Bitcoin and The Age of Bespoke Silicon

SAISRIKAR PARUCHURI 44751575

MICHAEL CONNOR 41773080

Agenda

- What is Bitcoin
- BTC/USD Exchange Rate
- Bitcoin Architecture
- How to Get Bitcoin
- Bitcoin Transaction Flow
- Bitcoin Mining
  - Solo Mining
  - Pooled Mining
- Evolution of the bitcoin mining hardware
  - CPU
  - GPU
  - FPGA
  - ASIC

What is Bitcoin

Bitcoin is a digital currency introduced in 2008 by pseudonymous developer "Satoshi Nakamoto". That can be exchanged for goods and services.

Digital: Bitcoins cannot be printed or physically made. They must be generated through computerized methods.

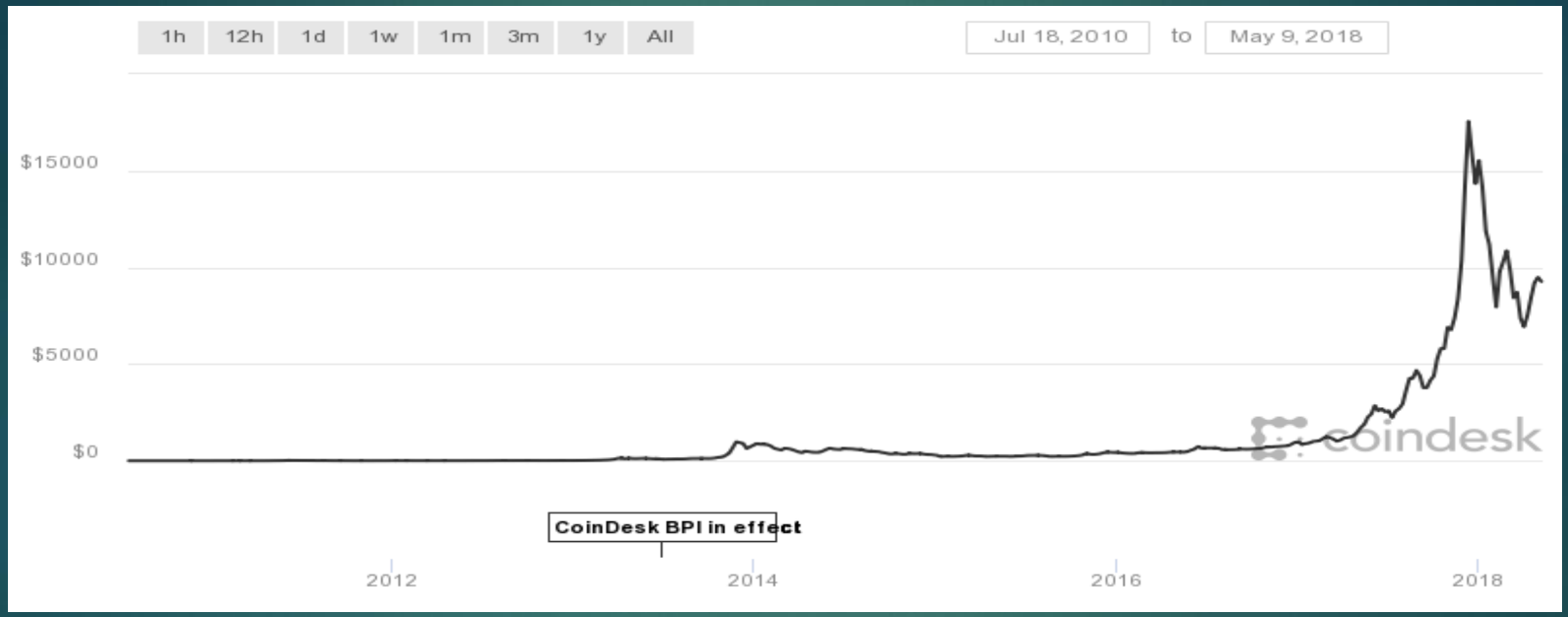
Decentralized: Bitcoins are not regulated by any government or banking institution.

Revolutionary: Transactions allow for anonymity and are almost instantaneous.

Global: Bitcoins are borderless currency and can be used anywhere.

BTC/USD Exchange Rate

Winklevoss twins, of The Social Network fame, have purchased $11 million worth of BTC, and have submitted a proposal to the SEC to create an Exchange Traded Fund (ETF) to allow broader access to investors which has increased the Bitcoin growth.



Exchange Rate

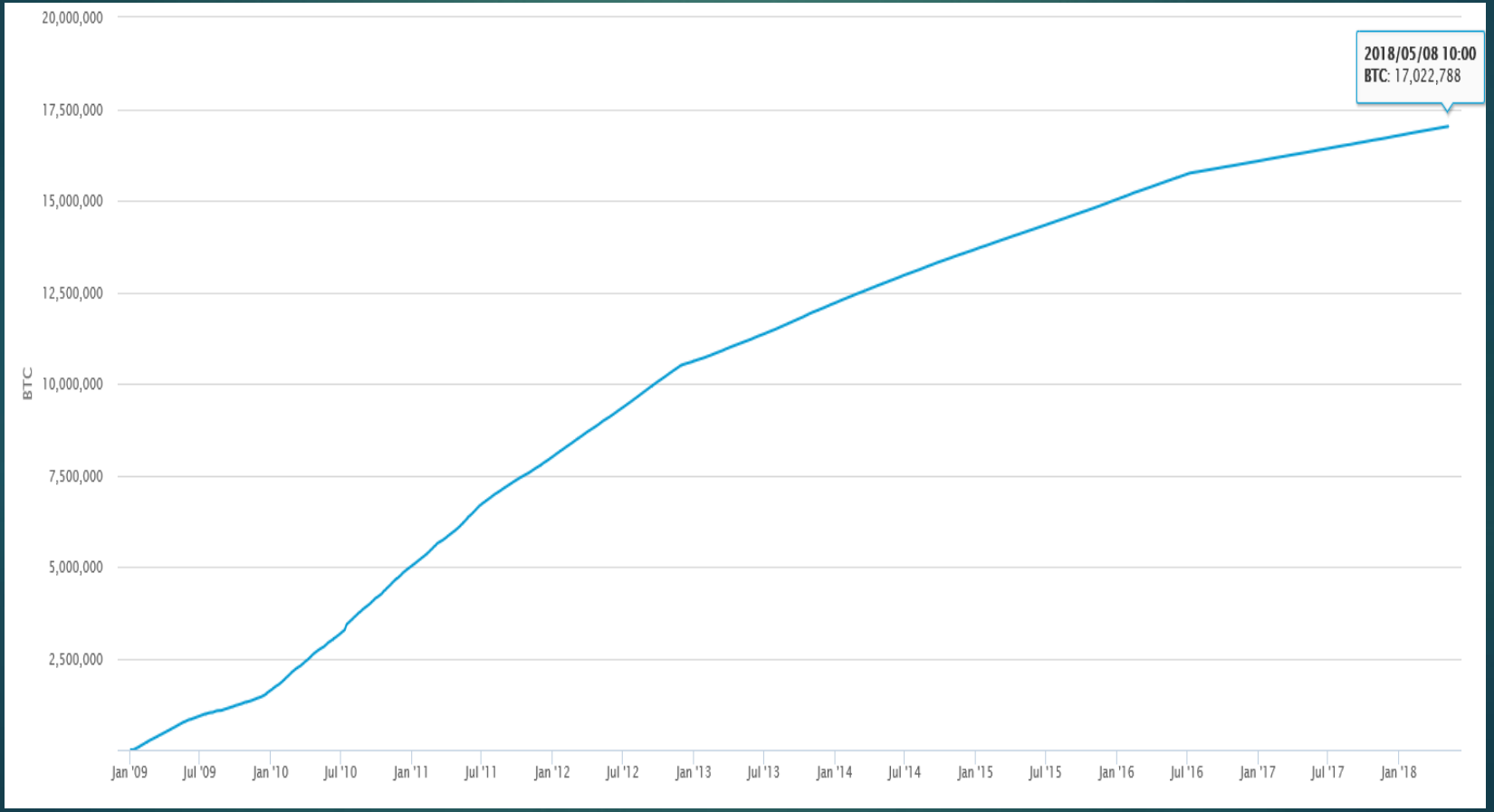
1 BTC = $9,273 (USD)

1 BTC = 12,427.67 (AUD)

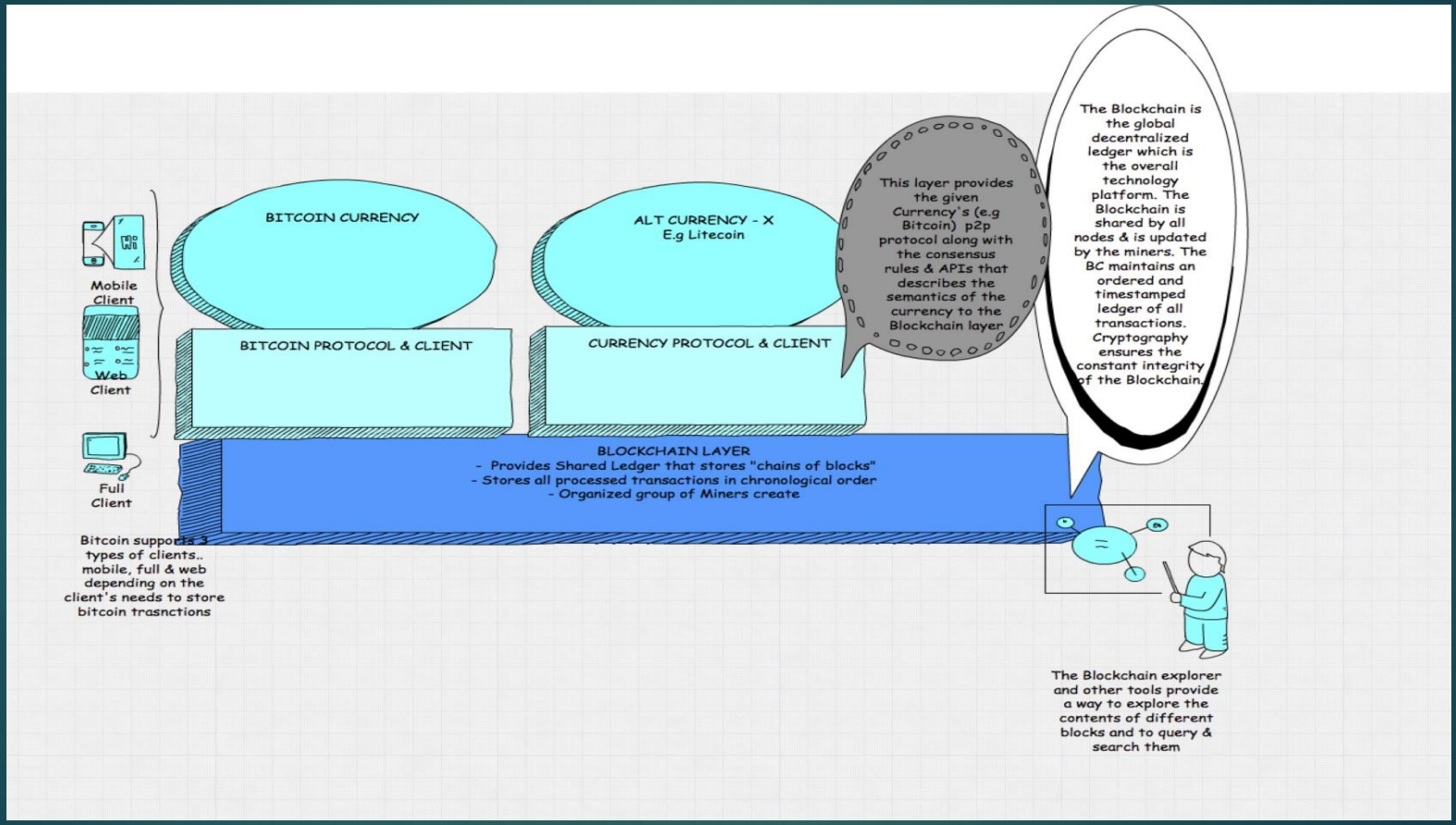
(as of 9/05/2018 22:00)

Bitcoins in Circulation

Currently, the circulation of number of Bitcoins as of April 2018 is 17 millions BTC. Market Capitalisation of Bitcoin is above $100 Billion USD.

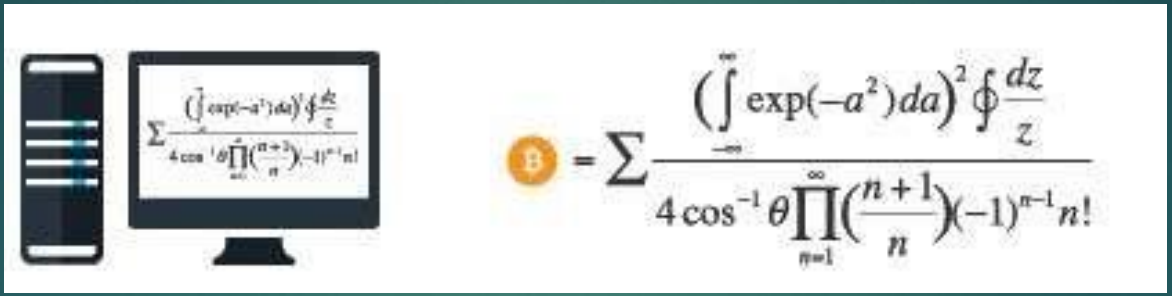


Bitcoin Architecture



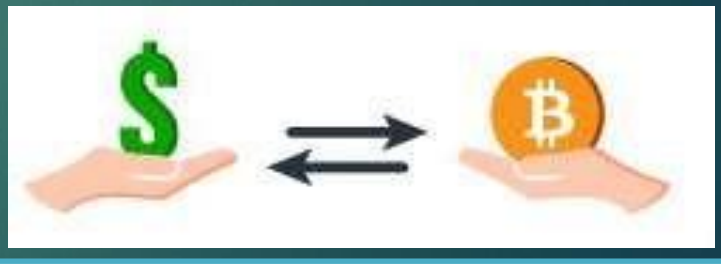
How to get Bitcoins

We can get **Bitcoins** from digital world. It's has 3 ways to get it



1 You can create Bitcoins through **Bitcoins Mining**, a process that involves running software on a computer to solve complex mathematical equations to generate a portion of the currency. if one of the equation is solved, then the payout is a Bitcoin.

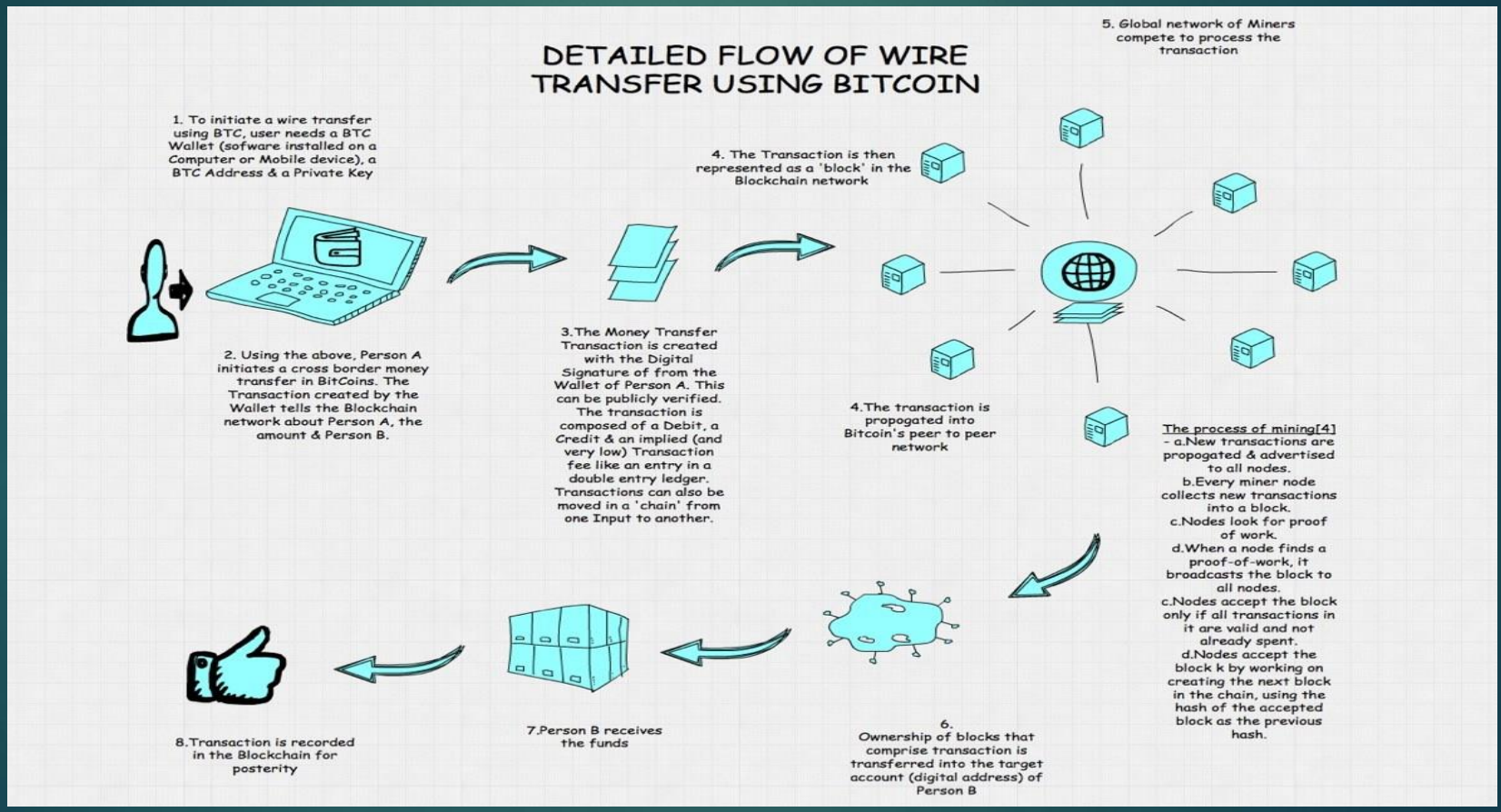
2 You can get Bitcoins from selling something in online markets.



3 You can buy Bitcoins outright at various Bitcoin exchange markets.

Bitcoin Transaction Flow

- The User has public key and private key. User will share public key to receive payments. Whereas private key should be confidential and used only while sending Bitcoins.
- New blocks are added to the Blockchain for every 10 minutes.



Bitcoin Mining

Mining requires a certain amount of work for each block of coins. This rate is controlled by the network so that bit coins are always created at a predictable and limited rate.

Bitcoin Mining
Handmade

Bitcoin Mining
Box set

Bitcoin Mining Intro

- If your hash rate is h and you mine for time t, on average the number of found blocks is

$$N = \frac{th}{2^{32} D}$$

- **D** =Difficulty, **h** =miner's hashrate

- Exp- User buys a mining computer with **h =1Ghash/s =10^9 hash/s**. If he mines for a day(**86,400 s**) when **D =1690906** and **B= 50BTC**

  Found Blocks =ht /(2^32 *D) =0.0119 blocks =0.0119 *B =0.595 BTC

- **Classification of mining**
  - **Solo Mining:** Mining alone.
  - **Pooled Mining:** Mining with other miners in a mining pool.

Solo Mining as a Poisson Process

- Number of trial is depends on miner's hash rate **h**
- **p:** Probability of success(very small).
- **n:** Number of blocks found by a miner
  - mining for time **t** with hash rate **h** results in on average $\frac{th}{2^{32}D}$ blocks.
  - **n** follows the Poisson distribution $P_0(\lambda)$ where λ is the parameter called intensity.

$$\lambda = \frac{th}{2^{32}D}$$

- Exp: User has **$V[P]=0.0119B^2$, $\sigma=5.454B$,**
  - About 3 months to find a block in solo mining.
  - The process is completely random and memoryless.
  - May wait on average 3 more months.

Pooled Mining

- Joint effort & reward distribution.
- **H:** Total hash rate of all miners.
- Single miner's hash rate **h = qH** (0<q<1)
- **$E[P_p]$:** Total average payout of the pool

$$E[P_p] = \frac{HtB}{2^{32}D}$$

Pooled Mining

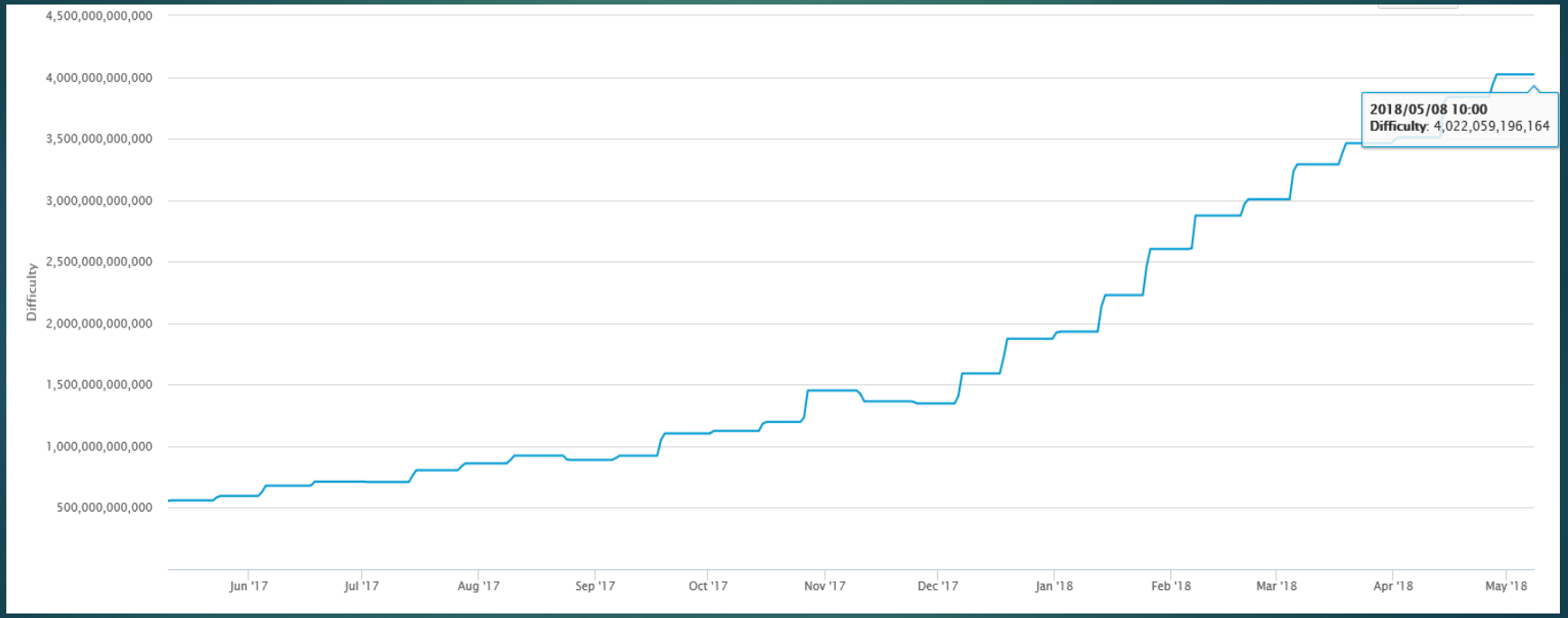
- **f:** Fee/Block, **B** = Block reward.
  - Operator's fee for a block = fB.
- Actual Reward for the pool miners = $B - fB = (1-f)B$.

- In a pool
  - Each miner submits **shares** into the pool.
  - **Share:** Hash of a block header calculated by a miner which is less than T_{cur} assuming **D=1** (e.g. $T_{cur} = T_{max}$).

- Each hash has a probability of $\frac{1}{2^{32}}$ to be a share in the pool.
- Each share has a probability $p = \frac{1}{D}$ to validate a block.
- For a single share, a miner's

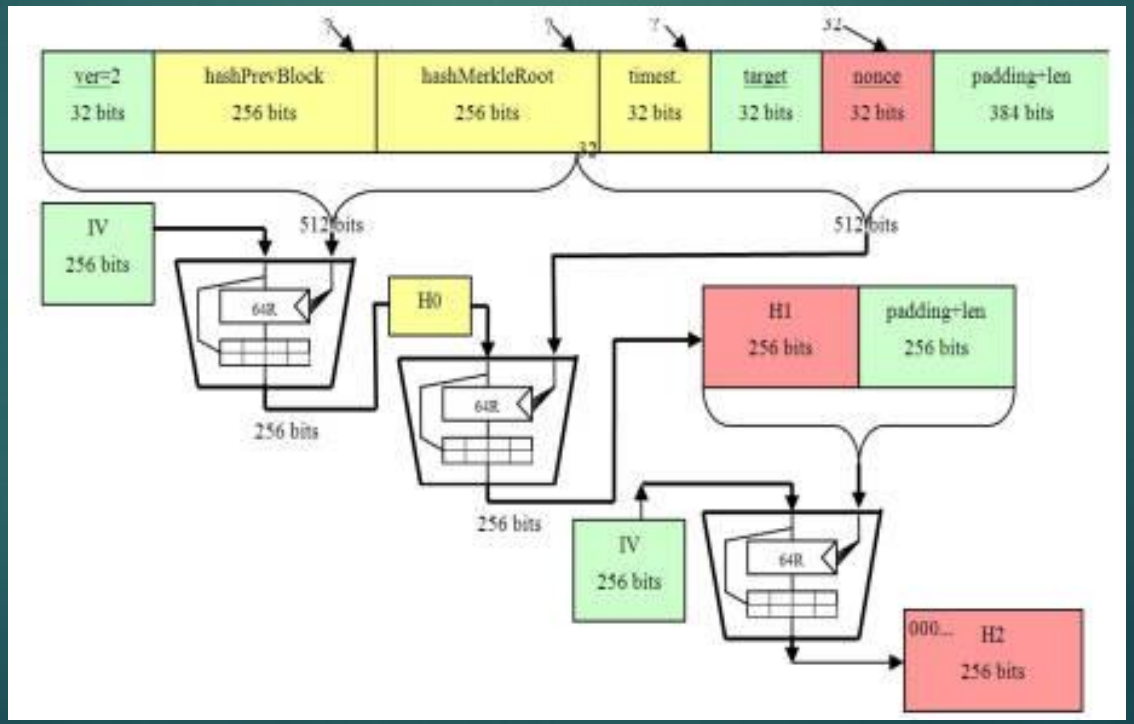
Expected payout = Expected contribution to total reward = pB

Bitcoin Mining Difficulty



CPU Mining and SHA256

```
while (1)
 HDR[kNoncePos]++;
 IF (SHA256(SHA256(HDR)) < (65535 << 208)/ DIFFICULTY)
   return;
```



GPU Mining

- First OpenCL in Oct 2010
  - Optimised by community
- Java/Python for Bitcoin protocol and OpenCL for nonce search run on ISA
- OpenCL became more advanced allowing more fine grained control of graphics card
- AMD > nVidia

GPU Mining

Field Programmable Gate Arrays (FPGA)

- A brief reign in bitcoin the mining hardware evolution
- One hardware for each 64 rounds of operations separated by pipeline register
- Higher power consumption due to extremely high LUT activity
- Require special boards

Application Specific Integrated Circuits (ASIC)

- The final major step to Mining rig evolution
- Work in similar way as FPGA but designed specifically for mining
- Design first announced by BFL in June 2012

ASICMINER

- Crowd-sourced
- Based in China
- Offered 50% of company share on sale
- Upon completion the company will run the boards and distribute the mined coins with the share holders
- Boards are sold to customers after

Avalon

- Crowd-Sourced
- Single double SHA256 pipeline ASIC implemented by TSMC
- 66GH/s on 600W
- Sold ASIC Chips in bulk to customers
- Allowed groups to design boards freely

ASIC Hardware Scaling

- Chip performance per $ influenced by
  - Transistor size
  - Hardware design for hash operations
- Hardware design is the non-limiting factor

Today

- ASIC still reigns
  - Dragonmint T16 by Halong Mining
  - 16 TH/s at 1480W

Summary

- Bitcoin is useful for anonymity and borderless transactions.
- Bitcoin transactions are public through block chain
- Bitcoin transactions are irreversable
- Unlikely to be profitable mining solo
- Mining technology advancement was largely due to effort of community and crowd funding
- Older rigs becomes obsolete as newer generation is released

References

- Michael Bedford Taylor. *Bitcoin and The Age of Bespoke Silicon.* University of California, San Diego. 2013
- Segendorf B. What is bitcoin. Sveriges Riksbank Economic Review. 2014;2:71-87.
- https://cryptomining24.net/gpu-table-with-hashrate/
- https://cryptomining24.net/table-of-mining-cpu/
- https://www.buybitcoinworldwide.com/mining/hardware/
- https://www.buybitcoinworldwide.com/mining/hardware/dragonmint-16t/

Questions?