Blockchains in 12 Easy Steps

and Observations to Ponder…

Alain Durand

ICANN60
2017
Blockchains at ICANN:

• Namecoin was presented at ICANN58 in the “Emerging identifier session”.

• The community requested ICANN/Office of the CTO to make a broader study of blockchains.
  – Focus is on understanding the technology and performing a risk analysis.
  – Main issue in mind: scalability

• Blockchain panel at ICANN60 at “Emerging identifier session”
Caveats:

• The steps described in the presentation are generic and not descriptive of any specific blockchain implementation.

• Thus, the list of those steps is neither fully accurate nor fully complete.

• Some steps reflect the Bitcoin model, some don’t.
Step 1: A Block

Blocks can contain arbitrary information. Each block is cryptographically signed.
A Blockchain is a list of blocks that are chained back to each other. In other words, each block in the chain has a pointer to the block immediately before.
Step 3: Nodes

Any node can maintain a local copy of the blockchain.
Step 4: The Nodes Form a Peer-to-Peer Network

Nodes have identical copies of the blockchain.
Step 5: A Node Wants to Add a New Block

New block: will be added at the end of the blockchain.
Step 6: Distributing Candidate Block to All Nodes

The requesting node sends the new block to all participating nodes.
Step 7: All Nodes Try to Solve a Complex Puzzle

This phase has to be completed within a specific time frame. Over time, the difficulty of the task will increase (the target value will decrease).

Proof of Work

There is an alternative approach: Proof of Stake

The proof of work is solely to build a “voting poll tax” into the system. Only nodes willing to offer significant compute power can participate. It protects against rogue node joining the network to perform the 51% vote attack.

Find nonce such that:

\[
\text{Hash(nonce+block)} < \text{Target}
\]
Step 8: A Node Finds the Answer First

Eureka!
Step 9: Winner Propagates Solution to All Nodes
Step 10: All Nodes Validate the Proposed Solution

Note: The validation phase is very fast (a single hash calculation).
Step 11: New Block is Inserted in the Blockchain

This phase is happening at a predefined clock time.

All Nodes that participated in the race insert the new block in the blockchain.
The “reward” is here to incentivize nodes to participate to the system and provide compute resources for proof-of-work.
Repeat: The New Block is Ready to Be Used

Repeat…!
Evolution: From Proof-of-Work to Proof-of-Stake

- Replace seemingly mindless random number generation by “Proof-of-Stake”
  - Token to update chain given (randomly or round-robin) to a party with stake

- Acceleration of the cycle
  - From 1 transaction per 10 seconds to 10 transaction per second: conflicts can happen often
  - This forces each node to decide which way to go in case of possible fork

- Strong incentive ($$$) to remain in the majority
  - Each node “guess” where the community is going
  - Whoever control the resources effectively controls the blockchain.
Observations: 1/2

• Every node keep a complete copy of the entire blockchain.
  – Blockchain size always increases… to infinity!
  – Scaling issue: Maximum size of the blockchain → May limit participation to few very large nodes.

• The complexity of the ”Proof-of-Work” always increases to protect against the 51% vote attack.
  – Access to low cost electric power becomes a selection factor that may create a bias in the system.
  – Proof-of-stake and smart contracts are proposed as a replacement of Proof-of-Work in newer blockchains.

• The rate of adding blocks to the chain is fixed.
  – Scaling issue: update rate is fixed → Not all transaction will be recorded immediately.
Observations: 2/2

• Transactions can’t be deleted
  – No way to correct a mistake

• All blocks are visible
  – No privacy, no “right to forget”.

• Control to a node is via public key/private key
  – No way to recover lost passwords

• What can blockchains be used for?
  – Just about anyplace where a community-managed open ledger is desirable…
    …as long as one is not concerned about the above considerations.
  – Today: mostly used by the financial sector, not just Bitcoin.
Examples of Application to Identifiers

Example 1:

BLOCKCHAIN FOR NAME MANAGEMENT

Namecoin
https://www.namecoin.org

See presentation from Jeremy Rand at the Emerging Identifier Session, ICANN58
Namecoin

- Fork of Bitcoin

- Names are registered on a first-come, first-serve basis.

- They are stored in the transaction blockchain database.

- Code is synced with Bitcoin, uses Proof-of-Work.
Examples of Application to Identifiers

Example 2:

BLOCKCHAIN FOR
IP ADDRESS MANAGEMENT

draft-paillisse-sidrops-blockchain-00

See presentation from Jordi Paillissé
at the Emerging Identifier Session, ICANN60

Preliminary research...
Blockchain for IP addresses

- IP addresses as coin: unique, divisible, transferable
- Starts from delegation of IANA to RIRs
- Proof-of-Stake: Party with more IP address controls the blockchain