机 数 搜 索 过 程 如 下 (参 照 图 3 区块结构) :

步骤 **1.** 搜集当前时间段的全网未确认交易, 并 增 加 一 个 用 于发 行 新 比 特 币 奖励 的 Coinbase 交 易,

形成当前区块体的交易集合;

步 骤 **2.** 计 算区 块 体交 易 集合 的 Merkle 根 记 入区块头, 并填写区块头的其他元数据, 其中随机数 Nonce 置零;

步 骤 **3.** 随 机 数 Nonce 加 1; 计 算 当前 区 块 头 的双 SHA256 哈希值, 如果小于或等于目标哈希值, 则成功搜索到合适的随机数并获得该区块的记账权; 否则继续步骤 3 直到任一节点搜索到合适的 随机数 为止;

步骤 **4.** 如果一定时间内未成功, 则更新时间戳 和 未 确认 交 易 集合 、重 新 计算 Merkle 根 后 继续 搜 索.

符 合 要求的 区 块头哈 希 值通 常由多个前导零构 成, 目 标 哈 希 值 越 小, 区 块头 哈希值的前导 零 越 多, 成 功找 到合 适的 随机 数并 “挖”出新 区块 的难 度越 大. 据 区 块 链实 时 监测 网 站 Blockchain.info 显 示, 截 止 到 2016 年 2 月, 符 合 要求 的 区 块头 哈 希 值一 般有 17 个前导零, 例如第 398 346 号区块哈希值为 “0000000000000000077f754f22f21629a7975cf *···*”. 按 照 概 率 计 算, 每 16 次 随 机 数 搜 索 将 会 有 找 到 一 个 含 有 一个 前 导 零 的 区 块 哈希 值, 因 而 比 特币 目 前 17 位 前 导 零 哈 希 值 要 求 16 次 随 机 数 搜 索 才 能 找 到 一 个 合 适 的 随 机 数 并 生 成 一 个 新 的 区 块. 由 此 可 见, 比 特 币区 块 链 系 统 的 安 全 性 和不 可 篡 改 性 是 由 PoW 共识机制的强大算力所保证的, 任何对于区块 数 据的攻 击或 篡改都必须重新计算该区块 以 及其 后 所 有 区 块 的 SHA256 难 题, 并 且 计 算 速 度 必 须 使 得 伪 造 链 长 度 超 过 主 链, 这 种 攻 击难度 导 致的 成本 将 远 超 其 收 益. 据 估 计, 截 止 到 2016 年 1 月, 比 特 币 区块链的算力已经达到 800 000 000 Gh/s, 即每秒进 行 8 *×* 10 次 运 算, 超 过 全 球 Top500 超 级 计 算 机 的算力总和.

PoW 共识机制是具有重要意义的创新, 其近乎 完 美 地 整 合 了 比 特 币 系 统 的 货 币 发 行 、交 易 支 付 和 验 证 等 功能, 并 通过 算 力 竞 争 保障 系 统 的 安 全 性 和 去 中心性; PoW 共 识机制同时存在 着显 著的 缺陷, 其强大算力造成的资源浪费 (如电力) 历来为研究者 所诟病, 而且长达 10 分钟的交易确认时间使其相对 不适合小额交易的商业应用.

PoS 共识机制: PoS 共识是为解决 PoW 共识机 制 的 资 源浪 费 和 安 全 性 缺 陷而 提 出 的 替 代 方案. 限 于 篇 幅, 本 文 主 要 聚 焦 于 PoS 相 对 于 PoW 的 创 新 之处. PoS 共识本质上是采用权益证明来代替 PoW 中 的 基 于 哈 希 算 力 的 工 作 量 证 明, 是 由 系 统中具 有 最 高 权 益 而 非 最 高 算 力 的 节 点 获 得 区 块 记 账 权. 权 益 体 现 为 节 点 对 特 定 数 量 货 币 的 所 有 权, 称 为 币 龄 或币天数 (Coin days). 币龄是特定数量的币与其最 后 一 次 交易 的 时 间 长 度 的 乘积, 每 次 交 易 都将 会 消

[19]

[24]

[25]

488

自

动

化

学

报

42 卷

耗掉特定数量的币龄. 例如, 某人在一笔交易中收到 10 个币后并持有 10 天, 则获得 100 币龄; 而后其花 掉 5 个币后, 则消耗掉 50 币龄. 显然, 采用 PoS 共 识机制的系统在特定时间点上的币龄总数是有限的, 长 期 持 币 者 更 倾 向 于 拥 有 更 多 币 龄, 因 此 币 龄可 视 为其在 PoS 系统中的权益. 此外, PoW 共识过程中 各 节点 挖矿难度 相 同, 而 PoS 共 识过 程中的难 度 与 交 易 输 入的 币 龄 成 反 比, 消 耗币 龄 越多 则 挖 矿 难 度 越 低. 节 点 判 断 主 链 的 标 准 也 由 PoW 共 识 的 最 高 累 计 难 度 转 变 为 最 高 消 耗 币 龄, 每 个 区 块的交 易 都 会 将 其 消 耗 的 币 龄 提 交 给 该 区 块, 累 计 消 耗币龄 最 高的区块将被链接到主链. 由此可见, PoS 共识过程 仅 依靠内 部币 龄和权益而不需要消耗外部 算 力和 资 源, 从根本上解决了 PoW 共识算力浪费的 问题, 并 且 能 够 在 一 定 程 度 上 缩 短 达 成 共 识 的 时 间, 因 而 比 特币之后的许多竞争币均采用 PoS 共识机制.

DPoS 共识机制: DPoS 共识机制的基本思路类 似 于 “董事会决 策”, 即 系 统 中每个 股 东 节点 可 以 将 其 持 有 的股 份 权 益 作 为 选 票 授 予一 个 代 表, 获 得 票 数 最 多 且愿意成 为 代 表的 前 101 个 节 点将进入 “董 事会”, 按照既定的时间表轮流对交易进行打包结算 并且签署 (即生产) 一个新区块. 每个区块被签署之 前, 必 须 先 验证 前 一个区 块 已 经 被 受 信 任 的 代 表 节 点 所签 署. “董事 会” 的 授权代 表 节点可 以从 每笔交 易 的 手 续 费 中 获 得 收 入, 同 时 要 成为 授 权 代表节 点 必 须 缴 纳 一 定 量 的 保 证 金, 其 金 额 相当于 生 产 一 个 区 块 收入 的 100 倍. 授 权 代 表节点 必 须对 其 他 股 东 节点负责, 如果其错过签署相对应的区块, 则股东将 会 收 回 选 票从而 将 该节 点 “投出” 董 事会. 因 此, 授 权 代 表 节 点 通 常 必 须 保 证 99 % 以 上 的 在 线 时 间 以 实现盈利目标 . 显然, 与 PoW 共识机制必须信任 最高算力节点和 PoS 共识机制必须信任最高权益节 点 不同 的是, DPoS 共 识机 制中 每个 节点 都能 够 自 主 决定其 信任 的授 权节 点且 由这 些节 点轮 流记账 生 成 新 区 块, 因 而 大 幅减少 了 参 与 验 证 和 记 账 的 节 点 数量, 可以实现快速共识验证.

除 上 述 三 种 主 流 共 识 机 制 外, 实 际区块 链 应 用 中 也 衍 生出 了 PoW+PoS、行 动 证 明 (Proof of ac- tivity) 等多个变种机制. 这 些共识机制各有 优劣势, 比 特 币 的 PoW 共 识 机 制 依 靠 其 先 发 优 势 已 经 形 成 成 熟 的 挖矿 产 业链, 支 持 者 众 多, 而 PoS 和 DPoS 等新兴机制则更为安全 、环保和高效, 从而使得共识 机 制的选 择问 题成 为区 块链 系统 研究 者最 不易 达成 共识的问题.

2.4 激励层

区 块 链共识 过 程通过 汇 聚大 规 模共识 节 点的 算 力 资源来 实现 共享 区块 链账 本的 数据 验证 和记 账工

作, 因 而 其本 质 上 是 一 种 共 识 节 点间 的 任 务 众 包 过 程. 去 中心 化系 统中 的 共识 节点 本身 是自 利的, 最 大化自身收益是其参与数据验证和记账的根本目标. 因 此, 必 须 设 计 激 励 相 容 的 合 理 众 包 机 制, 使 得 共 识 节点最 大化 自身 收益的 个体 理性 行为与 保障 去 中 心化区块链系统的安全和有效性的整体目标相吻合. 区 块链系 统通 过设计适度的经济激 励机制 并 与共识 过 程 相 集 成, 从 而 汇 聚大 规 模 的节点 参 与 并 形 成 了 对区块链历史的稳定共识.

以比特币为例, 比特币 PoW 共识中的经济激励 由 新发行 比特 币奖 励和 交易 流通 过程 中的 手续 费两 部 分 组 成, 奖 励 给 PoW 共 识过 程 中 成 功 搜 索 到 该 区块的随机数并记录该区块的节点. 因此, 只有当各 节 点通过 合作共 同构 建共 享和 可信的区块链 历 史记 录 、并维护比特币系统的有效性, 其获得的比特币奖 励 和 交 易手 续 费 才 会 有 价 值. 比 特币 已 经 形 成 成熟 的 挖 矿 生 态 圈, 大 量 配 备专业 矿 机 设 备 的 矿 工 积 极 参与基于挖矿的 PoW 共识过程, 其根本目的就是通 过获取比特币奖励并转换为相应法币来实现盈利.

发 行机 制: 比 特 币 系统 中 每个 区 块发 行 比特 币 的 数 量 是 随 着 时 间 阶 梯性 递 减 的. 创 世 区 块起 的 每 个 区 块 将 发 行 50 个 比 特 币 奖 励 给 该 区 块 的 记 账 者, 此 后每 隔 约 4 年 (21 万 个 区 块) 每 区 块 发 行 比 特币的数量降低一半, 依此类推, 一直到比特币的数 量 稳 定 在 上 限 2 100 万 为 止 . 比 特 币 交 易 过 程 中 会 产 生 手 续 费, 目 前 默 认手续 费 是 万 分 之 一 个 比 特 币, 这部分费用也会记入区块并奖励给记账者. 这两 部 分 费 用 将 会 封 装 在 每 个 区 块 的 第 一个 交易 (称 为 Coinbase 交 易) 中. 虽 然 现 在 每 个区块 的 总 手续费 相对于新发行比特币来说规模很小 (通常不会超过 1 个 比特 币), 但 随着 未来 比特 币发 行数 量的 逐步 减少 甚 至 停 止 发 行, 手 续 费 将逐渐 成 为 驱 动 节 点 共 识 和 记账的主要动力. 同时, 手续费还可以防止大量微额 交易对比特币网络发起的 “粉尘” 攻击, 起到保障安 全的作用.

分 配 机 制: 比 特 币 系 统 中, 大 量 的 小 算 力 节 点 通 常 会 选 择 加 入 矿 池, 通 过 相 互合作 汇 集 算 力 来 提 高 “挖”到 新 区 块 的 概 率, 并 共 享 该 区 块 的 比 特 币 和 手 续 费 奖 励. 据 Bitcoinmining.com 统 计, 目 前 已 经 存 在 13 种 不 同 的 分 配 机 制 . 主 流 矿 池 通 常 采 用 PPLNS (Pay per last *N* shares) 、PPS (Pay per share) 和 PROP (PROPortionately) 等 机 制. 矿 池将各 节点 贡献 的算 力按 比例 划分 成不 同的 股份 (Share), 其 中 PPLNS 机 制是指发现区 块 后, 各 合 作 节 点 根 据 其在 最后 *N* 个 股份内 贡献 的 实 际 股份 比 例 来分 配 区 块 中的比 特 币; PPS 则 直 接根据股份 比 例 为 各节 点 估 算 和 支 付 一个 固 定 的 理论 收益, 采 用 此方式 的矿 池将 会适 度收 取手 续费 来弥 补其 为各

[4]

[19]

[7]

4 期

袁勇等: 区块链技术发展现状与展望

489

节 点 承 担 的 收益不确 定 性 风险; PROP 机 制 则 根据 节 点 贡 献 的 股 份 按 比 例 地 分 配 比 特 币. 矿 池 的 出 现 是 对 比 特 币 和 区 块 链 去 中 心 化 趋 势 的 潜 在 威 胁, 如 何 设 计 合 理 的 分 配 机 制 引 导 各 节 点 合 理 地 合 作 、避 免 出现因 算力 过度 集中 而导 致的 安全 性问 题是 亟待 解决的研究问题.

2.5 合约层

合 约 层 封 装 区 块 链 系 统 的 各 类 脚 本 代 码 、算 法 以及由此生成的更为复杂的智能合约. 如果说数据 、 网 络和 共识三个 层次 作为 区块 链底 层 “虚拟 机” 分 别承担数据表示 、数据传播和数据验证功能的话, 合 约 层则是 建立 在区 块链 虚拟 机之 上的 商业 逻辑 和算 法, 是 实 现区 块 链系 统 灵活 编 程和 操 作数据 的 基 础. 包 括比特 币在 内的 数字 加密 货币 大多 采用 非图 灵完 备 的 简 单 脚 本 代 码 来 编 程 控 制 交 易 过 程, 这 也 是 智 能合约的雏形; 随着技术的发展, 目前已经出现以太 坊 等图灵 完备 的可 实现 更为 复杂 和灵 活的 智能 合约 的 脚 本 语 言, 使 得 区 块链 能 够 支持宏 观 金融 和社 会 系统的诸多应用. 本节将以比特币脚本为例, 从技术 角 度 简 述 合 约 层 的 基 本 技 术 和 方 法; 关 于 智 能 合 约 的延伸内容将在第 5 节讨论.

比 特币 采 用一 种 简单 的 、基 于堆 栈的、从 左 向 右 处 理 的 脚 本 语 言, 而 一 个 脚本本 质 上 是 附 着 在 比 特 币 交 易 上 的一 组 指 令 的 列 表. 比 特 币交 易 依 赖于 两 类 脚 本 来 加 以 验 证, 即 锁 定 脚 本 和 解 锁 脚 本, 二 者 的不同 组合 可在 比特 币交 易中 衍生 出无 限数 量的 控制条件. 其中, 锁定脚本是附着在交易输出值上的 “障碍”, 规 定 以 后 花 费 这 笔 交 易 输 出 的 条 件; 解 锁 脚 本则是 满足 被锁 定脚 本在 一个 输出 上设 定的花费 条 件 的 脚 本, 同 时 它 将 允 许 输 出 被 消 费. 举 例 来 说, 大 多数比 特币 交易 均是 采用 接受 者的 公钥 加密 和私 钥 解 密, 因 而其对应的 P2PKH (Pay to public key hash) 标 准 交 易 脚 本 中 的 锁 定 脚 本 即 是 使 用 接 受 者 的 公 钥 实现 阻 止 输 出 功 能, 而 使用 私 钥 对 应的 数 字 签名来加以解锁 .

比 特币 脚本 系统 可以 实现 灵活 的交 易控 制. 例 如, 通 过 规 定 某 个 时 间 段 (如 一 周) 作 为 解 锁 条 件, 可 以 实 现延 时 支 付; 通 过规 定 接 受 者 和 担 保人 必 须 共 同 私 钥 签 名 才 能 支 配 一 笔 比 特 币, 可 以 实 现担 保 交 易; 通 过 设 计 一 种 可 根 据 外 部 信 息 源 核 查 某 概 率 事 件是否 发生的 规则 并 作为 解锁 脚本 附着 在一 定数 量 的 比 特 币 交 易 上, 即 可 实 现博彩 和 预 测 市 场 等 类 型 的应 用; 通 过 设定 *N* 个 私 钥集 合中 至少 提 供 *M* 个私钥才可解锁, 可实现 *M −N* 型多重签名, 即 *N* 个 潜 在 接 受 者 中 至 少 有 *M* 个 同 意 签 名 才 可 实 现 支 付. 多重签名可广泛应用于公司决策 、财务监督 、中 介担保甚至遗产分配等场景.

比 特 币 脚 本 是 智 能 合 约 的 雏 形, 催 生了人 类 历 史 上第 一种 可 编程 的全 球性 货币. 然 而, 比 特币 脚 本 系 统 是 非 图 灵 完 备 的, 其 中 不 存在 复 杂 循环和 流 控 制, 这 在 损失 一 定 灵 活 性 的 同 时能 够 极 大 地 降 低 复 杂 性 和 不 确 定 性, 并 能 够 避免因 无 限 循 环 等 逻 辑 炸 弹 而 造成 拒 绝 服务 等类 型的 安全 性 攻 击. 为 提高 脚 本 系 统 的 灵 活 性 和 可 扩 展 性, 研 究 者 已经尝 试 在 比 特 币 协议 之 上 叠 加 新 的 协 议, 以 满足 在 区 块 链 上 构 建 更 为 复 杂 的 智 能 合 约 的 需 求. 以 太 坊 已 经 研 发 出 一 套 图 灵 完 备 的 脚 本 语 言, 用 户 可 基于 以 太 坊构 建任意复杂和精确定义的智能合约与去中心化应用, 从 而为基 于区 块链 构建 可编 程的 金融 与社 会系 统奠 定了基础 .

3 区块链的应用场景

由 区块 链独 特的 技术 设计 可见, 区 块 链 系统 具 有分布式高冗余存储 、时序数据且不可篡改和伪造 、 去 中 心化 信用 、自 动 执行 的智 能合 约 、安 全 和隐 私 保 护 等 显 著 的 特 点, 这 使 得 区块链 技 术 不 仅 可 以 成 功应用于数字加密货币领域, 同时在经济 、金融和社 会 系 统 中 也 存 在 广 泛 的 应 用 场 景. 根 据 区 块 链 技 术 应 用 的现 状, 本 文将 区 块 链 目 前的 主 要 应 用 笼统 地 归 纳 为 数字 货 币 、数 据 存储 、数 据 鉴 证、金 融 交 易、 资 产 管 理 和 选 举 投 票 共 六 个 场 景, 并 概 述 除数字 货 币外的五大应用场景以及区块链的三种应用模式.

数据存储: 区块链的高冗余存储 (每个节点存储 一 份数 据) 、去 中心化 、高 安全 性和隐 私保 护等特 点 使 其 特 别 适 合 存 储 和 保 护 重 要 隐 私 数 据, 以 避 免 因 中 心化机 构遭受 攻 击或 权限 管 理不 当而造成 的 大规 模数据丢失或泄露. 与比特币交易数据类似地, 任意 数 据 均 可 通 过 哈 希 运 算 生 成 相 应 的 Merkle 树 并 打 包 记 入 区 块 链, 通 过 系 统内共 识 节 点 的 算 力 和 非 对 称 加 密 技 术 来 保 证 安 全 性. 区 块 链 的 多 重 签 名 技 术 可以灵活配置数据访问的权限, 例如必须获得指定 5 个 人中 3 个 人的私 钥授权才可获得访问权限. 目 前, 利用区块链来存储个人健康数据 (如电子病历 、基因 数据等) 是极具前景的应用领域, 此外存储各类重要 电 子文 件 (视 频、图 片、文 本等) 乃 至 人类思 想和意 识等也有一定应用空间 .

数 据鉴 证: 区 块 链 数 据 带有 时间 戳 、由 共 识 节 点共同验证和记录 、不可篡改和伪造, 这些特点使得 区 块 链 可 广 泛 应 用 于 各 类 数 据 公 证 和 审 计 场 景. 例 如, 区 块 链可 以 永 久 地 安 全 存 储 由政 府机 构 核 发的 各 类许 可证 、登 记表 、执 照、证 明、认 证和 记录 等, 并 可在任 意时 间点 方便 地证 明某 项数 据的 存在 性和 一 定 程 度 上 的 真 实 性. 包 括 德 勤 在 内 的 多 家 专 业 审 计 公司已 经部 署区 块链 技术 来帮 助其 审计 师实 现低 成本和高效地实时审计; Factom 公司则基于区块链

[26]

[27]

[1]

[4]

48

490

自

动

化

学

报

42 卷

设 计 了 一 套 准 确 的 、可 核 查 的 和 不 可 更 改 的 审 计 公 证流程与方法 .

金 融 交 易: 区 块 链 技 术 与 金 融 市 场 应 用 有 非 常 高 的 契 合度. 区 块链 可 以 在 去中 心 化 系 统 中 自 发 地 产 生 信 用, 能 够 建 立无中 心 机 构 信 用 背 书 的 金 融 市 场, 从 而在 很大 程度 上实 现 了 “金融 脱媒”, 这 对 第 三 方 支 付 、资 金 托 管 等 存 在 中 介 机 构 的 商 业 模 式 来 说是颠覆性的变革; 在互联网金融领域, 区块链特别 适合或 者已经应用于股权众筹、P2P 网络 借贷和 互 联 网 保 险 等 商 业 模 式; 证 券和银行 业 务 也 是 区 块 链 的 重 要 应用 领 域, 传 统证 券 交 易 需 要 经 过 中央 结 算 机 构 、银 行 、证 券 公司 和交 易 所 等中 心机 构 的 多 重 协 调, 而 利 用区 块 链 自 动 化 智能 合 约 和 可 编 程 的特 点, 能够极大地降低成本和提高效率, 避免繁琐的中 心 化 清 算交 割 过 程, 实 现 方 便快 捷 的金 融 产品 交 易; 同 时, 区 块 链 和比特 币 的 即 时 到 帐 的 特 点 可 使 得 银 行 实 现 比 SWIFT 代 码 体 系 更 为 快 捷 、经 济 和 安 全 的 跨 境 转 账; 这 也 是 目 前 R3CEV 和 纳 斯 达 克 等 各 大 银 行 、证 券 商 和 金 融 机 构 相 继 投 入 区 块 链 技 术 研 发的重要原因.

资 产 管 理: 区 块 链 在 资 产 管 理 领 域 的 应 用 具 有 广泛前景, 能够实现有形和无形资产的确权 、授权和 实时监控. 对于无形资产来说, 基于时间戳技术和不 可 篡 改 等 特 点, 可 以 将 区块链 技 术 应 用 于 知 识 产 权 保护 、域名管理、积分管理等领域; 而对有形资产来 说, 通 过 结 合物 联网技 术 为 资 产 设 计 唯 一 标 识 并 部 署 到 区块 链上, 能 够形 成 “数字 智能 资 产”, 实 现基 于区块链的分布式资产授权和控制. 例如, 通过对房 屋 、车辆等实物资产的区块链密钥授权, 可以基于特 定 权限 来发放 和回 收资 产的使 用权, 有 助于 Airbnb 等 房屋租 赁或 车辆 租赁 等商 业模 式实 现自动化的资 产交接; 通过结合物联网的资产标记和识别技术, 还 可 以利用 区块 链实 现灵 活的 供应 链管 理和 产品 溯源 等功能.

选 举 投 票: 投 票 是 区 块 链 技 术 在 政 治 事 务 中 的 代 表 性 应 用. 基 于 区 块 链 的 分 布 式 共 识 验 证 、不 可 篡改等特点, 可以低成本高效地实现政治选举 、企业 股东投票等应用; 同时, 区块链也支持用户个体对特 定议题的投票. 例如, 通过记录用户对特定事件是否 发 生 的 投 票, 可 以 将 区块 链 应 用 于 博 彩 和 预 测 市 场 等 场 景 ; 通 过 记 录 用 户 对 特 定 产 品 的 投 票 评 分 与 建议, 可以实现大规模用户众包设计产品的 “社会制 造” 模式等.

根 据 实 际 应 用 场 景 和 需 求, 区 块链技 术 已 经 演 化出三种应用模式, 即公共链 (Public blockchain)、 联盟链 (Consortium blockchain) 和私有链 (Private blockchain). 公 共链 是完 全去 中 心化 的区 块链, 分 布 式 系 统 的 任 何 节 点 均 可 参 与 链 上 数 据 的 读 写 、验

证 和 共 识 过 程, 并 根 据 其 PoW 或 PoS 贡 献 获 得 相 应的经济激励. 比特币是公共链的典型代表. 联盟链 则 是部 分去 中心 化 (或 称多中 心化) 的 区块链, 适 用 于 多 个 实体 构 成 的 组 织 或 联盟, 其 共 识 过 程受 到 预 定义的一组节点控制, 例如生成区块需要获得 10 个 预 选 的 共 识 节 点 中 的 5 个 节 点 确 认; 私 有 链 则 是 完 全 中 心 化 的 区 块 链, 适 用 于 特定机 构 的 内 部 数 据 管 理与审计等, 其写入权限由中心机构控制, 而读取权 限可视需求有选择性地对外开放. 需要说明的是, 由 于 去 中 心化 程 度 不 同, 联 盟链 和 私有 链 可 能 不 完 全 符 合 第 2 节 提 出 的 区 块 链 模 型, 例 如 中 心 化 程 度 较 高的区块链可能不需要设计激励层中的经济激励等.

4 区块链的现存问题

作 为 近 年 来 兴 起 并 快 速 发 展 的 新 技 术, 区 块链 必 然 会 面临 各 种 制 约 其 发 展的 问 题 和 障 碍. 本 节 将 从 安 全、效 率、资 源和 博 弈 四方 面概 述区 块 链 技术 有待解决的问题.

4.1 安全问题

安 全 性威胁 是 区块链 迄 今为 止所面临的最重要 的问题. 其中, 基于 PoW 共识过程的区块链主 要面 临 的 是 51 % 攻 击 问 题, 即 节 点 通 过 掌 握 全 网 超 过 51 % 的 算 力 就 有 能 力 成 功 篡 改 和 伪 造 区 块 链 数 据. 以 比 特 币 为 例, 据 统 计 中国大 型 矿 池 的 算 力 已 占 全 网总算力的 60 % 以上, 理论上这些矿池可以通过合 作 实 施 51 % 攻 击, 从 而 实 现 比 特 币 的 双 重 支 付 . 虽 然 实 际 系 统 中 为 掌 握 全 网 51 % 算 力 所 需 的 成 本 投入远超成功实施攻击后的收益, 但 51 % 攻击的安 全性威胁始终存在. 基于 PoS 共识过程在一定程度 上解决了 51 % 攻击问题, 但同时也引入了区块分叉 时的 N@S (Nothing at stake) 攻 击问题. 研究 者已 经 提 出通 过 构 造 同 时依 赖 高 算力 和 高内 存 的 PoW 共识算法来部分解决 51 % 攻击问题 , 更为安全和 有效的共识机制尚有待于更加深入的研究和设计.

区 块 链 的 非 对 称 加 密 机 制 也 将 随 着 数 学 、密 码 学和计算技术的发展而变的越来越脆弱. 据估计, 以 目 前 天 河 二 号 的 算 力 来说, 产 生 比 特 币 SHA256 哈 希 算 法 的 一 个 哈 希 碰 撞 大 约 需 要 2 年, 但 随着 量 子 计 算 机等 新 计 算 技 术 的 发展, 未 来 非 对 称加 密 算 法 具 有 一 定 的 破解 可能性, 这 也 是 区块 链 技 术面临 的潜在安全威胁.

区 块 链 的隐 私 保 护 也 存 在 安 全 性 风 险. 区 块 链 系 统 内 各 节 点 并 非 完 全 匿 名, 而 是 通 过类 似 电 子邮 件地址的地址标识 (例如比特币公钥地址) 来实现数 据 传 输. 虽 然 地 址 标 识 并 未 直 接 与真 实 世 界的 人物 身份相关联, 但区块链数据是完全公开透明的, 随着 各 类 反 匿名 身 份 甄 别 技 术 的发 展, 实 现 部 分重 点 目

[30]

[28]

[1]

[29]

4 期

袁勇等: 区块链技术发展现状与展望

491

标的定位和识别仍是有可能的.

4.2 效率问题

区 块链 效率 也是 制约 其应 用 的重 要 因素. 首 先 是 区 块 膨胀 问 题: 区 块链 要 求 系 统 内 每 个 节点 保 存 一 份 数 据 备 份, 这 对 于 日益增 长 的 海 量 数 据 存 储 来 说 是极 为困 难 的. 以 比 特币 为 例, 完 全同 步自 创世 区 块至 今 的 区 块 数 据 需 要 约 60 GB 存 储空间, 虽 然 轻 量 级 节点 可 部 分 解 决 此 问 题, 但 适用 于 更大 规 模 的 工 业 级 解 决 方 案 仍 有 待 研 发 . 其 次 是 交 易 效 率 问题: 比 特 币区 块链目 前每 秒仅 能处理 7 笔 交易, 这 极大地 限制 了区 块链 在大 多数 金融 系统 高频 交易 场 景 中 的 应 用 (例 如 VISA 信 用 卡 每 秒 最 多 可 处 理 10 000 笔 交易) ; 最 后是 交 易 确 认 时 间 问 题: 比 特 币区块生成时间为 10 分钟, 因而交易确认时间一般 为 10 分钟, 这在一定程度上限制了比特币在小额交 易和时间敏感交易中的应用.

4.3 资源问题

PoW 共 识过 程 高 度 依 赖 区 块 链 网 络 节 点 贡 献 的 算 力, 这 些 算 力 主 要 用 于 解 决 SHA256 哈 希 和 随 机数搜索, 除此之外并不产生任何实际社会价值, 因 而 一 般 意 义上认 为 这 些 算 力资 源 是 被 “浪费” 掉了, 同 时 被 浪 费 掉 的 还 有 大 量 的 电 力 资 源. 随 着 比 特 币 的 日 益 普 及 和 专 业 挖 矿 设 备 的 出 现, 比 特 币 生态 圈 已经在资本和设备方面呈现出明显的军备竞赛态势, 逐 渐 成 为高 耗 能 的 资 本 密 集 型 行业, 进 一步 凸 显了 资源消耗问题的重要性. 因此, 如何能有效汇集分布 式 节 点 的 网络 算 力 来解 决 实 际 问 题, 是 区块 链 技术 需 要 解 决 的重 要 问 题. 研 究者 目 前 已 经 开 始尝 试 解 决 此 问 题, 例 如 Primecoin (质 数 币) 要 求 各 节 点 在 共 识 过 程 中 找 到 素 数 的 最 长 链 条 (坎宁安 链 和 双 向 双 链) 而 非无意 义的 SHA256 哈 希值 . 未 来的潜 在 发展趋 势是设计行之 有 效的交 互机 制来汇聚和利 用 分 布 式共 识 节 点 的 群体 智能, 以 辅 助 解 决 大规 模 的实际问题.

4.4 博弈问题

区 块链 网络 作为 去中 心化 的分 布式 系统, 其 各 节 点在交 互过 程中 不可 避免 地会 存在 相互 竞争 与合 作的博弈关系, 这在比特币挖矿过程中尤为明显. 通 常 来 说, 比 特 币 矿池 间 可 以通过 相 互 合 作 保 持 各 自 稳 定 的 收 益. 然 而, 矿 池 可 以 通 过 称 为 区 块 截 留 攻 击 (Block withholding attacks) 的 方 式 、通 过 伪 装 为 对 手 矿 池 的 矿 工 、享 受 对 手 矿 池 的 收 益 但 不 实 际 贡 献 完 整 工 作 量 证 明 来 攻 击 其 他 矿 池, 从 而 降 低对 手矿池的收益. 如果矿池相互攻击, 则双方获得的收 益 均 少 于不 攻 击 对 方 的 收 益. 当 矿池 收 益 函 数 满足 特 定 条 件时, 这 种 攻 击 和竞争将 会 造 成 “囚徒 困 境”

博 弈结 局 . 如 何设计合 理的惩 罚函数 来 抑制非 理 性 竞 争 、使 得 合 作 成 为 重 复 性 矿 池 博 弈 的 稳 定 均 衡 解, 尚需进一步深入研究. 此外, 正如前文提到的, 区 块 链 共 识 过 程 本 质 上 是 众 包 过 程, 如 何 设 计激励 相 容 的 共 识机 制, 使 得去 中 心 化 系 统中 的 自 利 节 点 能 够 自 发 地实 施 区 块 数 据 的 验证 和 记 账 工 作, 并 提 高 系统内非理性行为的成本以抑制安全性攻击和威胁, 是区块链有待解决的重要科学问题.

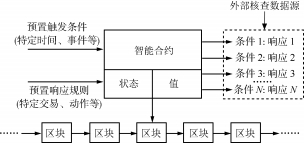
5 基于区块链的智能合约

智 能 合 约概 念 最 早在 1994 年 由学者 Nick Sz- abo 提 出, 最 初被 定义 为一 套以 数字形式定义的 承 诺, 包 括 合 约参 与方可 以 在 上 面 执 行 这 些 承 诺 的 协 议, 其 设 计初 衷 是希 望 通 过 将 智 能合 约 内 置 到 物 理 实 体 来 创 造 各 种 灵 活 可 控 的 智 能 资 产. 由 于 计 算 手 段 的 落后 和应 用 场 景 的 缺 失, 智 能合 约 并未 受 到 研 究者的广泛关注.

区 块 链 技术 的 出 现 重 新 定 义 了 智 能 合 约. 智 能 合 约 是 区 块 链 的 核 心 构 成 要 素 (合 约 层), 是 由 事 件 驱 动 的 、具 有状 态 的 、运 行 在可 复制 的共 享 区 块链 数 据 账 本上 的 计 算 机 程 序, 能 够实 现 主 动或 被 动 的 处理数 据, 接 受、储存和发送价值, 以及 控制和 管 理 各 类 链 上智 能资 产 等 功 能. 智 能 合约 作 为 一 种 嵌 入 式 程 序化合约, 可 以 内置在 任 何 区块 链 数据、交 易 、 有 形 或 无 形 资 产 上, 形 成 可 编程控 制 的 软 件 定 义 的 系 统、市 场 和 资 产. 智 能 合 约 不 仅 为 传 统 金 融 资 产 的 发 行、交 易、创 造和 管 理 提供 了创 新性 的解 决 方 案, 同 时能 够 在 社会系 统 中的 资 产 管理 、合 同 管理、 监管执法等事务中发挥重要作用.

具 体说 来, 智 能合 约是 一组 情景—应 对型 的程 序化规则和逻辑, 是部署在区块链上的去中心化 、可 信 共 享 的 程 序 代 码. 智 能 合 约 同 样 具 有 区 块 链 数 据 的一般特征, 如 分布式记录、存储和 验证, 不可篡改 和 伪 造 等. 签 署 合 约 的 各 参 与 方 就 合 约 内 容 、违 约 条件 、违约责任和外部核查数据源达成一致, 必要时 检 查 和 测 试 合 约 代 码 以 确 保 无 误 后, 以 智 能 合约的 形 式 部 署 在 区 块 链 上, 即 可 不 依赖任 何 中 心 机 构 地 自 动 化 代 表 各 签 署 方 执 行 合 约. 智 能 合 约 的 可 编 程 特性使得签署方可以增加任意复杂的条款.

智能合约的运作机理如图 5 所示: 通常情况下, 智 能 合 约 经 各 方 签 署 后, 以 程 序 代码 的形 式 附 着在 区 块 链数 据 (例 如一 笔比 特 币交 易) 上, 经 P2P 网 络 传 播 和 节 点 验 证 后 记 入 区 块 链 的 特 定 区 块 中. 智 能 合 约 封 装 了 预 定 义 的 若 干 状 态 及 转 换 规 则 、触 发 合 约 执 行 的 情 景 (如 到 达 特 定 时 间 或 发 生 特 定 事 件 等)、特 定 情景下的 应对行 动等. 区 块链 可实时 监 控 智能合约的状态, 并通过核查外部数据源 、确认满足 特定触发条件后激活并执行合约.



[31*−*32]

[33]

[1]

[34]

492

自

动

化

学

报

42 卷

图 5

智能合约的运作机理

至 去 中 心化 自 治 社会 (Decentralized autonomous society, DAS) 成为可能.

就 现 状 而 言, 区 块链和 智 能 合 约 技 术 的 主 要 发 展 趋 势 是 由 自 动 化 向 智 能 化 方 向 演 化. 现 存 的 各 类 智 能 合 约 及 其 应 用 的 本 质 逻 辑 大 多 仍 是 根 据 预 定 义 场景 的 “IF-THEN” 类 型的 条 件响 应 规则, 能 够 满 足 目 前 自 动 化 交 易 和 数 据 处 理 的 需 求. 未 来 的 智 能 合 约 应 具 备 根 据 未 知 场 景 的 “WHAT-IF” 推 演 、 计 算 实 验和 一 定 程 度 上 的 自 主 决策 功 能, 从 而实 现

Fig. 5 The rationale of smart contracts

区 块 链 和 智 能 合 约 有 极 为 广 阔 的 应 用 场 景. 例 如, 互联网金融领域的股权众筹或 P2P 网络借贷等 商 业 模 式 可 以 通 过 区 块 链 和 智 能 合 约 加 以 实 现. 传 统 方式 是通 过 股 权 众 筹或 P2P 借 贷 的 交 易 所或 网 络平台作为中心机构完成资金募集 、管理和投资, 实 际 操作过 程中 容易 出现 因中 心机 构的 信用 缺失 而导 致的资金风险. 利用智能合约, 这些功能均可以封装 在 去 中 心 化 可 信 的 区 块 链 上 自 动 执 行. 区 块 链 可 记 录 每 一 笔融 资, 当 成功 达 到 特 定 融资 额 度 时 计 算 每 个 投 资 人 的 股 权 份 额, 或 在 一 段 时 间 内 未 达 到 融 资 额度时自动将资金退还给投资人. 再如, 通过将房屋 和 车 辆 等实 体 资 产 进 行 非 对称 加 密, 并 嵌 入含 有 特 定 访 问 控 制 规 则 的 智 能 合 约 后 部 署 在 区 块 链 上, 使 用 者符 合特定 的访 问权限 或执行特定操作 (如 付款) 后 就 可 使 用 这 些 资 产, 这 能 够 有效解 决 房 屋 或 车 辆 租赁商业模式中资产交接和使用许可方面的痛点.

智能合约具有自治 、自足和去中心化等特征. 自 治 表 示 合 约 一 旦 启 动 就 会 自 动 运 行, 而 不 需 要其 他 签 署 方 进 行 任 何 干 预; 自 足 则 意 味 着 合 约 能 够 通 过 提 供 服 务 或 发 行 资 产 来 获 取 资 金, 并 在 需 要时使 用 这 些 资 金; 去 中 心 化 则 意 味 着 智 能 合 约 是 由 去 中 心 化 存储 和验证的 程 序代 码而 非中心 化实 体来 保障 执 行 的 合 约, 能 在 很 大程度 上 保 证 合 约 的 公 平 和 公 正 性 .

智能合约对于区块链技术来说具有重要的意义. 一 方 面, 智 能 合 约 是 区 块 链 的 激 活 器, 为 静 态 的 底 层 区 块 链 数 据 赋 予 了 灵 活 可 编 程 的 机 制 和 算 法, 并 为 构 建 区 块 链 2.0 和 3.0 时 代 的 可 编 程 金 融 系 统 与 社 会 系 统 奠 定 了 基 础; 另 一 方 面, 智 能 合 约 的 自 动 化 和可编 程特 性使 其可 封装 分布 式区 块链 系统 中各 节 点 的 复杂 行为, 成 为区 块 链 构 成 的 虚 拟 世 界 中的 软 件 代 理 机 器 人, 这 有 助 于促 进 区 块链技 术 在 各 类 分 布 式 人 工 智 能 系 统 中 的 应 用, 使 得 基 于 区 块 链 技 术 构 建 各 类 去 中 心 化 应 用 (Decentralized applica- tion, Dapp) 、去中心化自治组织 (Decentralized au- tonomous organization, DAO)、去中心化自治公司 (Decentralized autonomous corporation, DAC) 甚

由 目 前 “自动 化” 合 约 向 真 正 的 “智能” 合 约 的 飞 跃 .

6 区块链驱动的平行社会

互 联 网近年 来 的迅猛 发 展及 其与物理世界的深 度 耦 合 与 强 力 反 馈, 已 经 根 本性地 改 变 了 现 代 社 会 的生产 、生活与管理决策模式, 形成了现实物理世界 – 虚 拟网络 空 间 紧 密 耦 合 、虚 实 互 动 和 协 同 演 化 的 平行社会空间, 催生了 “互联网 +”和工业 4.0 等一 系 列 国 家战 略. 未 来社 会 的 发 展 趋势 则 必 将 从 物 理 + 网络的 CPS 实际世界 (Cyber-physical systems, CPS) 走 向 精 神 层 面 的 人 工 世 界, 形 成 物 理 + 网 络 + 人 工的 人–机–物一体 化的三 元耦 合系 统, 称 为 社会物理信息系统 (Cyber-physical-social systems, CPSS). 目前, 基于 CPSS 的 平行社会已现端倪, 其 核心和本质特征是虚实互动与平行演化 .

区块链是实现 CPSS 平行社会的基础架构之一, 其 主要贡 献是 为分 布式 社会系 统和分布 式 人工 智能 研 究 提 供 了 一 套 行 之 有 效 的 去 中 心 化 的 数 据 结 构 、 交 互 机 制 和 计 算 模 式, 并 为 实 现平行 社 会 奠 定 了 坚 实 的数 据基 础 和信 用基 础. 就 数 据基 础而 言, 管 理 学家爱德华戴明曾说过: 除了上帝, 所有人必须以数 据 说话. 然 而在 中心 化 社会 系统 中, 数 据通 常掌 握 在 政府 和大型 企业等 “少数 人”手 中, 为 少数 人 “说 话”, 其公正性 、权威性甚至安全性可能都无法保证. 区 块 链 数 据 则 通 过 高 度 冗 余 的 分 布 式 节 点 存 储, 掌 握 在 “所有 人” 手中, 能 够 做 到 真 正 的 “数据 民 主”. 就 信 用 基 础 而 言, 中 心 化 社会系 统 因 其 高 度 工 程 复 杂性和社会复杂性而不可避免地会存在 “默顿系统” 的特性, 即 不确定性、多样性 和复杂性, 社 会系统中 的 中心机 构和规则制定 者 可能会 因个 体利 益而 出现 失 信 行 为; 区 块链 技 术 有 助 于 实现 软 件 定 义 的 社 会 系 统, 其 基 本 理 念 就 是 剔 除 中 心 化 机构 、将 不 可 预 测 的行为 以智 能合 约的 程序 化代 码形 式提 前部 署和 固 化 在 区 块 链 数 据 中, 事 后 不 可伪造 和 篡 改 并 自 动 化执行, 从而在一定程度上能够将 “默顿” 社会系统 转化为可全面观察 、可主动控制 、可精确预测的 “牛 顿” 社会系统 .

ACP (人 工 社 会 Artiﬁcial societies 、计 算 实验



[35]

[36]

4 期

袁勇等: 区块链技术发展现状与展望

493

Computational experiments 和 平 行 执 行 Parallel execution) 方 法 是迄今为止平行社会管理领域唯 一 成体系化的 、完整的研究框架, 是复杂性科学在新时 代平行社会环境下的逻辑延展和创新 . ACP 方法 可 以 自 然地 与 区 块 链 技 术 相 结 合, 实 现区 块 链驱 动 的平行社会管理. 首先, 区块链的 P2P 组网 、分布式 共 识协作 和基 于贡 献的 经济 激励等 机制 本身 就是 分 布 式 社 会 系 统 的 自 然 建 模, 其 中 每 个节点 都 将 作 为 分 布式 系统 中的 一个自主 和自治 的智能体 (Agent). 随 着 区 块 链 生 态 体 系 的 完 善, 区 块 链 各共 识 节 点和 日 益复杂 与自 治的 智能 合约 将通 过参 与各 种形 式的 Dapp, 形成特定组织形式的 DAC 和 DAO, 最终形 成 DAS, 即 ACP 中的人工社会 . 其次, 智能合约 的 可 编 程 特 性 使 得 区 块 链 可 进 行 各 种 “WHAT-IF” 类型的虚拟实验设计 、场景推演和结果评估, 通过这 种 计算实 验过 程获 得并 自动 或半 自动 地执行 最优 决 策. 最 后, 区 块链 与物 联网 等相 结合 形成 的 智能 资 产使得联通现实物理世界和虚拟网络空间成为可能, 并 可通过 真实 和人 工社 会系 统的 虚实 互动 和平 行调 谐实现社会管理和决策的协同优化. 不难预见, 未来 现 实物理 世界 的实 体资 产都 登记为 链上 智能 资产 的 时候, 就是区块链驱动的平行社会到来之时.

7 结束语

随 着 以比特 币 为代表 的 数字 加 密货币 的 强势 崛 起, 新 兴 的区 块 链 技术逐 渐 成 为 学 术 界 和 产 业 界 的 热点研究课题. 区块链技术的去中心化信用 、不可篡 改和可编程等特点, 使其在数字加密货币 、金融和社 会系统中有广泛的应用前景. 然而, 与蓬勃发展的区 块 链 商 业应 用 相 比, 区 块链 的 基 础 理 论 和 技术 研 究 仍处于起步阶段, 许多更为本质性的 、对区块链产业 发 展 至 关 重 要 的 科 学 问 题 亟 待 研 究 跟 进. 本 文 系 统 地 梳 理了 区块 链技 术的 基 本 原理 、技 术 、方 法 与应 用, 以期为未来研究提供有益的启发与借鉴.

**References**

1. Swan M. *Blockchain: Blueprint for a New Economy*. USA: O Reilly Media Inc., 2015.
2. Technical report by the UK government chief scientiﬁc ad- viser [Online], available: <https://www.gov.uk/government/>

uploads/system/uploads/attachment data/ﬁle/492972/gs-

16-1-distributed-ledger-technology.pdf, February 21, 2016 3 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system

[Online], available: <https://bitcoin.org/bitcoin.pdf,>2009 4 Ethereum White Paper. A next-generation smart con-

tract and decentralized application platform [Online], available: <https://github.com/ethereum/wiki/wiki/White->

Paper, November 12, 2015

5 Ding Wei. Block chain based instrument data management system. *China Instrumentation*, 2015, (10): 15*−*17

(丁 未. 基 于 区 块 链 技 术 的 仪 器 数 据 管 理 创 新 系 统. 中 国 仪 器 仪 表, 2015, (10): 15*−*17)

6 Zhao He, Li Xiao-Feng, Zhan Li-Kui, Wu Zhong-Cheng. Data integrity protection method for microorganism sam- pling robots based on blockchain technology. *Journal of Huazhong University of Science and Technology (Natural Science Edition)*, 2015, **43**(Z1): 216*−*219

(赵 赫, 李 晓 风, 占 礼 葵, 吴 仲 城. 基 于 区 块 链 技 术 的 采 样 机 器 人 数 据 保 护 方 法. 华 中 科 技 大 学 学 报 (自 然 科 学 版), 2015, **43**(增 刊): 216*−*219)

1. Swan M. Blockchain thinking: the brain as a decentral- ized autonomous corporation. *IEEE Technology and Society Magazine*, 2015, **34**(4): 41*−*52
2. Davidson Eric. Letter. *New Scientist*, 2015, **228**(3043): 52*−*52
3. Anonymous. New kid on the blockchain. *New Scientist*, 2015, **225**(3009): 7
4. Godsiﬀ P. Bitcoin: bubble or blockchain. In: Proceedings of the 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KES- AMSTA). Sorrento, Italy: Springer, 2015, **38**: 191*−*203
5. Kraft D. Diﬃculty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, 2016, **9**(2): 397*−*413
6. Wilson D, Ateniese G. From pretty good to great: enhanc- ing PGP using Bitcoin and the blockchain. In: Proceedings of the 9th International Conference on Network and Sys- tem Security. New York: Springer International Publishing, 2015, **9408**: 368*−*375
7. Zyskind G, Nathan O, Pentland A S. Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW 2015). San Jose, CA: IEEE, 2015. 180*−*184
8. Kypriotaki K N, Zamani E D, Giaglis G M. From Bit- coin to decentralized autonomous corporations: extending the application scope of decentralized peer-to-peer networks and blockchains. In: Proceedings of the 17th International Conference on Enterprise Information Systems(ICEIS2015). 2015, **3**: 284*−*290
9. Blockchain Monitoring Website [Online], available: <https://blockchain.info/,>January 8, 2016
10. Cryptocurrency Monitoring Website [Online], available: <http://coinmarketcap.com/,>November 24, 2015
11. World Economic Forum Survey [Online], available: http:// www.coinfox.info/news/3184-world-economic-forum-survey

-10-of-global-gdp-may-be-stored-with-blockchain-technolog

y-by-2027, February 21, 2016

1. CoinDesk Report [Online], available: http://www. bit- coin86.com/news/3527.html, February 21, 2016
2. Antonopoulos A M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. USA: O Reilly Media Inc., 2014.
3. Fan Jie, Yi Le-Tian, Shu Ji-Wu. Research on the technolo- gies of Byzantine system. *Journal of Software*, 2013, **24**(6): 1346*−*1360

(范捷, 易乐天, 舒继武. 拜占庭系统技术研究综述. 软件学报, 2013, **24**(6): 1346*−*1360)

1. Bitcoin Sourcecode [Online], available: <https://github.com/>bitcoin/bitcoin/, January 18, 2016
2. Merkle R C. Protocols for public key cryptosystems. In: Pro- ceedings of the 1980 IEEE Symposium on Security and Pri- vacy. Oakland, CA, USA: IEEE, 1980. 122



494

自

动

化

学

报

42 卷

23 Larimer D. Transactions as proof-of-stake [Online], available: <http://7fvhfe.com1.z0.glb.clouddn.com/@/wp->

content/uploads/2014/01/TransactionsAsProofOfStake10.

pdf, 2013

1. Larimer D. Delegated proof-of-stake white paper [Online], available: <http://www.bts.hk/dpos-baipishu.html,>2014
2. Bitcoinmining Article [Online], available: <https://www.>bitcoinmining.com/bitcoin-mining-pools, December 8, 2015
3. Factom White Paper [Online], available: http://bite01. com/bit/1421, December 29, 2015
4. Brito J, Shadab H, Castillo A. Bitcoin ﬁnancial regulation: securities, derivatives, prediction markets, and gambling. *The Columbia Science & Technology Law Review*, 2014, **16**: 144*−*221
5. Eyal I, Efe Gencer A, Sirer E G, van Renesse R. Bitcoin-NG: a scalable blockchain protocol. *Cryptography and Security*, arXiv: 1510.02037
6. Primecoin Website [Online], available: http:// prime- coin.io/, February 9, 2016
7. Courtois N T, Bahack L. On subversive miner strategies and block withholding attack in Bitcoin digital currency. *Cryp- tography and Security*, arXiv: 1402.1718
8. Wang Fei-Yue. Computational experiments for behavior analysis and decision evaluation of complex systems. *Jour- nal of System Simulation*, 2004, **16**(5): 893*−*897

(王 飞 跃. 计 算实验 方法 与复 杂 系 统行为分 析 和 决 策评估. 系统 仿真 学报, 2004, **16**(5): 893*−*897)

32 Wang Fei-Yue, Qiu Xiao-Gang, Zeng Da-Jun, Cao Zhi- Dong, Fan Zong-Chen. A computational experimental plat- form for emergency response based on parallel systems. *Complex Systems and Complexity Science* , 2010, **7**(4): 1*−*10

(王飞跃, 邱晓刚, 曾大军, 曹志冬, 樊宗臣. 基于平行系统的非常规 突 发事件 计 算 实 验 平 台研 究. 复 杂 系 统 与 复杂性 科 学, 2010, **7**(4): 1*−*10)

33 Wang Fei-Yue, Wang Xiao, Yuan Yong, Wang Tao, Lin Yi-Lun. Social computing and computational societies: the foundation and consequence of smart societies. *Chinese Sci- ence Bulletin*, 2015, **60**(5*−*6): 460 *−*469

(王 飞 跃, 王 晓, 袁 勇, 王 涛, 林 懿伦. 社 会计 算 与 计算社 会: 智 慧 社 会的基础与必然. 科学通报, 2015, **60**(5*−*6): 460*−*469)

34 Wang Fei-Yue. Software-deﬁned systems and knowledge au- tomation: a parallel paradigm shift from Newton to Merton. *Acta Automatica Sinica*, 2015, **41**(1): 1*−*8

(王飞跃. 软件定义的系统与知识自动化: 从牛顿到默顿的平行升华. 自动化学报, 2015, **41**(1): 1*−*8)

35 Wang Fei-Yue. Artiﬁcial societies, computational experi- ments, and parallel systems: a discussion on computational theory of complex social-economic systems. *Complex Sys- tems and Complexity Science* , 2004, **1**(4): 25*−*35

(王 飞 跃. 人 工 社 会 、计 算 实 验 、平 行 系 统: 关 于 复 杂 社 会 经 济 系 统 计算研究的讨论. 复杂系统与复杂性科学, 2004, **1**(4): 25*−*35)

36 Wang Fei-Yue, Jiang Zheng-Hua, Dai Ru-Wei. Population studies and artiﬁcial societies: a discussion of artiﬁcial pop- ulation systems and their applications. *Complex Systems and Complexity Science* , 2005, **2**(1): 1*−*9

(王飞跃, 蒋正华, 戴汝为. 人口问题与人工社会方法: 人工人口系统 的设想与应用. 复杂系统与复杂性科学, 2005, **2**(1): 1*−*9)

袁 勇 中 国 科 学 院 自 动 化 研 究 所 复 杂 系 统 管 理 与 控 制 国 家 重 点 实 验 室 副 研 究 员. 2008 年 于 山 东 科技 大 学 获 得 计算 机 软 件 与 理 论 专 业 博 士 学 位. 主 要 研 究 方 向 为 商 务 智 能 与 计 算 广 告 学. 本 文 通 信 作者. E-mail: yong.yuan@ia.ac.cn (**YUAN Yong** Associate professor at the State Key Laboratory of Man-

agement and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences. He received his Ph. D. degree in computer software and theory from Shan- dong University of Science and Technology in 2008. His research interest covers business intelligence and computa- tional advertising. Corresponding author of this paper.)

王 飞 跃 中 国 科 学 院 自 动 化 研 究 所 复 杂 系统管理与控制国家重点实验室研究员, 国 防 科 技 大 学 军 事 计 算 实 验 与 平 行 系 统 技 术 中 心 教 授. 主 要 研 究 方 向 为 智 能 系 统和复杂系统的建模, 分析与控制. E-mail: feiyue.wang@ia.ac.cn

(**WANG Fei-Yue** Professor at the State Key Laboratory of Management

and Control for Complex Systems, Institute of Automa- tion, Chinese Academy of Sciences. He is also a professor at the Research Center of Military Computational Experi- ments and Parallel System, National University of Defense Technology. His research interest covers modeling, analysis, and control of intelligent systems and complex systems.)