Why?
- Started doing some research on Bitcoin
  - What is it?
  - How can you make money?
- Stumbled across Bitcoin mining calculators and …
- Calculators resembled what we do today for enterprise capacity planning
Baseline
Use Diff Change = NO
Result
Profitable in 4 months

Scenario #1
Use Diff Change = YES
Result
Never Profitable
Bitcoin Mining & The Capacity Planning Stack

Agenda
- Introduction to Bitcoin
- Bitcoin Mining
- Mining & the Stack
- Wrap-up

What is Bitcoin?
- Ideas in a white paper by Satoshi Nakamoto in 2008
  - “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Digital/crypto currency created in 2009
- Operated by a decentralized authority, unlike government-issued currencies
- Not backed by any country's central bank or government
- A decentralized electronic payment scheme based on cryptography
- Nothing is hidden:
  - Source code is viewable by everyone
  - Every transaction performed since its inception on January 3, 2009 is publicly available
**Timeline - Satoshi Nakamoto**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 2008</td>
<td>The domain name bitcoin.org is registered</td>
</tr>
<tr>
<td>Oct 2008</td>
<td>Satoshi Nakamoto published paper titled &quot;Bitcoin: A Peer-to-Peer</td>
</tr>
<tr>
<td></td>
<td>Electronic Cash System&quot; on the Cryptography mailing list at</td>
</tr>
<tr>
<td></td>
<td>metzdowd.com</td>
</tr>
<tr>
<td>Jan 3, 2009</td>
<td>The first Bitcoin block is mined - Genesis Block (#0)</td>
</tr>
<tr>
<td></td>
<td>Created the first 50 BTC</td>
</tr>
<tr>
<td>Jan 8, 2009</td>
<td>The first version of the Bitcoin software is announced on the</td>
</tr>
<tr>
<td></td>
<td>Cryptography mailing list</td>
</tr>
<tr>
<td>Jan 9, 2009</td>
<td>Block #1 is mined, and Bitcoin mining commences in earnest</td>
</tr>
<tr>
<td>Dec 2010</td>
<td>Satoshi handed the leading position to Gavin Andresen and ceased all</td>
</tr>
<tr>
<td></td>
<td>involvement in the project</td>
</tr>
<tr>
<td>April 2011</td>
<td>Satoshi emailed a software developer with &quot;I've moved on to other</td>
</tr>
<tr>
<td></td>
<td>things. It's in good hands with Gavin and everyone&quot;</td>
</tr>
<tr>
<td>Feb 2018</td>
<td>Satoshi Nakamoto’s net worth $10B - derived from the 980,000</td>
</tr>
<tr>
<td></td>
<td>Bitcoins he/she/they are estimated to own</td>
</tr>
</tbody>
</table>

**Bitcoin Symbol & Currency Code**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTC</td>
<td>Original currency code</td>
</tr>
<tr>
<td></td>
<td>Violates international standard for currency codes (ISO 4217)</td>
</tr>
<tr>
<td></td>
<td>It begins with “BT” (country code of Bhutan)</td>
</tr>
<tr>
<td>XBT</td>
<td>If a currency is not associated with a country then it starts with an “X”</td>
</tr>
<tr>
<td></td>
<td>Examples: USD = US Dollar, XAU = gold, XAG = silver</td>
</tr>
<tr>
<td></td>
<td>Unofficial code according to the ISO 4217 standard</td>
</tr>
</tbody>
</table>

Symbol designed by Satoshi Nakamoto for the icon of an early version of the original Bitcoin client.

The *satoshi* is currently the smallest unit of the Bitcoin that can currently be sent.

It is a one hundred millionth of a single Bitcoin (0.00000001 BTC).
**Bitcoin - Some Important Numbers**

- Finite number of Bitcoins: 21,000,000
  - Approximately 80% of BTC are in circulation
- Paced creation of blocks
  - 1 new block discovered every 10 minutes
  - Pacing mechanism invoked every 2,016 coins (≈ 2 weeks)
- Transactions are packaged into 1 MB blocks on the blockchain
- Miners earn new BTC when they “mine” a new block
  - Block reward started at 50 BTC/block
  - Reward is halved every 210,000 blocks
  - Current reward is 12.5 BTC

**Bitcoin Workflow**

1. **Bitcoin Wallet**
   - Private Key (≈ 23 M)
2. **Memory Pool**
   - (≈ 10 MB)
   - (≈ 6,700 Trans)
3. **Blockchain**
   - (≈ 510,100 Blks)
   - (≈ 157 GB)
4. **Estimated network hash rate**: ≈ 23 EH/s
5. **Add new block** (10 Min/Blk)
   - BLOCK #150
   - BLOCK #151
   - BLOCK #152
   - BLOCK #153
Bitcoin Mining - Introduction

Bitcoin mining is the process by which
- Transactions are verified and added to the public ledger (blockchain)
- New Bitcoins are released into circulation

**Work Product:** a new block of transactions is added to the blockchain

Other fanciful descriptions of mining
- Use computers to solve difficult math problems
- Solve a cryptographic problem called a “hash puzzle”
- Global, statistical gamble which is played every 10 or so minutes
- Mining is more akin to rolling dice than solving problems

More accurate description of the **difficult math problem**
- Find \( n \) such that: \( \text{Hash} ( \text{Hash} ( n ) ) \leq \text{target} \)
- Hash is SHA-256
- **Target** is a global parameter used to pace the creation of new coins

---

Bitcoin Mining - Motivation

**Block Reward**
- Every time a miner succeeds in posting a new block, they receive a reward.
  - Block reward started at 50 BTC
  - Reward is halved every 210,000 blocks
  - Current reward is 12.5 BTC

**Transaction Fee**
- Each transaction has an associated (and optional) transaction fee. When a miner includes a transaction in a new block they collect the corresponding transaction fee.

**Greater Good**
- Ideological reason - the more machines that mine, the more secure the cryptocurrency network is from attack.
SHA-256 (Secure Hash Algorithm)

- Cryptographic hash function
  - Input: arbitrary amount of input data
  - Output: Fixed size (seemingly random) 256-bit hash
- One way function – it cannot be decrypted back
- Output is consistent every time you perform the function on a given input
- SHA-2 set of cryptographic hash functions was designed by the National Security Agency

SHA256("Richard Gimarc #1") = 3FF94791DF6FA0B36B2483F1370222DFA2112E87063601E041CDA43FC955FF80
SHA256("Richard Gimarc #2") = 5DF25A3EB436881F10ED17CF6534367500E5203797F87C841F6C3708279136F

Block Structure

<table>
<thead>
<tr>
<th>Size (bytes)</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Block Size</td>
<td>The size of the block, in bytes, following this field</td>
</tr>
<tr>
<td>80</td>
<td>Block Header</td>
<td>Several fields form the block header (next page)</td>
</tr>
<tr>
<td>1-9</td>
<td>Transaction Counter</td>
<td>Number of transactions in the block</td>
</tr>
<tr>
<td>Variable</td>
<td>Transactions</td>
<td>Transactions recorded in this block</td>
</tr>
</tbody>
</table>

- Block size is limited to 1,000,000 bytes (often described as 1 MB)
- Average transactions per block: 1,864 (avg 2017-present)
- Blockchain size (Feb 13, 2018)  
  - 509,000 blocks  
  - 152.9 GB
Block Structure - Block Header

<table>
<thead>
<tr>
<th>Size (bytes)</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Version</td>
<td>Block version number</td>
</tr>
<tr>
<td>32</td>
<td>Previous block hash</td>
<td>Hash of the previous blocks header</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pointer – determines order of blocks in blockchain</td>
</tr>
<tr>
<td>32</td>
<td>Merkle Root</td>
<td>Hash of the Merkle tree containing transactions in this block</td>
</tr>
<tr>
<td>4</td>
<td>Timestamp</td>
<td>Approximate creation time of this block</td>
</tr>
<tr>
<td>4</td>
<td>nBits</td>
<td>Target threshold - find &quot;nonce&quot; such that hash of this header ≤ target threshold</td>
</tr>
<tr>
<td>4</td>
<td>nonce</td>
<td>An arbitrary number miners change to modify the header hash in order to produce a hash less than or equal to the target threshold.</td>
</tr>
</tbody>
</table>

- Block size is limited to 1,000,000 bytes (often described as 1 MB)
- Average transactions per block: 1,864 (avg 2017-present)

Block Structure - Blockchain

- Each block points to the previous block in the blockchain
- Pointer is the hash of the previous block's header
Transaction

- Transactions are cryptographically signed records that reassign ownership of Bitcoins to new addresses
  - INPUT - reference funds from other previous transactions
  - OUTPUT - records which determine the new owner of the transferred Bitcoins, will be referenced as inputs in future transactions as those funds are respent

Block #210000 – 456 total transactions

Transaction - Coinbase

- Miners earn a Block Reward when then mine a new block.
- Block Reward paid via a Coinbase Transaction
  - INPUT – no inputs
  - OUTPUT – address of the miner that mined the block – this is how new Bitcoins are added to circulation
- The Coinbase Transaction is the first transaction in a block

Block #100000 – 4 total transactions
**Mining - Pacing Block Creation**

**Goal:** Create a new block every 10 minutes

**Problem:** As the number of miners increases, new blocks will be discovered at a faster rate

**Solution:** Bitcoin has a self-pacing mechanism that controls block creation time

**How is this done?**
- A new block is discovered if a nonce is found that satisfies the following condition:
  \[ \text{SHA256( SHA256( block\_header ) )} \leq \text{Target} \]
- Large Target vs. Small Target
  - Large target makes it easier to discover a new block
  - As the target decreases, finding a valid hash becomes more difficult
- The target is adjusted every 2016 blocks (≈ 2 weeks) to re-target for 10-minute block generation
- Target is encoded in the block header as “nBits”

**Nonce – definition**
- Concatenation of “number used once”
- For Bitcoin, an integer between 0 and 4,294,967,296 (4-byte integer)

The goal of mining is to find a nonce such that:

\[ \text{SHA256( SHA256( block\_header ) )} \leq \text{Target} \]

**Example – Block # 100799**
- nBits = 0x1b04864c
- Nonce = 2,933,804,432

Hash: 0000000000000000000000000000000000000000000000000000000000000000

Target: 0000000000000000000000000000000000000000000000000000000000000000
Bitcoin Workflow

- Bitcoin Wallet: Private Key (≈ 23 M)
- Pull transactions to include in new block (≈ 1,800 Tran/Blk)
- Memory Pool: (≈ 10 MB), (≈ 6,700 Trans)
- Blockchain: (≈ 510,100 Blks), (≈ 157 GB), (10 Min/Blk)
- Add new block

Estimated network hash rate: ≈ 23 EH/s

Bitcoin Mining - Capacity Planning

<table>
<thead>
<tr>
<th>Business</th>
<th>How much money can I earn?</th>
<th>How long does it take to recover initial mining investment?</th>
<th>Expected amount of BTC per day, week, month, quarter, …</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Mining software (everyone uses the same software)</td>
<td>Total hash rate (H/s) across planning horizon</td>
<td>Pacing mechanism – difficulty changes every 2 weeks based on how much work other miners are doing</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Number of mining machines to satisfy Application hash rate</td>
<td>Hash rate per mining machine (GH/s, TH/s, PH/s)</td>
<td>Cost per machine</td>
</tr>
<tr>
<td>Facilities</td>
<td>Power – mining machine kWh used &amp; cost per kWh (#1 resource)</td>
<td>Space</td>
<td>Cooling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Noise (mining machines are noisy)</td>
<td></td>
</tr>
</tbody>
</table>
The Capacity Planning Stack
A structured way to think about & perform Capacity Planning

Capacity Planning Stack
- Multi-level hierarchy
  - Demand (down)
  - Feedback (up)
- Supports all elements of today's Digital Infrastructure
- Implementation is straightforward & transparent

Reference:
- "Capacity Planning: A Revolutionary Approach for Tomorrow's Digital Infrastructure"
- Amy Spellmann & Richard Gimarc
- CMG 2013

The Capacity Planning Stack
The Bitcoin Mining View

Capacity Planning Stack
- Multi-level hierarchy
  - Demand (down)
  - Feedback (up)
- Supports all elements of today's Digital Infrastructure
- Implementation is straightforward & transparent
The Capacity Planning Stack was initially designed for enterprise Capacity Planning. However, we have shown how the Stack can also be applied to a decentralized cryptocurrency like Bitcoin.

Questions?