网录科技
Wanglu Tech

区块链存证

信任润滑经济，技术驱动变革

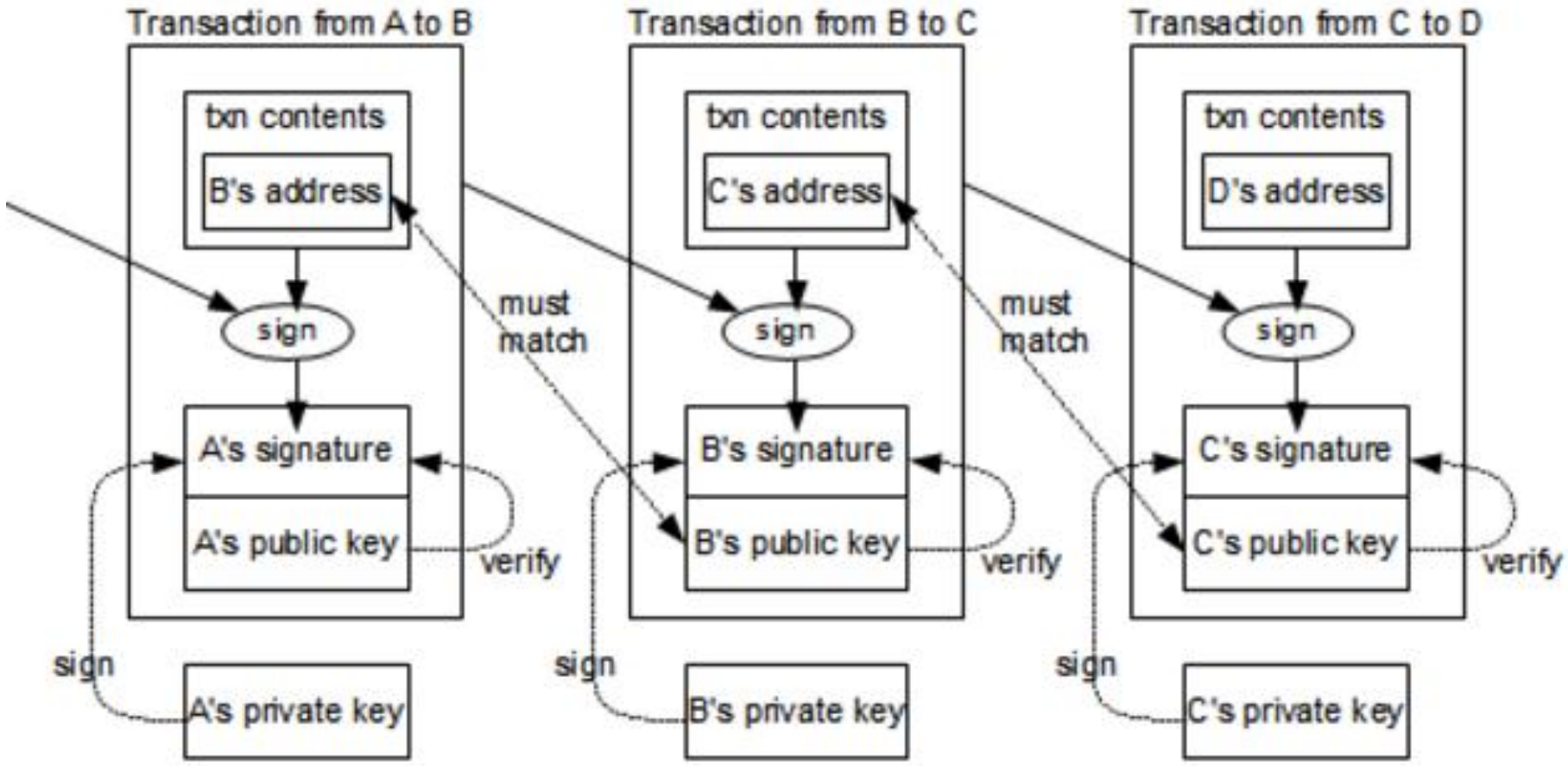
BLOCKCHAIN

汪 波

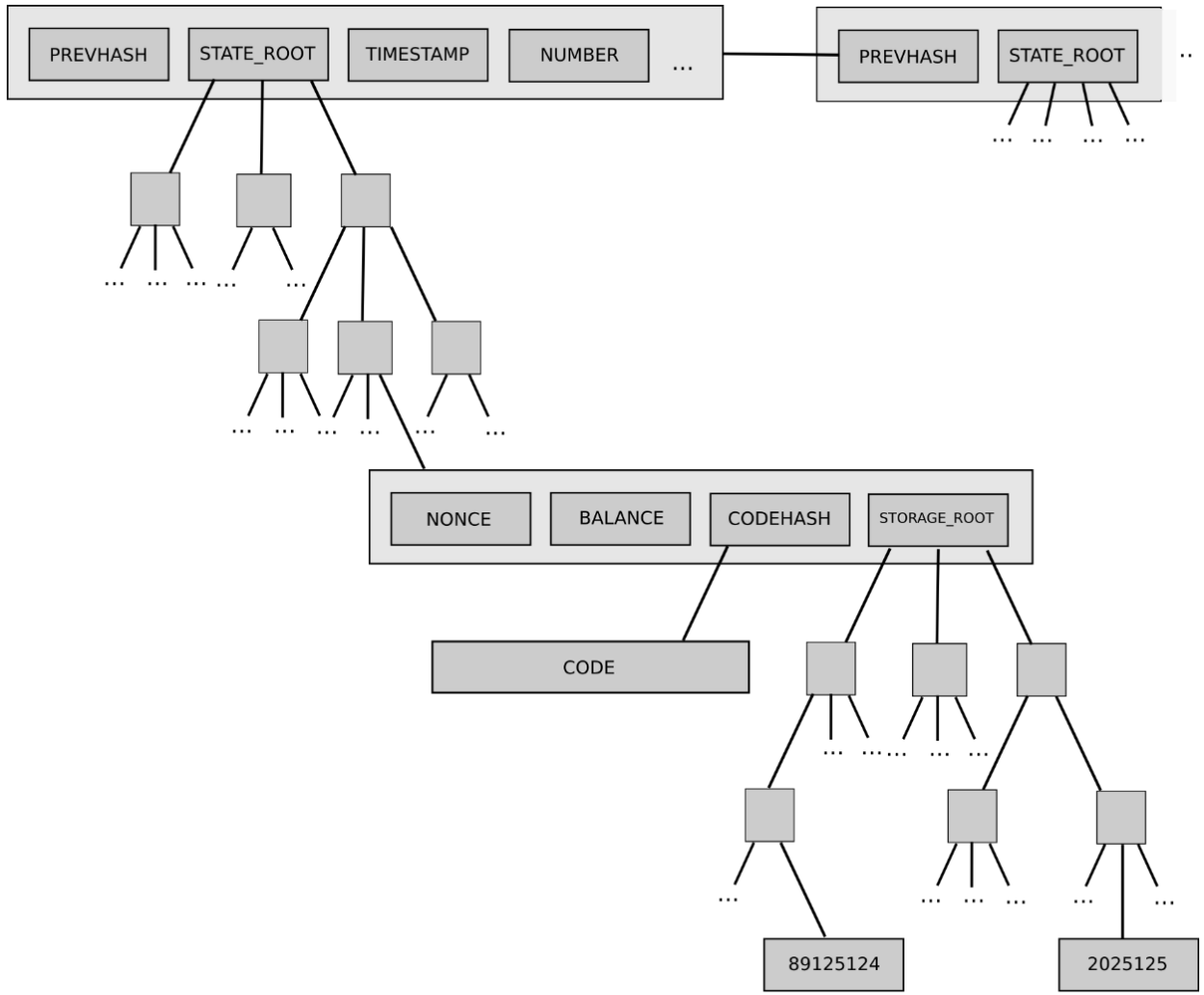
Agenda

- 为什么区块链是一个好的存证工具
- 怎么做存证
- 存证的现状
- 企业级的存证解决方案
- Q & A

区块链作为存证工具：交易结构



存证工具：区块链

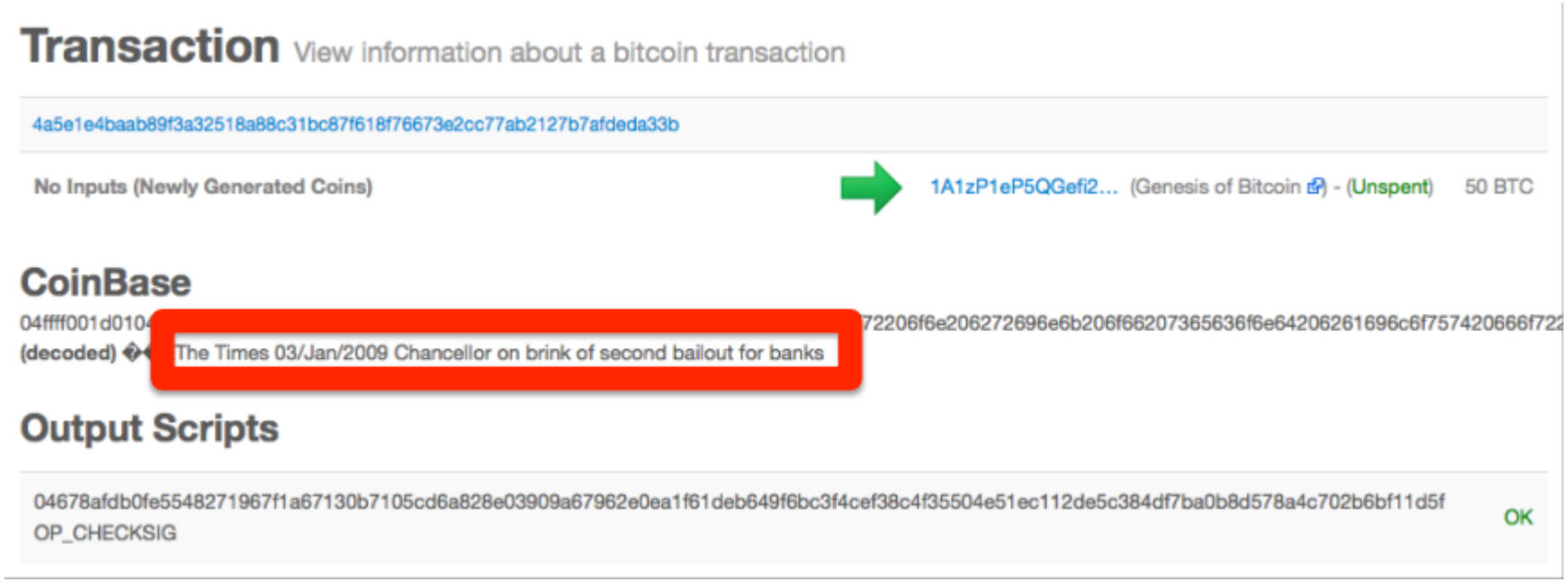

PREVHASH
STATE_ROOT
TIMESTAMP
NUMBER
PREVHASH
STATE_ROOT
NONCE
BALANCE
CODEHASH
STORAGE_ROOT
CODE
89125124
2025125

存证工具：共识机制

- 共识算法 （+ 挖矿）
  - PoW: Proof of Work
  - PoS / DPOS: Proof of Stake
  - PBFT: Practical Byzantine Fault Tolerance
  - Raft
  - Paxos

- 保证了整个区块链不可完全被重写

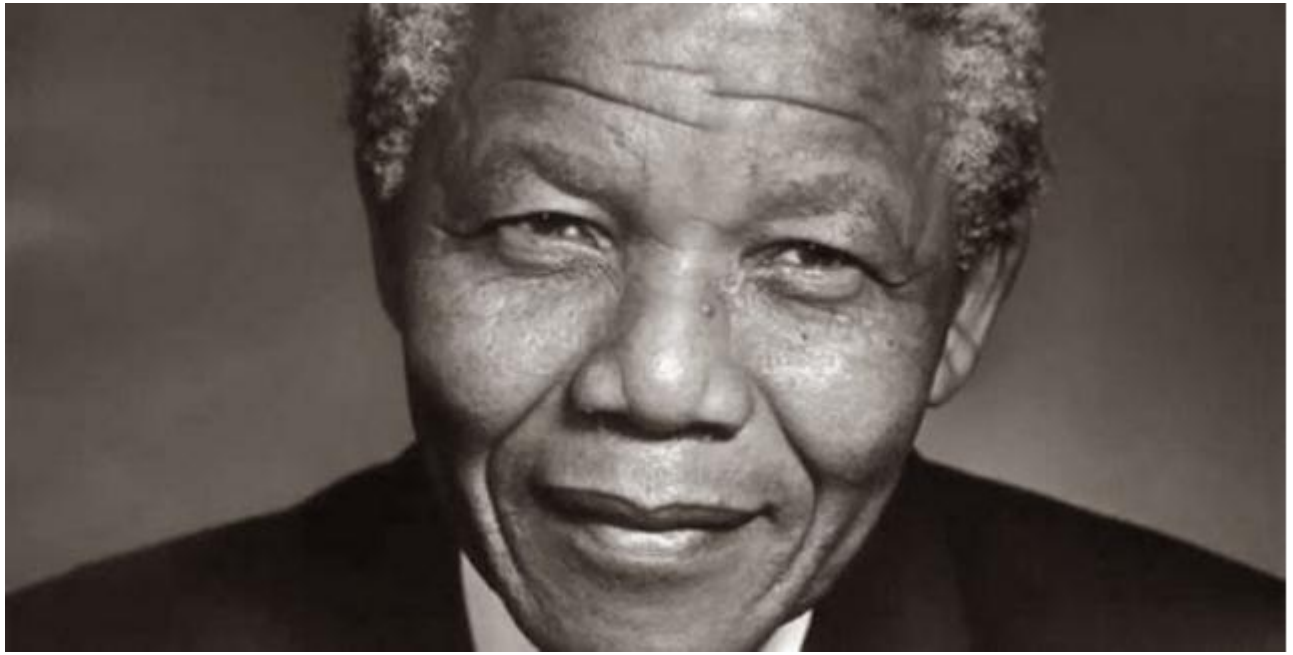
如何做存证(Bitcoin)：coinbase



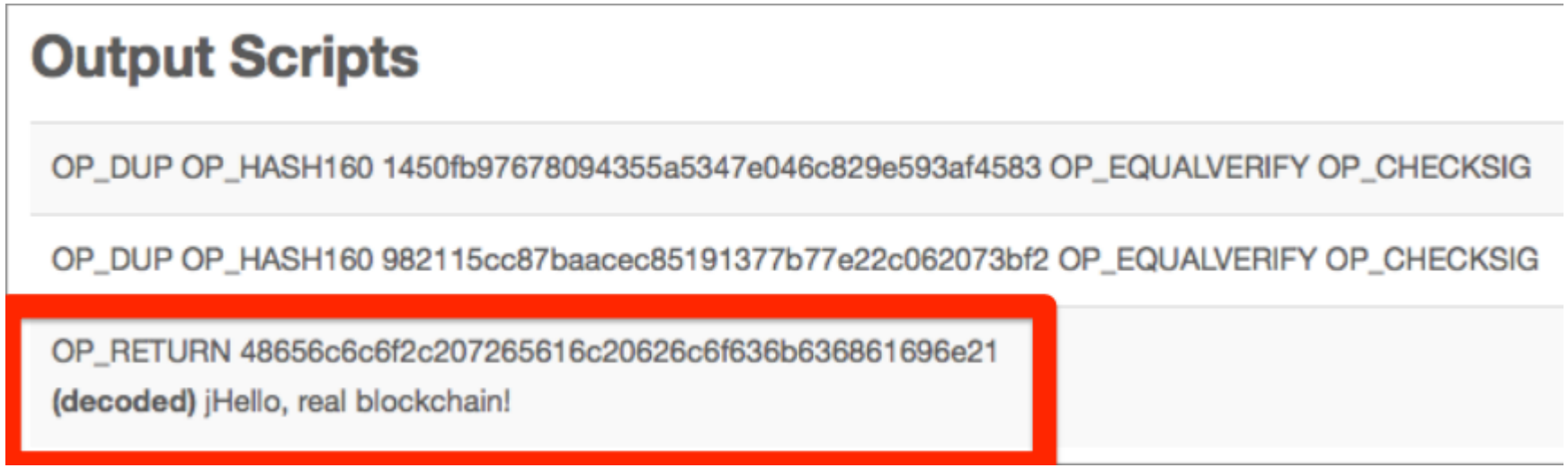
如何做存证：btc address

16LseQUKmhA1XUq39QmxNg9c1bPQq6Jxvh (0.157245 BTC - Output)

1AFZvFuA5Pv3RTw679GfVYbAzykZqm3Ys2 - (Unspent)	0.000055 BTC
1AcHQwytpRKkX71DQasUk5TMw6qNED2Yqw - (Unspent)	0.000055 BTC
15gHNr4TCKmhHDEG31L2XFNvpnEcnPSQvd - (Unspent)	0.000055 BTC
15VAeb5KsRqbyNWWp7WHSACuVQahe5ngS7 - (Unspent)	0.000055 BTC
112CUyPHVEi3zyHViBzP3poagnvyUomYZ - (Unspent)	0.000055 BTC
1A8gyj9ETeGkS1hea2crNp1oJ7HfcRMuK8 - (Unspent)	0.000055 BTC
17mkD8JSfeVDx11ZumnEuKo6wVNw9mhipU - (Unspent)	0.000055 BTC



如何做存证：OP_RETURN



Provably prunable, no unspent output

OP_RETURN (0x6a) + 80 bytes

网录锚定(Anchor)

Output Scripts

OP_RETURN 466100000000fd3dad0571dad4b3371adad1a2f6dcc20092e89c43e90ad0020b7400dea170680d5d
(decoded) j(Fa[illegible]=[illegible]q[illegible]Q7[illegible]ъ[illegible]C[illegible] [illegible]tsph]

OP_DUP OP_HASH160 c5b7fd920dce5f61934e792c7e6fcc829aff533d OP_EQUALVERIFY OP_CHECKSIG

- Encoding: ‘Wa’ (2 bytes) + block_height (6 bytes) + block_hash(32 bytes)

```
anchorHash = append([]byte{'W', 'a'}, blockHeight, hash...)

builder := txscript.NewScriptBuilder()
builder.AddOp(txscript.OP_RETURN)
builder.AddData(anchorHash)

opReturn, err := builder.Script()
msgtx.AddTxOut(wire.NewTxOut(0, opReturn))
```

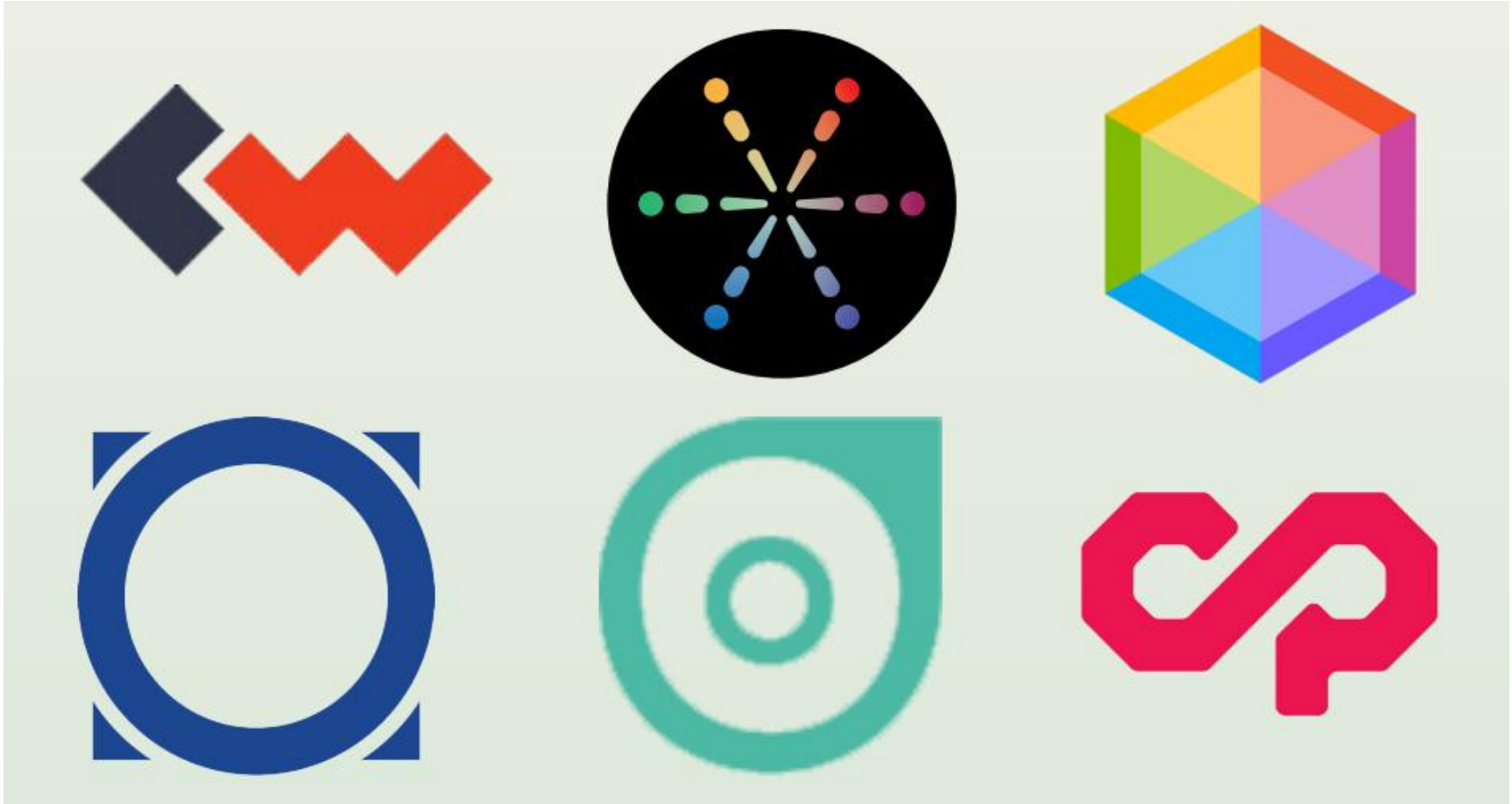
锚定算法

- Update UTXOs
- Create New Tx
- UTXO -> TXIn
- Create TxOut, including OP_RETURN
- Validate TX
- Send Tx to network

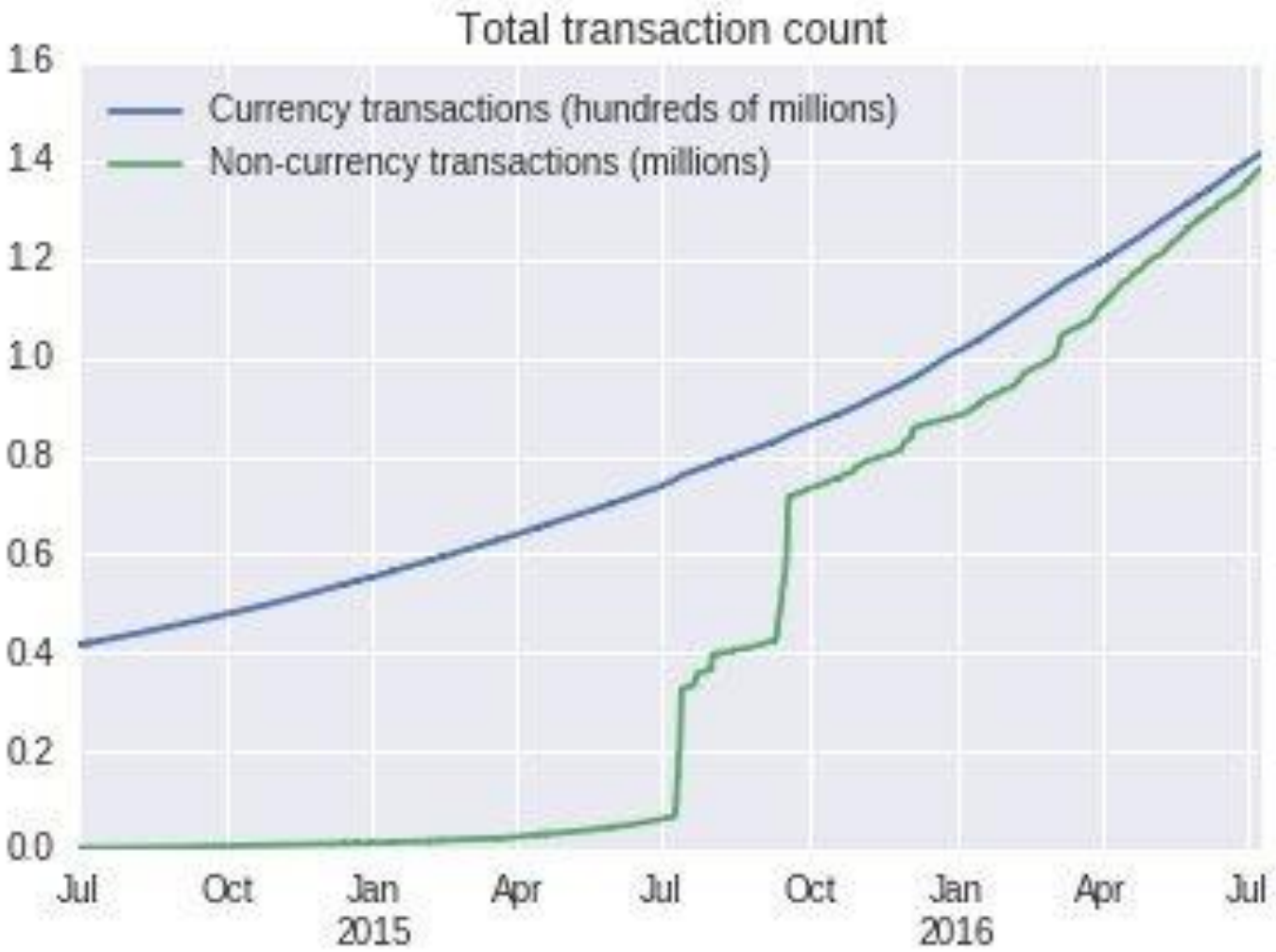
- Wait for callback notification
- Tx Confirmed (6 times, 20 times, etc)

OP_RETURN: Color Coins

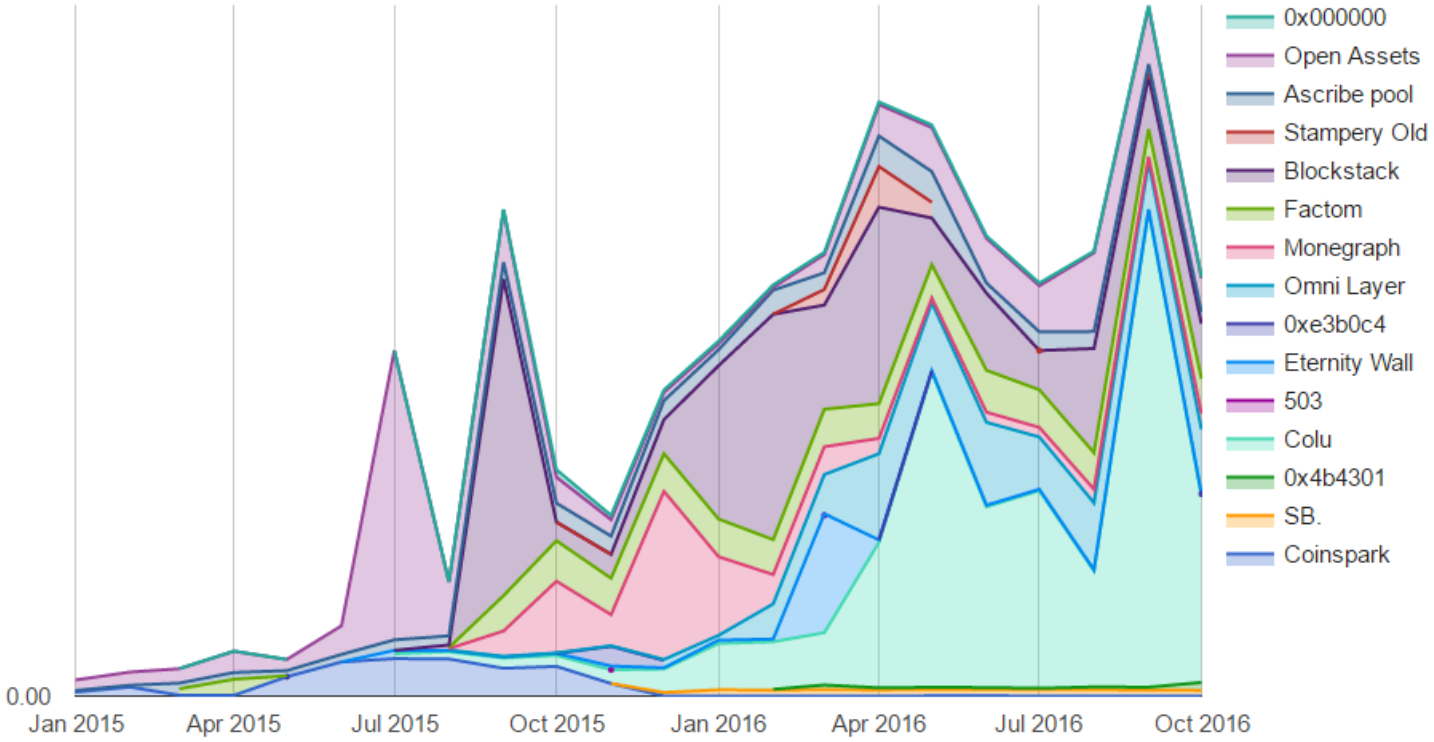
- 利用Op_return来发布数字资产

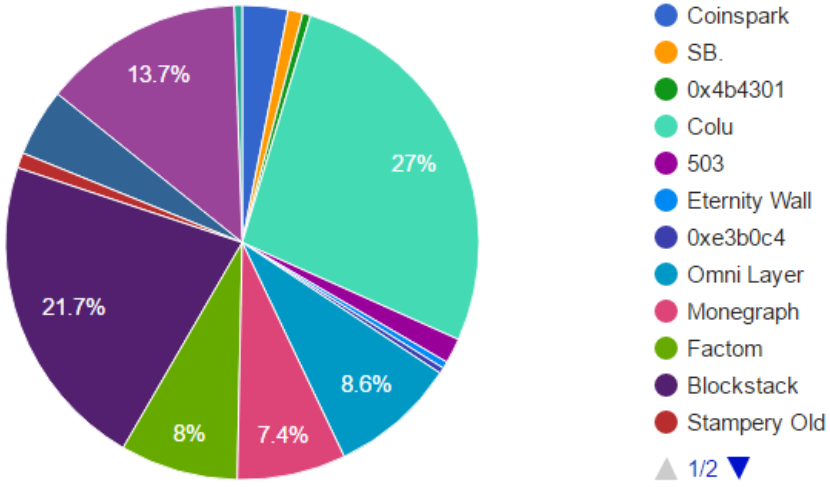


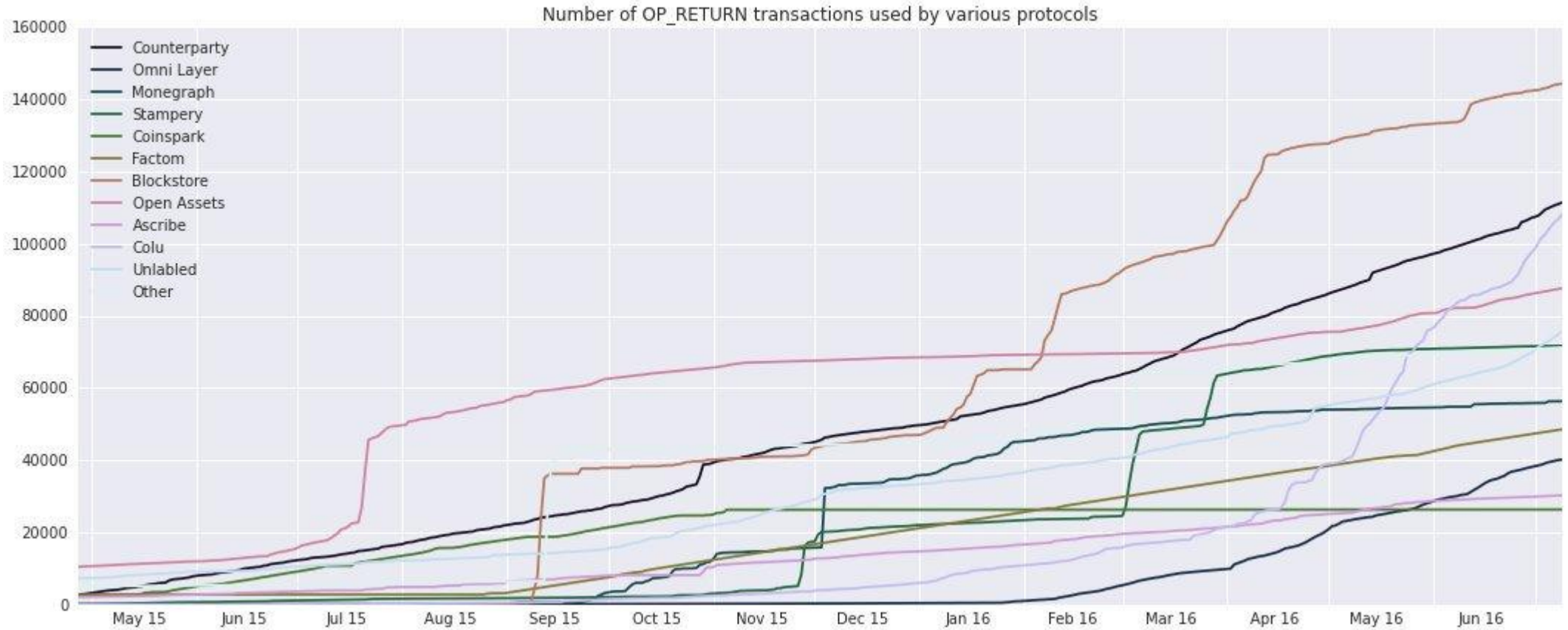
OP_RETURN 交易现状



OP_RETURN 交易（协议）



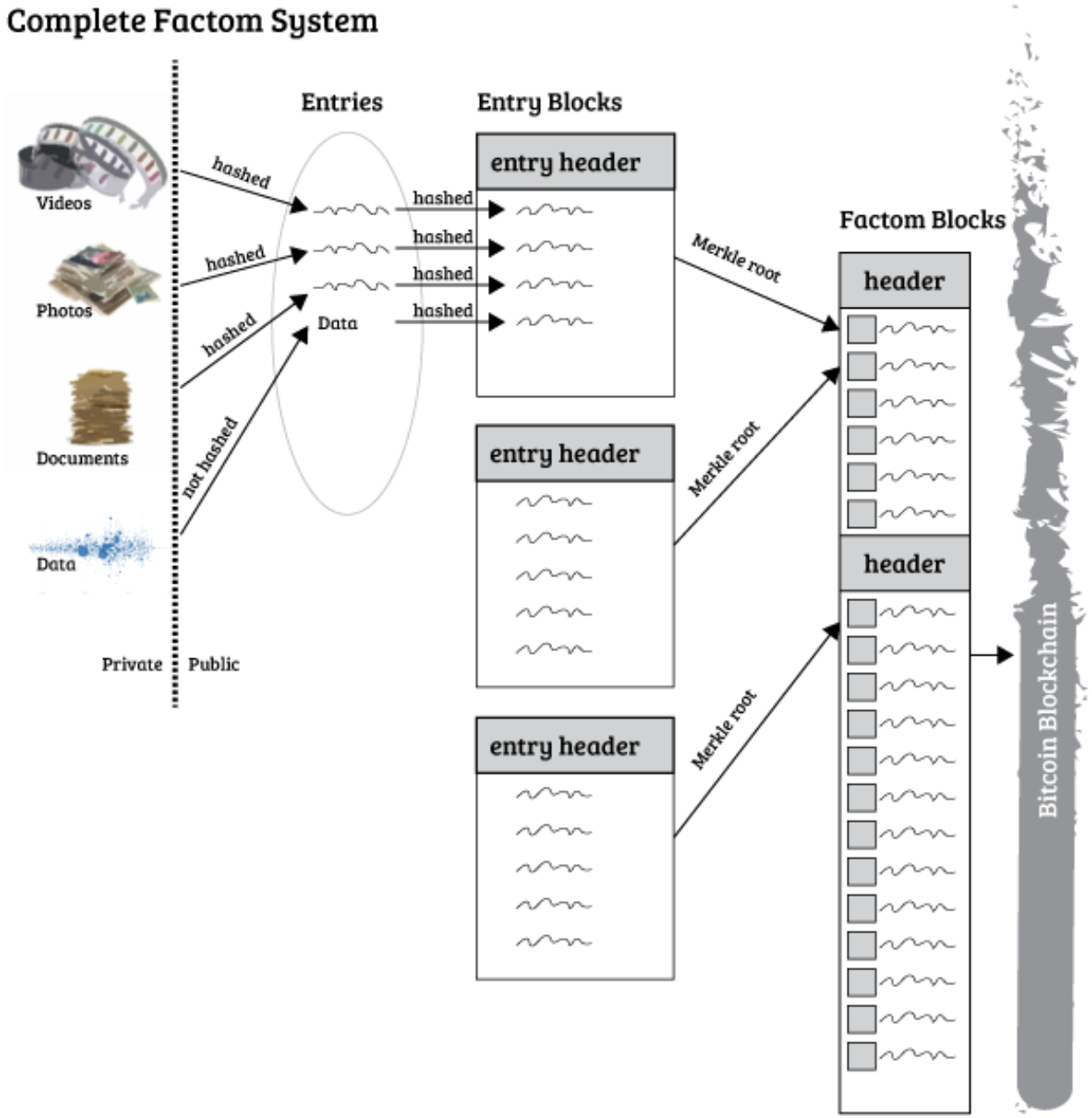



Number of OP_RETURN transactions used by various protocols
160000
140000
120000
100000
80000
60000
40000
20000
0
Counterparty
Omni Layer
Monegraph
Stampery
Coinspark
Factom
Blockstore
Open Assets
Ascribe
Colu
Unlabled
Other
May 15
Jun 15
Jul 15
Aug 15
Sep 15
Oct 15
Nov 15
Dec 15
Jan 16
Feb 16
Mar 16
Apr 16
May 16
Jun 16

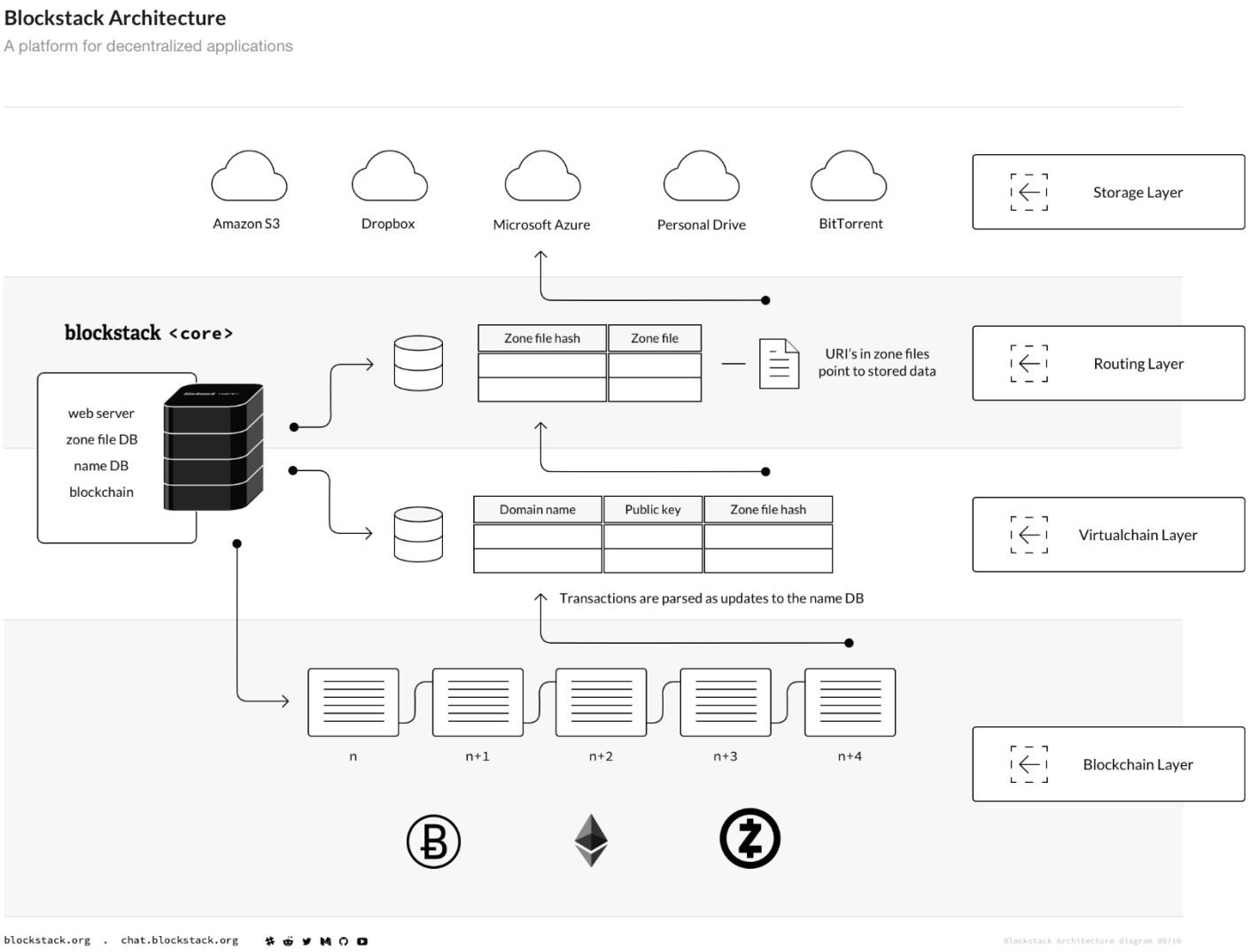
企业级的存证解决方案

- 成功的锚定
  - ✓交易不被收录、区块链的重组
- 锚定数据的语义和关联
  - ✓Encoding、
  - ✓数据之间的关系（版本、M:N）
  - ✓数据检索
- 交易的吞吐量和速度
- 隐私和权限控制

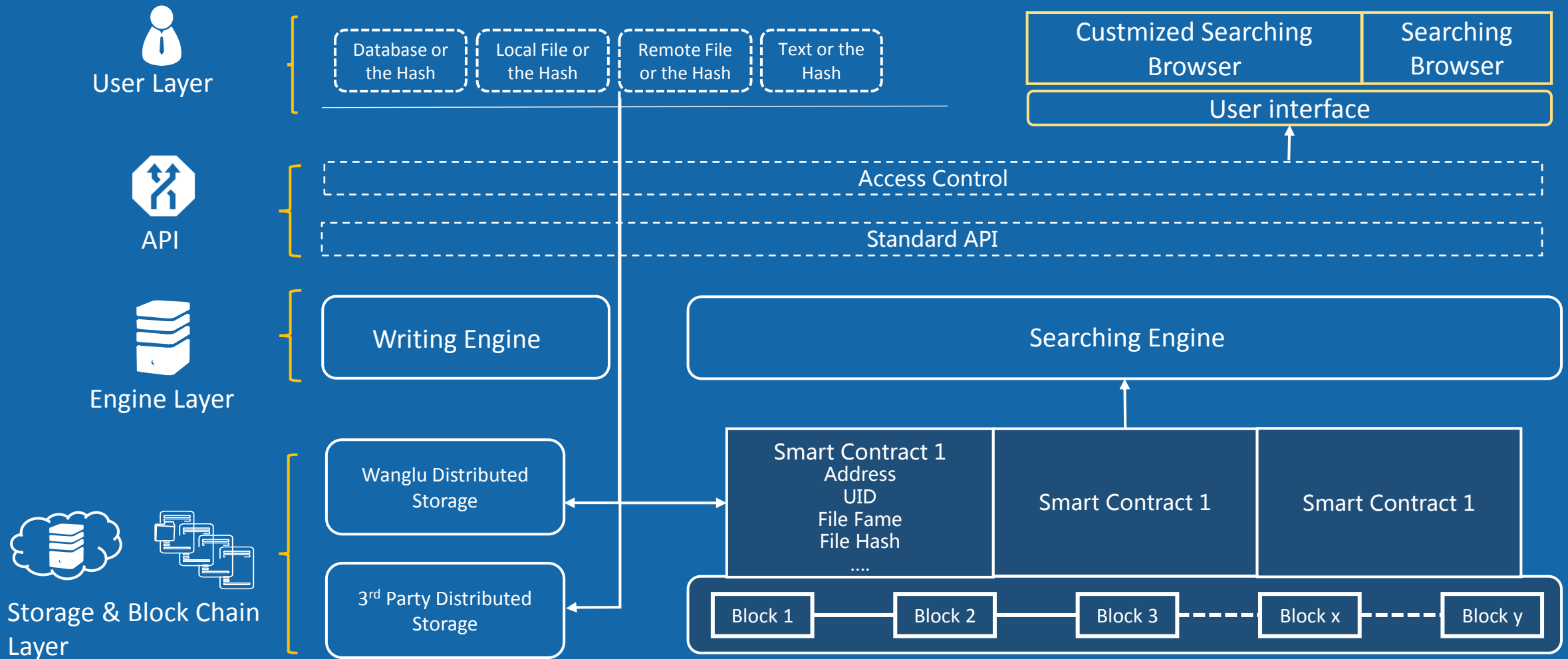
存证实例：Factom


Complete Factom System
Entries
Entry Blocks
Factom Blocks
Videos
Photos
Documents
Data
hashed
hashed
hashed
not hashed
Data
hashed
hashed
hashed
hashed
entry header
entry header
entry header
Merkle root
Merkle root
Merkle root
header
header
Bitcoin Blockchain
Private
Public

存证实例：blockstack



存证实例：网录（Walud）



谢谢！

网录科技 Wanglu Tech
010-51727302
www.wanglutech.com
北京市海淀区北三环西路48号北京科技会展中心2号楼23A