Bitcoin Mining & The Capacity Planning Stack

Richard Gimarc - rgimarc@featherfall.com
Amy Spellmann - amy@optimalinnovations.com

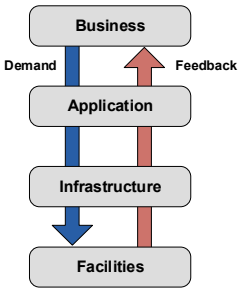
Southwest CMG
February 21, 2018

Bitcoin Mining & The Capacity Planning Stack

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

≈



2

MyCryptoBuddy.com Bitcoin Mining Calculator **[1/2]**

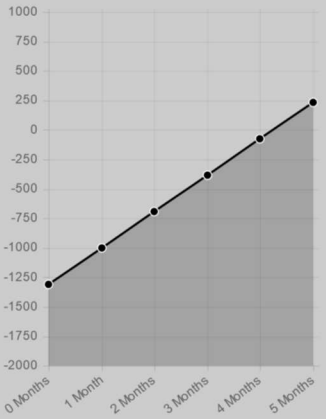
Hashrate	14	TH/s
Difficulty	2874.6742	G
Block Reward:	12.5	BTC
BTC Price	11198.61	USD
Power	1372	W
Power Cost	0.1	USD / kWh
Pool Fee	0	%
Reject Rate:	1	%
Live Stats	On	

Profits At This Difficulty

Period	BTC	USD	Costs (USD)	Profit (USD)
Hourly	0.0000505	$0.566	$0.137	$0.429
Daily	0.00121	$13.58	$3.29	$10.28
Weekly	0.00849	$95.04	$23.05	$71.99
Monthly	0.0364	$407.31	$98.78	$308.52

Hardware: Antminer S9

Estimated Future Profits (USD)



View Total Profits Time Frame: 5 Months

Use Diff Change:

Long-Term Projections

Profitable in **4 Months 7 Days**

Hardware Cost	1310	USD
Recurring Costs	0	USD / Month
Price Change	0	% / Month
Selling Profile	Sell Coins Montl	
Diff Change	22.5	% / Month
Use Diff Change		

Baseline
Use Diff Change = NO

Result
Profitable in 4 months

3

MyCryptoBuddy.com Bitcoin Mining Calculator **[2/2]**

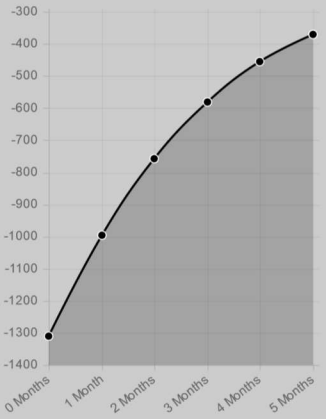
Hashrate	14	TH/s
Difficulty	2874.6742	G
Block Reward:	12.5	BTC
BTC Price	11351.63	USD
Power	1372	W
Power Cost	0.1	USD / kWh
Pool Fee	0	%
Reject Rate:	1	%
Live Stats	On	

Profits At This Difficulty

Period	BTC	USD	Costs (USD)	Profit (USD)
Hourly	0.0000505	$0.573	$0.137	$0.436
Daily	0.00121	$13.76	$3.29	$10.47
Weekly	0.00849	$96.34	$23.05	$73.29
Monthly	0.0364	$412.87	$98.78	$314.09

Hardware: Antminer S9

Estimated Future Profits (USD)



View Total Profits Time Frame: 5 Months

Use Diff Change:

Long-Term Projections

Profitable in **Never**

Hardware Cost	1310	USD
Recurring Costs	0	USD / Month
Price Change	0	% / Month
Selling Profile	Sell Coins Montl	
Diff Change	22.5	% / Month
Use Diff Change		

Scenario #1
Use Diff Change = YES

Result
Never Profitable

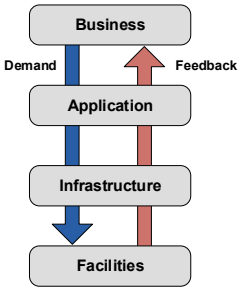
4

Bitcoin Mining & The Capacity Planning Stack

Agenda

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

≈



5

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

6

Timeline - Satoshi Nakamoto

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

7

Bitcoin Symbol & Currency Code

BTC	Original currency code Violates international standard for currency codes (ISO 4217) It begins with "BT" (country code of Bhutan)
XBT	If a currency is not associated with a country then it starts with an "X" Examples: USD = US Dollar, XAU = gold, XAG = silver Unofficial code according to the ISO 4217 standard

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).

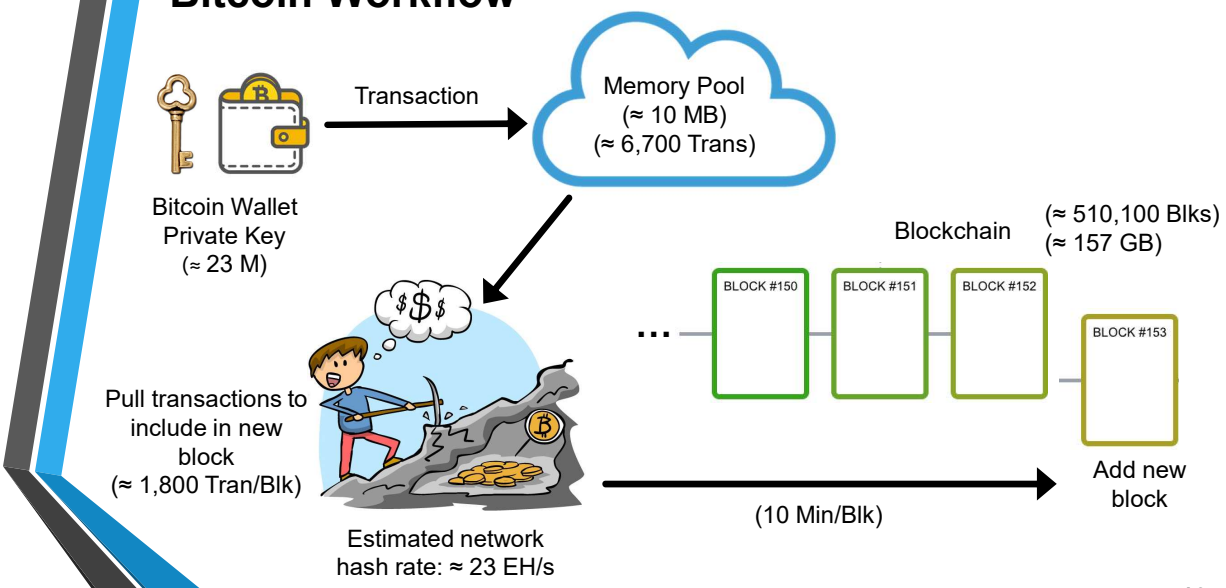
8

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

9

Bitcoin Workflow



10

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 : **Hash(Hash(n)) ≤ target**
- Hash is SHA-256
- **Target** is a global parameter used to pace the creation of new coins

11

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.

12

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`

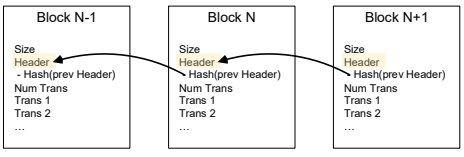
SHA256("Richard Gimarc #2") = `5DF25A3EBB436881F10ED17CF6534367500E5203797F87C841F6C3708279136F`

13

Block Structure [1 of 3]

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

- 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



14

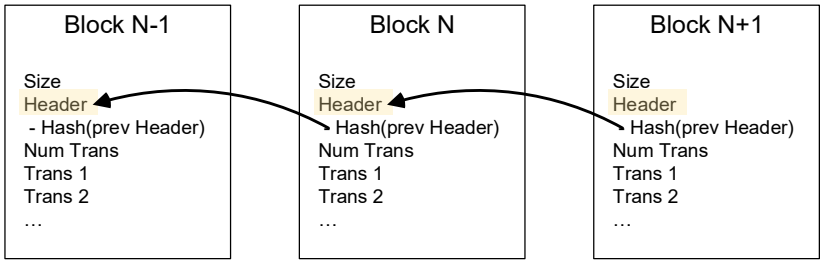
Block Structure - Block Header [2 of 3]

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

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

15

Block Structure - Blockchain [3 of 3]



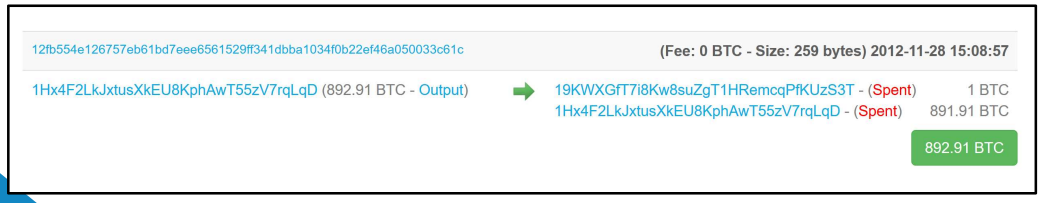
- Each block points to the previous block in the blockchain
- Pointer is the hash of the previous block's header

16

Transaction [1 of 2]

- 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



17

Transaction - Coinbase [2 of 2]

- 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

18

Mining - Pacing Block Creation [1 of 2]

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
  SHA256(SHA256(block_header)) ≤ **Target**
- Large Target vs. Small Target
  - Large target make 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**"

Block Header
Version
Previous Block Hash
Timestamp
nBits
nonce

19

Mining - Pacing Block Creation [1 of 2]

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

SHA256(SHA256(Block Header: Version, Previous Block Hash, Merkle Root, Timestamp, nBits, nonce)) ≤ Target

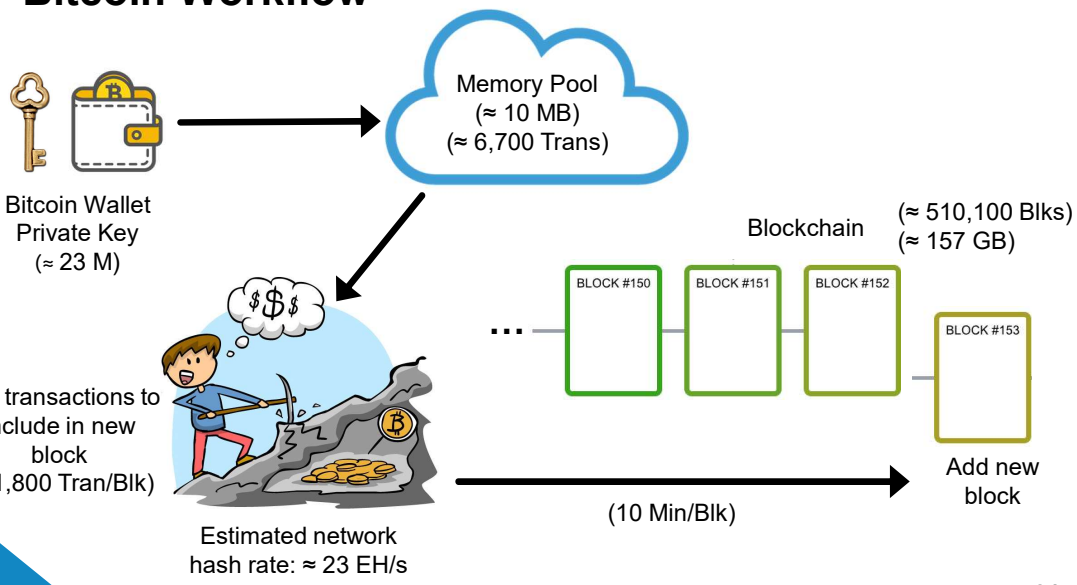
Example – Block # 100799

- nBits = `0x1b04864c`
- Nonce = 2,933,804,432

Hash: `0000000000025AFE84E27423011AF25F777E5A94545DBD00FD04BEBE9050F7DD`
Target: `00000000004864C000000000000000000000000000000000000000000000000`

20

Bitcoin Workflow



21

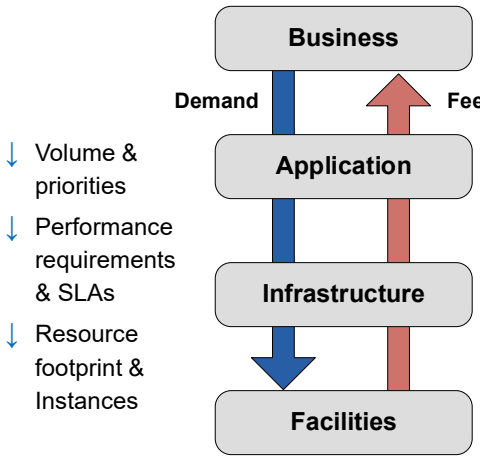
Bitcoin Mining - Capacity Planning

Business	How much money can I earn? How long does it take to recover initial mining investment? Expected amount of BTC per day, week, month, quarter, …
Application	Mining software (everyone uses the same software) Total hash rate (H/s) across planning horizon Pacing mechanism – difficulty changes every 2 weeks based on how much work other miners are doing Block reward change date (when is it halved?)
Infrastructure	Number of mining machines to satisfy Application hash rate Hash rate per mining machine (GH/s, TH/s, PH/s) Cost per machine
Facilities	Power – mining machine kWh used & cost per kWh (#1 resource) ~~Space~~ Cooling Noise (mining machines are noisy)

22

The Capacity Planning Stack

A structured way to think about & perform Capacity Planning



↓ Volume & priorities

↓ Performance requirements & SLAs

↓ Resource footprint & Instances

↑ Cost

↑ Total time to satisfy

↑ Expected performance

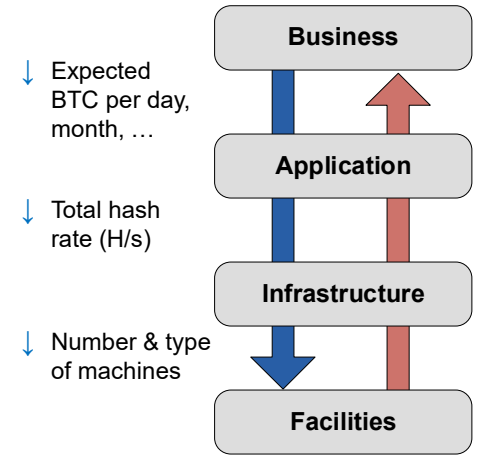
Capacity Planning Stack
- Multi-level hierarchy
  - Demand (down)
  - Feedback (up)
- Supports all elements of today's Digital Infrastructure
- Implementation is straightforward & transparent

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

23

The Capacity Planning Stack

The Bitcoin Mining View



↓ Expected BTC per day, month, …

↓ Total hash rate (H/s)

↓ Number & type of machines

↑ BTC count & cost (I+F)

↑ Total hardware cost

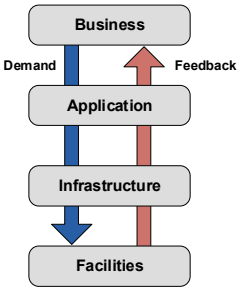
↑ Total facilities cost

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

24

Bitcoin Mining & The Capacity Planning Stack

≈

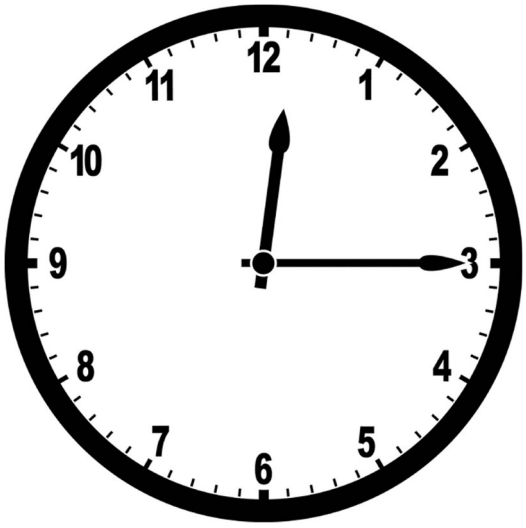


The Capacity Planning Stack was initially designed for enterprise Capacity Planning

However, we have shown how the Stack can also be applied to a decentralized cryptocurrency like Bitcoin

25

Questions?



26