\Orchestrating a brighter world NEC

Towards Secure and Scalable Permissionless Blockchains – The PoW Experience

Dr. Ghassan Karame
NEC Laboratories Europe

\Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create
the ICT-enabled society of tomorrow.
We collaborate closely with partners and customers around the world,
orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to
greater safety, security, efficiency and equality,
and enable people to live brighter lives.

PoW-based Blockchains

Pros:

- *Open permissionless system.*
- *No need for identity management.*
- *Scales to millions of nodes.*
- ***"Immutable" ledger.***

PoW-based Blockchains

Cons:

- *Wasteful of energy and resources.*
- *Security against selfish mining*
- *Network-layer attacks*
- *Slow consensus*
- *Limited decentralization due to mining pools*
- *Lack of incentives*

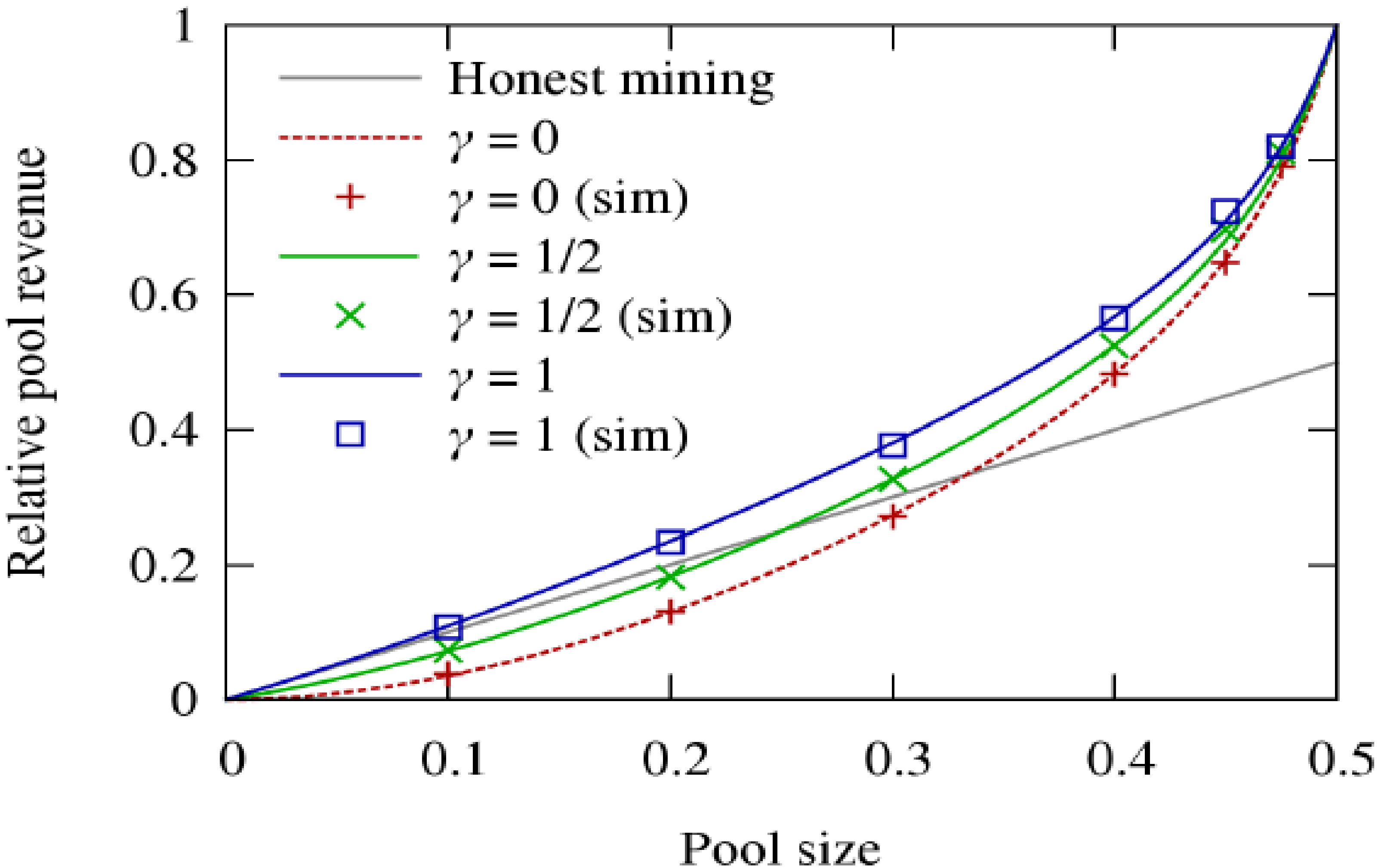
Experience with Existing PoW-based Open Blockchains

Problem 1: Selfish Mining

- The goal of selfish mining is to obtain revenue larger than its actual share of computing power.

- This can be achieved by “wasting” the computing power of honest nodes.
  - Malicious colluding miners work on a secret block chain.
  - Malicious colluding miners reveal parts of their secret blocks as new blocks are released.
  - This ensures that their secret chain is bigger than the public chain sustained by honest miners.

The attack

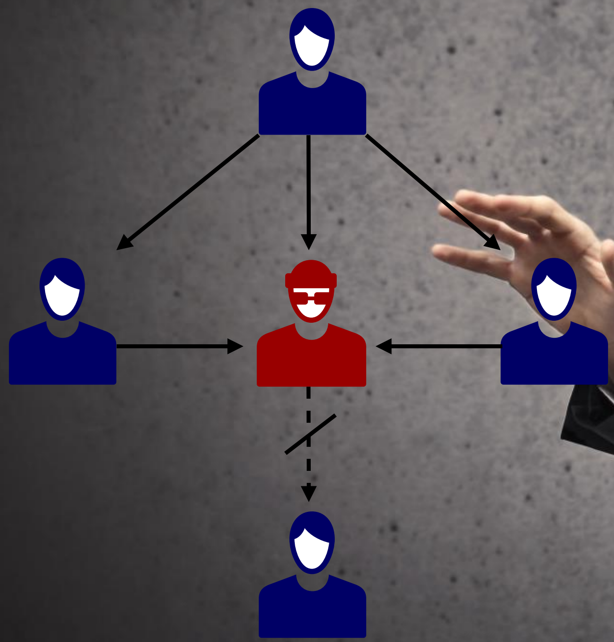


Source: Eyal and Sirer, FC'13

Eclipse attacks

Denial of Service

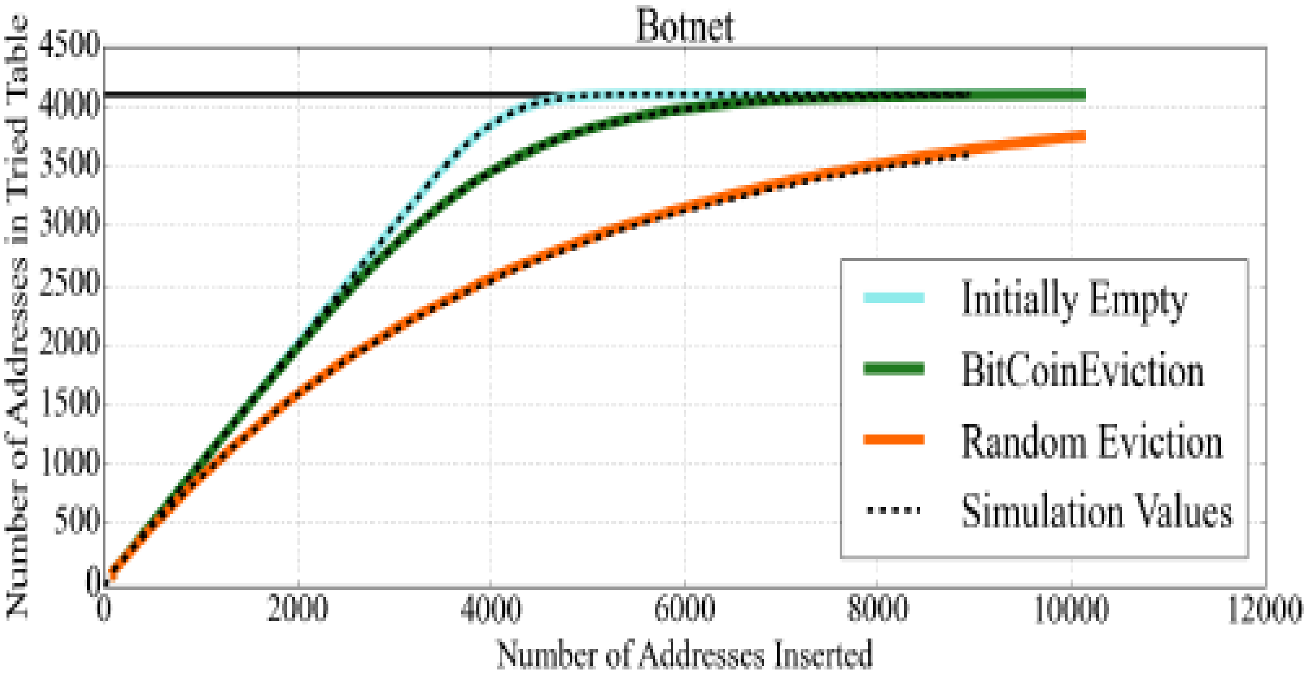
Double Spending



Eclipse attacks

- Experimental eclipse attacks succeed with probability **84%**.

- The adversary is required to have ~5120 IP addresses at his disposal.



Source: Heilman et al. Usenix Security 2015

Implications

Implication 1: The adversary can split the mining power in the network, since he can prevent blocks to be received by some nodes.

➡ More pronounced selfish mining attacks!

Implication 2: The adversary can double-spend transactions, even if these transactions are confirmed by 6 consecutive blocks.

Implication 3: The adversary can mount large-scale DoS attacks on the network.

Countermeasures

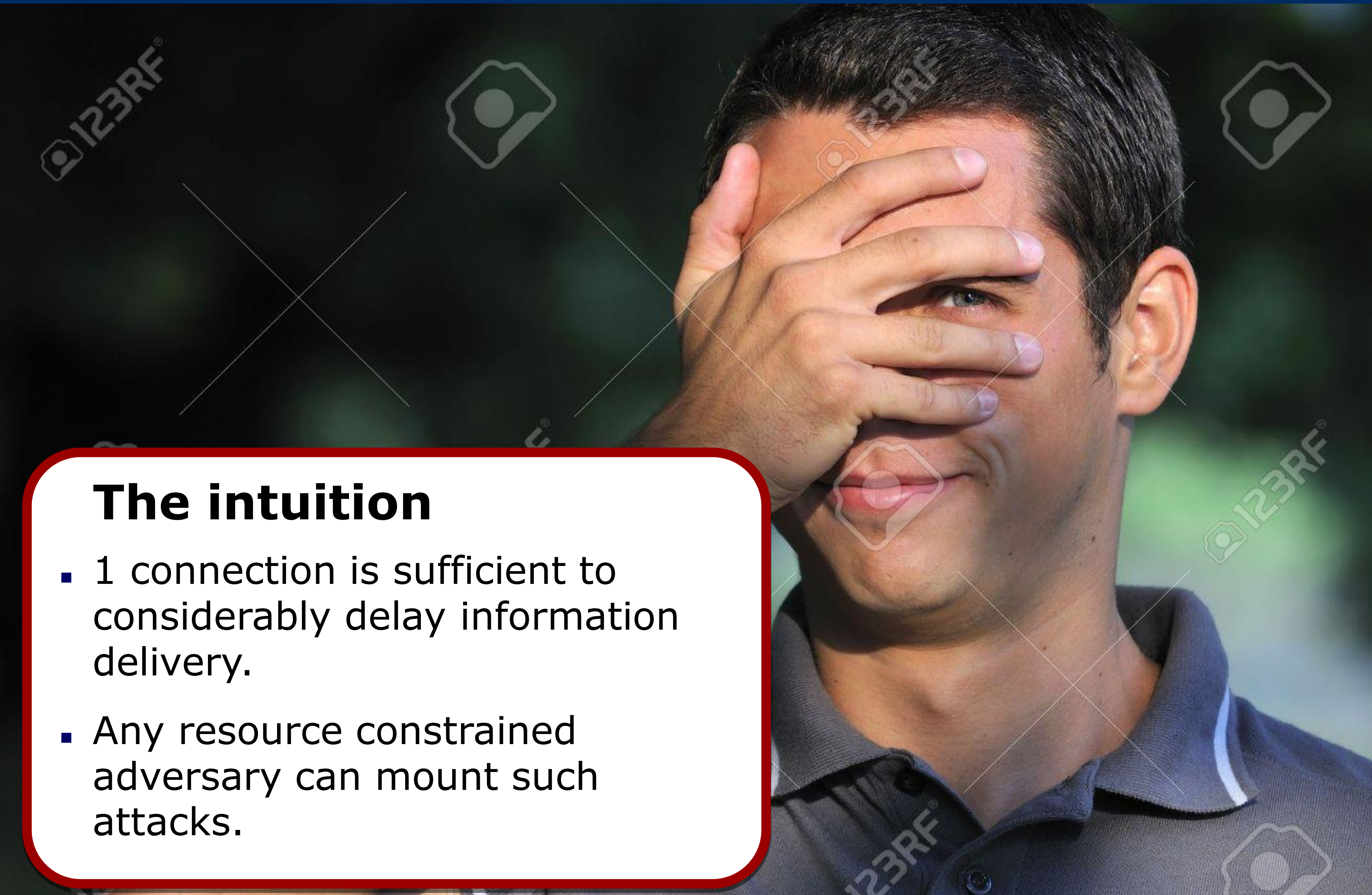
- **Countermeasure 1:** make sure that the same address hashes to the same bucket, and the same location. By doing so, one can prevent the adversary to re-use the same address more than once to fill the **tried** table.

- **Countermeasure 2:** avoid any bias in choosing addresses that are recent. This reduces the probability to rely on the adversary's addresses.

- **Countermeasure 3:** make sure that the new IP address exists before replacing an old address in **tried** and **new**.

- **Countermeasure 4:** add new buckets.

- **Countermeasures 1,2, and 4 are part of the official client v0.10.1.**

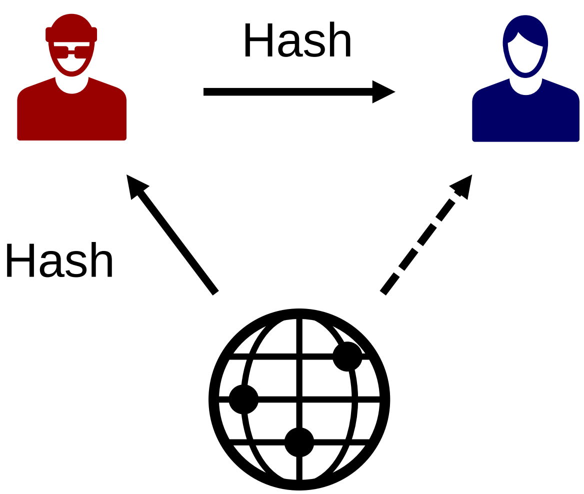


The intuition

- 1 connection is sufficient to considerably delay information delivery.
- Any resource constrained adversary can mount such attacks.

Denying Information Delivery: Requirements

1. Must be **first** peer to advertise Tx / block

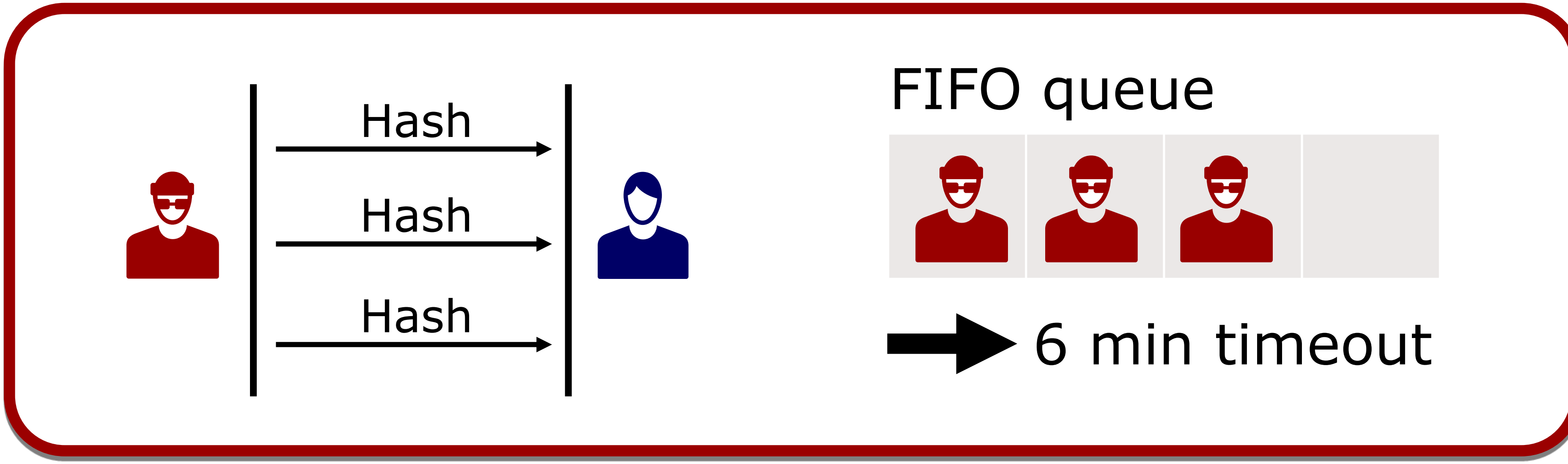


2. This would result in delaying information reception by:

- 20 minutes for blocks
- 2 minutes for transactions

Transactions

- After 2 min request from other peer



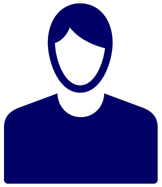
Blocks

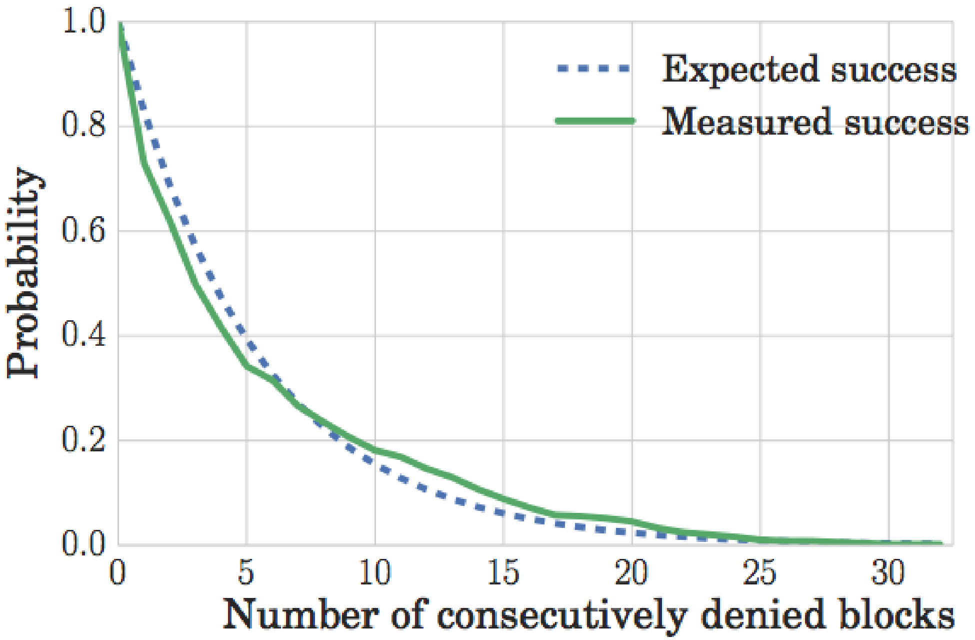
- After 20 minutes, disconnect and request block from another peer

Extending block delivery beyond 20 minutes

Requirements for victim

- Must not receive block header
- Must not receive version message

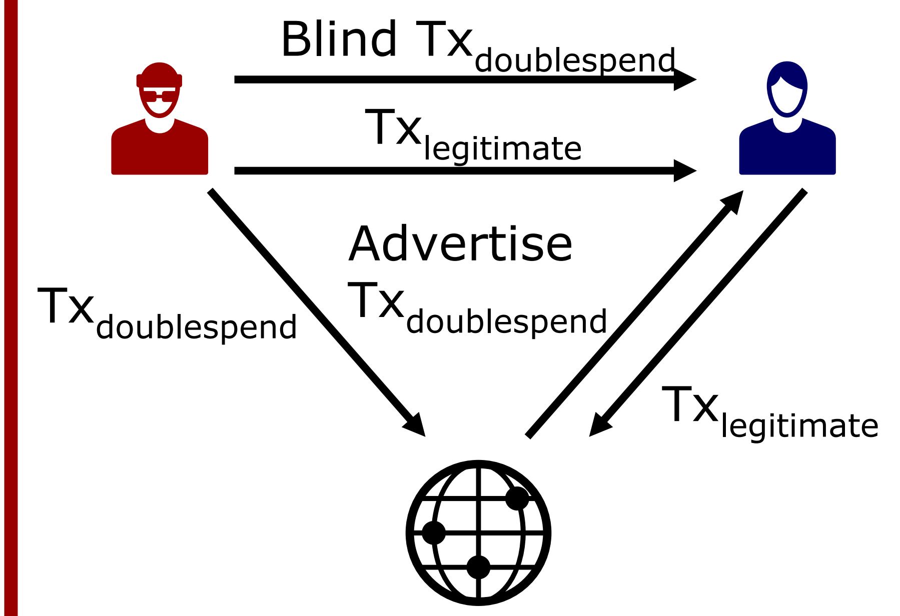




Probability for n blocks = p^n, with p = 0.83

Implications

- **Double Spending**
  - Regardless of protection
    - Double spend relay



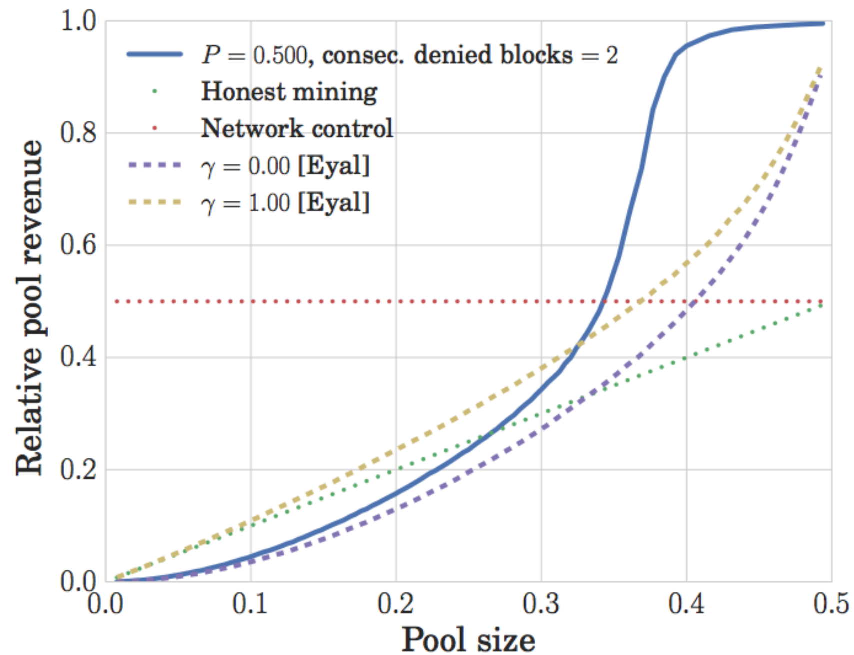
Implications

- **Double Spending**
  - Without risk
  - Regardless of protection
    - Double spend relay
- **Denial of Service**
  - Easily-realizable Denial of Service Attacks

- 6000 reachable nodes
- 450,000 TCP connections required
- 600 KB of advertisement / block / 20 min

Implications

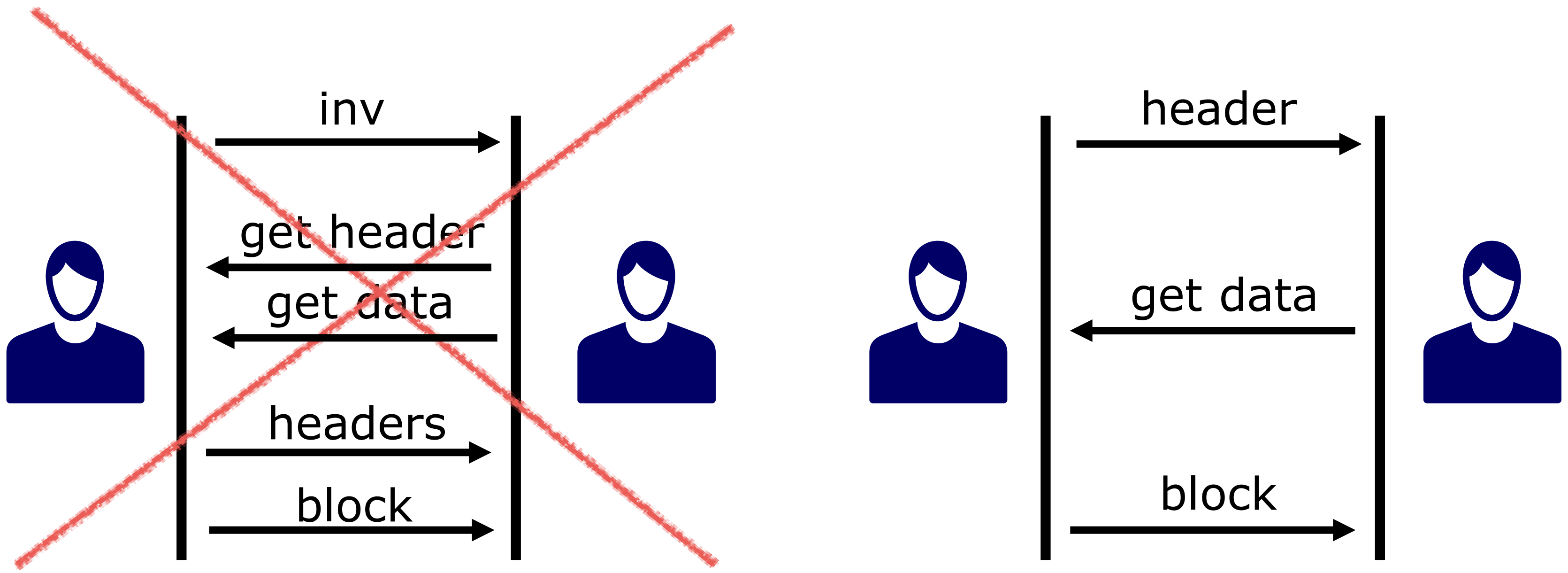
- **Double Spending**
  - Without risk
  - Regardless of protection
    - Double spend relay
- **Denial of Service**
  - Easily-realizable Denial of Service Attacks
- **Increasing Mining Advantage**
  - **33% attacker can control the network**



Dr. Ghassan Karame, NEC Laboratories Europe

Countermeasure

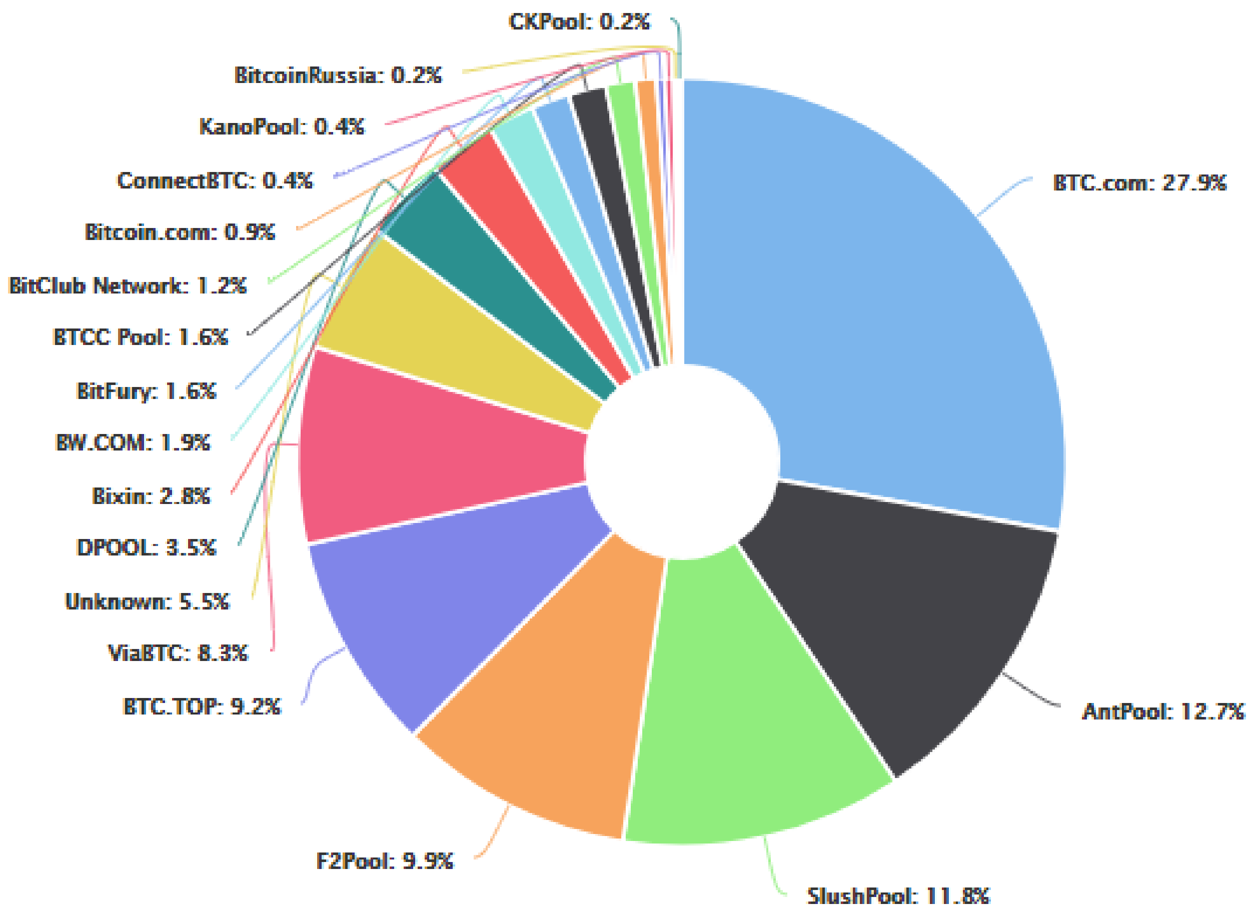
Integrated in Bitcoin v0.12



Size of inv messages = 36 bytes
Size of the header = 80 bytes

Problem 4: (De-)centralization in Bitcoin [IEEE S&P Magazine'14]

- ~5 mining pools control Bitcoin. They can decide the fate of all transactions in the system.



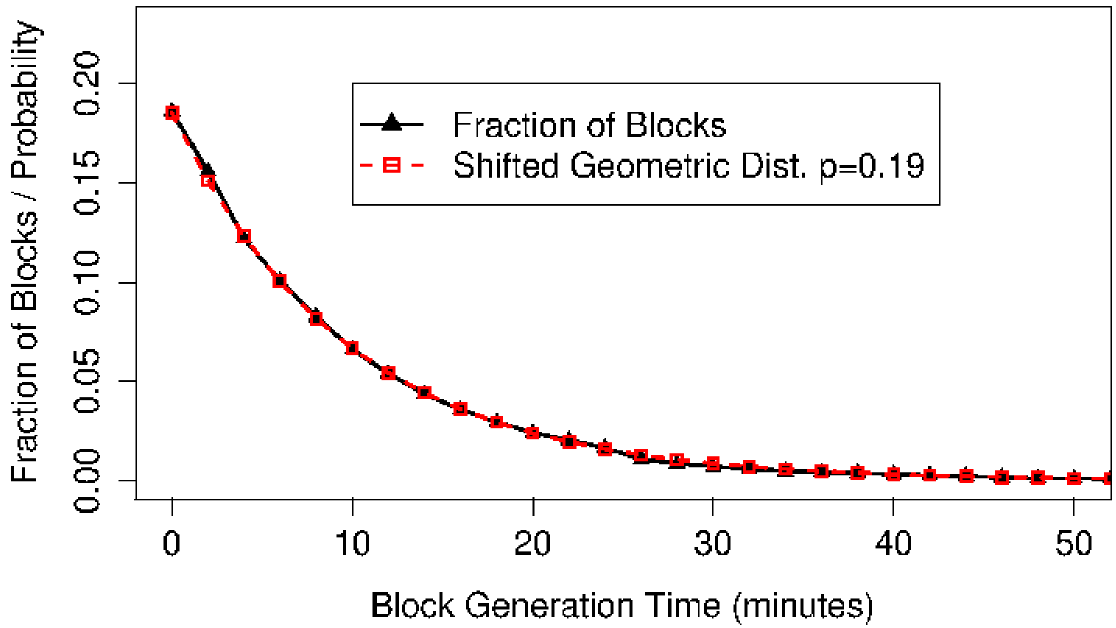
Problem 5: Slow Confirmation/Double spending [CCS'12]

Experimentally:

- In Bitcoin, blocks are generated every 10 minutes with a standard deviation of 15 minutes.

Analytically:

- We show that block generation in Bitcoin follows a shifted geometric distribution with p=0.19



How to increase consensus performance?

10 minutes

2.5 minutes

1 minute

10-20 seconds

	Bitcoin	Litecoin	Dogecoin	Ethereum
Block interval	10 min	2.5 min	1 min	10-20 seconds
Public nodes	6000	800	600	4000 [11]
Mining pools	16	12	12	13
t_{MBP}	8.7 s [8]	1.02 s	0.85 s	0.5 - 0.75 s [12]
r_s	0.41%	0.273%	0.619%	6.8%
s_B	534.8KB	6.11KB	8KB	1.5KB

Understanding Security/Performance of PoW Blockchains [CCS'16]

Due to the ***smaller block rewards*** and the ***higher stale block rate*** of Ethereum compared to Bitcoin (from 0.41% to 6.8% due to the faster confirmation time), Ethereum (block interval10-20 seconds) needs at least ***37 confirmations*** to match Bitcoin security (block interval of 10 minutes on average) *with* ***6 confirmations*** against an adversary with 30% of the total mining power.

Similarly, Litecoin would require 28, and Dogecoin 47 block confirmations respectively to match the security of Bitcoin.

Some good parameters:

- **1 MB block size**
- **1 minute block generation time**
- **Throughput of almost 60 transactions per second!**
  - **Much larger than Bitcoin's 7 tps!**

Entangling Proofs of Knowledge with PoW [Armknecht et al. 2017]

Idea: tie blockchain storage with the only well-incentivized process in PoW blockchains: mining.

- Miners have to store a considerable portion of the blockchain in order to have a correct PoW solution.

Other ideas:

- Permacoin [Oakland'14]: replace PoW with PORs

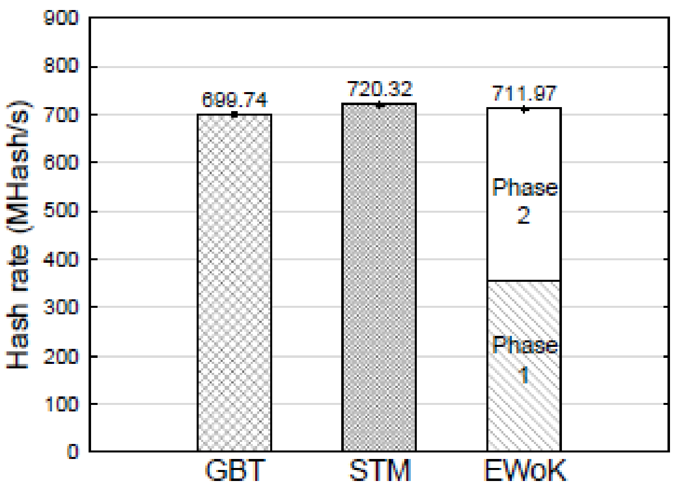


Fig. 5: Effective hash rate performance of EWoK when compared to GBT and STM.

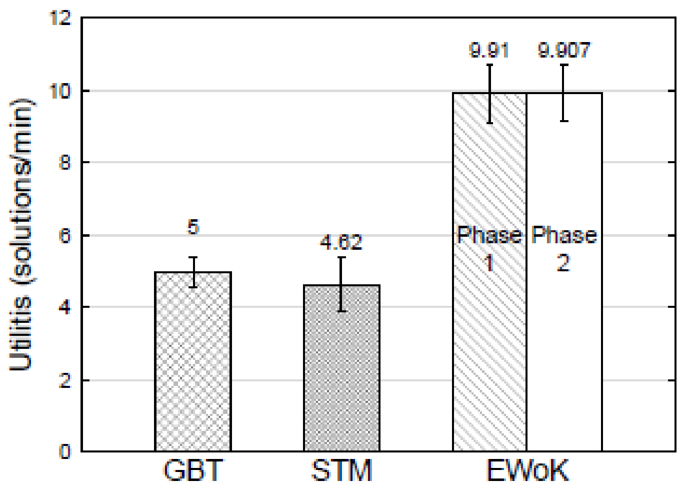


Fig. 6: Number of solutions mined in EWoK when compared to GBT and STM.

Some challenges in PoW-based Blockchains

Outlook & Challenges

- ***Throughput***: Existing open blockchains can only reach modest throughputs! How can we reach higher throughputs?
  - **Lightning networks and other off-chain techniques**
  - **Proof of Stake**
  - **Hybrid BFT protocols**

- ***Security***: Ensure full resilience to network attacks and consensus-layer attacks.
  - **Formal models for PoW blockchains**
  - **Smart contract security**

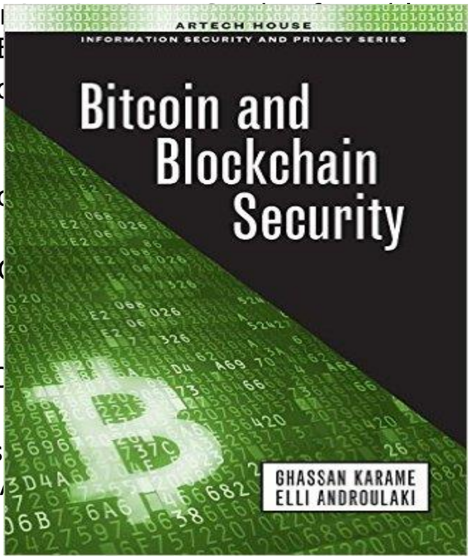
- ***Privacy***: Ensure user privacy and transactional privacy in open systems.
  - **ZeroCash**

- ***Accountability***: Punish misbehaving nodes in permissionless open system.
  - **eCash**

- ***Decentralizing blockchains:*** Ensure that the deployment of distributed protocols is indeed decentralized.
  - Outsourceable scratch-off puzzles?

Selected Publications

- Damian Gruber, Wenting Li, Ghassan Karame, Unifying Lightweight Blockchain Client Implementations, In Proceedings of the NDSS Workshop on Decentralized IoT Security and Standards (**NDSS-DISS**), San Diego, California, USA, 2018.
- Jian Liu, Wenting Li, Ghassan Karame, N. Asokan, Towards Fairness of Cryptocurrency Payments**,** In **IEEE Security and Privacy**, 2017.
- Wenting Li, Sebasiten Andreina, Jens-Matthias Bohli, Ghassan Karame, Securing Proof of Stake Blockchain Protocols**,** In Proceedings of the ESORICS Workshop on Cryptocurrencies and Blockchain Technology (**ESORICS-CBT**), Oslo, Norway, 2017.
- Wenting Li, Alessandro Sforzin, Sergey Fedorov, Ghassan Karame, Towards Scalable and Private Industrial Blockchains**,** In Proceedings of the ACM ASIACCS Workshop on Blockchain, Cryptocurrencies, and Contracts (**ACM ASIACCS-BCC**), *(Acceptance rate: ~30%),* Abu Dhabi, UAE, 2017.
- Arthur Gervais, Ghassan Karame, K. Wuest, V. Glykantzis, Hubert, Ritzdorf, Srdjan Capkun, On the Security and Performance of Proof of Work Blockchain. In Proceedings of the ACM Conference on Computer and Communications Security (**ACM CCS**), Vienna, Austria, (Acceptance rate: 16.5%) (to appear) 2016.
- Arthur Gervais, Hubert Ritzdorf, Ghassan Karame, Srdjan Capkun, Tampering with the Delivery of Blocks and Transactions in Bitcoin, In Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS), Denver, USA,(Acceptance rate: 19.8%) 2015
- Frederik Armknecht, Ghassan Karame, Avikarsha Mandal, Franck Youssef, Erik Zenner, Ripple: Overview and Outlook, In Proceedings of International Conference on Trust & Trustworthy Computing (TRUST), Crete, Greece, 2015
- Ghassan Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, Srdjan Capkun, Misbehavio spending and Accountability, In ACM Transactions on Information and System Security (TISSE
- Arthur Gervais, Ghassan Karame, Damian Gruber, Srdjan Capkun, On the Privacy Provisions c Bitcoin Clients, In Proceedings of the 30th Annual Computer Security Applications Conference Louisiana, USA, 2014 (Acceptance rate: ~19.9%)
- Elli Androulaki, Ghassan Karame, Hiding Transaction Amounts and Balances in Bitcoin, In Proc Conference on Trust & Trustworthy Computing (TRUST), Crete, Greece, 2014
- Arthur Gervais, Ghassan Karame, Srdjan Capkun, Vedran Capkun, Is Bitcoin a Decentralized (Privacy, 2014
- Elli Androulaki, Ghassan Karame, Marc Roeschlin, Tobias Scherer, Srdjan Capkun, Evaluating Proceedings of the International Conference on Financial Cryptography and Data Security, (FC (Acceptance rate: 12.5% for regular papers)
- Ghassan Karame, Elli Androulaki, Srdjan Capkun, Double-Spending Attacks on Fast Payments ACM Conference on Computer and Communications Security (CCS), Chicago, IL, USA, 2012,(
- **Bitcoin and Blockchain Security**



\Orchestrating a brighter world

NEC