CBS
创意区块学院

区块链技术应用基础

龙辉

1

导言

- 什么是区块链
- 课程目标

区块链

愿景：

去中心化、共识机制、代码即法律、互信社会

范式：

区块链不仅仅是一套调解和记录支付行为的系统，事实上它还是个功能强大、用途广泛的商品账本。

形态：

公有链、联盟链、私有链

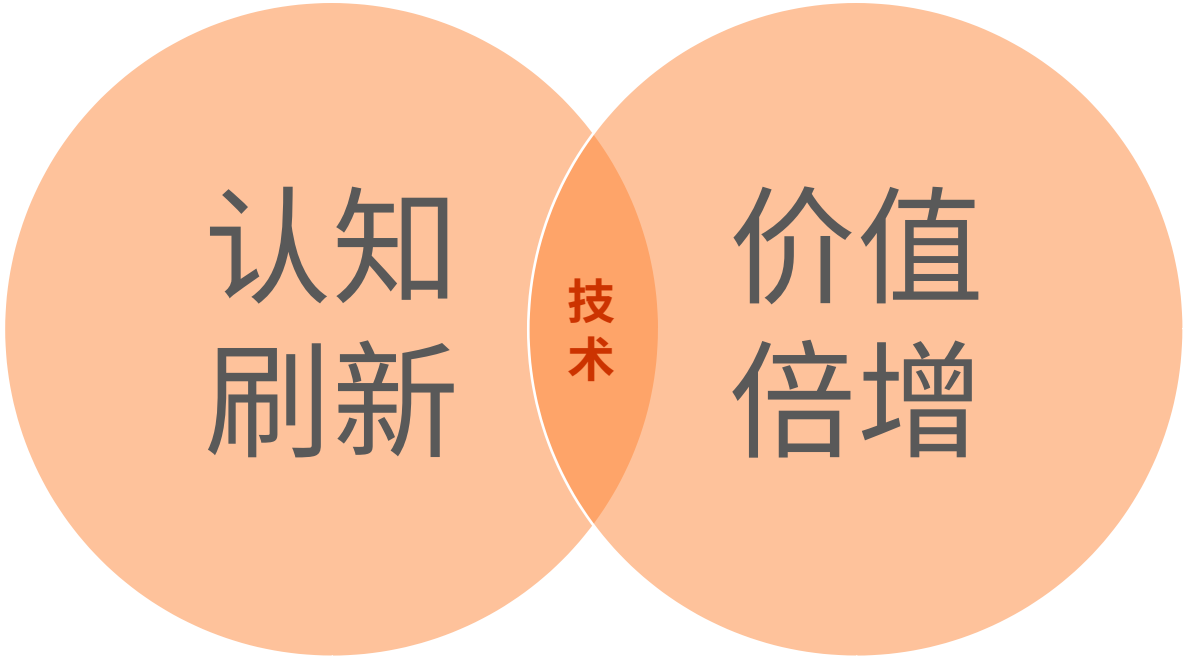
架构：

1.0 、 2.0 、 3.0

赋能：

传统行业、数字资产、智能合约、全球交易、行业应用、解决方案

分享目标



- 了解区块链的一些技术概念
- 理解区块链不仅仅只有比特币
- 了解比特币、以太坊等主流公链
- 了解区块链架构演变
- 知道一些密码学、共识常识
- 了解区块链常见应用和解决方案
- 为进入区块链做一些技术储备

2

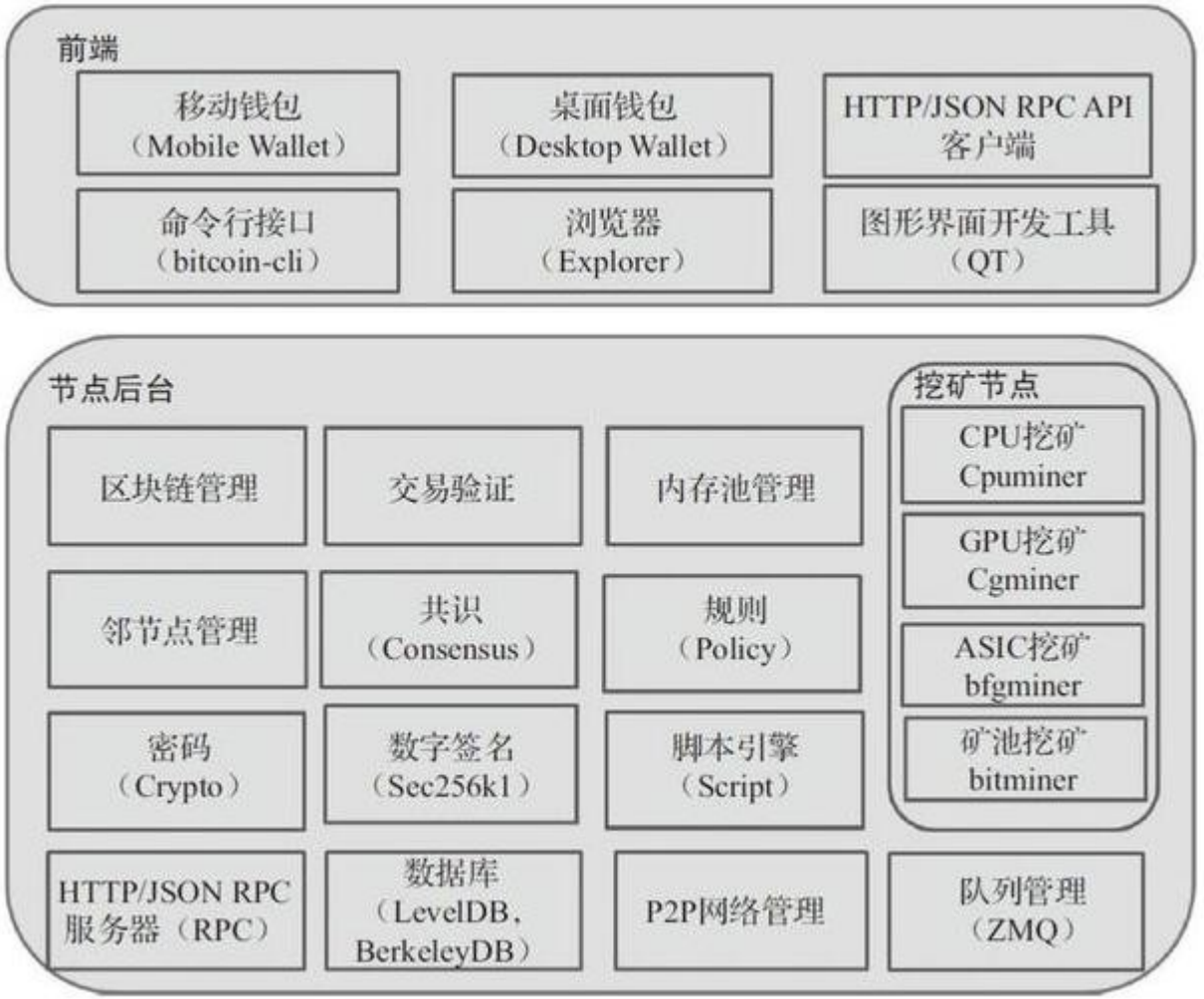
区块链

- 区块链
- 比特币
- 以太坊

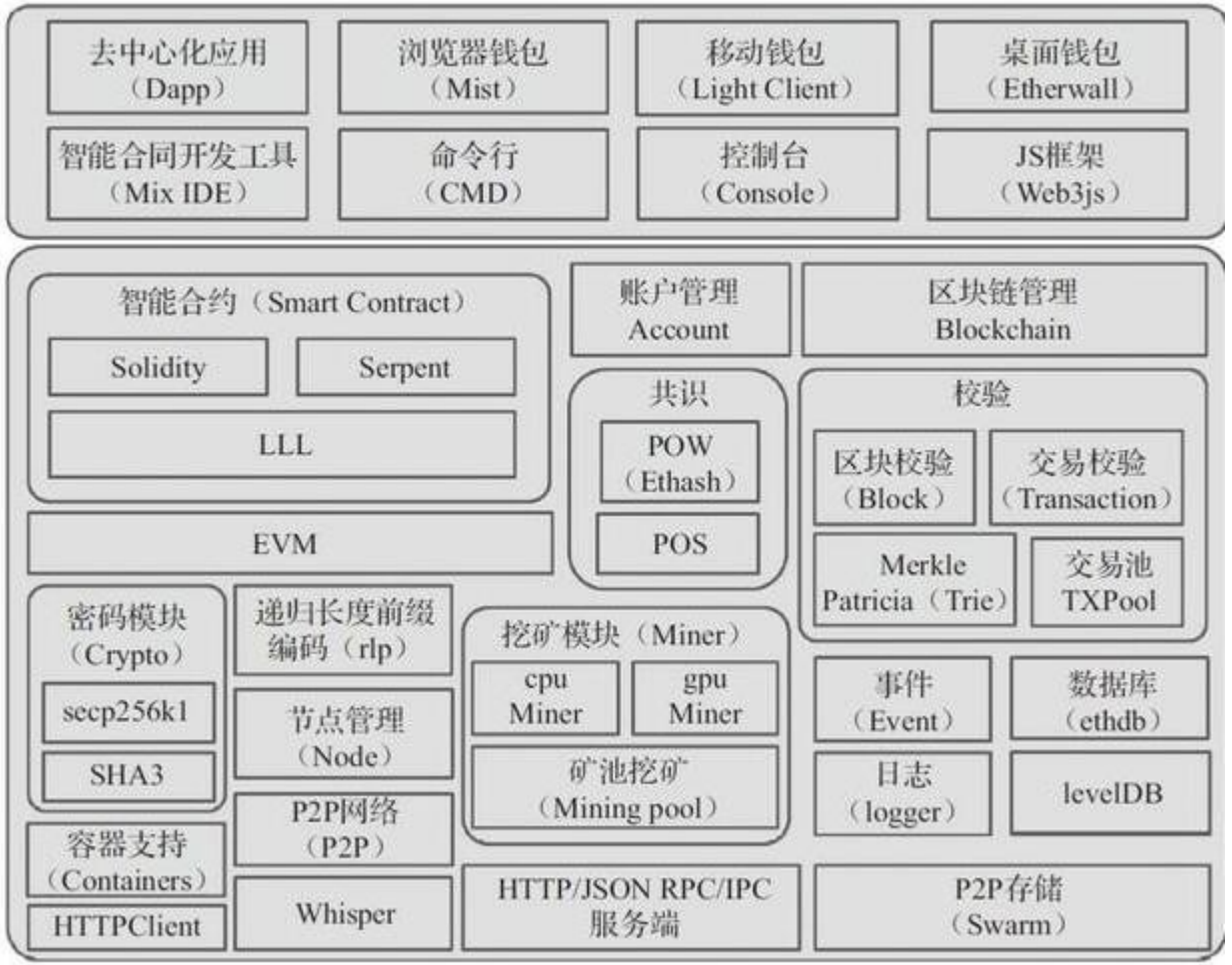
2.1 用区块链技术实现的各种链即为区块链

2.2 区块链架构

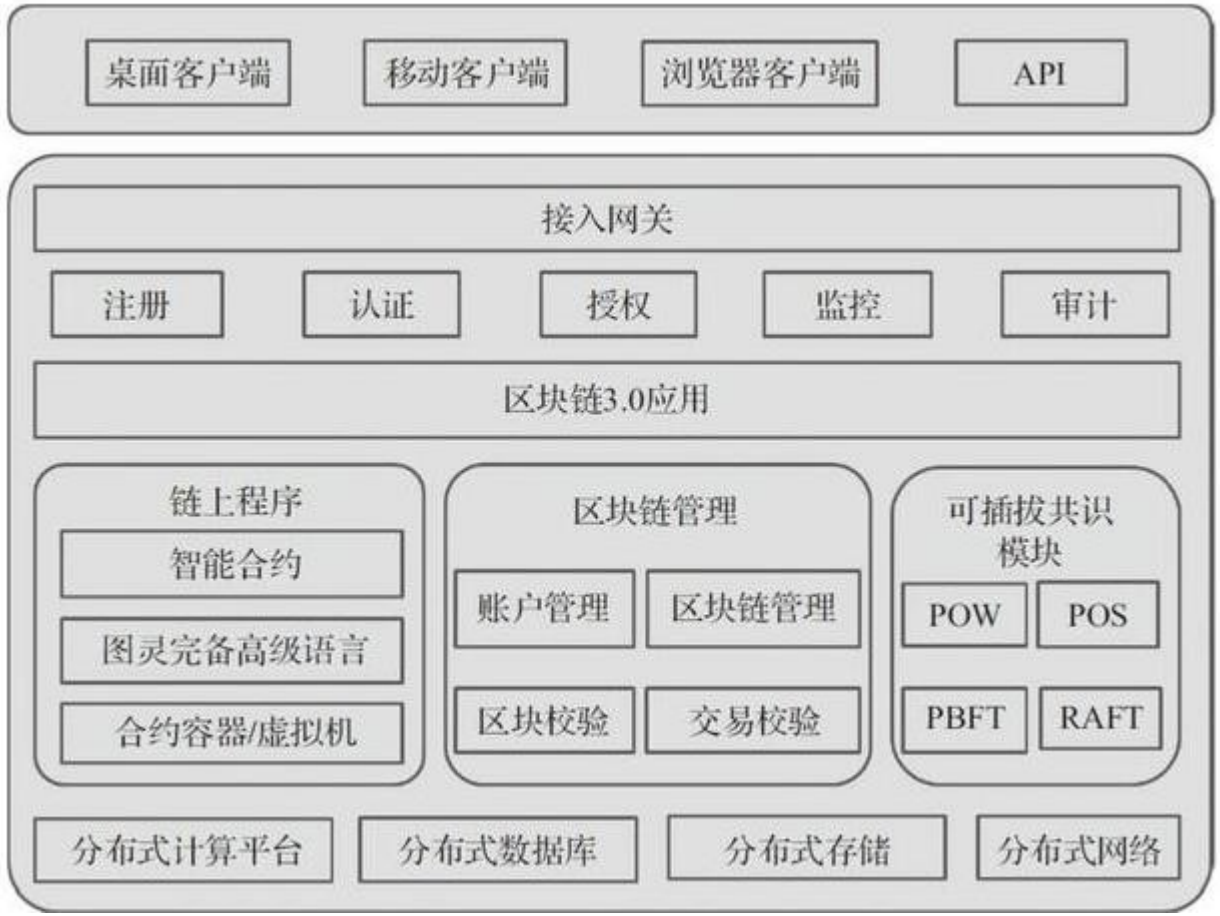
区块链 1.0


前端
移动钱包
（Mobile Wallet）
桌面钱包
（Desktop Wallet）
HTTP/JSON RPC API
客户端
命令行接口
（bitcoin-cli）
浏览器
（Explorer）
图形界面开发工具
（QT）
节点后台
区块链管理
交易验证
内存池管理
挖矿节点
CPU挖矿
Cpuminer
GPU挖矿
Cgminer
ASIC挖矿
bfgminer
矿池挖矿
bitminer
邻节点管理
共识
（Consensus）
规则
（Policy）
密码
（Crypto）
数字签名
（Sec256k1）
脚本引擎
（Script）
HTTP/JSON RPC
服务器（RPC）
数据库
（LevelDB，
BerkeleyDB）
P2P网络管理
队列管理
（ZMQ）

区块链 2.0


去中心化应用（Dapp）
浏览器钱包（Mist）
移动钱包（Light Client）
桌面钱包（Etherwall）
智能合同开发工具（Mix IDE）
命令行（CMD）
控制台（Console）
JS框架（Web3js）
智能合约（Smart Contract）
Solidity
Serpent
LLL
EVM
账户管理 Account
区块链管理 Blockchain
共识
POW（Ethash）
POS
校验
区块校验（Block）
交易校验（Transaction）
Merkle Patricia（Trie）
交易池 TXPool
密码模块（Crypto）
secp256k1
SHA3
递归长度前缀编码（rlp）
节点管理（Node）
P2P网络（P2P）
Whisper
挖矿模块（Miner）
cpu Miner
gpu Miner
矿池挖矿（Mining pool）
事件（Event）
数据库（ethdb）
日志（logger）
levelDB
容器支持（Containers）
HTTPClient
HTTP/JSON RPC/IPC 服务端
P2P存储（Swarm）

区块链 3.0


桌面客户端
移动客户端
浏览器客户端
API
接入网关
注册
认证
授权
监控
审计
区块链3.0应用
链上程序
智能合约
图灵完备高级语言
合约容器/虚拟机
区块链管理
账户管理
区块链管理
区块校验
交易校验
可插拔共识模块
POW
POS
PBFT
RAFT
分布式计算平台
分布式数据库
分布式存储
分布式网络

2.3 公有链、联盟链、私有链

公有链　　联盟连　　私有链

参与者	任何人可自由进出	联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	自定义
激励机制	需要	可选	不需要
中心化程度	去中心化	多中心化	中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
典型场景	虚拟货币	支付、结算	审计、发行
典型应用	比特币、以太坊	超级账本、 R3	Eris Industries

2.4 比特币

区块链为比特币而生

比特币：区块链的杀手级应用

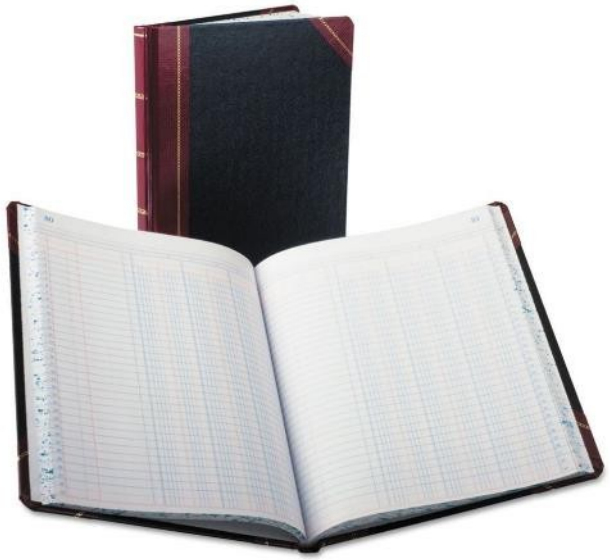
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

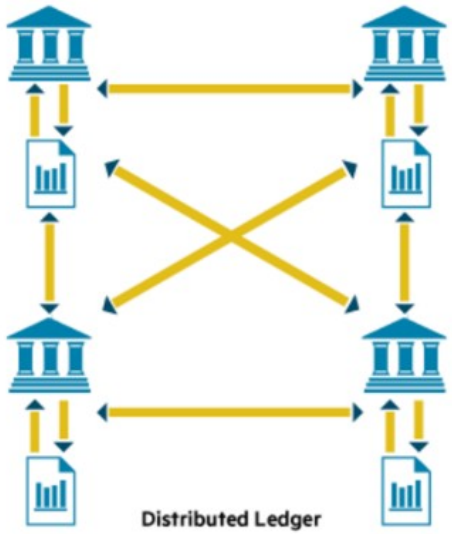
价值的两种表达形式

现金



记账

比特币：一个去中心化（分布式）的区块链账本

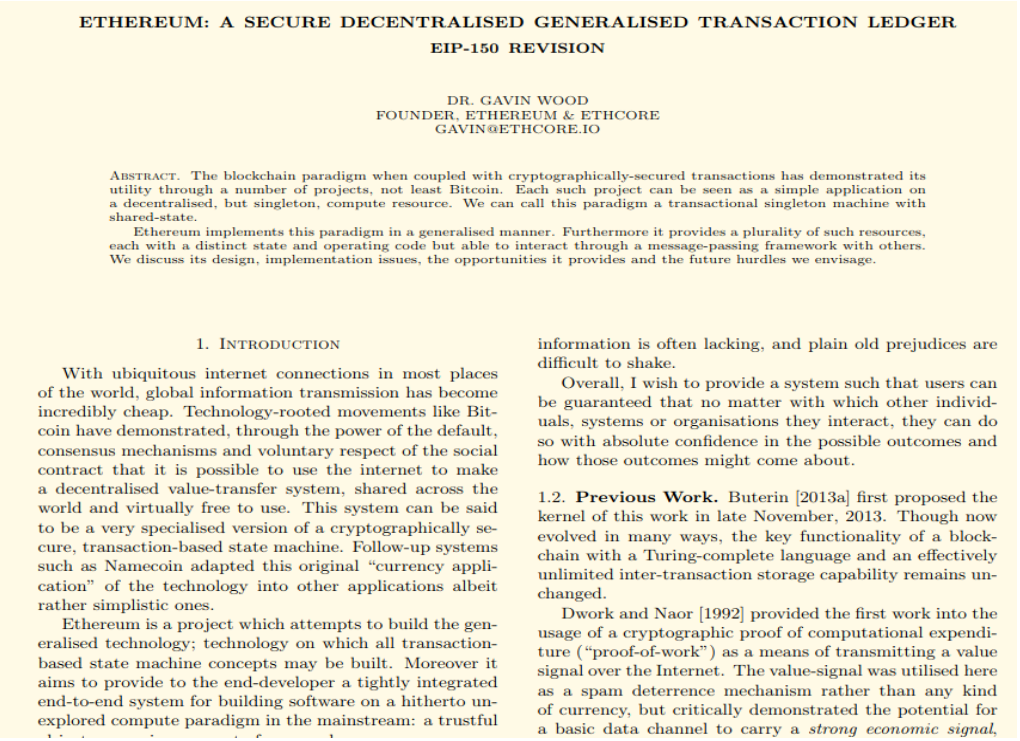


- 是账本，但是匿名、无中心、公开、 不可篡改
- 是现金，但是可追溯、不可伪造
- 电子化，可以作为“数字资产”管理的基础
- 通用，可以表达各种价值和凭证

2.5 以太坊

以太坊为去中心应用（DApp）而生

ETH：可用于支付，或将其作为价值存储或抵押品。



ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER
EIP-150 REVISION

DR. GAVIN WOOD
FOUNDER, ETHEREUM & ETHCORE
GAVIN@ETHCORE.IO

Abstract. The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, not least Bitcoin. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state.

Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

1. Introduction

With ubiquitous internet connections in most places of the world, global information transmission has become incredibly cheap. Technology-rooted movements like Bitcoin have demonstrated, through the power of the default, consensus mechanisms and voluntary respect of the social contract that it is possible to use the internet to make a decentralised value-transfer system, shared across the world and virtually free to use. This system can be said to be a very specialised version of a cryptographically secure, transaction-based state machine. Follow-up systems such as Namecoin adapted this original "currency application" of the technology into other applications albeit rather simplistic ones.

Ethereum is a project which attempts to build the generalised technology; technology on which all transaction-based state machine concepts may be built. Moreover it aims to provide to the end-developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful

information is often lacking, and plain old prejudices are difficult to shake.

Overall, I wish to provide a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.

1.2. **Previous Work.** Buterin [2013a] first proposed the kernel of this work in late November, 2013. Though now evolved in many ways, the key functionality of a blockchain with a Turing-complete language and an effectively unlimited inter-transaction storage capability remains unchanged.

Dwork and Naor [1992] provided the first work into the usage of a cryptographic proof of computational expenditure ("proof-of-work") as a means of transmitting a value signal over the Internet. The value-signal was utilised here as a spam deterrence mechanism rather than any kind of currency, but critically demonstrated the potential for a basic data channel to carry a *strong economic signal*,

智能合约和传统合约

比较维度	智能合约	传统合约
自动化维度	自动判断触发条件	人工判断触发条件
主客观维度	适合客观性的请求	适合主观性的请求
成本维度	低成本	高成本
执行时间维度	事前预防	事后预防
违约惩罚维度	依赖于抵押资产	依赖于刑罚
适用范围维度	全球范围	受限于具体辖区

构建智慧型契约社会

- 是条款，以计算机语言，而非法律语言记录
- 是可编程货币、可编程金融的技术基础
- 自动化，从传统契约社会过渡到智慧型自动社会
- 文明进化，从“身份社会”进化到“契约社会”

3

区块链应用及解决方案

- 区块链行业
- 区块链领域应用
- 区块链解决方案

3.1 区块链行业

区块链与实体产业的融合

1. 金融领域（加密数字货币、跨境支付、票据管理、供应链金融）
2. 专项试点（农业、能源、物流、制造等领域以产品溯源、确权认证、供应链管理）
3. 民生服务、社会治理领域开展区域性示范工程，培育社会服务和管理的新模式、新手段
4. 面向数据开放与交易、权利运行与监督、个人隐私与保护等场景，实施具有代表性的区块链技术应用工程
5. 行业龙头企业加强区块链技术与既有产品与服务的融合创新，构建成熟的区块链应用产品体系及行业解决方案

3.2 区块链金融领域应用

区块链金融领域应用

加密数字货币

供应链金融

跨境支付与汇款

资产管理

票据管理…

1、法定数字货币：货币是金融的基础，是所有基于价值交换的经济活动的通用介质。

2、数字身份：基于区块链的数字身份可以作为实现数字普惠金融的基础性协议。

3、更广泛的金融安全（监管）基础架构：这是一种开放式的、主动的全局强监管，

3.3 区块链解决方案

供应链金融解决方案

- 可以说，供应链管理是企业最重要的核心竞争力
- 整体架构：供应链、供应链管理、供应链金融
- 传统金融：与之相比，供应链具有的优势和特点
- 区块链：联盟链、私有链，降低成本、追溯交易、可信免信任
- 特点：
  - 真实性：不完全依靠企业基本面来判断，而是以真实贸易背景出发。
  - 自偿性：金融机构将借款企业销售收入作为还款来源，自动归还借款。
  - 闭环性：注入资金使用限制在可控范围之内，按照合同预定模式流转。
  - 灵活性：可获得流程及系统内部多个主体信息，个性化服务，优化管理。


供应链长期发展整体架构
High
Low
协同度要求逐渐提升
供应链金融
应收账款融资
库存融资
预付账款融资
信用融资
.....
供应链管理
客户关系管理
制造流程管理
信息技术管理
需求管理
库存管理
物流管理
采购管理
供应商管理
回收管理
供应链
供应商
核心企业
承销商
最终客户
SALE
商流 + 信息流 + 物流 + 资金流

传统金融与供应链金融对比

	传统金融	供应链金融
授信主体	大型企业、核心企业等	核心企业及其上下游中小企业
授信条件	担保、动产及不动产抵押	货权、应收账款、未来的存货等
融资渠道	银行	银行及其他非银机构
参与程度	跟踪融资企业	跟踪全周期经营流程
融资及时性	手续复杂，效率低	高效、及时
解决问题	解决核心企业的融资困境	盘活整个供应链资产
信息披露	不充分	全链条信息透明，连贯度高
还款来源	还款来源不明	还款来源明确

垂直细分市场深耕

更加细分的市场
将进行精细化运作

农业

药品

机械机电

电子元器件

服装

酒水食品

礼品

……

技术赋能

技术的创新发展持续赋能于供应链各环节

大数据
风控、征信和反欺诈等

人工智能
智能化、深度学习等

区块链
安全存储、随时追踪信息

物联网
实实追踪、分析监测和预测

供应链金融互联网化

在信用风控基础上发展互联网供应链金融

信息化 + 数字化

信用

资金端 + 资产端

供应链金融

风控

交易信息化　收入自偿化
管理垂直化　风险结构化
声誉资产化

产业生态圈闭环化

产融结合加深，打造闭合生态圈

横向并购战略

全产业链并购战略

多元化并购战略

金融控股并购战略

生态链并购战略

投资集团战略

……

	供应链金融 1.0	供应链金融 2.0	供应链金融 3.0	供应链金融 4.0
关键特征	中心化	线上化	平台化	数字化
商业模式	传统供应链金融线下模式，以核心企业信用作为支持	通过ERP对接供应链的上下游及参与各方，整体服务线上化	依托互联网技术打造立体化综合服务平台	高度深透细分行业领域各个运营环节 定制化、实时化、去中心化
参与主体	银行	银行 供应链参与者	银行 供应链参与者 平台搭建者	银行 供应链参与者 互联网金融
技术应用	不动产抵押与信用评价	互联网技术 动产质押	云技术应用 数据风控模型	物联网、云计算、区块链 数据质押
要素和信息流	强调有形要素，注重物联网中物的利用，重点关注资金运用和偿还	增加物流方面关注度，注重供应链中各关节环节的信息掌握	清晰的交易结构和关系，信息来源和展现形式呈现出高度复杂性	在明确交易结构的同时，渗透到整个管理运营环节

4

区块链常见概念和观点

- 多一点认知
- 多一些常识

区块链的一些原理和原则

去中心化原则	分布式系统， P2P 网络，平等协作，无单点控制。
信任原则	通过密码学建立共识系统，通过为数据加时间戳的方式来验证价值的唯一性。两个节点之间能够互相信任，可以直接进行价值交换。
劳有所得原则	激励机制使每个为网络发展付出的人都能得到价值回报。
安全性原则	非对称加密技术为数据提供了一个公匙和一个私匙，只有用户的私匙才能具有对数据的支配权。
隐私保护原则	在区块链中，没有身份认证，用户不需要提供个人信息。别人并不知道某条数据的归属人是谁。
权利保护原则	通过代码编写智能合约可以将规则或者法律数字化，代码化，用户利用自己的私匙对合约进行签署，只有满足了对应的条件才会执行合约的内容。
包容性原则	在区块链网络中，每个节点的权利都是平等的，所有人都必须遵守同

一些观点

有关货币	要成为货币，就必须是难以生产的，否则借便宜生产手段渔利的诱惑会破坏储蓄者的财富，并破坏人们存储该货币的动力。
有关数学	数学是信任的基石，人会说谎，但数字不会骗人。
人类文明	人类文明的繁荣通常出现在健全货币被广泛接受的时代和地区，与之对应的，非健全货币通常意味着文明的消亡和崩溃。
有关共识	没有一种共识机制是完美的。
代码币值	代码即法律，币值即权力，法律的本质是“合约”。
互联网和区块链	互联网是在混乱中产生秩序，而区块链是在秩序中连接混乱。互联网的用户越多越不安全，而区块链的节点越多则越稳定。
区块链	促进了社会价值的创造与交易，使互联网从信息互联网向价值互联网转变。
Token	区块链技术的进步，让每一个自然人都可以发行基于自我信用背书的 Token 。

一些技术名词和概念

共识机制	PoW （工作量证明）、 PoS （权益证明）、 DPoS （ 股份授权证明）
一些名词	挖矿、分叉、时间戳、 UTXO 、哈希函数 (SHA256) 、 P2P 网络、加密算法（ ECC/Secp256K1 ）、 DAO 、 DApp 、 DeFi 、金本位、币本位、拜占庭 ...
数字签名	验证信息是否被篡改，保证信息是真实的，真实二字在当前很贵。
智能合约	确保合同契约按照程序自动执行，杜绝老赖。
治理	链上治理依靠共识机制来运转，而链下治理一般由基金会运作。
节点和选举	这点和公民选举也很类似，节点都是平等的，都可参与网络选举。
Token 代币通证	Token 可以代表任何权益和价值， Token 三要素：信用、价值、流通。
石墨烯技术	它是 BTS 、 Steem 、 EOS 背后的技术，采用 DPoS 共识机制，使得区块链应用有更高的交易吞吐量和并发能力。

CBS
创意区块学院

Thank You!

龙辉

四川 成都

扫一扫上面的二维码图案，加我微信