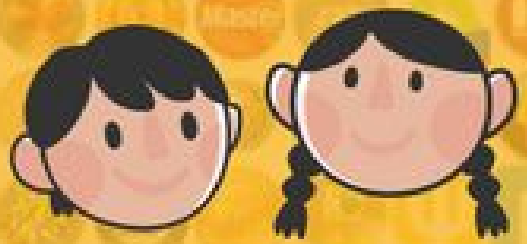
CRYPTOCURRENCY 101

workshop series



Mining vs. Cloud Mining

Cryptocurrency 101

Mining vs. Cloud Mining

Where do Bitcoins come from?

They are mined out of the system

There is a finite amount of bitcoins

21 million Bitcoins exist

Requires electricity to mine, because computers need to hash

They don’t just generate Bitcoins, they verify transactions

More miners = Reliable & more secure network

What do miners get paid for?

Verifying transactions

mining Bitcoins

Is Bitcoin mining profitable?

No, as miners increase, the difficulty goes up to make the Bitcoin reward constant

In 2009- 200 BTC could be mined in a few days

2014- 1 BTC in 98 years

How does a blockchain work?

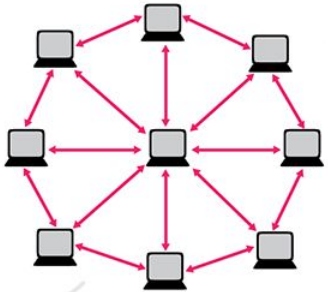
-Blockchains make use of hash function. Data on the blockchain is hashed in each block. If block is changed, hash value is different and others can detect something changed.

-Hashed value of the previous block is used to calculate the hashed value of the current block creating the link between the blocks.

What is block chain?

Source: blockgeeks

Someone requests a transaction.



The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**

A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger,**

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

In short

“The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.”

Don & Alex Tapscott, authors Blockchain Revolution (2016)

What is a hash function?

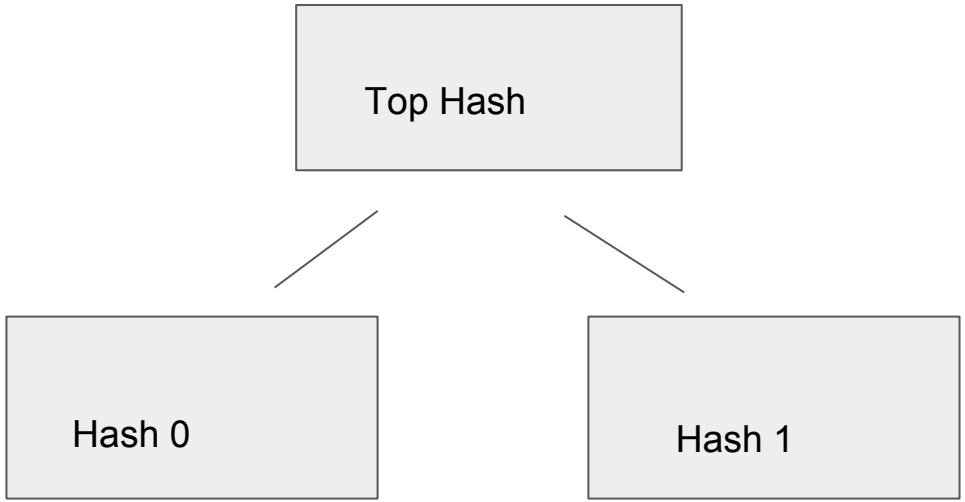
Takes an input of any length and creates an output of fixed length.

Example of a hash function

```
cloudnthings:bin cloudnthings$ echo "I owe my sister $5" | md5
a0680c04c4eb53884be77b4e10677f2b
cloudnthings:bin cloudnthings$
```

“a0680c04c4eb53884be77b4e10677f2b”. This is referred to as the message digest. It is also known as the digital fingerprint. This is because there is no way this digest can represent any other string. If I try and modify this to “I owe my sister $2” the message digest will be completely different.

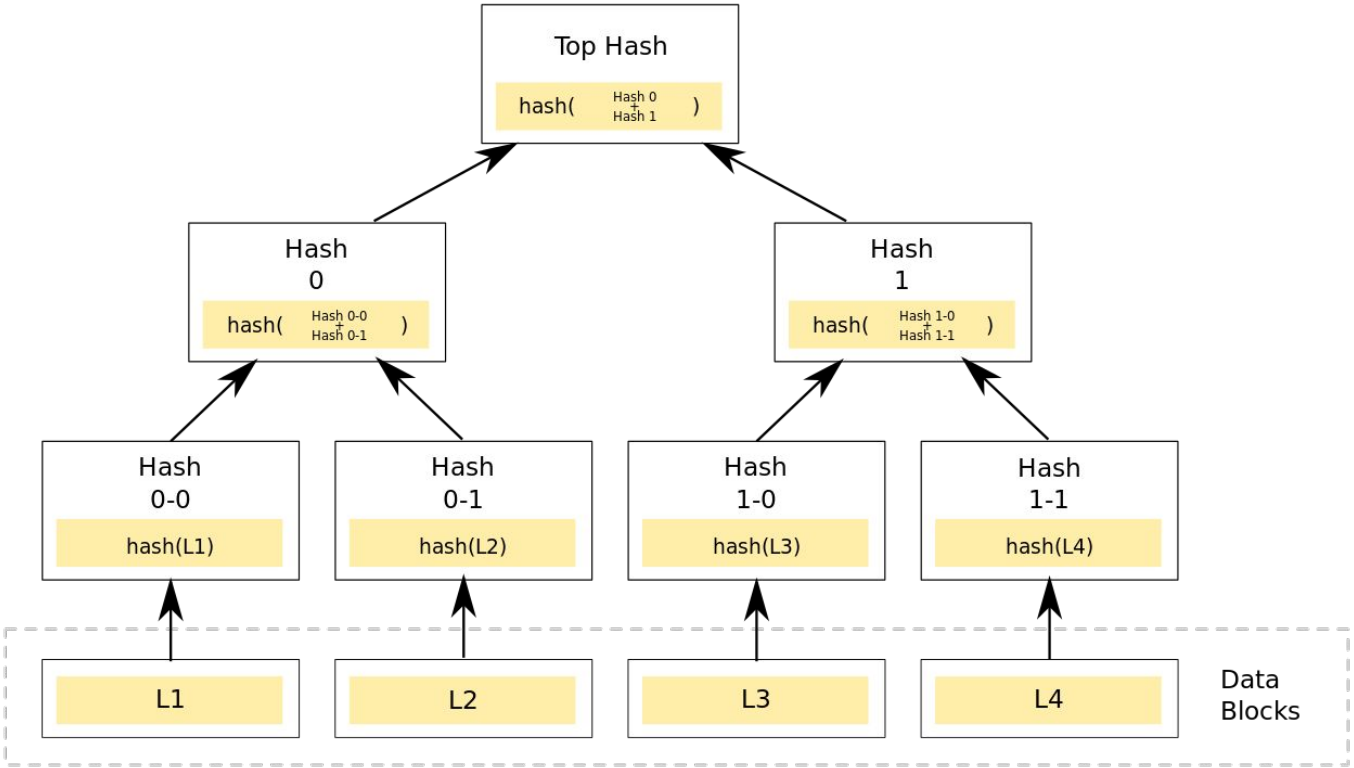
In the big picture



Merkle Tree

Used to verify any kind of data stored, handled, and transferred in and between computers

Used for cryptocurrency and peer to peer network +check other peers aren't lying and sending fake blocks



Mining Algorithm

SHA-256, Scrypt, or X11

3 objectives here

1. Provide bookkeeping services to the coin network. Mining is essentially 24/7 computer accounting called ‘verifying transactions’
2. Get paid a small reward for your accounting services by receiving fractions of coins every couple of days
3. Keep your personal costs down, including electricity and hardware.

How to get started

1. Get a coin wallet
2. A free mining software made up of cgminer + stratum
3. Membership in an online mining pool
4. Membership at online currency exchange
5. Reliable full time internet connection, ideally 2 megabits/ sec or faster speed
6. Hardware set-up location in your basement or other cool + air conditioned
7. Desktop or custom-built computer designed for mining. If you use your own PC, can’t use PC while it is mining. Laptop + gaming console not effective enough to generate income
8. ATI GPU or a mining ASIC [Application Specific Integrated Chip]~$90-3000
9. A house fan to blow cool air across mining computer

Mining Pools

Pooling of resources by miners who share their processing power over a network to split reward according to the amount of work they contributed to solve a block

2 types of Mining Pools

Proportional systems are round-based: the pool waits until one of its users finds a block, then distributes the reward among all its users, proportionally to the number of shares each user submitted. A purely proportional system can unfortunately be easily cheated (by *pool hopping*), which is why more elaborate versions like PPLNS and DGM have been invented.

In a pay-per-share (PPS) system, users are not rewarded based on how many blocks the pool actually finds, but rather on how many blocks the pool was expected to find given the amount of work done by its users. The pool pays a fixed amount of litecoins for each valid shares its users submit, based on the mathematical laws of probability. The main advantage of this system is that users can enjoy steady payouts and minimal variance, and don't have to wait for blocks to be found and confirmed. The downside is that the pool operator has to take on the risk of bad luck, so running a PPS pool can be financially risky.

What to mine?

Dogecoins, Litecoins, Feathercoins are good choices for beginners right now

Antminer L3+ ~$1,600

Includes BM1485 ASIC chip

Uses Texas Instruments' AM 335x 1GHz ARM Cortex-A8 microprocessor

A high-grade aluminum case, customized heat-sinks and two computer-controlled fans to keep it cool

Payback ~ 151 days

Power	Power cost per day	Return Per Week	Cost per MH/s
800	$ 2.30	$ 75.76	$ 3.26
Hash Rate	**Return Per Day**	**Return Per Month**	**Payback period**
504.0 MH/s	$ 10.82	$ 324.68	151 days
Mines	**Profit Ratio**	**Return Per Year**	**Annual Return Percentage**
Litecoin	469%	$ 3,950.29	240%

Some notes:

504MH/s but give and take +/-5%

Power consumption 800W+10%

Ethernet connection

DC Voltage input 11.60-13V

Litecoin Mining Softwares

Sgminer - cgminer 3.7.2 fork, continues GPU/ scrypt mining, AMD GPUs only

Cgminer- supports GPU/ scrypt mining

Cpuminer- Fastest CPU miner

cudaMiner- Fastest miner for NVIDIA GPUs

GUIMiner-scrypt- Provides a GUI for cgminer and cudaMiner- does not allow Linux and lack of back end transparency

BFGMiner- CPU and GPU miner

MultiMiner- Provides GUI for BFGMiner||| Reaper+ScryptMiner GUI, no longer maintained

What is hash rate?

Hash rate measures how powerful a miner’s machine is. Specifically, it measures the number of times a hash function can be computed per sec. Miner’s expected profit is directly proportional to the hash rate.

Mining Pools for Litecoin

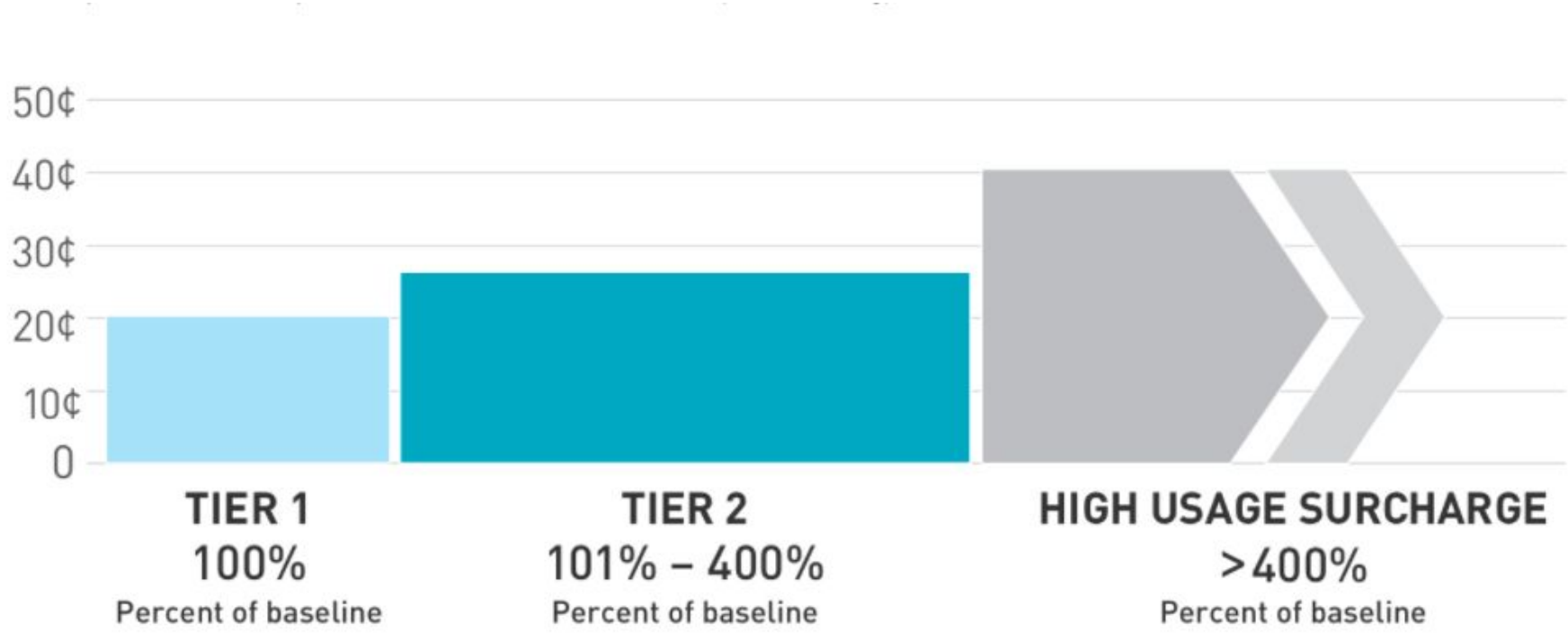
https://coinotron.com/coinotron/AccountServlet?action=home

https://www.litecoinpool.org/

http://give-me-coins.com/

TBDice

PG&E Rate


50¢
40¢
30¢
20¢
10¢
0
TIER 1
100%
Percent of baseline
TIER 2
101% – 400%
Percent of baseline
HIGH USAGE SURCHARGE
>400%
Percent of baseline

Modern Malware

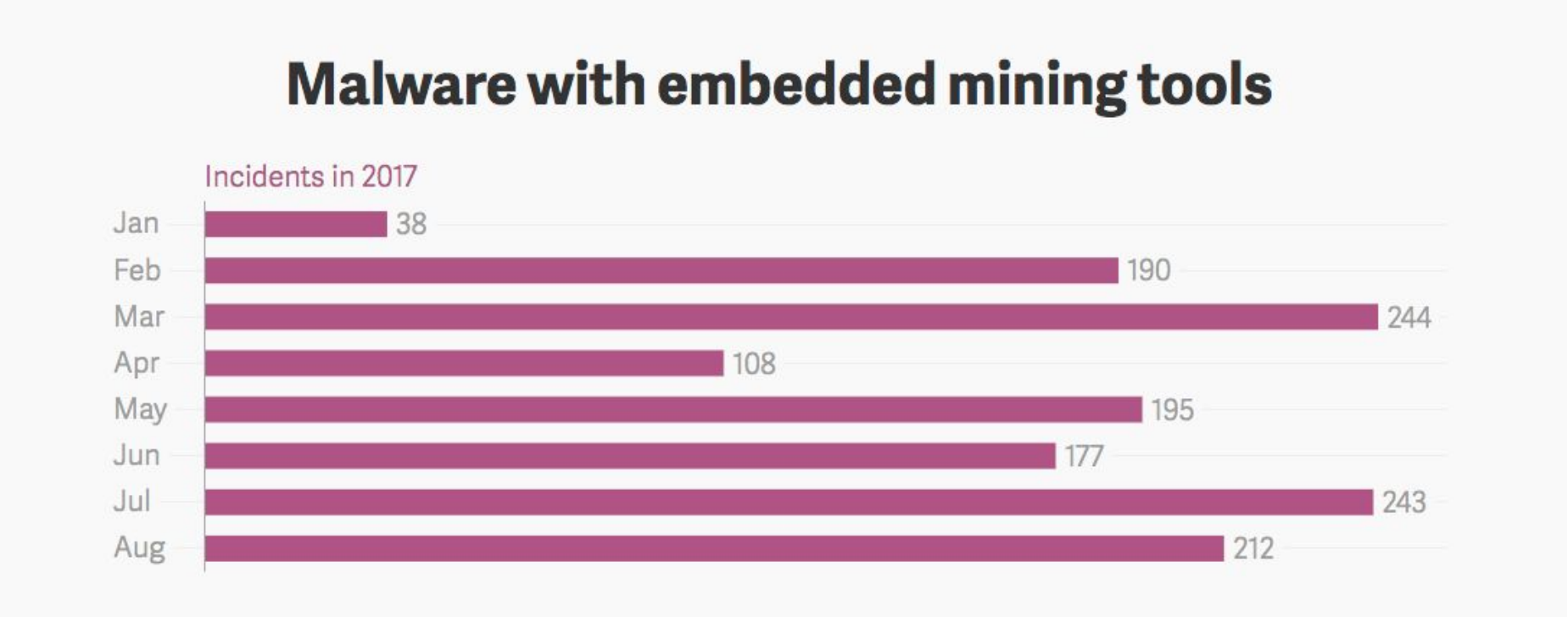
Smart devices around the household, router is the only doorkeeper

Home routers are susceptible to cross-site scripting XSS and PHP arbitrary code injection attacks as well as DNS amplification attacks.

Since Bitcoin mining’s encryption technique needs extensive computing power, malware developers infect a large amount of victims to offset the computing power.

How to figure it out?

Check your CPU usage; Mac: Activity Monitor/ Windows: Task Manager



Crypto Mining in the Browser

Instead of ads spaces, there are in-browser mining as revenue stream.

Coin Hive

Can I integrate Coin Hive onto my website?

Technically yes, economically probably not. If you run a blog that gets 10 visits/day, the payout will be miniscule. For the captcha and shortlinks with a sensible hash goal (1024–16384) you'll need to have a whole lot of users to make this worthwhile.
Implementing a reward system for your site or game where users have to keep mining for longer durations is far more feasible. With just 10–20 active miners on your site, you can expect a monthly revenue of about 0.3 XMR (~$27).
If you run a streaming video site, a community site, an online game or anything else where you can give your users an incentive to run the miner for longer durations, then by all means: try it.

Why does Coin Hive mine Monero?

To mine Monero, you have to calculate hashes with an algorithm called Cryptonight. This algorithm is very compute heavy and – while overall pretty slow – was designed to run well on consumer CPUs.
There are solutions to run the Cryptonight algorithm on a GPU instead, but the benefit is about 2x, not 10000x like for other algorithms used by Bitcoin or Ethereum. This makes Cryptonight a nice target for JavaScript and the Browser.

Pirate Bay

Miner

As you may have noticed we are testing a Monero javascript miner.

This is only a test. We really want to get rid of all the ads. But we also need enough money to keep the site running.

Let us know what you think in the comments. Do you want ads or do you want to give away a few of your CPU cycles every time you visit the site?

Of course the mining can be blocked by a normal ad-blocker.

Note :
Initially there was a small typo so all CPU for a client was used. This should be corrected now so only 20-30% should be used.
Also it is restricted to run in one tab only so even if you have 10 tabs oven it will only be running in 1.

Posted 09-16 17:10 by admin

Cloud Mining

Cryptocoin mining utilizing a remote datacenter with shared processing power

Pros:

A Quiet and cooler home

Lower electricity cost

No need to manage the equipment- no need to repair and no need to configure hardware

Cons:

Management Cost- cost for maintenance of the equipment

Lack of control- can’t choose from your fave mining pool

Security- some cloud mining companies are actually ponzi schemes

Some not so legit ones

HashOcean

BitMinister

Coince

Some choices for cloud mining

www.genesis-mining.com use promo code: 4yaeUE

To get 3% discount when buying

Lifetime SHA-256 mining or 2-year X11 contracts

Eobot.com

Is it profitable?

Suppose your budget is **$5000**

Cloud Mining :-

25% ($2500) for **Bitcoin** Mining , buy 10Th/S , you will get ***0.005*** *bitcoins* ***daily***

25% ($1250) for **Ethereum** Mining, buy 60 MH/S you will get 0.56 Ethereum daily

25% ($1250) for **Monero** Mining , buy 4000 H/S you will get ***0.15*** *Monero* ***daily***

25% ($1250) for **DASH** Mining, buy 22 MH/S you will get ***0.07*** *DASH* ***daily***

So , In an year

Total Coins

Bitcoins : 1.80 (mining) = **2.05**

Ethereum : 20.5 (mining) = 2**0.5**

Monero : 60 (Mined) = **6**0

DASH : 30 (Mined) = **3**0

Total Value (using Predicted Rate based on Current Growth+Market)

Bitcoins : 2.05 * $3000 = $**6000**

Ethereum : 20.5 * $200 = **$4000**

Monero : 60 * $50 = $**3000**

DASH : 3 0* $150 = $**3000**

Total = $16500

Yes, cloud mining is profitable if the coin value goes up