Scalable Log Auditing on Private Blockchains via Lightweight Log-Fork Prevention

Yuzhe Tang
Syracuse University

Kai Li
Syracuse University

Yibo Wang
Syracuse University

Sencer Burak Somuncuoglu
Chainalysis

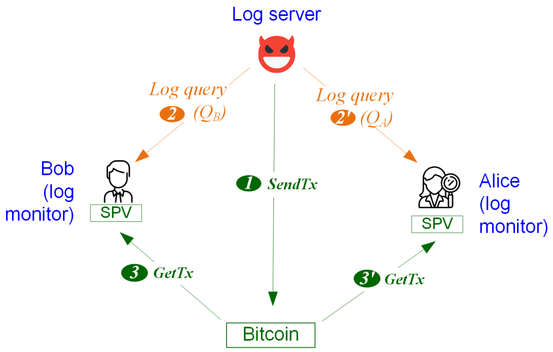
System Model: Monitoring a CT log w Bkc

Untrusted log server [CCS18]

Bitcoin to prevent forks among Monitors [SP17,USS17,NDSI20].

Monitor's overhead:

- ➢ O(1) txs via SPV client
- ➢ O(N) log entries
- ➢ A CT log of N=2.9 billion Certs (15.8 TB)



Goal: Light Log Monitor Client

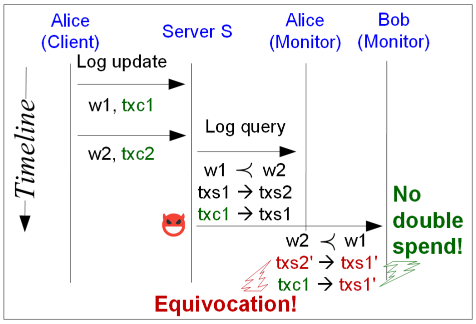
Can a browser possibly monitor CT log without TTP (exc. BKC)?

- ➢ Preventing forks with O(1) log entries and txs?

	Security goal	Monitor's cost	
	Prevent log forks	O(1) log entries	O(1) txs
Catena[SP17], Chainiac[USS17], Ghostor[NSDI20].	✅	❌ O(N)	✅
This work	✅	✅ O(1)	✅

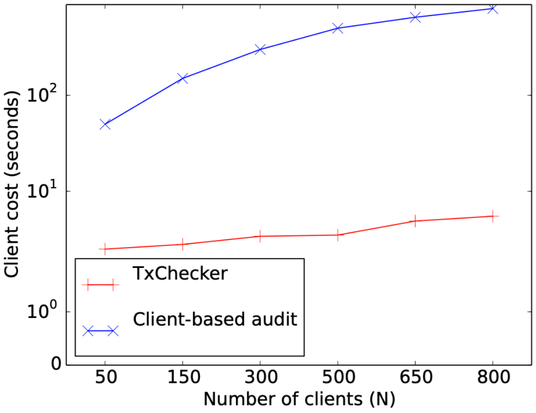
The TxChecker Protocol

Step 1 : Client log attestation
Step 2 : Server log attestation
Step 3 : Submitting log query
Step 4 : Log auditing based on query results



Evaluation

- System prototyping
  - ➢ with FabToken in HyperLedger Fabric
  - ➢ Each log update is a FabToken transfer
- Cost evaluation
  - ➢ Measure monitors' costs



(a) With varying number of clients