Bitcoin-NG
A Scalable Blockchain Protocol

Ittay Eyal
Adem Efe Gencer
Emin Gün Sirer
Robbert Van Renesse

Computer Science, Cornell University
Initiative for Cryptocurrencies and Contracts

NSDI, Santa Clara, CA, March 2016
Cryptocurrency

Exchanges

Bitcoin Exchanges
(180 Companies)

Security

Bitcoin Wallets
(90 Companies)

Hardware

Bitcoin Mining
(49 Companies)

Payment Services

Bitcoin Payments
(83 Companies)
The Blockchain Promise

- Bank-to-bank settlements
- Cheap remittance
- Device-to-device payments (IoT)
The Blockchain Promise
Requires a bigger and faster boat

- Bank-to-bank settlements
- Cheap remittance
- Device-to-device payments (IoT)

![Brands](citibank, NASDAQ, intel, SWIFT, UBS, vmware, IBM, BARCLAYS, HYPERLEDGER)
Bitcoin-NG: A Scalable Blockchain Protocol

- A replicated state machine (Monte-Carlo)
- Extreme-churn robustness
- High performance
  (10x throughput, fraction of latency)

Evaluation

- Novel performance metrics
- Experiments with unmodified nodes
  - Low latency
  - High throughput
Blockchain: A Replicated State Machine

Diagram showing a network of interconnected nodes with transactions labeled:
- $A_1 \rightarrow B_1$
- $A_1 \rightarrow A_2$
- $B_1 \rightarrow C_1$

Log entries are shown on the right side of the diagram.
The Blockchain

Log

header

block

→ t →
The Blockchain

Log

header

block

--- t ---
The Blockchain

Log

\[ \text{hash( } \square \text{ )} < \text{target}^* \]

*target*: a deterministic function of previous blocks
The Blockchain
The Blockchain
The Blockchain

Exponential, with constant mean interval
Incentive for Mining

- **Internal Prize:**
  - Minting
  - Fees

*Wins* proportional to computation power
Forks

- Natural in a distributed system
Fork Resolution

• **Longest** chain wins
• Transactions are reverted
• Double-spending a threat
A transaction is **confirmed** when it is **buried** “deep enough”
Security-Performance Tradeoff

Nakamoto’s Blockchain exhibits a tradeoff:
[Sompolinsky+’15, Lewenberg+’15]
Metrics

• Bandwidth

• Latency
  • Consensus delay

• Security
  • Mining power utilization
  • Fairness
Mining Power Utilization

\[ \sum \frac{\sum \square}{\sum (\square + \square)} \]

\[ \rightarrow \text{vulnerability to rollback} \]
Known Miner Sizes
[blockchain.info, April 2015]

Presence:

\[
\frac{\sum_{all} \neq \Box}{\sum_{all} \Box} = 80\%
\]

\[
\frac{\sum_{main} \neq \Box}{\sum_{main} \Box} = 60\%
\]

Fairness:

\[
\frac{\text{Actual presence}}{\text{Fair presence}} = \frac{60\%}{80\%} = \frac{3}{4}
\]

\[\Rightarrow \text{tendency towards centralization}\]
Block Frequency Experiments

- Increasing block frequency
- Static bandwidth

==> More forks ==> worse security
Block Size Experiments

- Static block frequency
- Increasing block size

==> More forks ==> worse security
Replicated state machine performance is typically bounded by single node performance.

Can this be achieved for the blockchain model?
Nakamoto Blocks
Nakamoto Blocks
Nakamoto Blocks
Nakamoto Blocks

epoch

Serialization
Nakamoto Blocks

epoch

Serialization

Serialization

Serialization

$\rightarrow t$
Nakamoto Blocks

1. Leader election
2. Serialization
Bitcoin-NG

epoch

Leader election → Serialization → Serialization → Serialization → Serialization → t
Bitcoin-NG

• Key blocks:
  • No content
  • Leader election

• Microblocks:
  • Only content
  • No contention
Bitcoin-NG

• PoW
• public key K

signed with k
Bitcoin-NG

long exponential intervals (10 min)

short deterministic intervals (10 sec)
Bitcoin-NG Incentives

**Next miner:** Include previous microblocks
**Leader:** Place transactions in microblocks

Counting microblocks for chain selection breaks security (Selfish Mining)
**Bitcoin-NG Incentives**

**Next miner:** Include previous microblocks

**Leader:** Place transactions in microblocks

**Chain selection rule**
- Heaviest chain
- Microblocks carry no weight

**Fee distribution**
(exact bounds and analysis in paper)

- **40%**
- **60%**
Test Bed

~1000 standard clients (no virtualization)
Implemented based on the Bitcoin-Core client

Infrastructure: 150 machines x 7 cores
1Gb network
Network emulation:

- **Latency and BW:** Based on our measurements [Croman+’15]
- **Implementation:** Virtual network interfaces and kernel rate limiting
- **Validation:** Block propagation matches known trends [Decker&Wattenhofer’13]
Mining power distribution: Based on one-year statistics of operational Bitcoin system.
Block Frequency

Consensus Delay

good

Block frequency [1/sec]
Block Frequency

![Graph showing block frequency for Bitcoin and Bitcoin-NG](image)

- **Block frequency [1/sec]**
- **Fairness**
- **good**

- **Bitcoin**
- **Bitcoin-NG**
Block Frequency

- Bitcoin
- Bitcoin-NG

Mining Power Utilization

good
Block Size

Mining Power utilization

- Good

Block size [byte]

Bitcoin

Bitcoin-NG
Related Work

“The Block Size Debate”
Bitcoin-NG solves an inherent protocol shortcoming.

GHOST protocol, inclusive blockchains
Partial solutions. Perhaps could be used in concert with NG

Centralized solutions of the BFT consensus family
Bitcoin-NG maintains Bitcoin’s weak model

Byzcoin, Hybrid Consensus
Uses Bitcoin-NG’s technique with epoch-length quorums to improve security and latency even further.
Summary

Bitcoin-NG

- High bandwidth
- Low latency
- Secure

Security Concern

• Unlike Nakamoto’s chain, Bitcoin-NG’s leader is a sitting duck
  • Only the leader’s key is static. Microblock generation can be distributed
Microblock Guarantees

• With Nakamoto’s Blockchain:
  fork by risking block prize
• With Bitcoin-NG:
  Free forking?
Microblock Guarantees

• With Nakamoto’s Blockchain:
  fork by risking block prize
• With Bitcoin-NG:
  Free forking? No.

• Poison transaction cancels cheater reward
• Poisoner receives nominal prize
Incentive Compatibility

\[ \pi \]
Broken Chain Selection Rule

**Next miner:** Include previous microblocks
Microblocks carry small weight?

**Leader:** Place transactions in micro blocks
Leader gets fees?
**Broken Chain Selection Rule**

**Next miner:** Include previous microblocks  
Microblocks carry small weight?

**Leader:** Place transactions in microblocks  
Leader gets fees?

- Create secret chain:
  ![Diagram of secret chain creation]

- Always beat majority:
  ![Diagram of majority beating]
Block Size

Consensus Delay

3 Consensus Delay

Block size [byte]

Bitcoin

Bitcoin-NG

good