An Architecture for Blockchain

Bimal Kumar Roy

Hash Functions and SHA-3

Hash Function

- Mapping of arbitrary length message to a fix length bit string called **digest**.
- $h : \{0, 1\}^* \rightarrow \{0, 1\}^d$ (d is digest length).
- Digest hides possible structure in message.

Desirable Properties

- Deterministic and fast.
- Infeasible to generate a message from digest (preimage)
- Small change in the message produce an uncorrelated digest (second preimage)
- Infeasible to find two different messages with the same digest (collision).

Hash Function

Collision Resistance

- Hard to find $m, m' \in \{0, 1\}^*$ for which $h(m)=h(m')$.
- Usage : Commitment, Signature.

Preimage Resistance

- Given $D \in \{0, 1\}^d$, hard to find m such that $h(m) = D$.
- Usage : Commitment.

Second Preimage Resistance

- Given $m \in \{0, 1\}^*$, hard to find $m' \neq m$ such that $h(m') = h(m)$.
- Usage : Commitment.

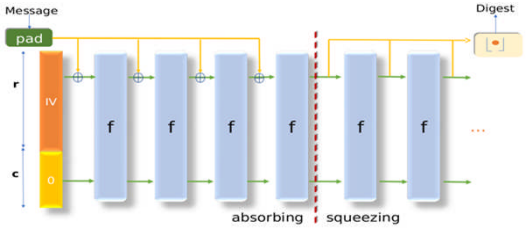
Before SHA-3

- MD4 was to be broken by Dobbertin, but still used occasionally.
- MD5 have theoretical weaknesses but still widely used.
- SHA-1 was thought to be very strong.
- SHA-2 looked like the future, with security up to 256 bits.
- MD was normal way to build hashes.

SHA-3

- 02/11/2007: Call for Proposals.
- 31/10/2008: Submission deadline.
- 10/12/2008: First-round candidates announced.
- 24/07/2009: Second-round candidates announced.
- 09/12/2010: SHA-3 finalists announced.
- 02/10/2012: Keccak announced as the SHA3 winner.

Sponge

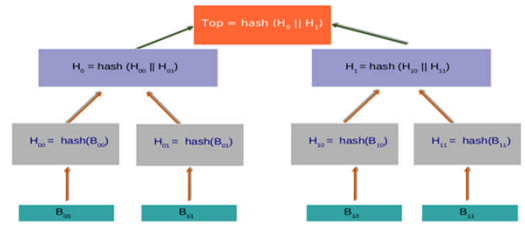


Sponge

- Introduced in SHA-3 winner Keccak Specification.
- Calls a b-bit permutation f .
- **Memory friendly** mode: Implementation stores only the b-bit state.
- r is called **rate** and $c = b - r$ is called **capacity**
- Efficiency depends on r. Security depends on c.

Merkle Tree

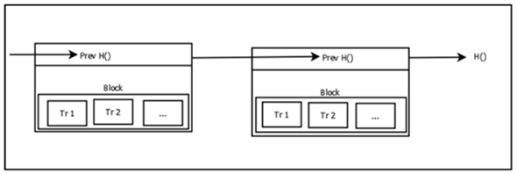
Merkle Tree



Merkle Tree

- Leaf nodes are labelled with hash of a data block $H_{ij} = h(B_{ij})$.
- Non leaf nodes are labelled with cryptographic hash of labels of its child nodes.
- Used in
  - Used for set-membership proof at **log** time.
  - Hash-based signatures.
  - Blockchain Protocol.
  - Distributed hash table.
  - ZCASH - cryptocurrency protocol with anonymous payments..

Merkle Tree in Blockchain

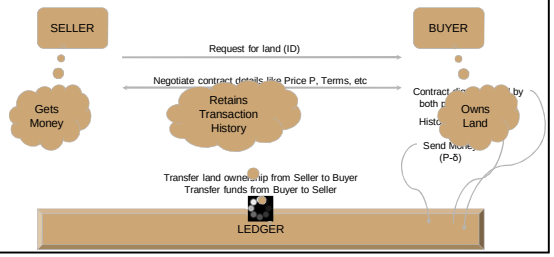


Maintaining Land Records using Blockchain

Participants and Roles

- Buyer: Interested in
  - Historical records of a particular land
  - Paying for transfer of ownership
  - Buying from authentic owner
  - Avoiding disputed lands
- Seller: Wants to
  - Transfer land ownership in lieu of money
  - Not reveal land history without money payment
  - Not violate legislation and norms
- Blockchain
  - Ensures fairness in transactions
  - Guaranteed adherence to legal norms
  - Acts as attestor to mediate and finalize land transfer
  - Delivers transparency
  - Ownership transfer process expedited

Sample Protocol Outline



Design Choices

- Government agencies can host the blockchain and act as attestor.
- May use private blockchains to achieve transactional privacy using certificate authority and ephemeral keys. Government can use data for individual asset computation.
- An optional storage component can be introduced to save contract details and other history. This data can be used to enforce norms like non-transfer of assets.
- Arbitrary logic can be enforced by smart contract hosted on blockchain like commission for attestor, enforcing land not part of bank guarantees, handling cases with middlemen facilitating trade, etc.

Problems

Historical Data

- Need to scan entire blockchain from latest block to genesis to create a transaction graph.
- To prove that a particular transaction was part of a block, we show the Merkle path from the transaction to the root of the Merkle tree, which is included in the block header.

Inheritance, Mortgage and other legal issues

- To enforce inheritance laws and fair land division among heirs is a difficult problem.
- Liens in case of partial failure in repayment is hard to settle without arbitrators.

THANK YOU