Tangler: A Censorship-Resistant Publishing System Based on Document Entanglements

Zhou Li

Sept. 29th, 2009

A brief introduction to Tangler

- A Censorship-resistant publishing system
- 10 – 30 Tangler servers
  - *Like anonymous remailers*
- Entanglement of blocks.
  - *Distribute the blocks of files*
  - *An incentive of storing others' content*

Adversary model

- Exhaust the Storage
- Document Deletion
- Document Tampering
- Rubber – Hose Cryptanalysis
  - ➢ *Find the source and blackmail*

Goals

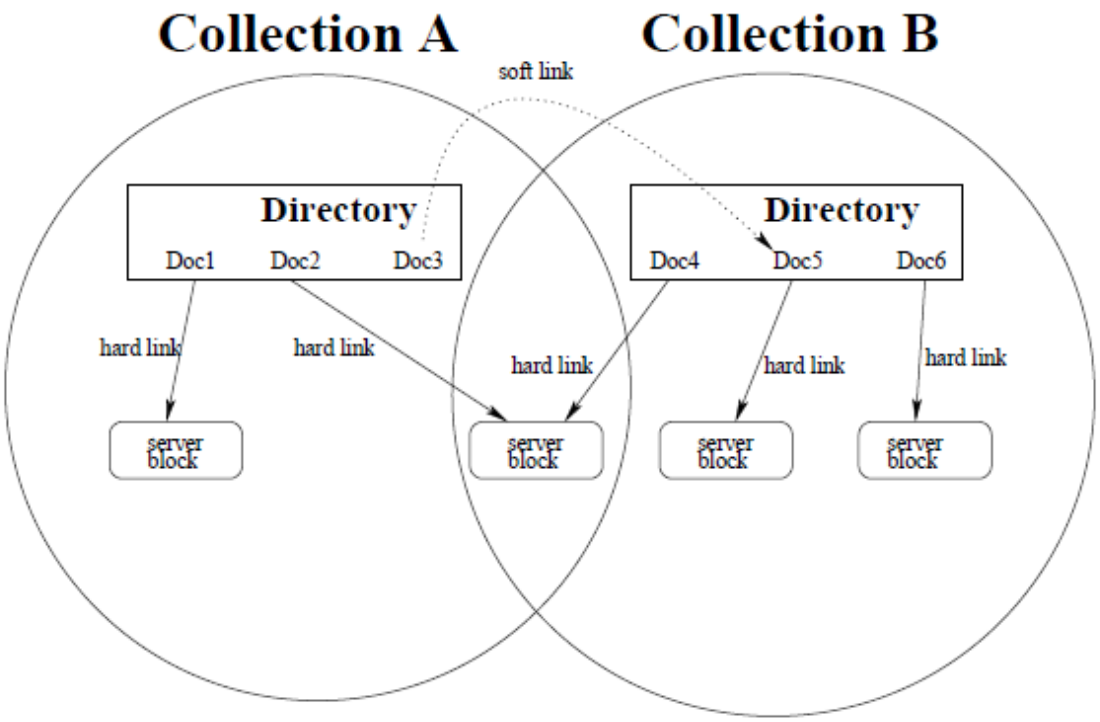
- Dynamic server Participation
- Previous Document Replication
- Publisher and reader Anonymity
- Secure Update
- Publisher caching incentive
- Publishing limit
- Location-independent naming
- Self-policing
- All servers perform useful work

Related Work

- Store files
  - *Freenet*
  - *Publius*
- Store blocks
  - *Free Haven*
  - *Intermemory*
  - *Mojonation*

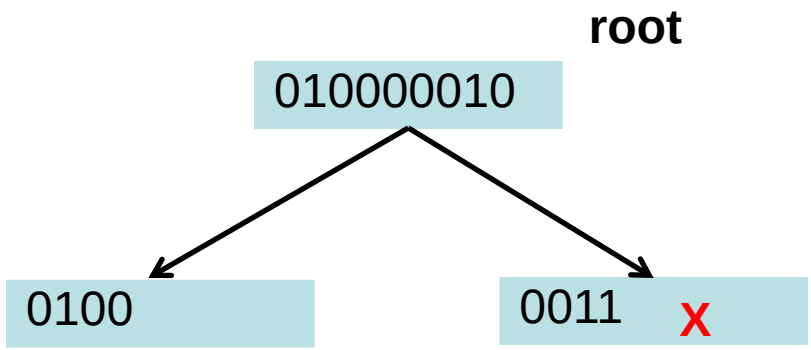
Document organization

- Collections
  - *A group of documents that are published by the same person under the same public key*

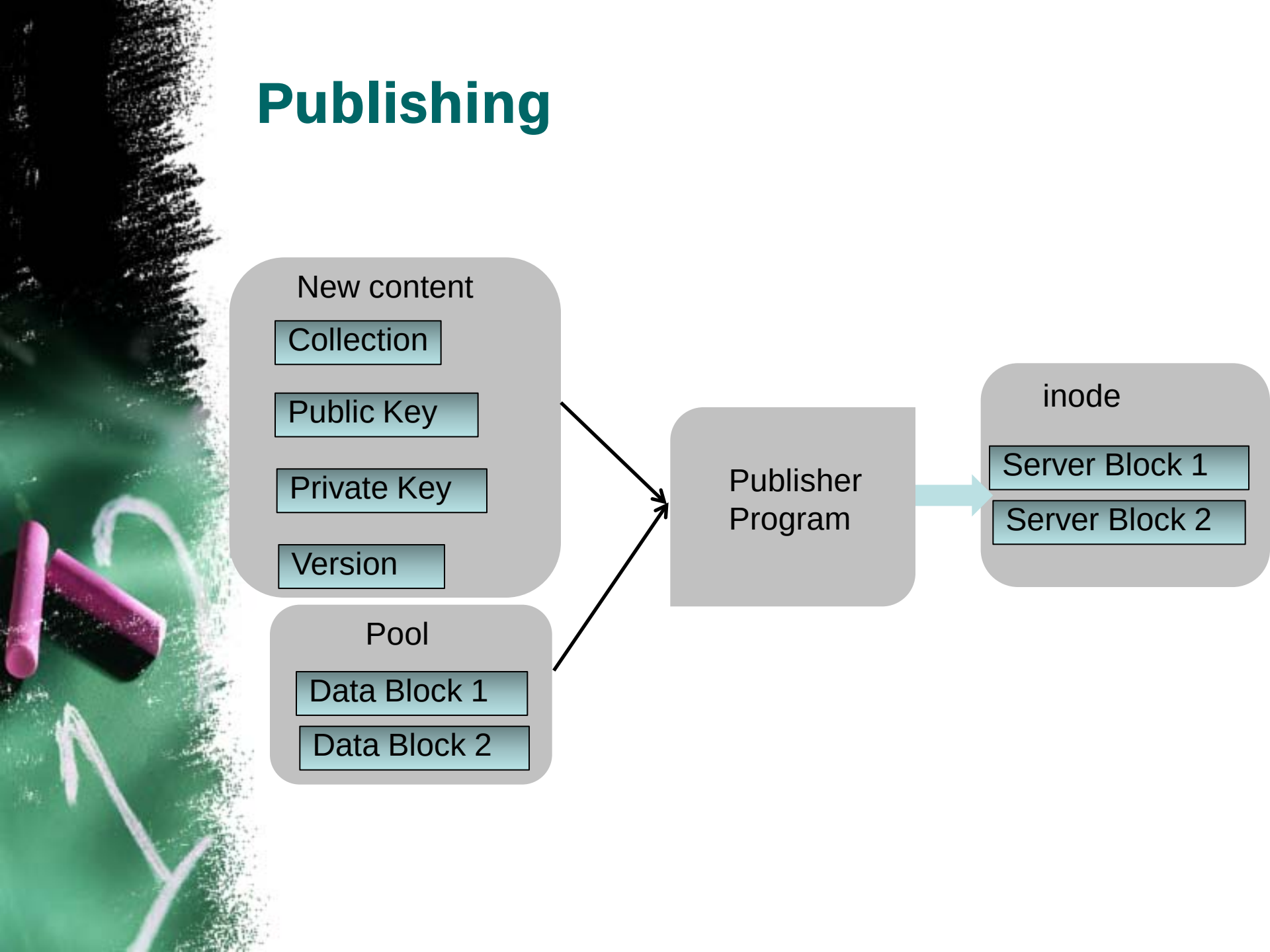


Integrity verification

- Hash tree.



Publishing


New content
Collection
Public Key
Private Key
Version
Pool
Data Block 1
Data Block 2
Publisher Program
inode
Server Block 1
Server Block 2

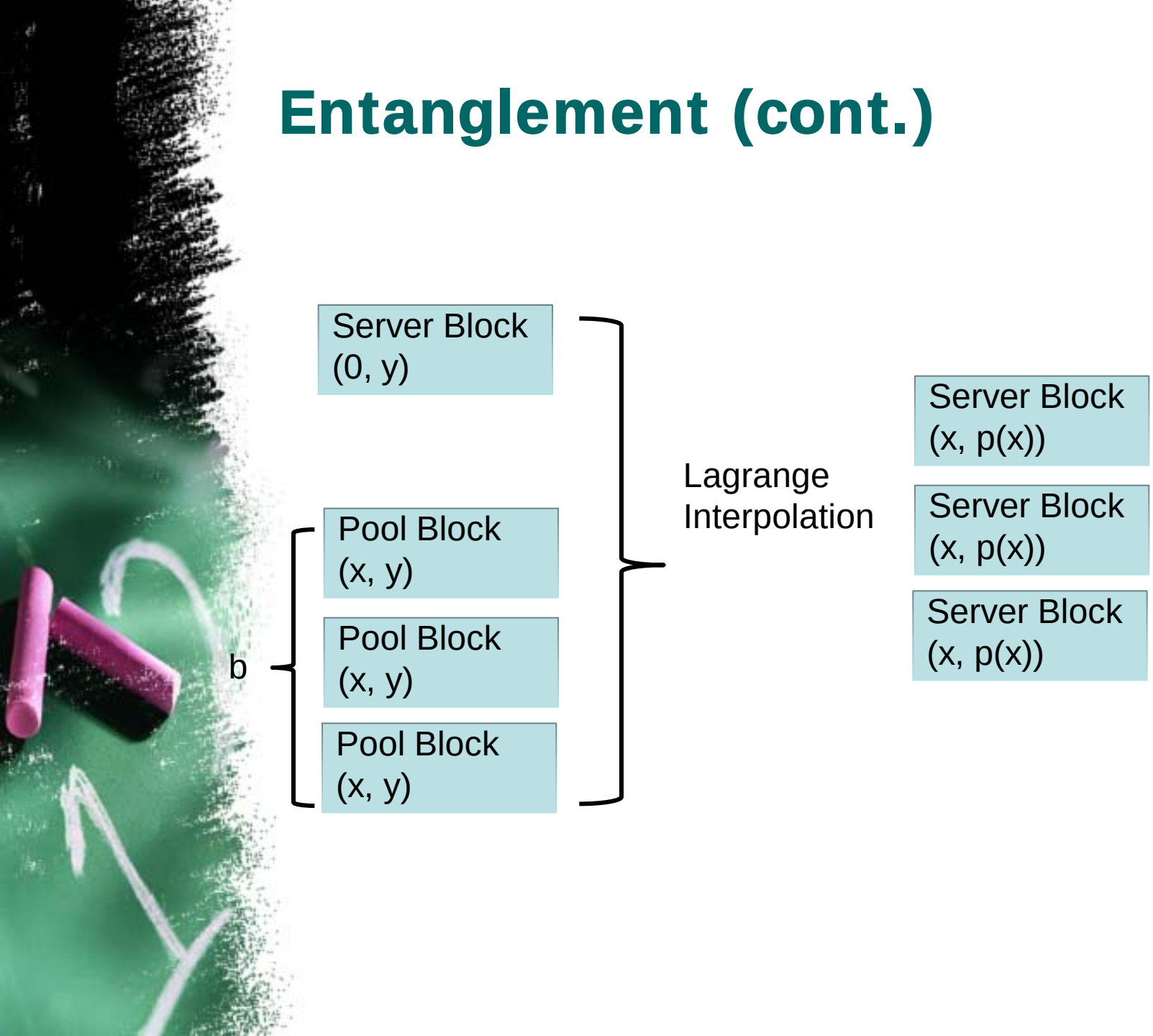
Elaboration

- Public Key
  - *Name of the Collection*
  - *Made by Hash tree*
- Private Key
  - *Used to identify the modifier*

Entanglement

- Shamir's Secret Sharing
  - *Secret:* $6 \in \mathbf{Z}_{11}$
  - *K = 3*
  - *Polynomial:* $y(x) = 7x^2 + 4x + 6$
  - *N pairs of (x,y), N > K*
  - *Less than k pieces reveals nothing about the secret*

Entanglement (cont.)

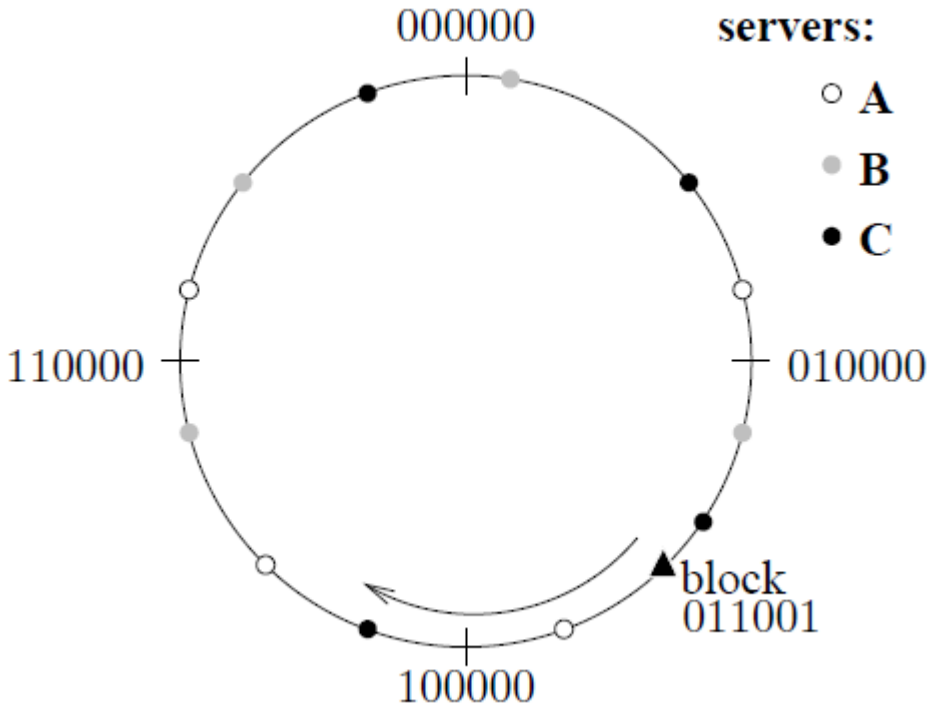


Tangler Network

- Accepting new server without fully trust
  - *Audit server's behaviors*
  - *Require contribution*
  - *Witness*
- Storage management
  - *Storage credits*
  - *Storage receipts*
  - *Storage commitment*

Tangler Network (cont.)

- Block – to – Server mapping
  - *Consistent hashing*
  - *Chord alike*



Benefits

- An incentive mechanism
- Collections
- A high efficient integrity checking mechanism

Limitations

- Less popular content not entangled
- An adversary deleted all the newly created blocks
- Participant is forced to store the content from others?
- Denial of Service
- No implementation

Thanks