Unit 5: Cryptographic Puzzles and Mining

SI 486I: Randomized and Blockchain Technology

Assoc. Prof. Daniel S. Roche
United States Naval Academy

Spring 2022

Goals of this unit

- Know why and how each new block must solve a cryptographic "puzzle"
- Understand what properties of puzzles make them more or less suitable for proof of work
- Follow the details of the hash-based puzzle used in Bitcoin
- Understand how the puzzle difficulty and block reward are adjusted over time, and for what reasons
- Know about how major mining operations work in the real world

Recall: Blockchain structure so far

(What operations are fast, slow, and impossible?)

Slowing down block creation

Two key reasons we want mining to be slow:

- Economic reason:
- Technical reason:

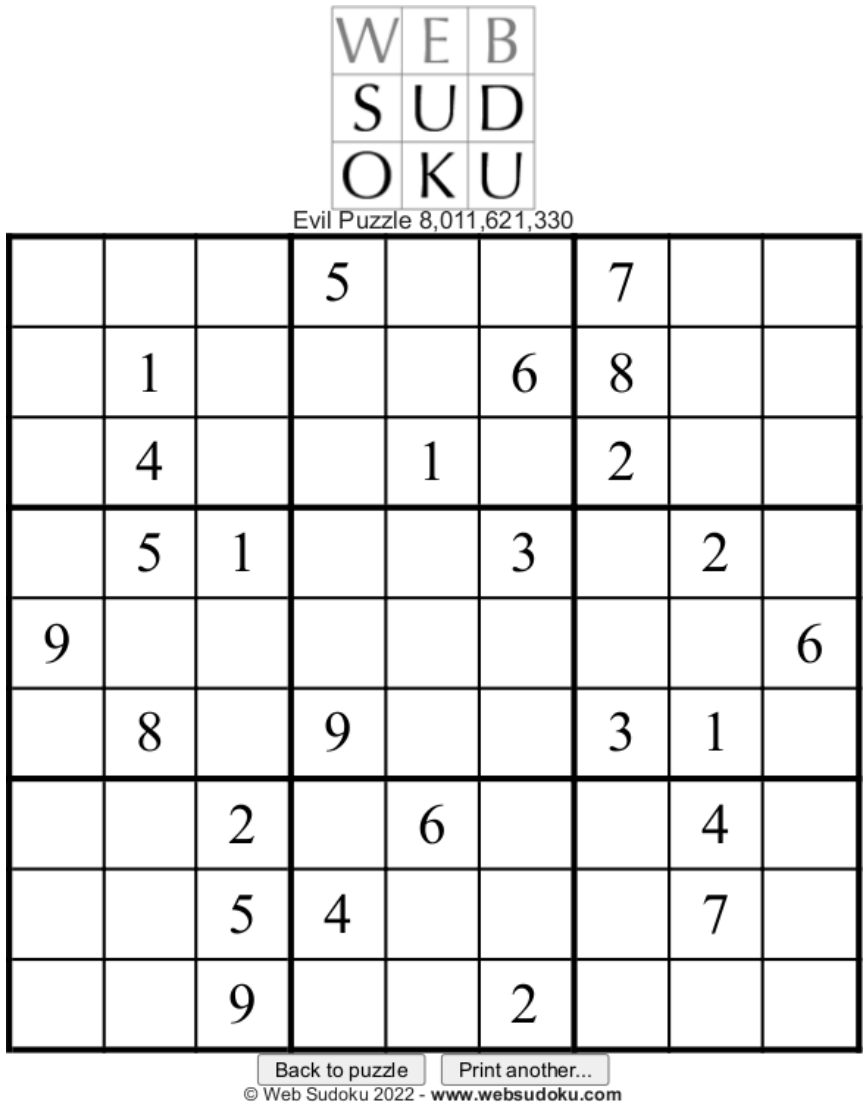
Cryptographic puzzle

Properties of a good cryptographic puzzle for mining:

- Easily generated based on a "seed"
- Easy to verify a proposed solution
- Difficulty to solve is scalable
- Everyone has perfect information (no secrets)
- No better way to solve than guess & check

Analogy: Sudoku

Is this a good cryptographic puzzle?



			5			7		
	1				6	8		
	4			1		2		
	5	1			3		2	
9								6
	8		9			3	1	
		2		6			4	
		5	4				7	
		9			2			

Analogy: Numismatics

Precursor: Hashcash and spam fighting

Credit:

- Cynthia Dwork & Moni Naor, CRYPTO 1992
- Adam Back, "Hashcash", 2002

Overall idea:

- Email senders must attach a valid hashcash stamp to the header
- Stamp contains a random nonce and counter, as well as the date, time, and recipient
- Validity: SHA-1 hash of stamp must start with k leading zero bits
- "Price": Number of required 0 bits k

This is called a **proof of work**.

Bitcoin Proof of Work

- Each block has a target number
- Hash of the next block must be below this target
- Each block includes a nonce and counter
  (Keep incrementing until hash is below the target)

Target adjustment

Nakamoto's goal: new Bitcoin block every $\approx$10 minutes

How to enforce this timing?

Block rewards

Mining a block earns some currency (why do this?)

- Original Bitcoin block reward: 50 BTC
- Decreases by half every 210000 blocks ($\approx$4 years)
- Therefore:
- Current block reward: 6.25 BTC