Blockchain & Distributed Internet Infrastructure

Dirk Kutscher

NEC Laboratories Europe
Purpose of this Meeting

• Discuss blockchain-based and Distributed Internet Infrastructure concepts, state of the art, new ideas
  – Useful applications beyond financial sector?
  – Relationship to other efforts (ICN?)
  – Potential next steps
Agenda

1. Overview of blockchain and related frameworks -- Dirk
2. Blockchain registries - the future of protocol operations -- Alex
3. Internet-wide Federation -- Jeffrey
4. Discussion of potential next steps
Bitcoin

- P2P payment network
- Transactions: broadcasting signed bitcoin transfer message
- Transactions are recorded in distributed and replicated public database: blockchain
- Blockchain groups transactions into blocks by timestamp
- Blockchain cryptographically protected
- Consensus algorithm based on proof-of-work
- Longest blockchain prevails
- Blockchain is distributed by P2P file transfer
Interesting Properties

• No centralized coordination, no trusted parties
• Sufficiently robust against fraud (double-spending)
• Transaction irreversibility
• Some level of pseudonymity
• Blockchain can be generalized to other distributed ledger applications
  – Bitcoin: digital currency transfers
  – Other digital artifacts would work as well (names etc.)
Blockchain Illustrated

Simplified Bitcoin Block Chain
Proof of Work

- Blockchain is collaboratively maintained by peers on the network
- Each block to provide verifiable proof of work invested in its creation (here: finding a hash with certain properties)
- Blocks referring to previous blocks (chain)
- Chaining makes it impossible to modify transactions later
Consensus Protocol

- Blockchain can be modified concurrently
- Networks converges on longest chain (following the most difficult-to-recreate chain)
- Relatively robust against attacks (51% mining power required to attack blockchain)
Transactions

• Addresses: RIPEMD-160(SHA-256(PK))
  – Value is moved between addresses using transactions

• Verification according to specified rules
Bitcoin Nodes

• Full nodes
  – Store entire blockchain (~15GB)

• Light nodes
  – Download block headers only
  – Verify proof of work on block headers
  – Download branches associated to a given transaction only
Bitcoin Merits

- **Dentralized consensus based on proof-of-work concept**
  - Implemented through blockchain
- **Applicable to other applications that can benefit from a public, distributed ledger**

- **Caveats**
  - Update & convergence times not really suitable for time-critical applications
  - Considerable cost for mining (i.e., for proof of work)
Alternative Blockchain Applications

• Namecoin
  – Decentralized name registration database
  – Map names to arbitrary identifiers (DNS names, Bitcoin IDs etc.)
  – *First-to-file paradigm* to avoid impersonation

• Other currencies
  – Colored coins (persistent attributes to Bitcoin units)
  – Metacoin (configurable state transitions)
Namecoin

- Can store data in blockchain database
- Records
  - Hierarchical names (keys)
  - Byte array values (520 max length)
- Potential applications
  - Identity systems
  - Notary systems
  - Decentralized name resolution ("censorship-free DNS")
.bit

• TLD outside DNS (independent of ICANN)
• Names resolved through Namecoin-enabled resolver (web-browser plugin or supporting DNS server)
• draft-grothoff-iesg-special-use-p2p-bit-00
• Differences to DNS
  – Domain names not delegated to an authority that can assign them – they are directly acquired by interested users
  – Namecoin blockchain is the complete domain database
  – Namecoin not limited to domain names – there are actually multiple namespaces in Namecoin
• Namecoin seems to be rarely used today
OneName

• Decentralized identity system
Generalizing State Transition / Validation
Ethereum

• Blockchain with Turing-complete programming language
• Smart contracts and decentralized applications
• Users can write arbitrary rules for ownership, transaction formats, and state transition functions
• Generalized platform for specific applications, e.g., Namecoin-like systems
Ethereum Applications

• Financial
  – Different ways of managing and entering into contracts using money
  – Sub-currencies, financial derivatives, saving wallets etc.

• Other decentralized applications
  – Online voting, decentralized governance

• Decentralized File Storage
  – Storing file blocks as encrypted bloby in Merkle tree
  – Micropayments for storage and distribution services
Blockchain in OSS/Standards

• Hyperledger Linux Foundation project
  – create an enterprise grade, open source distributed ledger framework and code base, upon which users can build and run robust, industry-specific applications, platforms and hardware systems to support business transactions
  – create an open source, technical community to benefit the ecosystem of HLP solution providers and users, focused on blockchain and shared ledger use cases that will work across a variety of industry solutions
  – promote participation of leading members of the ecosystem, including developers, service and solution providers and end users
  – host the infrastructure for HLP, establishing a neutral home for community infrastructure, meetings, events and collaborative discussions and providing structure around the business and technical governance of HLP

https://www.hyperledger.org/
Maidsafe

• P2P-like communication network based on blockchain
• Includes own Safecoin currency for incentivization (micropayments for resource usage) – built on top of bitcoin
• Network stores and replicates encrypted chunks of published data
• Chunk transport with caching support
MaidSafe Tech Stack

Third Party Broker Application

Proof of Resource

safecoin

Transaction Manager

Transaction

Transfer Mechanism

Wallet

Transaction Manager

Transaction

Transfer Mechanism

Wallet

Transaction Manager

Transaction

Transfer Mechanism

Wallet

Trusted Group

MaidSafe Network
Maidsafe Implementations

• Distributed Transaction Manager (corresponding to Bitcoin’s blockchain)
  – Stores users’ account info
  – Not in a linked chain, but by other nodes that are (P2P-address-wise) close to user

• Proof-of-Resource
  – Validates users and their value to the network
  – Storage, computation and communication resources made available to network
MaidSafe Technologies

- Kademlia DHT
- UDP-based transport protocol
MaidSafe Assessment

• Many similarities to DHT-based ICN
  – E.g., Telecom Italia’s Global Information Network (GIN)
  – Strangely, none of this seems to be considered in MaidSafe documents

• Documentation seems incomplete
  – Mostly on YouTube...
  – Some skeptical reviews on the web
  – https://letstalkbitcoin.com/the-brokenness-of-maidsafe
Interplanetary Filesystem (IPFS)

- Hypermedia distribution protocol based on P2P file system
- Addressed by content and identities
- Aims at distributed application creation

IPFS is The Permanent Web
A new peer-to-peer hypermedia protocol
IPFS: P2P distributed file system

- Seeks to connect all computing devices with the same system of files
- Analogy: a single BitTorrent swarm, exchanging objects within one Git repository
- Provides a high throughput content-addressed block storage model, with content-addressed hyperlinks
- Forms a generalized Merkle DAG, a data structure upon which one can build versioned file systems, blockchains, and even a Permanent Web
- Combines a distributed hashtable, an incentivized block exchange, and a “self-certifying namespace”
- No single point of failure, and nodes do not need to trust each other
IPFS (1)

• Identities
  – NodeIDs: public key hash
• DHT: S/Kademlia
  – Eliminates some attacks on Kademlia’s routing system (among other properties)
• Transport
  – In principle agnostic to transport, but typically used with WebRTC DataChannels or uTP
  – Can add reliability service on top of chosen underlay
  – ICE for NAT traversal
  – Optional support for integrity and authenticity
  – Does not necessarily assume IP
IPFS (2)

• Routing in DHT, based on
  – Other peers’ network addresses
  – Object names

• Block exchange
  – Like BitTorrent, but not exchange not limited to blocks in a torrent
  – Incentivizing cooperation (different strategies: tit-for-tat, currency-based etc.)
  – Per-node ledger for accounting transfers that is exchanged when nodes „connect“
IPFS (3)

- **Object Merkle DAG**
  - On top of DHT/block exchange
  - DAG links objects (based on their hash values)
  - Objects are immutable
  - Generalization of Git data structure
  - Similar to ICN manifests

- **Special namespace for mutable objects**
  - Signature verification with publisher/owner node’s public key („self-certifying names“)

- **Aliases for human-friendly names, URIs**

- **Different possible applications**
  - Document publishing, cryptocurrency blockchains etc.
IPFS Advertized Use Cases

1. As a mounted global filesystem, under /ipfs and /ipns
2. As a mounted personal sync folder that automatically versions, publishes, and backs up any writes.
3. As an encrypted file or data sharing system
4. As a versioned package manager for all software
5. As the root filesystem of a Virtual Machine
6. As the boot filesystem of a VM (under a hypervisor)
7. As a database: applications can write directly to the Merkle DAG data model and get all the versioning, caching, and distribution IPFS provides
8. As a linked (and encrypted) communications platform
9. As an integrity checked CDN for large files (without SSL)
10. As an encrypted CDN
11. On webpages, as a web CDN
12. As a new Permanent Web where links do not die
IPFS Assessment

• „Marrying P2P and Github“
• Not directly an application of blockchain
• Seems to ignore existing work in ICN and P2P
Summary

• Blockchain: useful for decentralized recording of transactions – not only for crypto currency
• Consensus protocol does not lend itself to real-time applications
  – Takes some time until transaction can be considered accepted
• Hence: decentralized ledger
  – Registries, namespace management
  – Ethereum: generalized, programmable blockchain
  – Caveat: proof of work requires real work – cf. ressource consumption for bitcoin mining
• Related communication frameworks
  – Decentralized, censorship-free communication with crypto currency seem to be main drivers
  – Understanding merits and detailed security properties needs deeper analysis

http://dirk-kutscher.info/misc/blockchain-resources/
Next

• Blockchain registries - the future of protocol operations -- Alex

• Internet-wide Federation -- Jeffrey
BACKUP
Transactions in a Block
Bitcoin Transfer

Transaction

Owner 1's Public key

Hash

Owner 0's Signature

Transaction

Owner 2's Public key

Hash

Owner 1's Signature

Transaction

Owner 3's Public key

Hash

Owner 2's Signature

Owner 1's Private Key

Owner 2's Private Key

Owner 3's Private Key