DDoSCoin

Cryptocurrency with a Malicious Proof-of-Work

Eric Wustrow

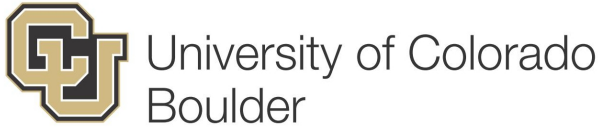
University of Colorado Boulder

ewust@colorado.edu

Benjamin VanderSloot

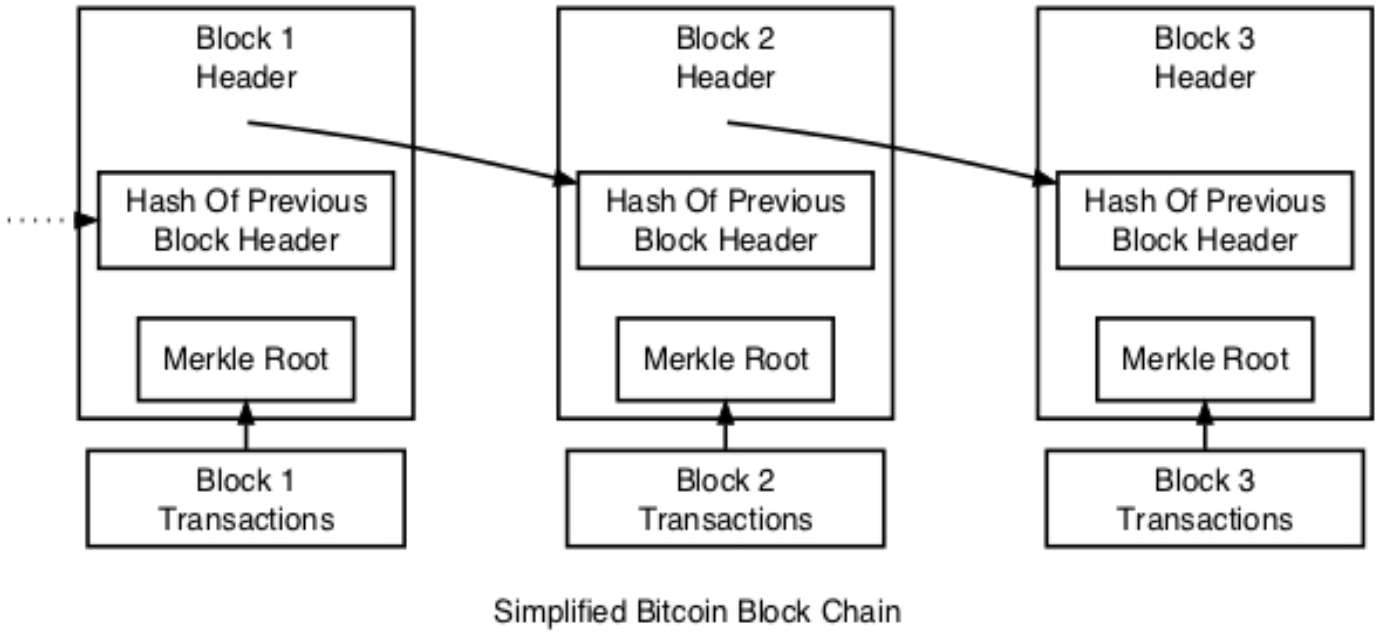
University of Michigan

benvds@umich.edu



Cryptocurrencies

- Digital, decentralized cash
- Public ledger of transactions
- Mining rewards



Simplified Bitcoin Block Chain

Source: bitcoin.org

Proof-of-Work

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a93
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245c
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464
```

Source: bitcoin.org

Alternate Proofs-of-Work

- Bitcoin
- Litecoin
- Peercoin
- Permacoin
- TorPath
- Primecoin

- **DDoSCoin**

Proof-of-Stake

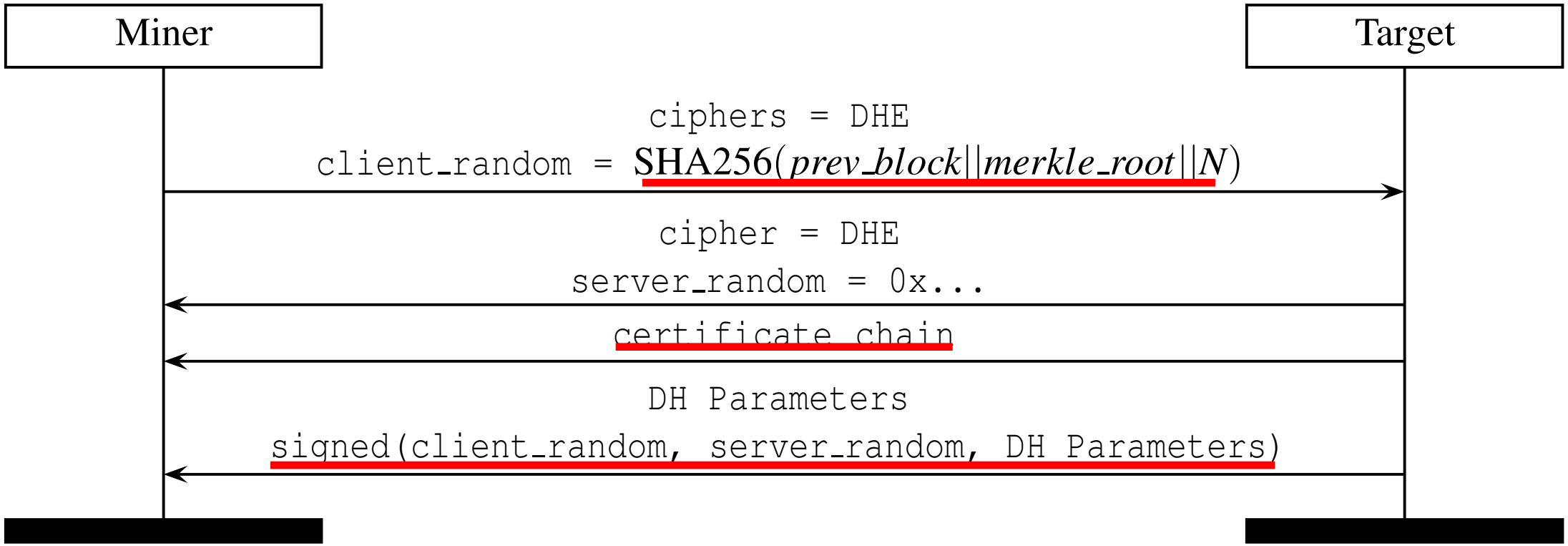
- Peercoin
- Coin-days are proof
- Rate-limiting prevents proof-of-work
- Coins can only age 90 days

Proof-of-DDoS

SHA256(DH Parameters || signature || N)

Block Validation

Proves many connections to a target server, and leaves the blockchain in a good state



SHA256(DH Parameters || signature || N)

Target Selection

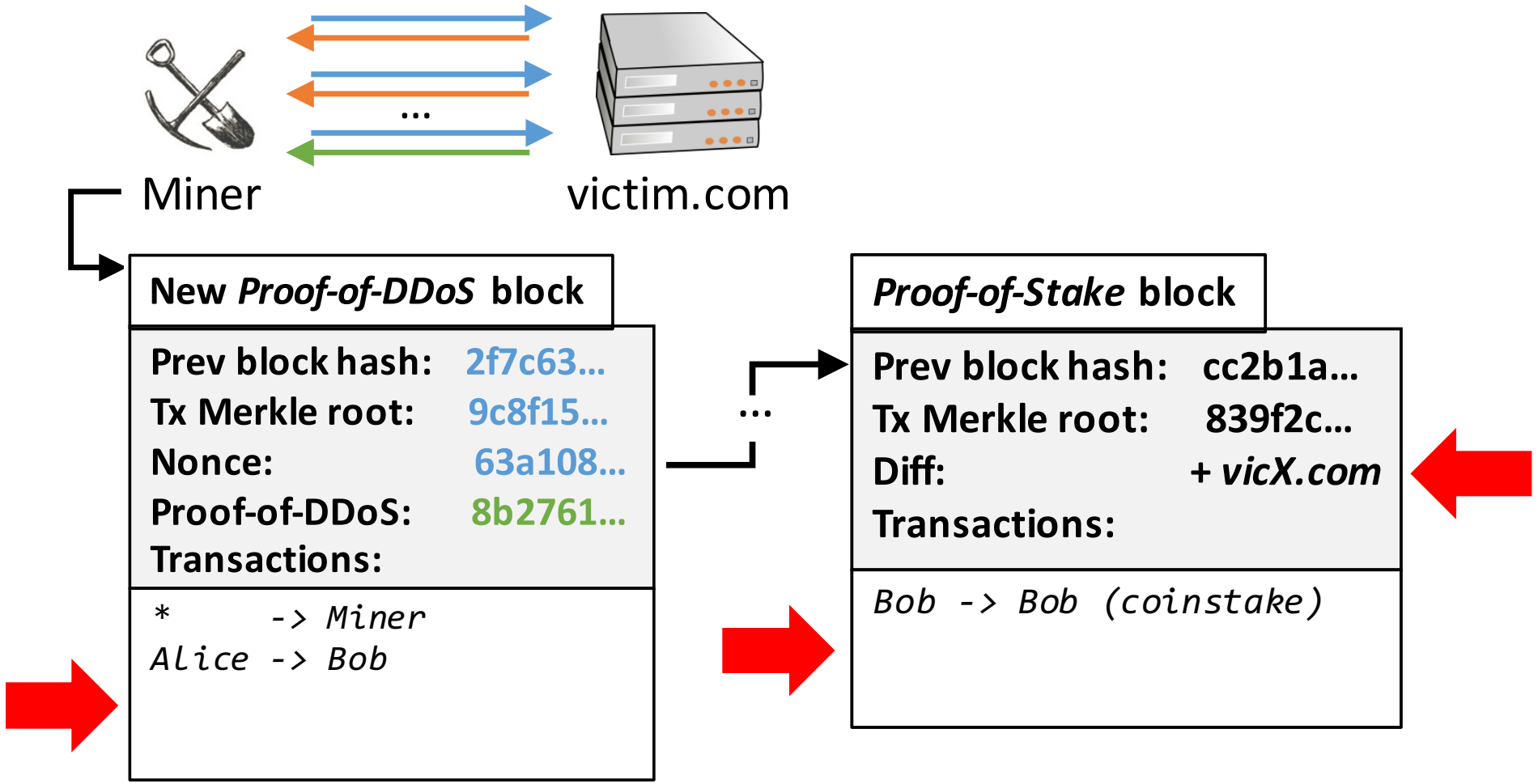
~~• Any server?~~

~~• Fixed set of servers?~~

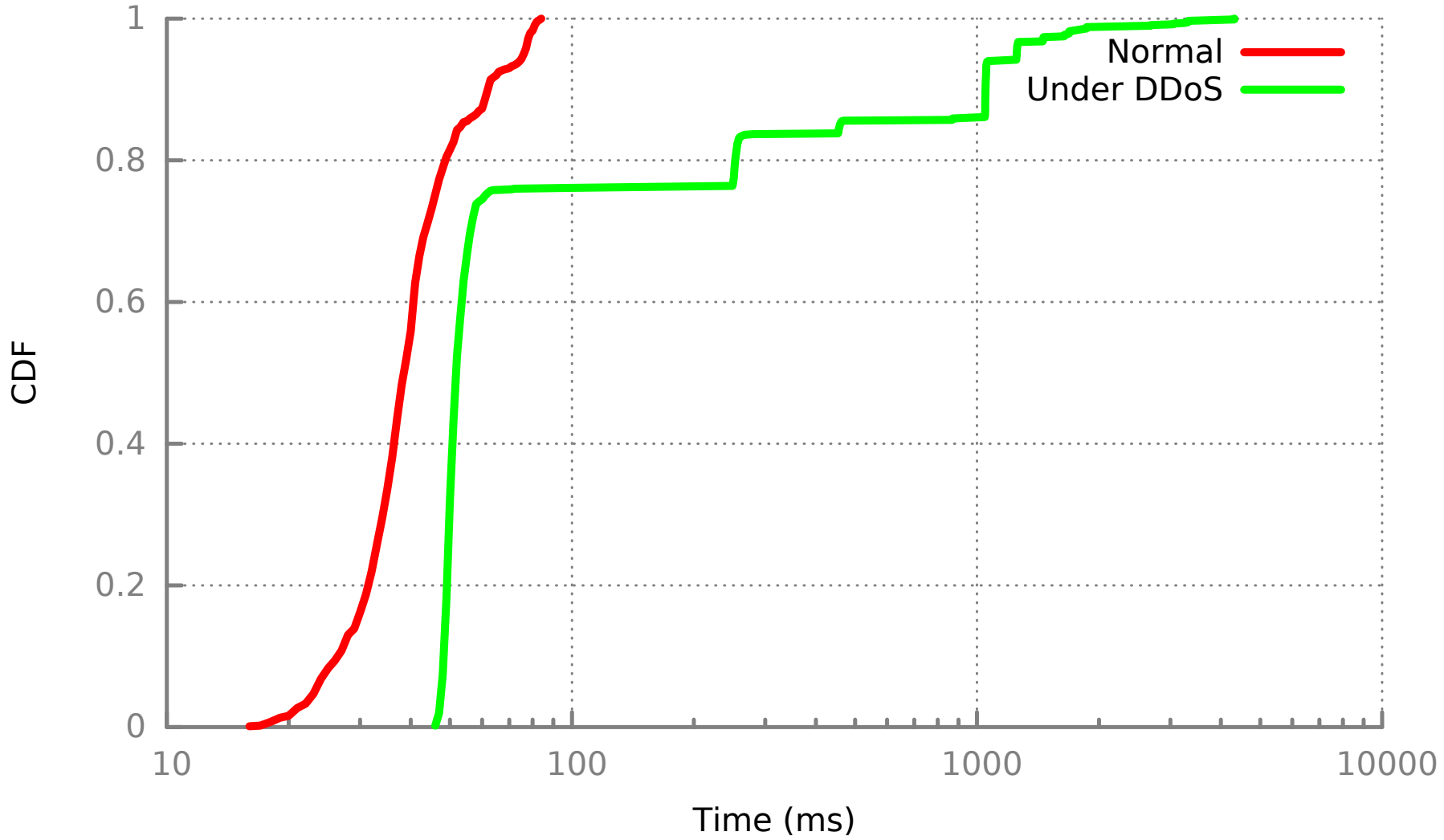
Our Solution

- Proof-of-Stake blocks
- PAY_TO_DDOS transactions

Target Selection



Proof-of-DDoS Implementation



Defenses

- Version or cipher suite changes
- Victims claiming own rewards
- Stakeholding
- Legal action

Discussion

- Malicious “useful” proof-of-work
- Challenges regarding bandwidth availability
- Ethereum smart contracts
- Ethical Forks
- Barriers to adoption

Ethics

- Did not attack real servers
- Did not publish the full coin

Ethics

- Did not attack real servers
- Did not publish the full coin
- Full disclosure

DDoSCoin

Cryptocurrency with a Malicious Proof-of-Work

Eric Wustrow

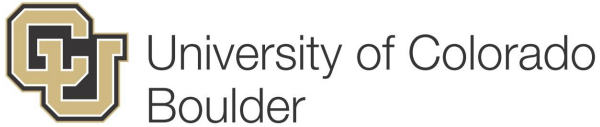
University of Colorado Boulder

ewust@colorado.edu

Benjamin VanderSloot

University of Michigan

benvds@umich.edu



Target Difficulty

- Global difficulty parameter
  - Adjust the rate at which transactions are processed
- Per-domain difficulty parameter
  - Allow all targets to be viable
- Constant time intervals
- Initial difficulty set by user