Bitcoin SV 开发技术与工具概览 2.0

Gu Lu, 2021.04

Bitcoin SV 1st Bootcamp

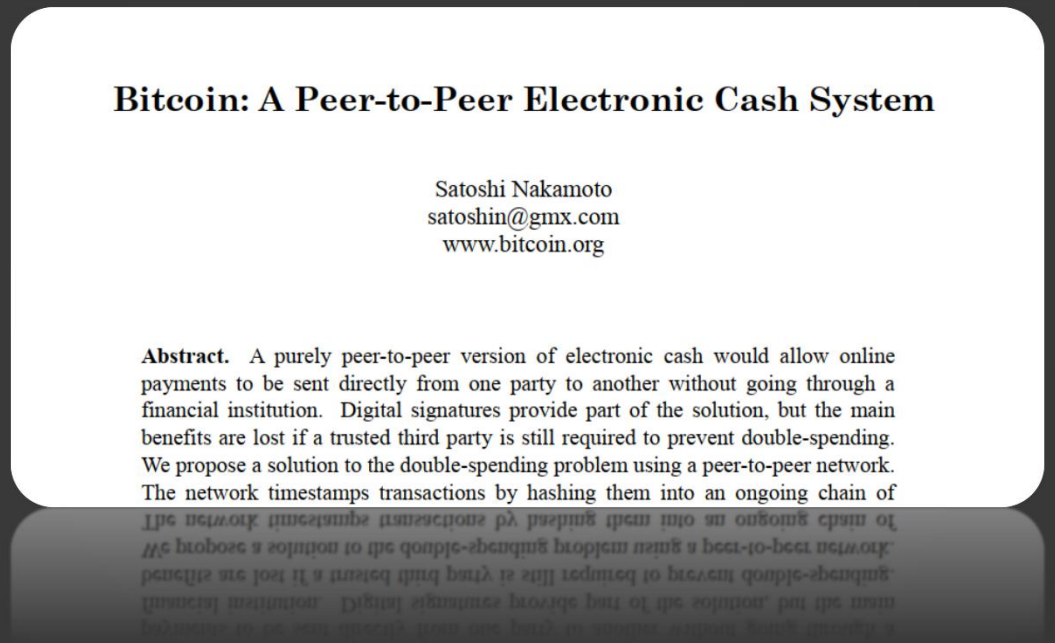
Overview

- 协议 Protocols
- 工具 Libs & Tools
- 服务 Services
- 框架 Frameworks
- 理论 Theory

- **nChain** Tech
- **Xoken** Tech
- **Sensible** Tech

协议 Protocols

the bitcoin whitepaper



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

交易

交易，是比特币的核心目的。链状的签名只是一种实践。

第一性原理：打破知识的藩篱，回归到事物本源去思考基础性的问题，在不参照经验或其它已有系统的情况下，从物质/世界的最本源出发思考事物/系统。

时间

时间的不可逆特性，被固化为“区块”，由 POW 保证。

这种不可逆，既体现为链状数据结构，也体现在区块内交易按照时间的自然排序。

P2P 节点网络

激励 & 诚实

效率 & 优化

尺寸优化，SPV，良好的 UTXO 集管理

隐私 & 信任

“去掉 trusted third party”所带来的实际效用

用户体验：“隐私友好”&“信任无关”

	理论	实践
目的	交易（第一性原理）	链状签名
方式	时间（不可逆性）	链状区块 & POW
增长	P2P 节点网络	激励 & 诚实
效率	极大规模下的可持续性	紧凑化、SPV & UTXO 管理
体验	保护隐私，降低信任成本	去除第三方、公私钥管理

Bitcoin: A Peer-to-Peer Electronic Cash System

协议 Protocols

应用层协议 (B/C/D/BCAT)	数据的存储和索引
metanet	数据的结构化组织

库

- bitsv (Python)
- bsv (JavaScript)

工具

sCrypt

服务

- MetaSV
- whatsonchain
- Sensible API

框架

- runonbitcoin
- MetaID
- Sensible Contract

理论

- craigwright.net
- Theory of bitcoin (on Youtube)

协议 Protocols

工具和库 Libs & Tools

服务 Services

框架 Frameworks

理论 Theory

- **nChain** Tech
- **Xoken** Tech
- **Sensible** Tech

SATOPLAY
SATOPLAY.COM

Sensible SV

nChain Tech

mAPI	fee discovery; tx submission
SPV	tx & utxo validation
nakasendo	threshold signature

SPV Channels（incorrect）

SPV Channels 依托于矿工网络的高效 P2P 通信

- 借助矿工网络（高效，scalable）
- 端对端加密（无许可通信）
- NAT 穿透（peer 主动发起连接）
- 消息缓存（客户端可离线）

兼具 P2P 和中心服特性

不准确的说法！

SPV Channels (revised)

SPV Channels 中心服辅助通信

- 端对端加密 (无许可通信)
- NAT 穿透 (peer 主动发起连接)
- 消息缓存 (客户端可离线)

一个典型的中心化
消息业务服

2021.04 修正

SATOPLAY
SATOPLAY.COM

Sensible SV

TouchStone

依托于矿工网络的 P2P 加密通信

协议 Protocols

工具和库 Libs & Tools

服务 Services

框架 Frameworks

理论 Theory

- **nChain** Tech
- **Xoken Tech**
- **Sensible** Tech

Infrastructure

TeraNode

Xoken

Massive Distributed

Parallel TX processing

SATOPLAY
SATOPLAY.COM

Sensible SV

Transpose Merkle Tree (TMT)

通过转置所有中间的缓存节点，使得由叶节点向根节点的遍历直接包含了所需的默克尔证明。所有的叶节点和根节点，仍保持原位置不变。

通过对默克尔树一次预处理并存到 Graph DB 里，极大地降低了处理T级区块的内存占用，这样（即使树莓派这样的）运算单位也能处理 T 级区块了

Xoken – NEXA

- 高性能处理 T 级区块的 SPV
- Neo4j (Graph DB) 对 TMT 友好
- TMT 实现针对 T 级默克尔树计算的极低资源开销
- Haskell 惰性求值实现 tx 流式处理

Xoken – VEGA

分布式，并行，长 tx 链友好，重组友好，TMT，bitcoin sharding

- Fully distributed transaction processing cluster, scale-out by adding more nodes.
- Massively parallel transaction processing – Parallel Fork/ Block/ Transaction processing
- Virtually instantaneous chain-reorgs, no additional processing required to accommodate the chain re-organizations.
- Sharding done right: ensures low cross-shard communication (storage and compute nodes), and is thus a "true scale-out" solution, i.e. provides linear or near-linear increase in performance
- Potentially Unlimited chained transactions – can validate tx-chain in logarithmic time

Xoken

Massive Distributed Parallel TX processing

交易，是比特币的核心目的。

物理存储，拓扑结构，代码实现在这一层不重要。（第一性原理）

Token Solutions

Tokenized	Centralized	Regulation friendly
Fabriik SFP	Centralized	UTXO + OP_RETURN
Badge	Open-source Processor	UTXO + OP_RETURN
CUP	3rd Party Authentication	Lightweight Contract
BTP	UTXO-Set in Oracle	Full-featured Contract Payload

SATOPLAY SATOPLAY.COM

Sensible SV

协议 Protocols

工具和库 Libs & Tools

服务 Services

框架 Frameworks

理论 Theory

- **nChain** Tech
- **Xoken** Tech
- **Sensible** Tech

Sensible Tech

1. full-featured contract logic

   no stateful oracle — no 3rd-party authentication

2. full-featured contract data payload

   verifiable critical fields — no op-return for this

3. fully decentralized

   miner validation — no need for authenticator / validator

4. " bitcoinic "

   suite well with metanet — support SPV exactly as same as bitcoin

SATOPLAY SATOPLAY.COM

Sensible SV

Sensible Tech (comes at a price)

1. full–featured contract logic
2. full–featured contract data payload
3. fully decentralized
4. “bitcoinic”

comes at a price:

1. a minimal signature service (external)
2. heavy–weighted scripting (bigger size)

SATOPLAY SATOPLAY.COM

Sensible SV

BCPs

BCP 01

NFT

BCP 02

Token (FT)

BCP 03

Unique Contract

BCP 0x ...

(to be revealed)

"automation of agreements with easily definable transaction steps"

– the "official narratives" about contract

SATOPLAY SATOPLAY.COM

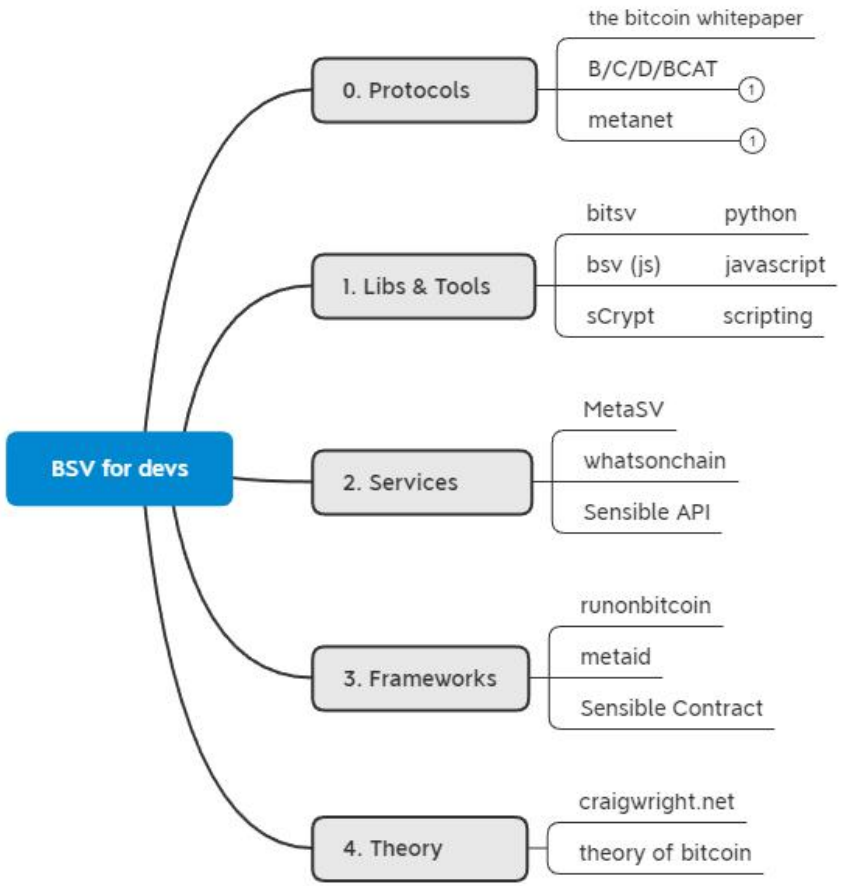
Sensible SV

Review

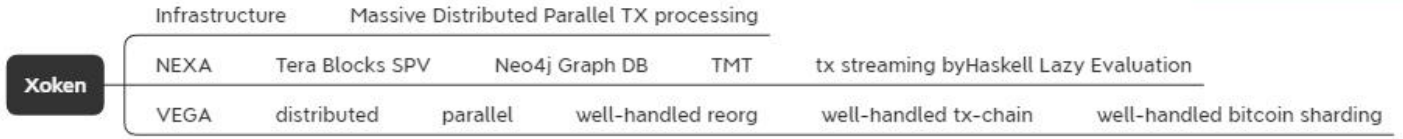
- 协议 Protocols
- 工具和库 Libs & Tools
- 服务 Services
- 框架 Frameworks
- 理论 Theory

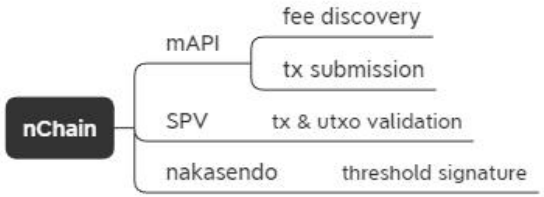
- **nChain** Tech
- **Xoken** Tech
- **Sensible** Tech

Take–away



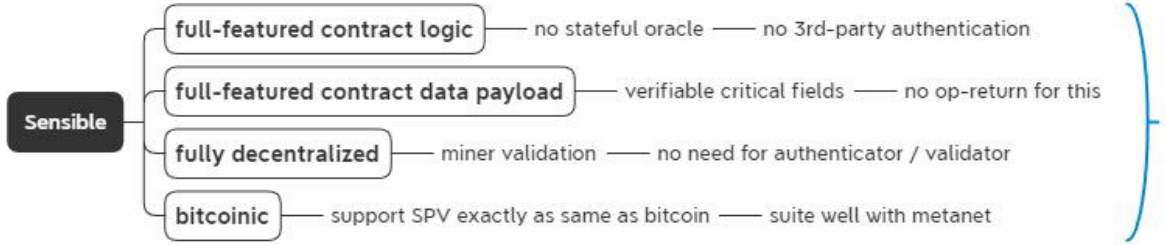
Bitcoin SV 开发技术概览 (v0.2)
2021.04.08
Gu Lu





"automation of agreements with easily definable transaction steps"

- the "official narratives" about contract



comes at a price:

1. a minimal signature service (external)

2. heavy-weighted scripting (bigger size)

SATOPLAY
SATOPLAY.COM

SensibleSV

Thank you

Gu Lu