Applying Proof of Work

Stephen Haunts
LEADER, DEVELOPER, SPEAKER AND TRAINER

@stephenhaunts www.stephenhaunts.com

Overview

Add immutability

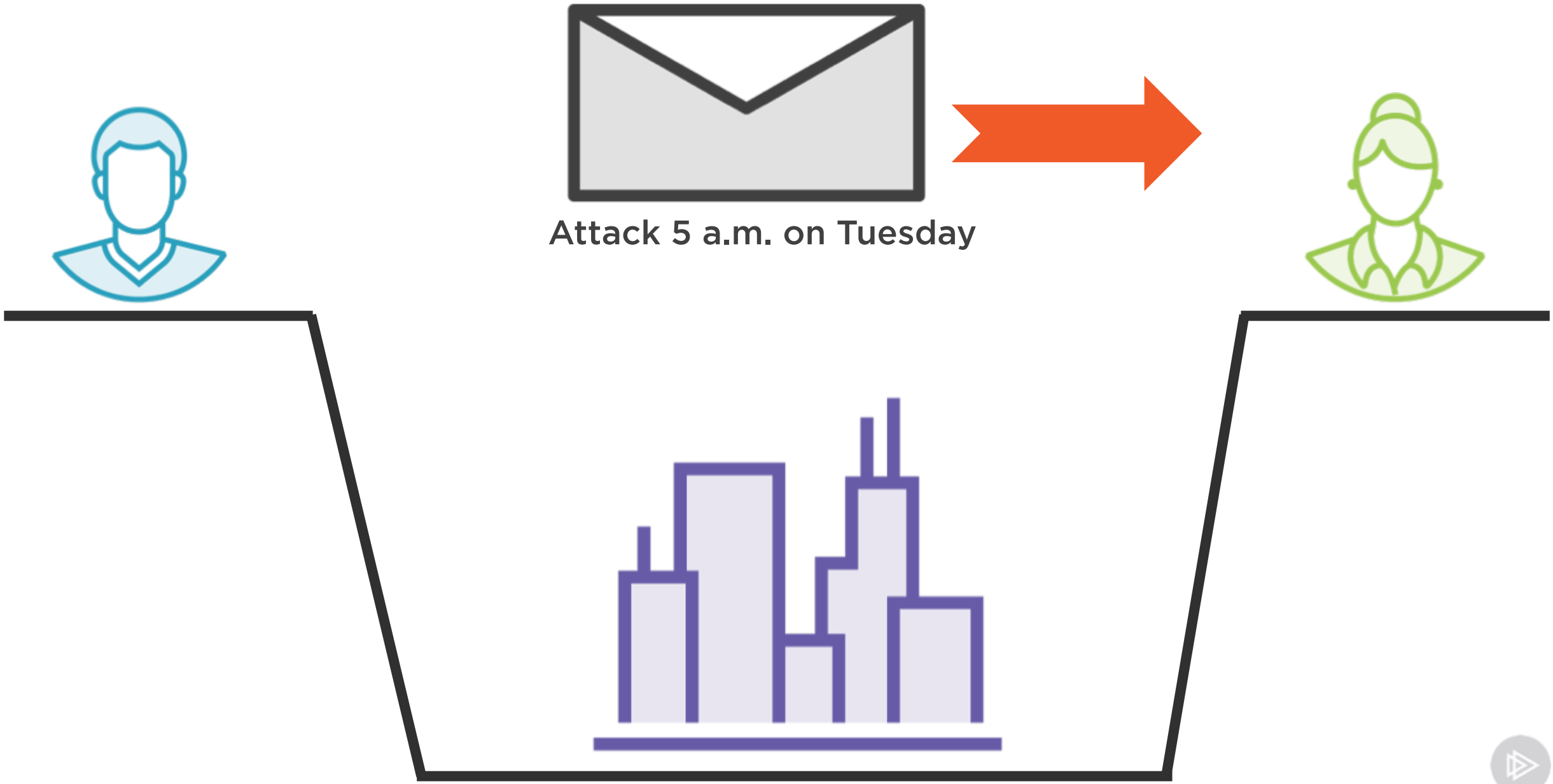
Proof of work

Byzantines Generals' Problem

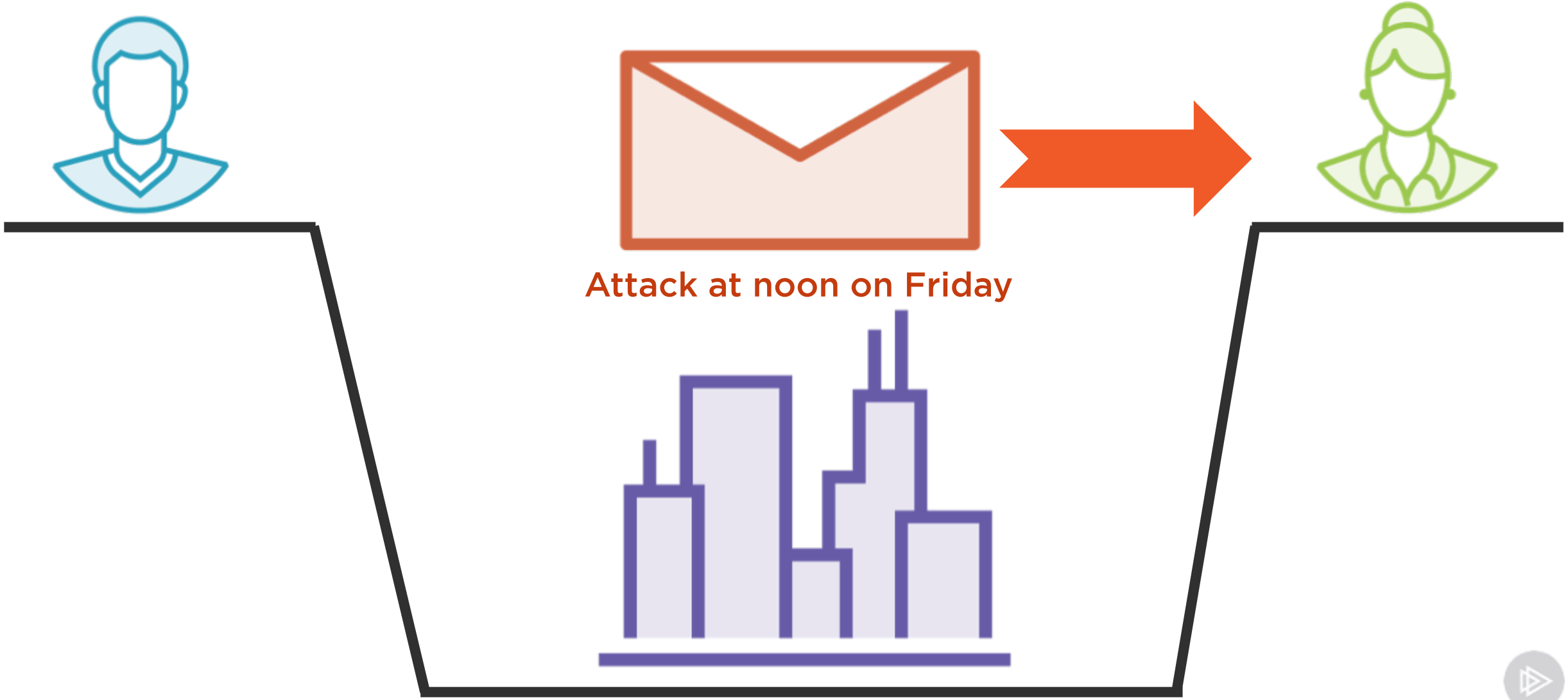
Byzantine Generals' Problem

Leslie Lamport, Robert Shostak and Marshall Pease

http://lamport.azurewebsites.net/pubs/byz.pdf


Attack 5 a.m. on Tuesday


Acknowledged

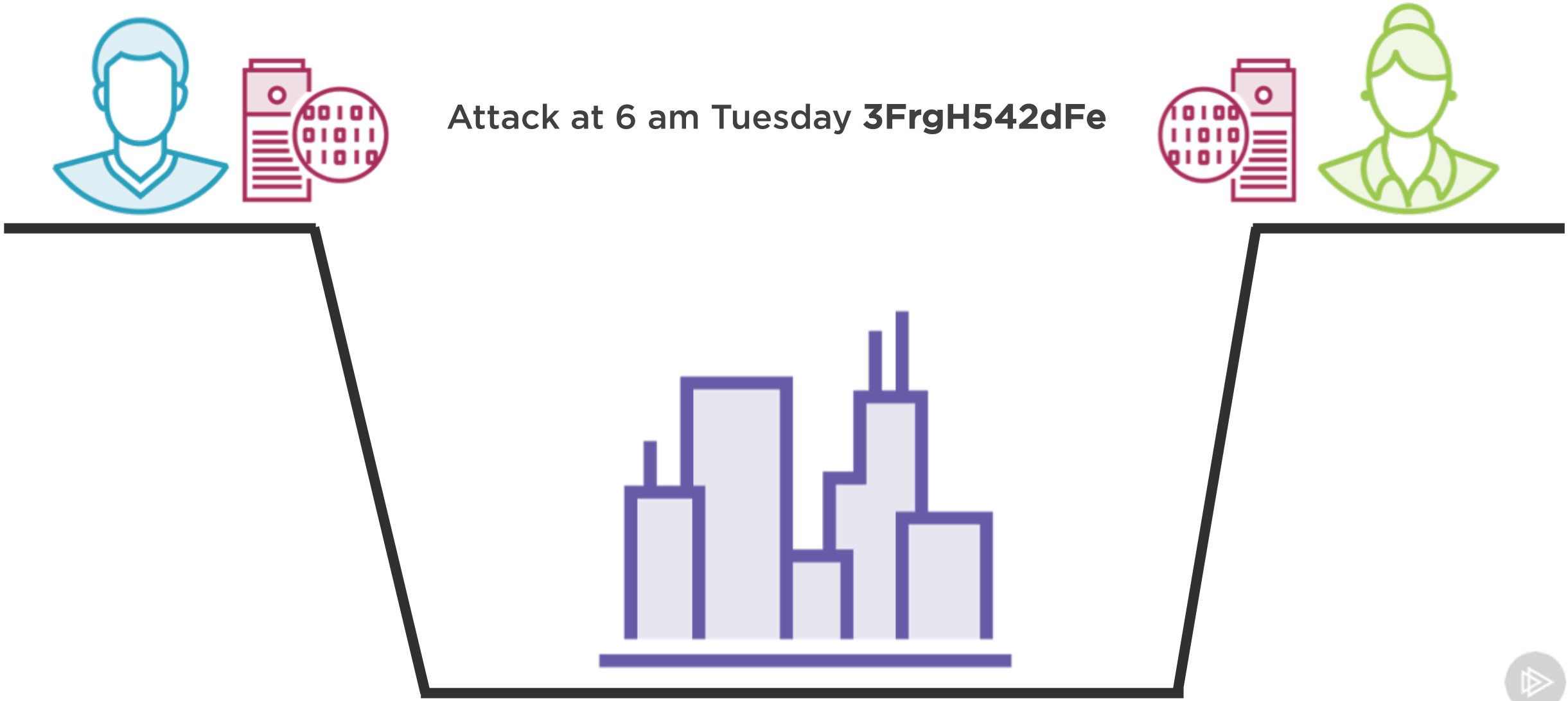

Attack at noon on Friday

Once a message has been written it should be immutable

Solving the Problem with Hashing

Solving the Problem with Hashing

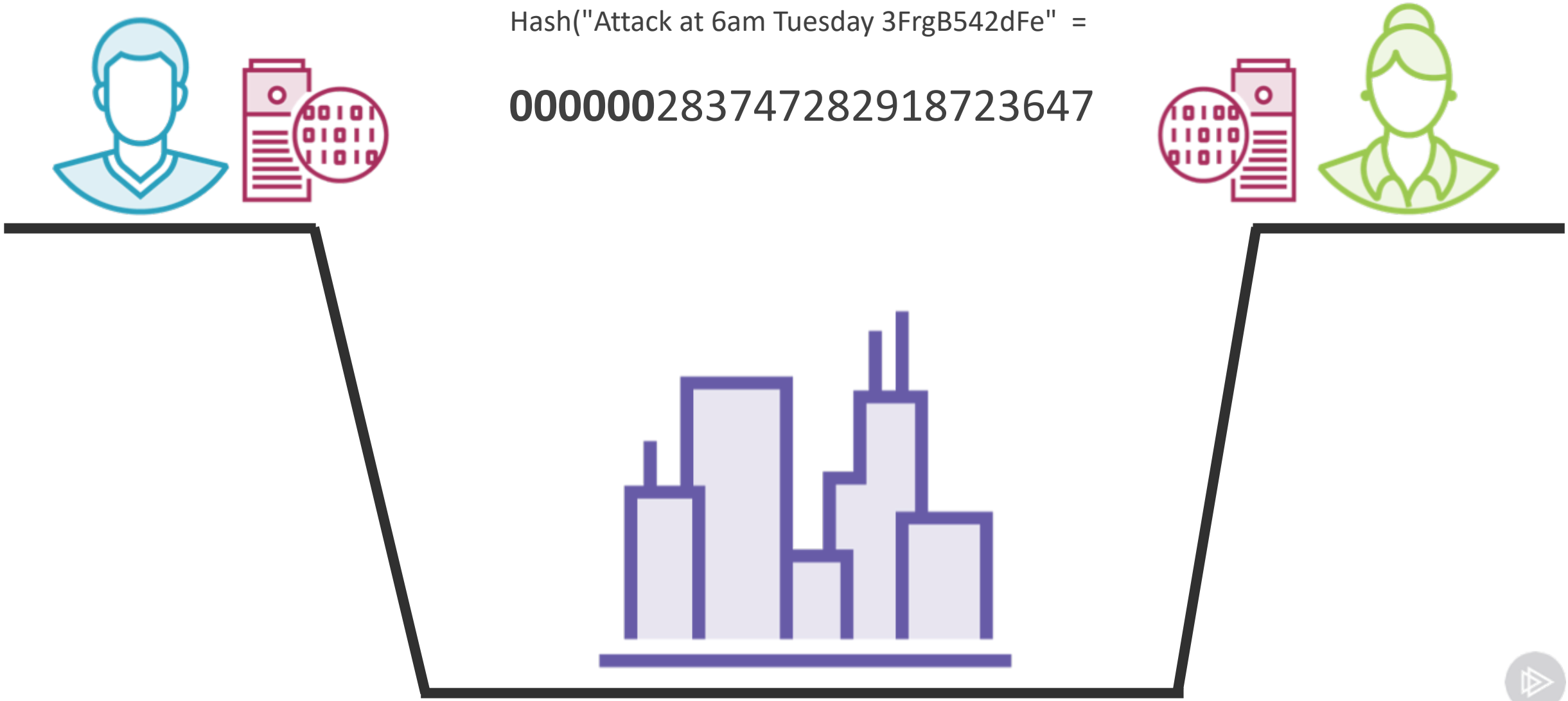
Solving the Problem with Hashing



Solving the Problem with Hashing

Hash("Attack at 6am Tuesday 3FrgB542dFe" =

00000028374728291872364 7



Solving the Problem with Hashing

Hash("Attack at 6am Tuesday 3FrgB542dFe" =
000000283747282918723647

Solving the Problem with Hashing

Hash("Attack at 6am Tuesday 0" =
3847239574932 5f79385s7394f573495b

Solving the Problem with Hashing

Hash("Attack at 6am Tuesday 1" =
096709458590240 9b09d900980c0980a

Solving the Problem with Hashing

Hash("Attack at 6am Tuesday 3FrgB542dFe" =
000000283747282918723647

Solving the Problem with Hashing

Expensive to calculate

Easy to verify

Solving the Problem with Hashing

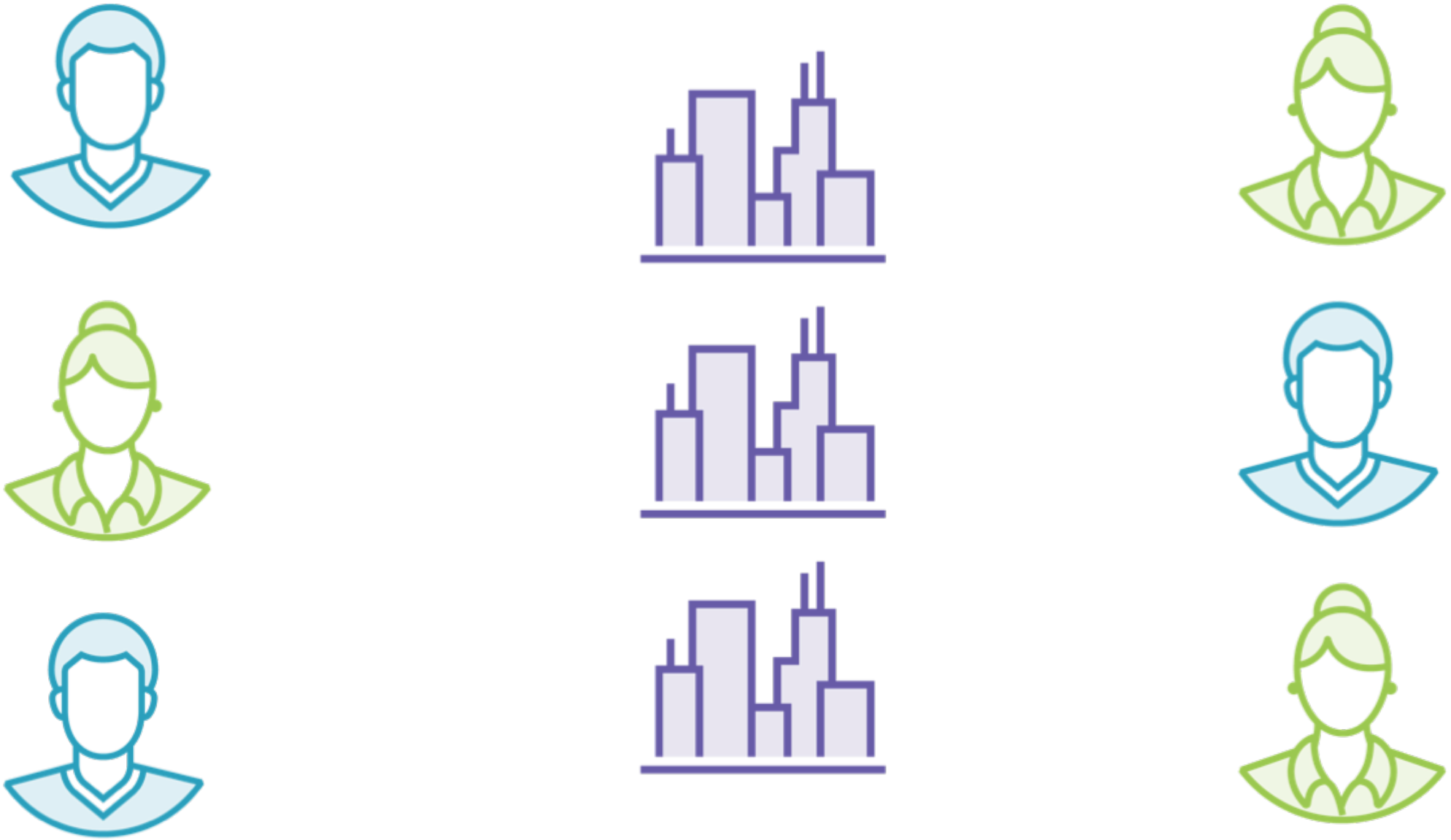
Changing the message Requires recalculation of the hash and nonce

Solving the Problem with Hashing

Proof of work

Solving the Problem with Hashing

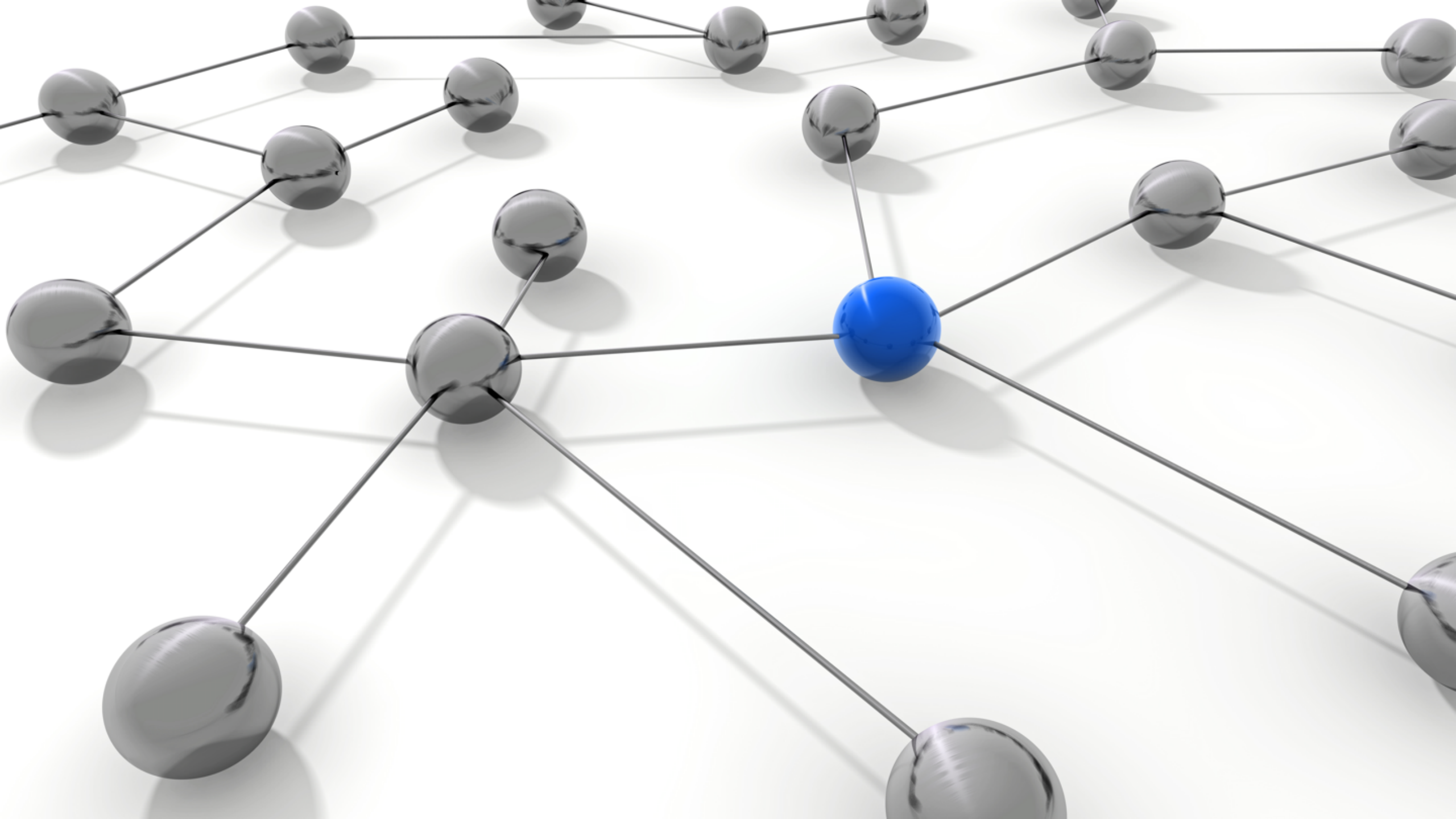
Strength in Numbers



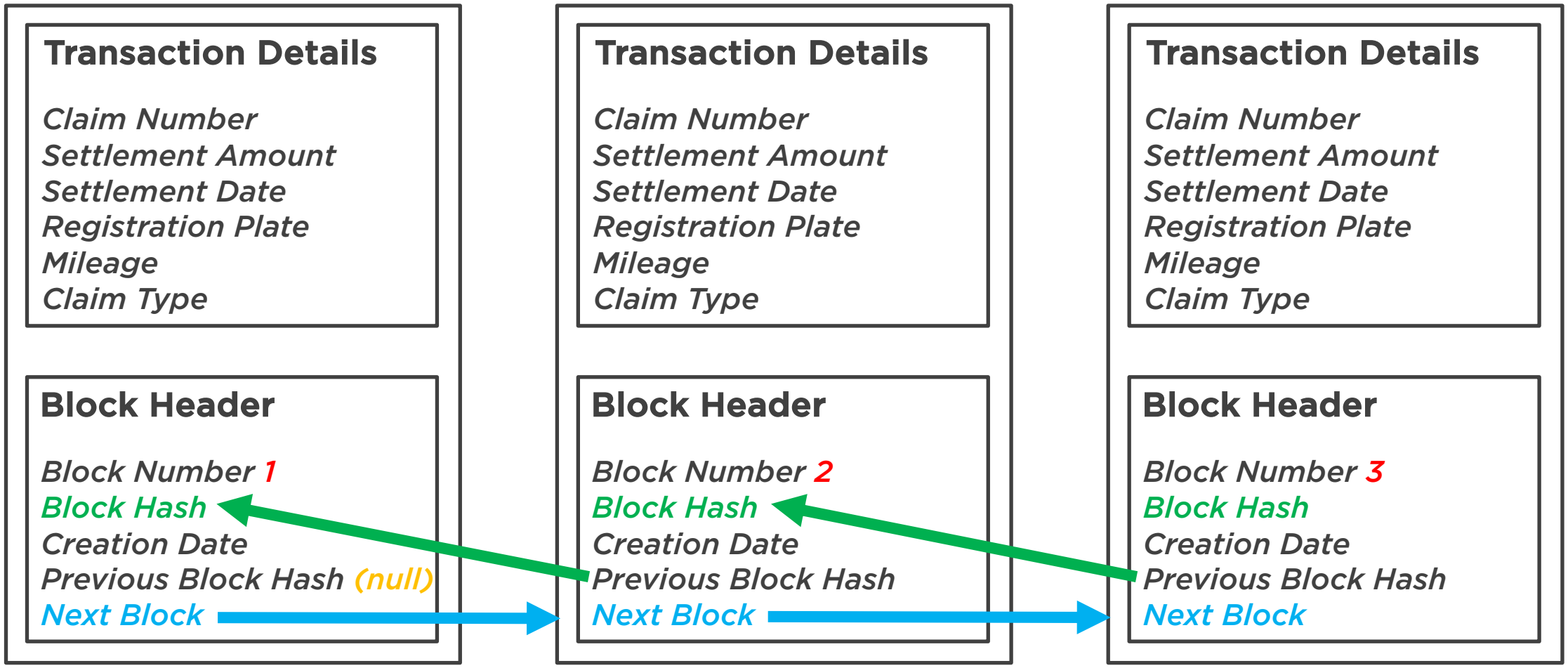
Hash("Attack at 6am Tuesday 3FrgB542dFe" = **0000000000**7282918723647

Hash("Attack at 6am Tuesday 3FrgB542dFe" = **0000000000**72829187236 47

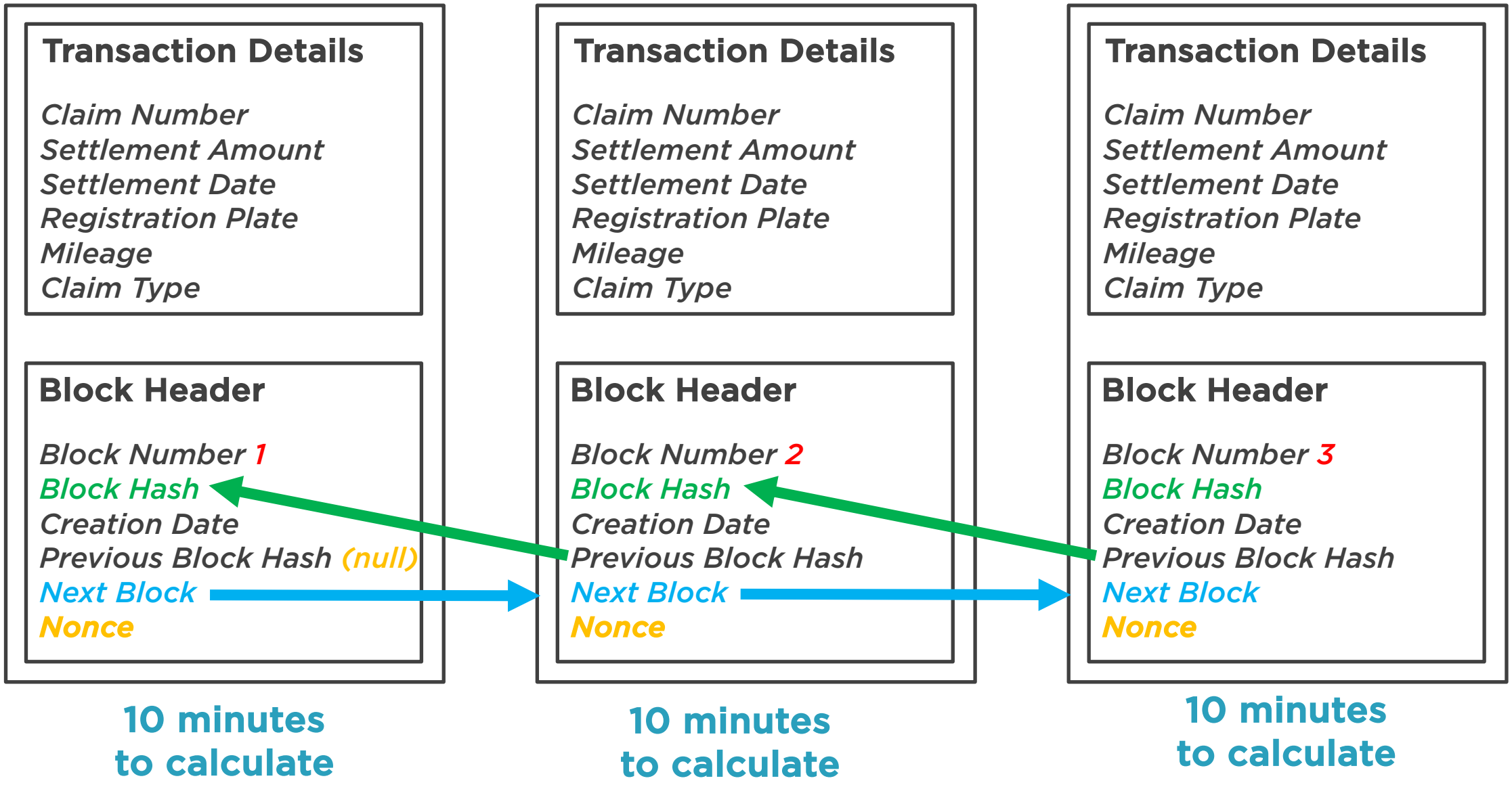
Hash("Attack at 6am Tuesday 3FrgB542dFe" = **0000000000**72829187236 47



Preventing Block Tampering



Preventing Block Tampering



Preventing Block Tampering

5000 blocks at 10 minutes per block

Preventing Block Tampering

5000 blocks at 10 minutes per block

833 hours effort

Preventing Block Tampering

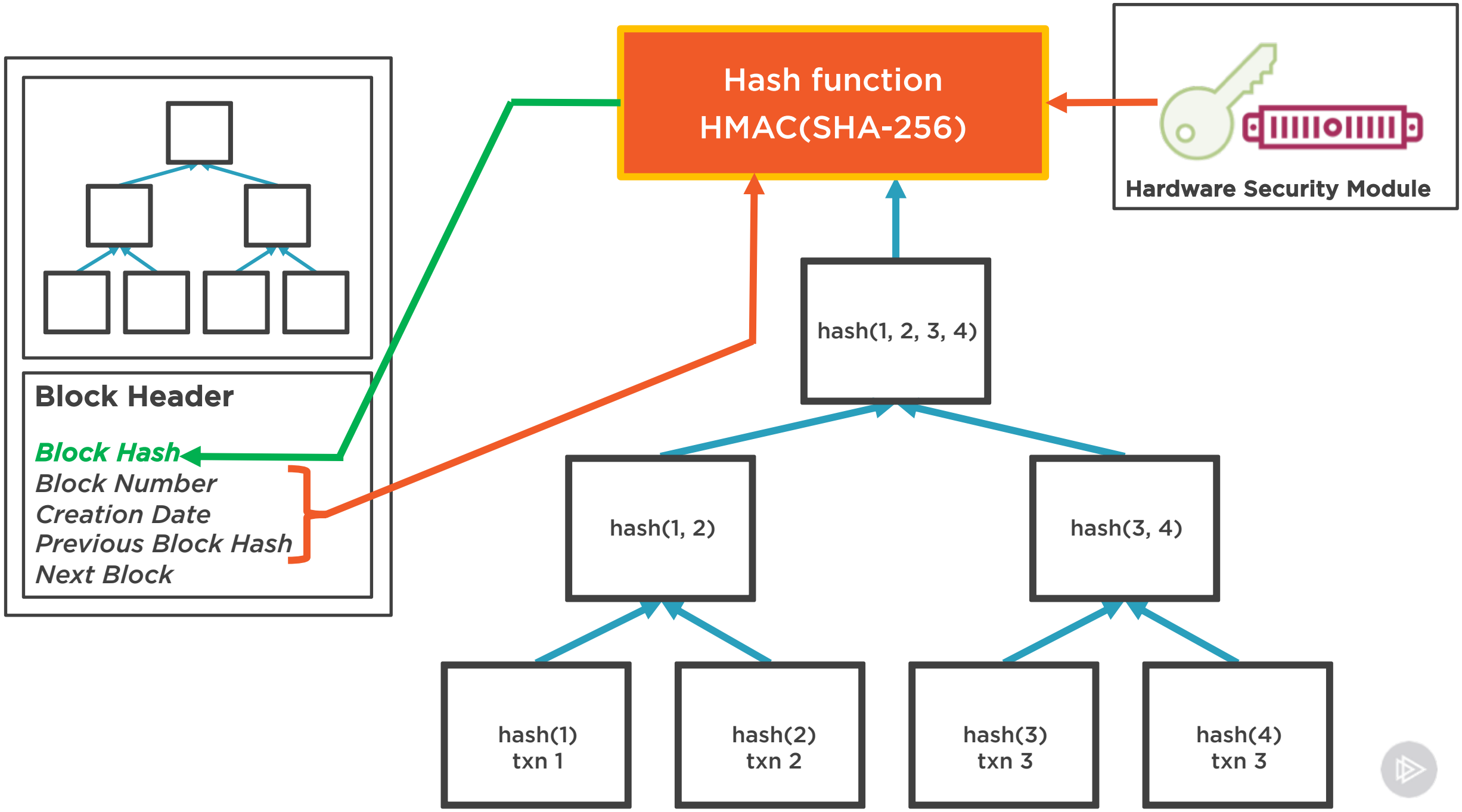
5000 blocks at 10 minutes per block

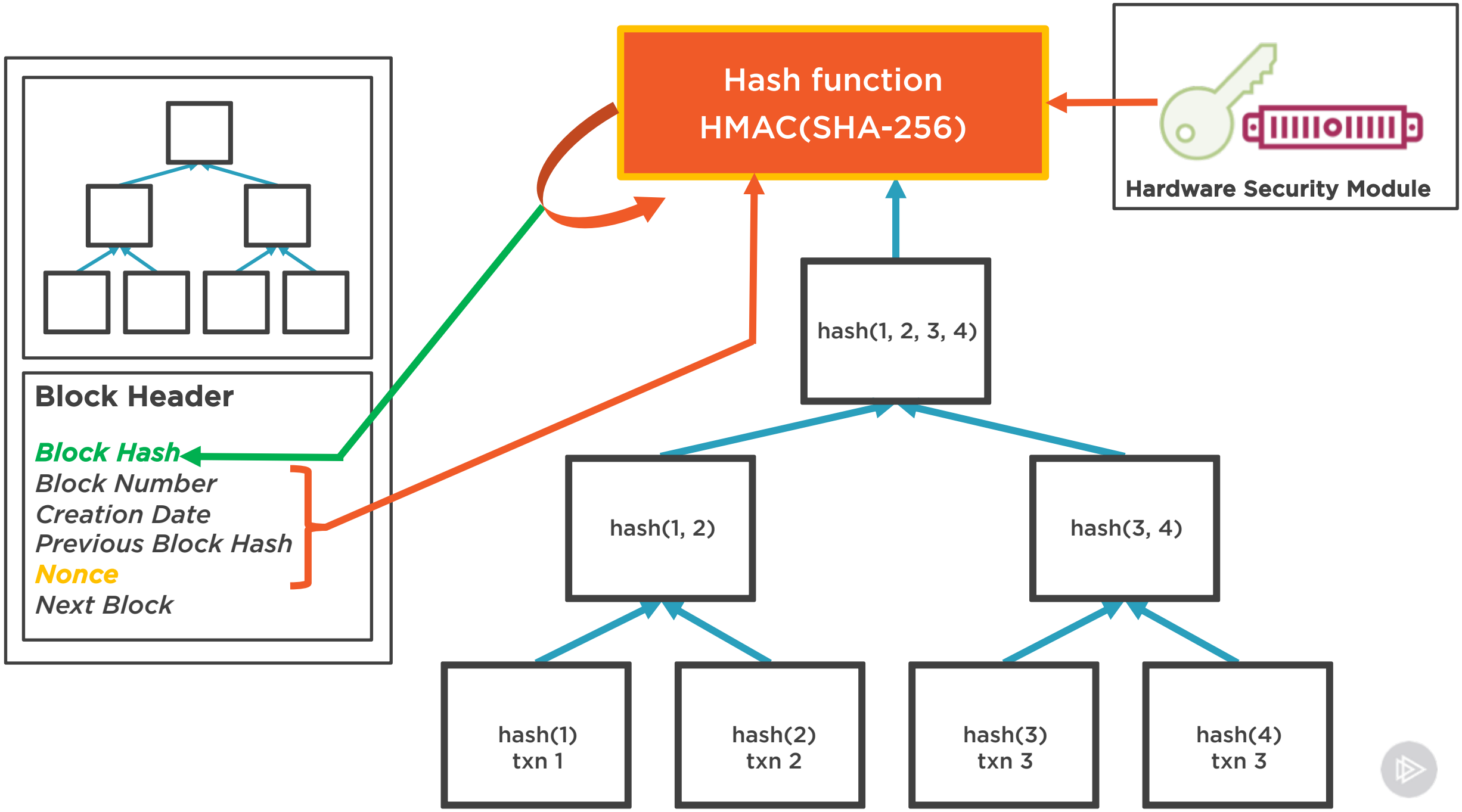
833 hours effort

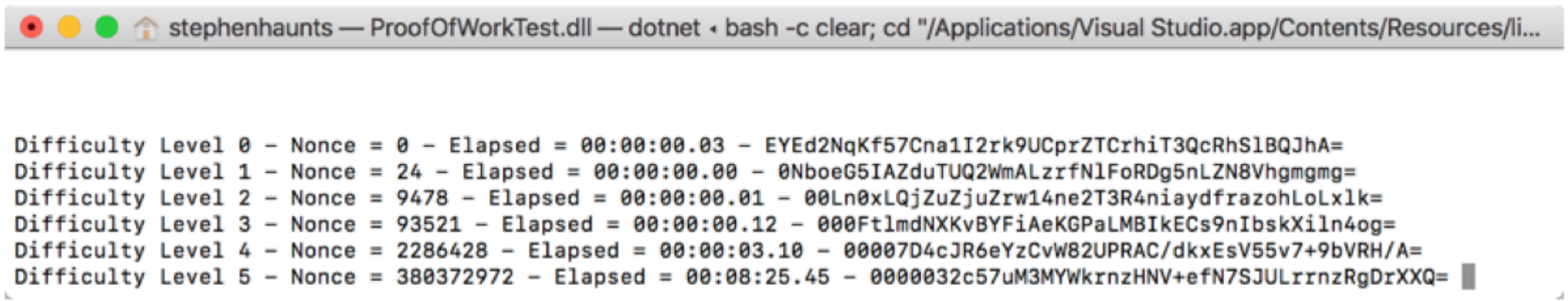
35 days

Demo

Proof of Work

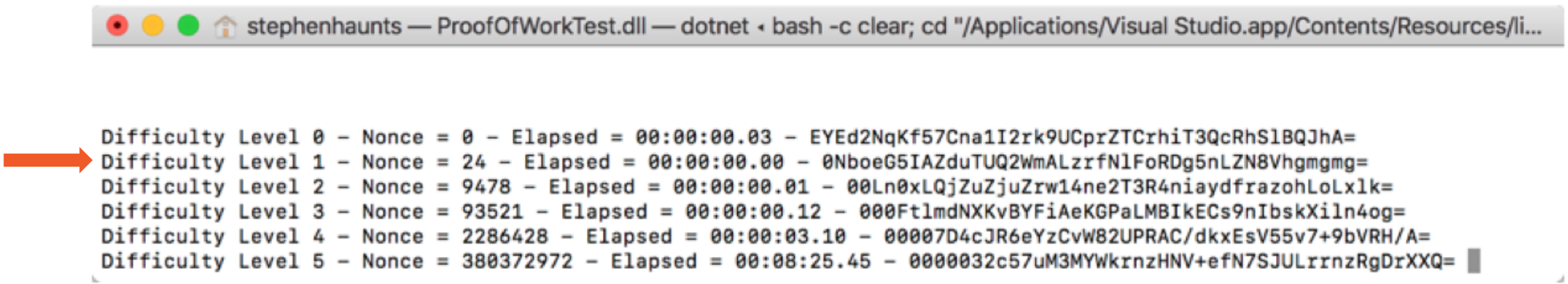

Hash function
HMAC(SHA-256)
Hardware Security Module
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Next Block
hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 3

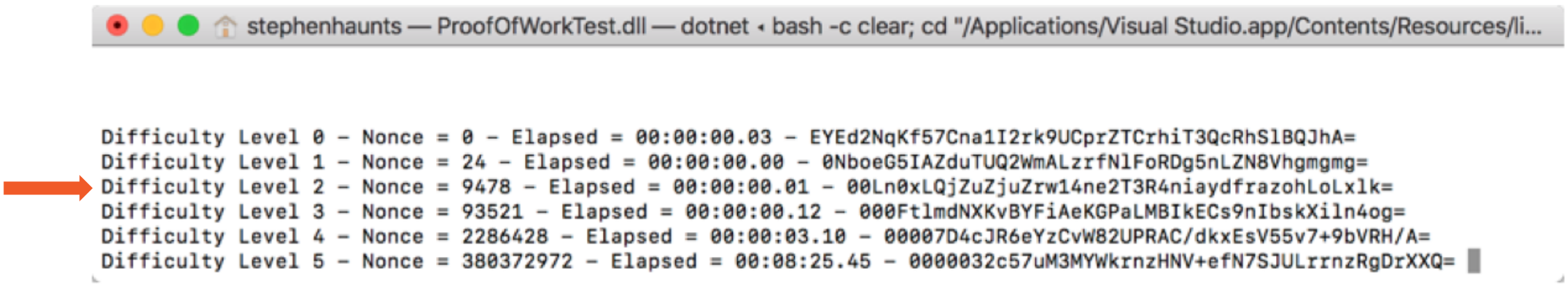

Hash function
HMAC(SHA-256)
Hardware Security Module
Block Header
Block Hash
Block Number
Creation Date
Previous Block Hash
Nonce
Next Block
hash(1, 2, 3, 4)
hash(1, 2)
hash(3, 4)
hash(1)
txn 1
hash(2)
txn 2
hash(3)
txn 3
hash(4)
txn 3

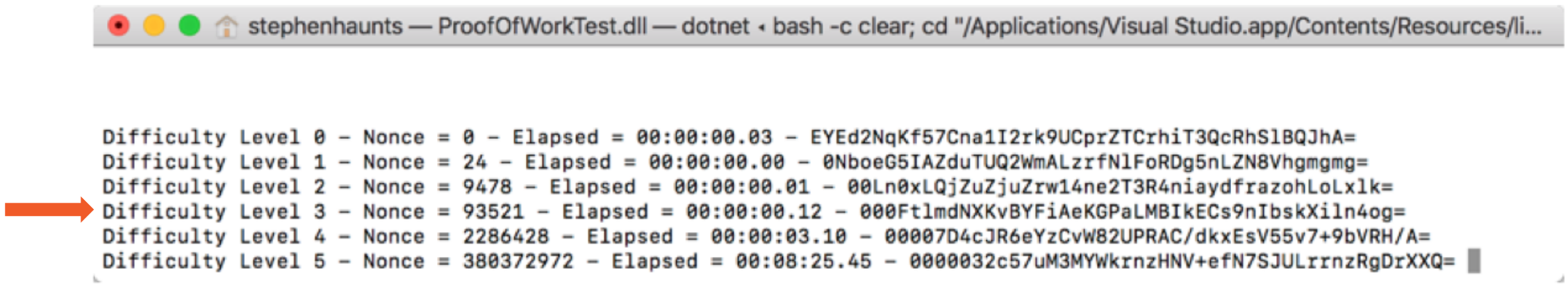

stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLx1k=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=

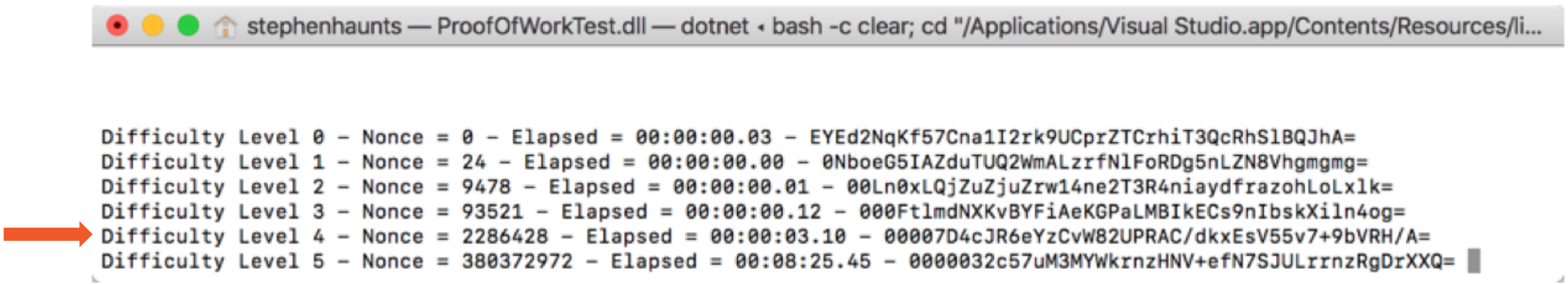
stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...

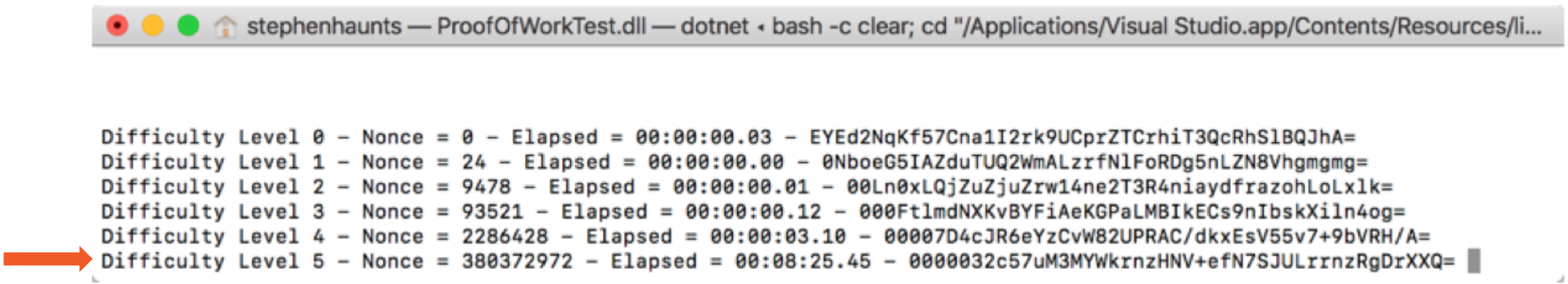
```
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLxlk=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=
```


stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLx1k=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=


stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLxlk=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=


stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLxlk=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=


stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLxlk=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=


stephenhaunts — ProofOfWorkTest.dll — dotnet ◂ bash -c clear; cd "/Applications/Visual Studio.app/Contents/Resources/li...
Difficulty Level 0 - Nonce = 0 - Elapsed = 00:00:00.03 - EYEd2NqKf57Cna1I2rk9UCprZTCrhiT3QcRhSlBQJhA=
Difficulty Level 1 - Nonce = 24 - Elapsed = 00:00:00.00 - 0NboeG5IAZduTUQ2WmALzrfNlFoRDg5nLZN8Vhgmgmg=
Difficulty Level 2 - Nonce = 9478 - Elapsed = 00:00:00.01 - 00Ln0xLQjZuZjuZrw14ne2T3R4niaydfrazohLoLxlk=
Difficulty Level 3 - Nonce = 93521 - Elapsed = 00:00:00.12 - 000FtlmdNXKvBYFiAeKGPaLMBIkECs9nIbskXiln4og=
Difficulty Level 4 - Nonce = 2286428 - Elapsed = 00:00:03.10 - 00007D4cJR6eYzCvW82UPRAC/dkxEsV55v7+9bVRH/A=
Difficulty Level 5 - Nonce = 380372972 - Elapsed = 00:08:25.45 - 0000032c57uM3MYWkrnzHNV+efN7SJULrrnzRgDrXXQ=

Demo

Integrating Proof of Work

Summary

Our Blockchain was not immutable

Byzantines Generals' Problem

Proof of work

Computationally expensive

Uses a lot of electricity

Proof of stake