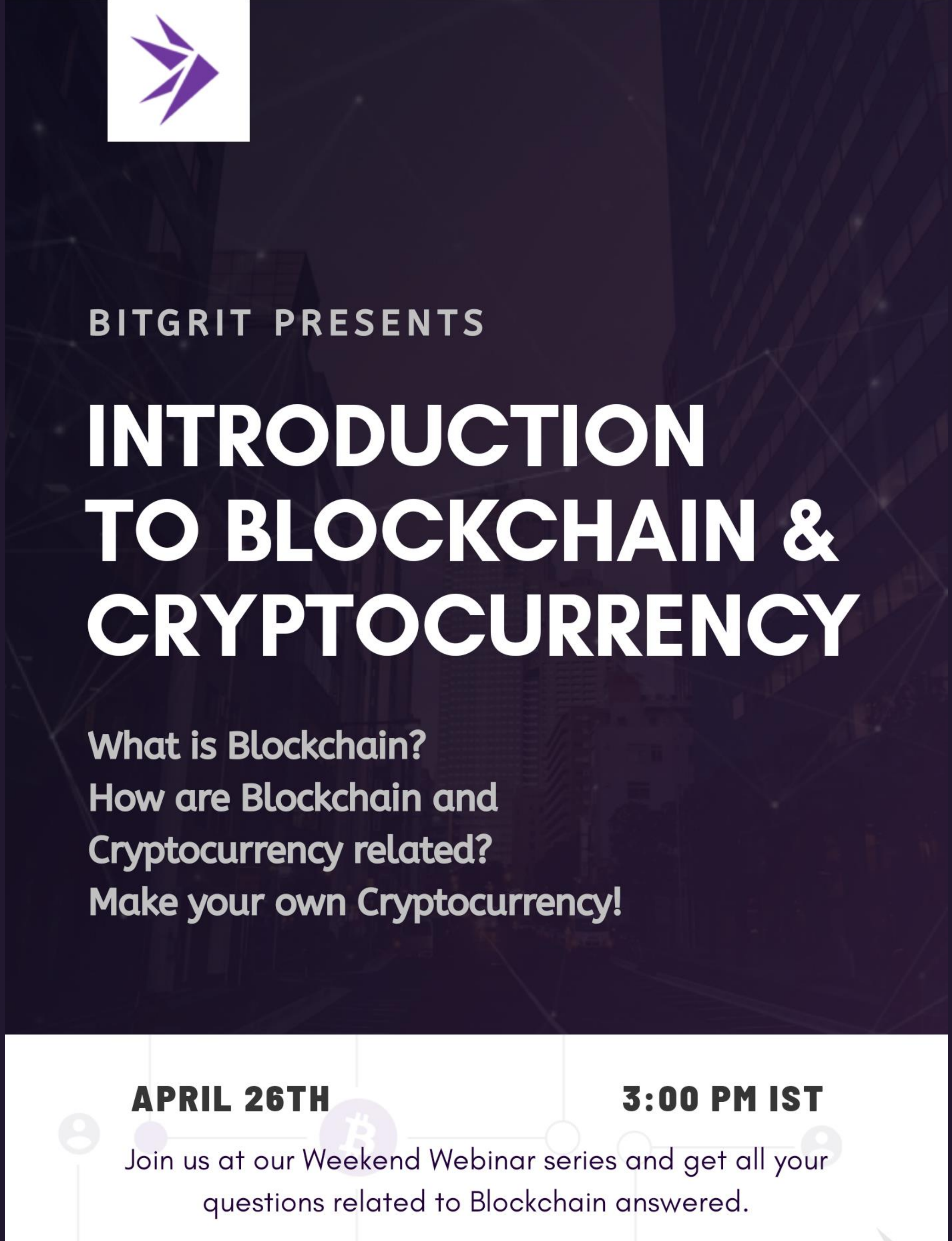


BITGRIT PRESENTS

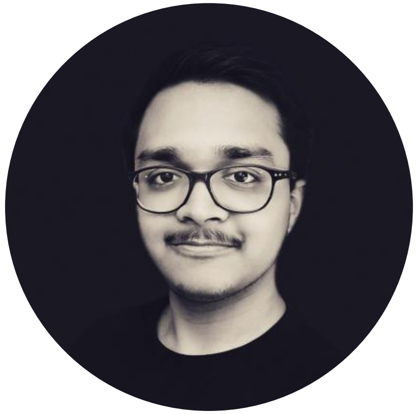
INTRODUCTION TO BLOCKCHAIN & CRYPTOCURRENCY

What is Blockchain?
How are Blockchain and Cryptocurrency related?
Make your own Cryptocurrency!

APRIL 26TH **3:00 PM IST**

Join us at our Weekend Webinar series and get all your questions related to Blockchain answered.

bit.ly/bitgritmeetup



Introduction to

Blockchain & Cryptocurrency

Ritom Gupta

bitgrit

Campus Ambassador
MIT-WPU Pune

What is Blockchain?

Security

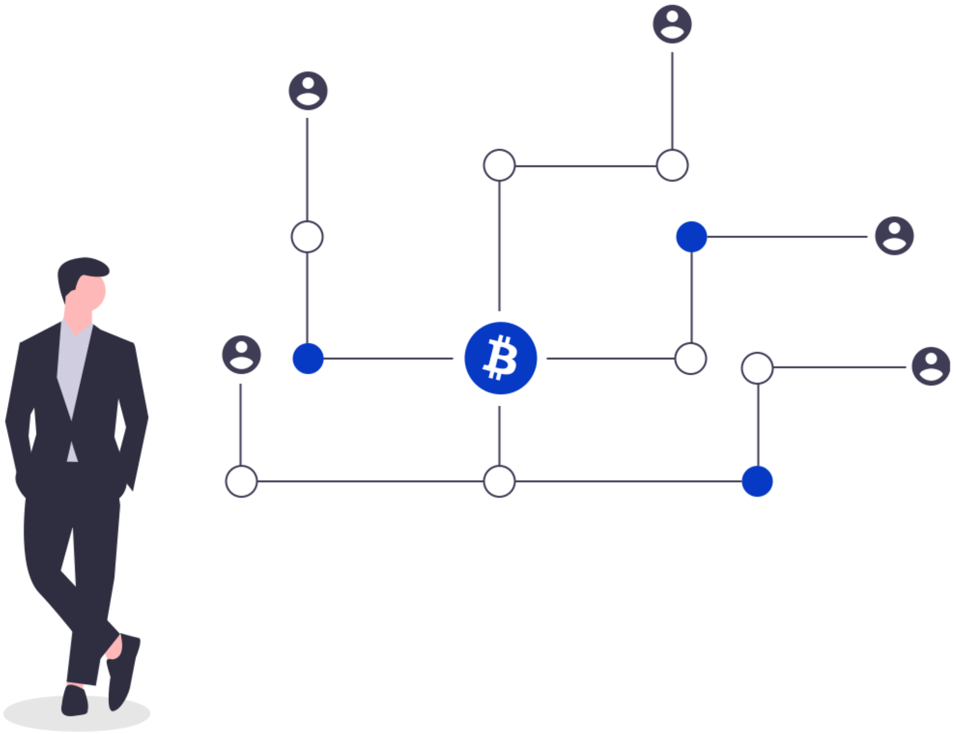
Cryptocurrency

Proof of Work

bitgrit

What is Blockchain?

- Data structure which holds transactional records
- Not controlled by any single authority
- Tamper-proof records
- Need of consensus



bitgrit

What is Blockchain?

Security

Cryptocurrency

Proof of Work

bitgrit

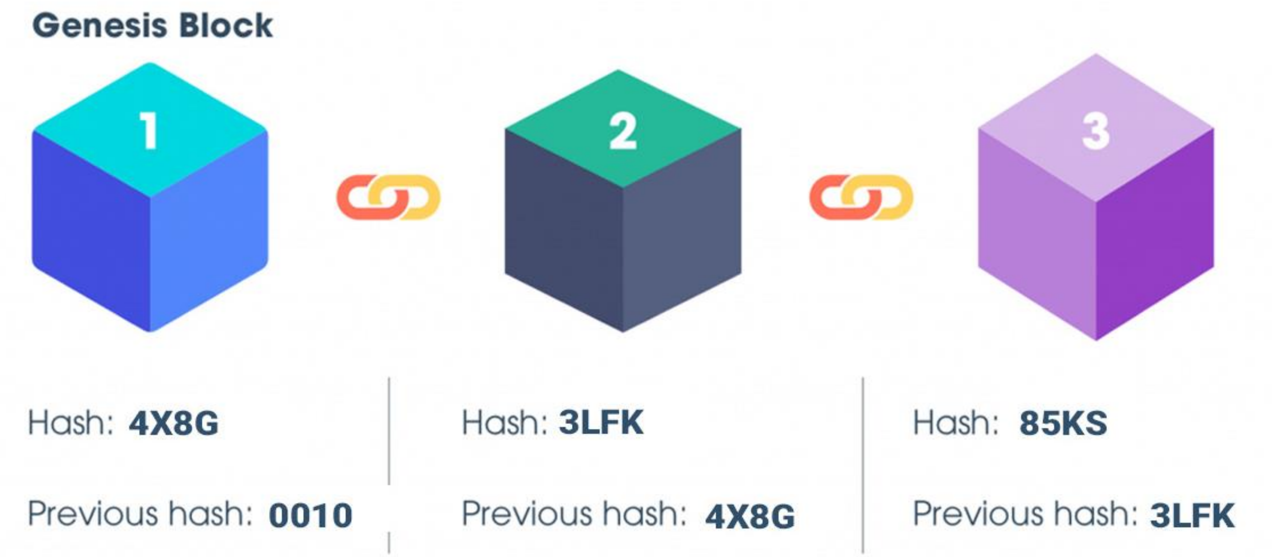
Security

1 Cryptographic fingerprint

2 Consensus Protocol

3 Hashes link back

4 Not attack-proof



bitgrit

https://blockchaindemo.io/

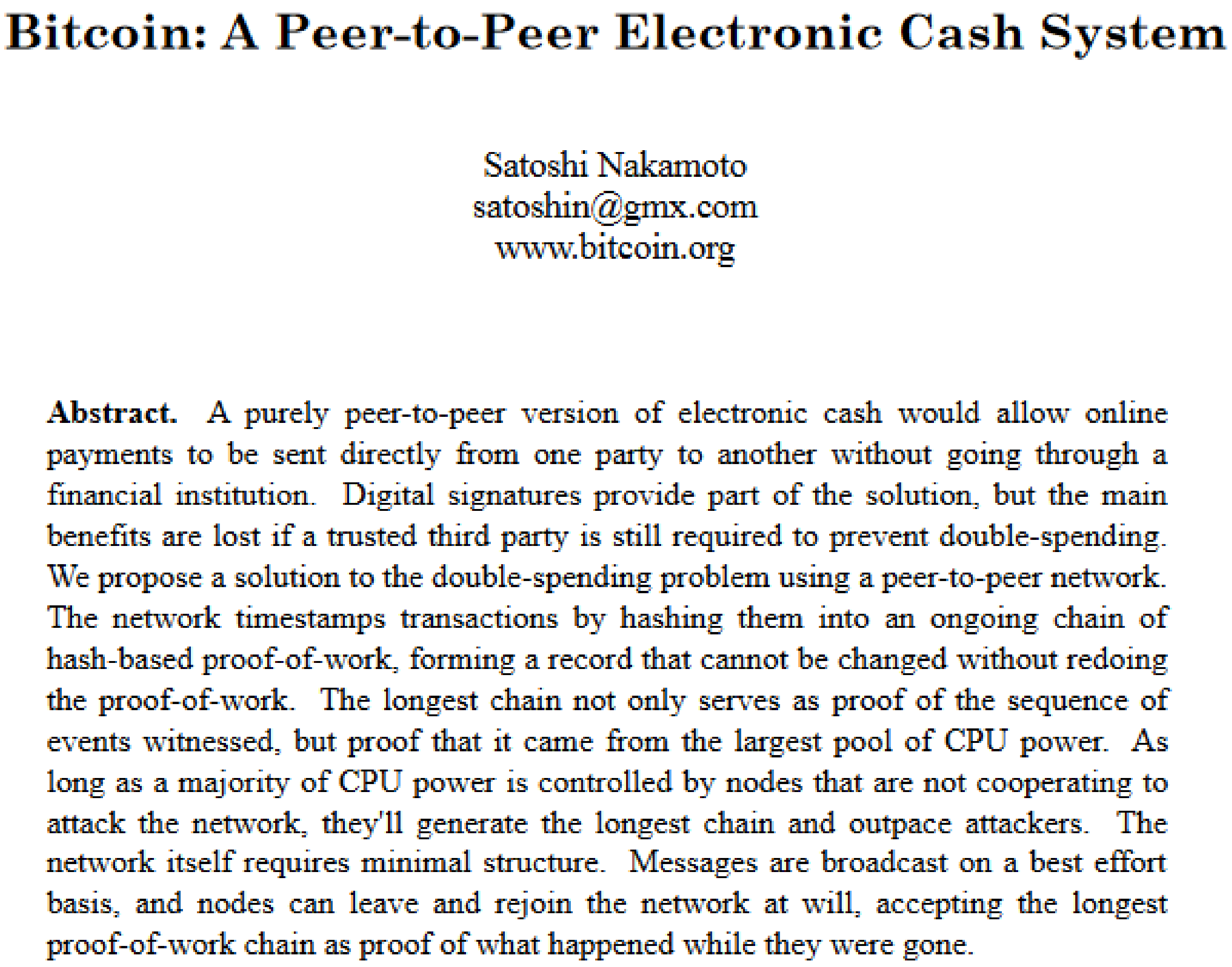
What is Blockchain?

Security

Cryptocurrency

Proof of Work

bitgrit



Bitcoin: A Peer-to-Peer Electronic Cash System

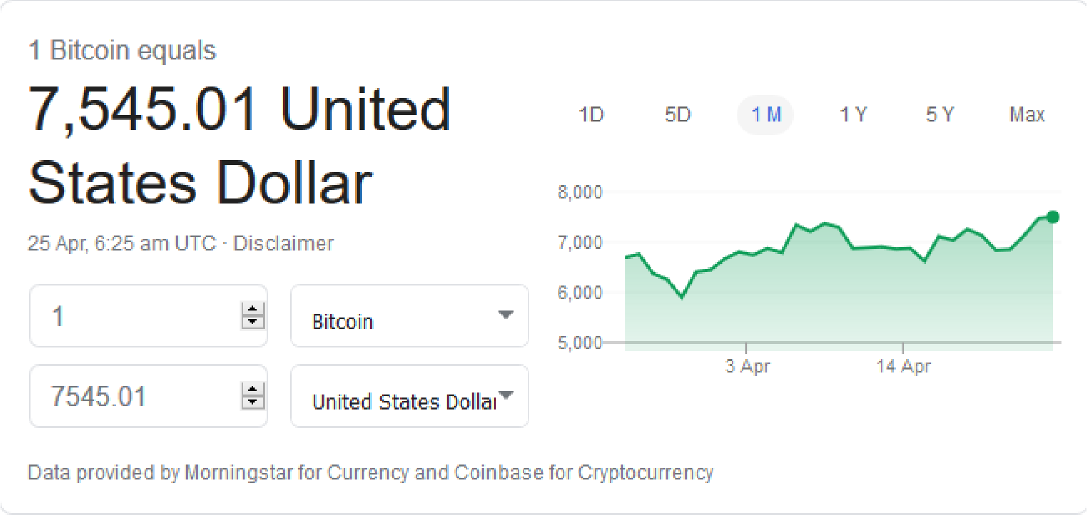
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Source: bitcoin.org
https://bitcoin.org/bitcoin.pdf

Cryptocurrency

1. Digital asset, medium of exchange
2. Use decentralized control
3. Over 6,000 altcoins created since Bitcoin
4. Hottest, yet high-risk investment



1 Bitcoin equals

7,545.01 United States Dollar

25 Apr, 6:25 am UTC · Disclaimer

1	Bitcoin
7545.01	United States Dollar

Data provided by Morningstar for Currency and Coinbase for Cryptocurrency

6 conditions

No central authority

Overview of units and ownership

New units, origin and ownership

Cryptographic proof of ownership

Transactions change ownership

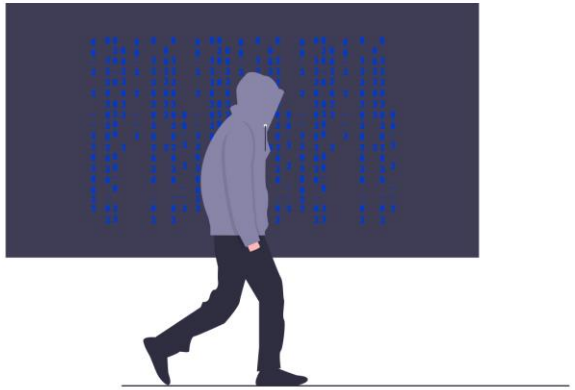
At most 1 ownership changed at a time

What is Blockchain?

Security

Cryptocurrency

Proof of Work



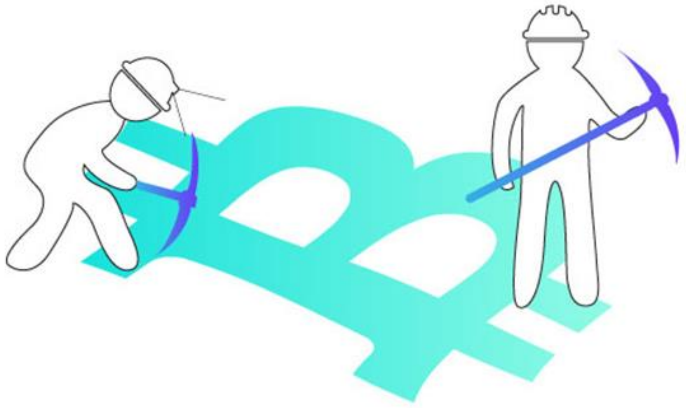
Proof of Work

1 Original consensus algorithm

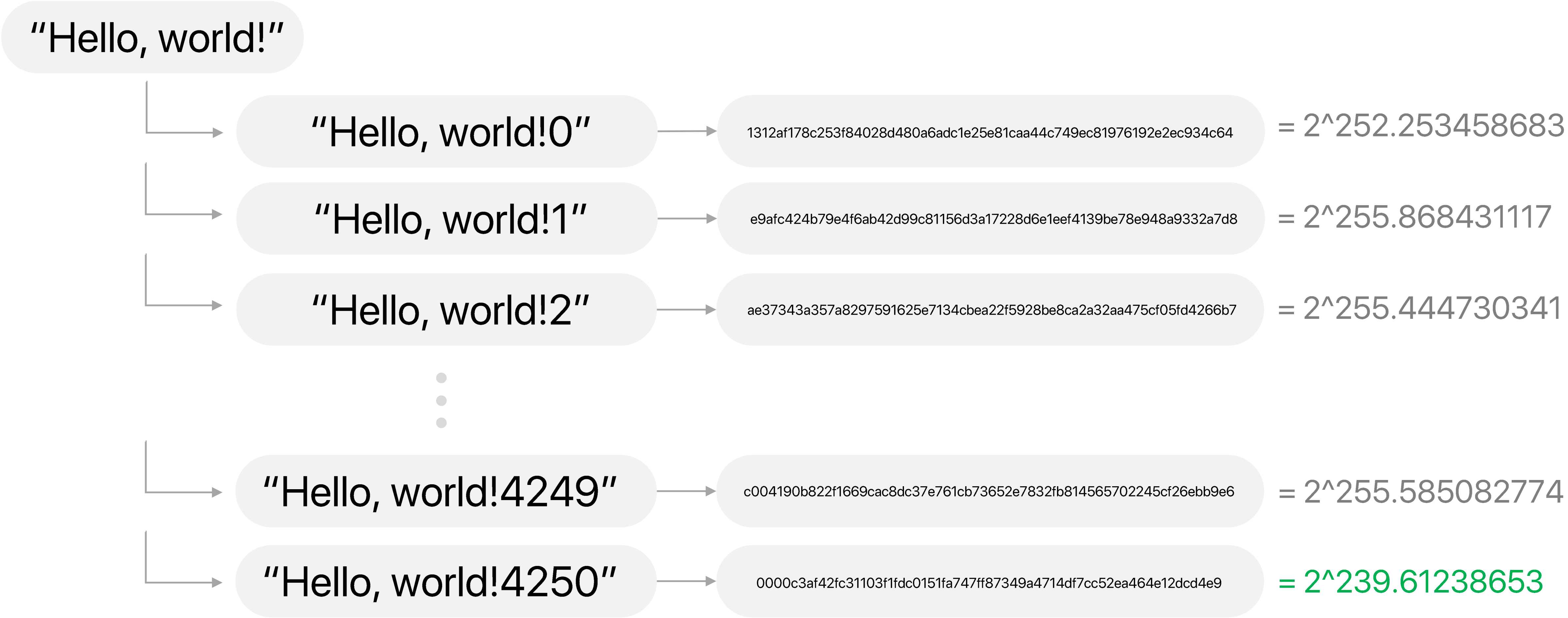
2 Confirms transactions, produces blocks

3 Defence from DoS attacks

4 Prone to 51% attack, useless computations



Example



"Hello, world!"

"Hello, world!0" → 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64 = 2^252.253458683

"Hello, world!1" → e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8 = 2^255.868431117

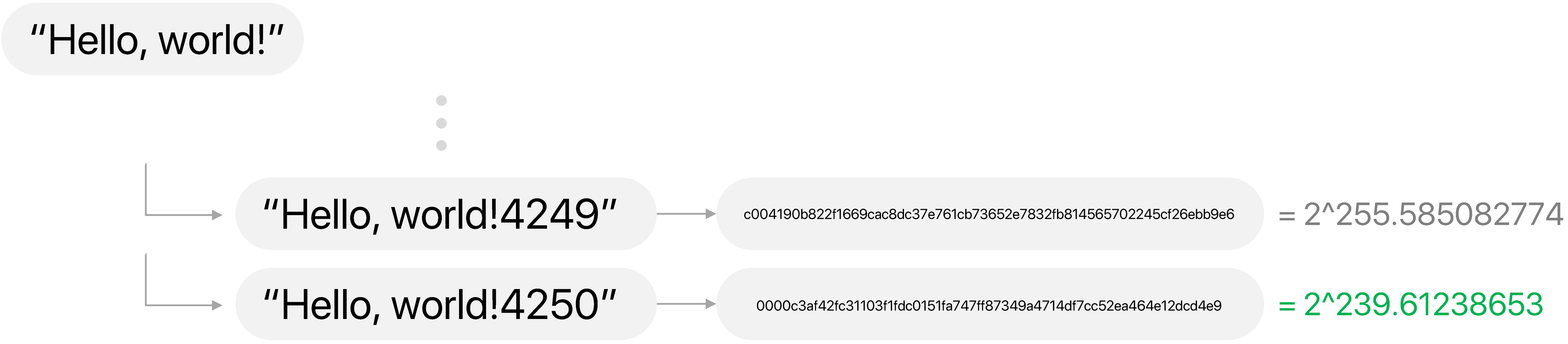
"Hello, world!2" → ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7 = 2^255.444730341

⋮

"Hello, world!4249" → c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6 = 2^255.585082774

"Hello, world!4250" → 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 = 2^239.61238653

Example



"Hello, world!"

"Hello, world!4249" → c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6 = 2^255.585082774

"Hello, world!4250" → 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 = 2^239.61238653

"Hello, world!"

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

on Sun, 26 Oct 2017 19:53:20 GMT

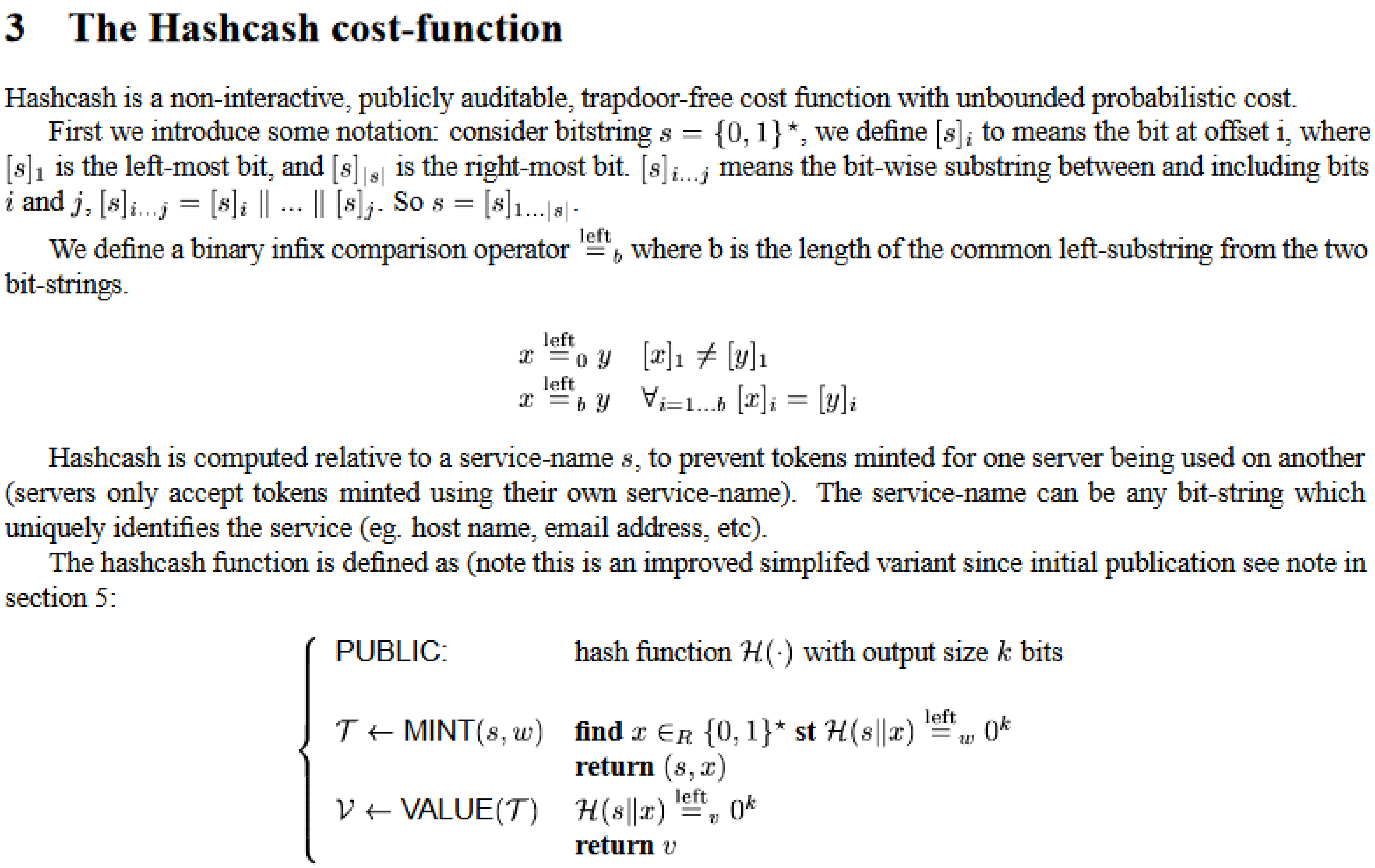
Traditional Proof of Work

1 Hashcash with double iterated SHA256

2 Hashcash with scrypt internal hash

3 Momentum birthday collision

4 Cuckoo Cycle https://github.com/tromp/cuckoo



3 The Hashcash cost-function

Hashcash is a non-interactive, publicly auditable, trapdoor-free cost function with unbounded probabilistic cost.

First we introduce some notation: consider bitstring $s = \{0,1\}^\star$, we define $[s]_i$ to means the bit at offset i, where $[s]_1$ is the left-most bit, and $[s]_{|s|}$ is the right-most bit. $[s]_{i\ldots j}$ means the bit-wise substring between and including bits i and j, $[s]_{i\ldots j} = [s]_i \parallel \ldots \parallel [s]_j$. So $s = [s]_{1\ldots|s|}$.

We define a binary infix comparison operator $\overset{\text{left}}{=}_b$ where b is the length of the common left-substring from the two bit-strings.

$$\begin{array}{ll} x \overset{\text{left}}{=}_0 y & [x]_1 \neq [y]_1 \\ x \overset{\text{left}}{=}_b y & \forall_{i=1\ldots b}\ [x]_i = [y]_i \end{array}$$

Hashcash is computed relative to a service-name s, to prevent tokens minted for one server being used on another (servers only accept tokens minted using their own service-name). The service-name can be any bit-string which uniquely identifies the service (eg. host name, email address, etc).

The hashcash function is defined as (note this is an improved simplifed variant since initial publication see note in section 5:

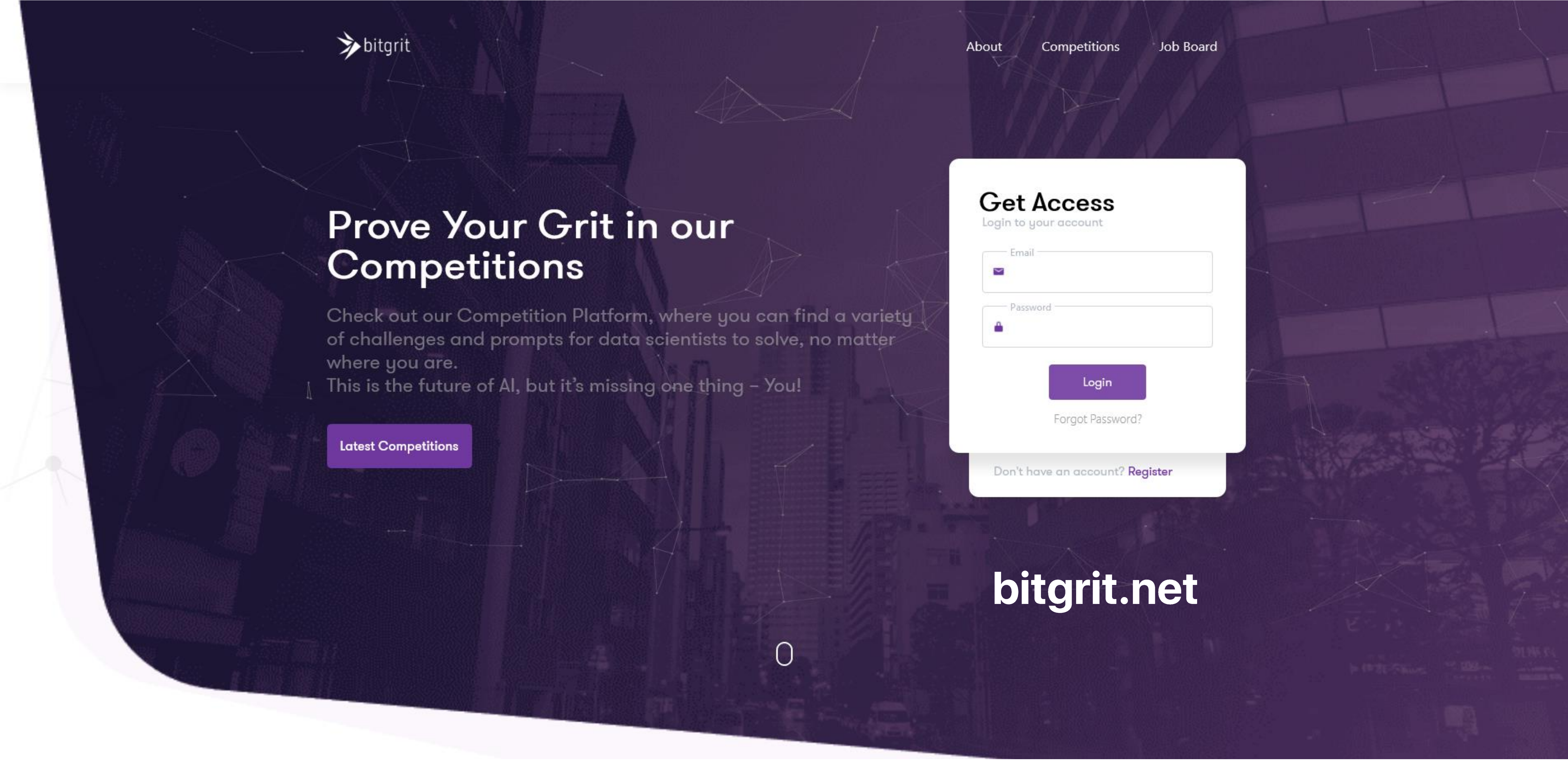
$$\left\{ \begin{array}{ll} \text{PUBLIC:} & \text{hash function } \mathcal{H}(\cdot) \text{ with output size } k \text{ bits} \\ & \\ \mathcal{T} \leftarrow \text{MINT}(s, w) & \textbf{find } x \in_R \{0,1\}^\star \textbf{ st } \mathcal{H}(s \| x) \overset{\text{left}}{=}_w 0^k \\ & \textbf{return } (s, x) \\ \mathcal{V} \leftarrow \text{VALUE}(\mathcal{T}) & \mathcal{H}(s \| x) \overset{\text{left}}{=}_v 0^k \\ & \textbf{return } v \end{array} \right.$$

Source: hashcash.org

http://www.hashcash.org/papers/hashcash.pdf

bitgrit and blockchain?

bitgrit



Prove Your Grit in our Competitions

Check out our Competition Platform, where you can find a variety of challenges and prompts for data scientists to solve, no matter where you are.
This is the future of AI, but it's missing one thing – You!

Get Access
Login to your account

Email

Password

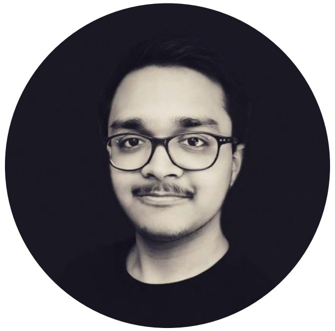
Don't have an account? Register

bitgrit.net

bitgrit

White Paper

Talent Resume Form



Ritom Gupta

ritomgupta@thescriptgroup.in

/rittmang

/rittmang

/monsieur_rittman

/in/ritomgupta

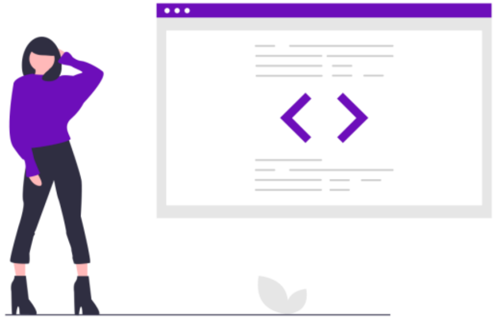
https://rightonrittman.in/presentations/bitgrit-BlockchainCrypto.pdf

Questions?

in chat box

bitgrit

Make your own cryptocoin



https://github.com/aniket-spidey/bitgrit-webinar

bitgrit