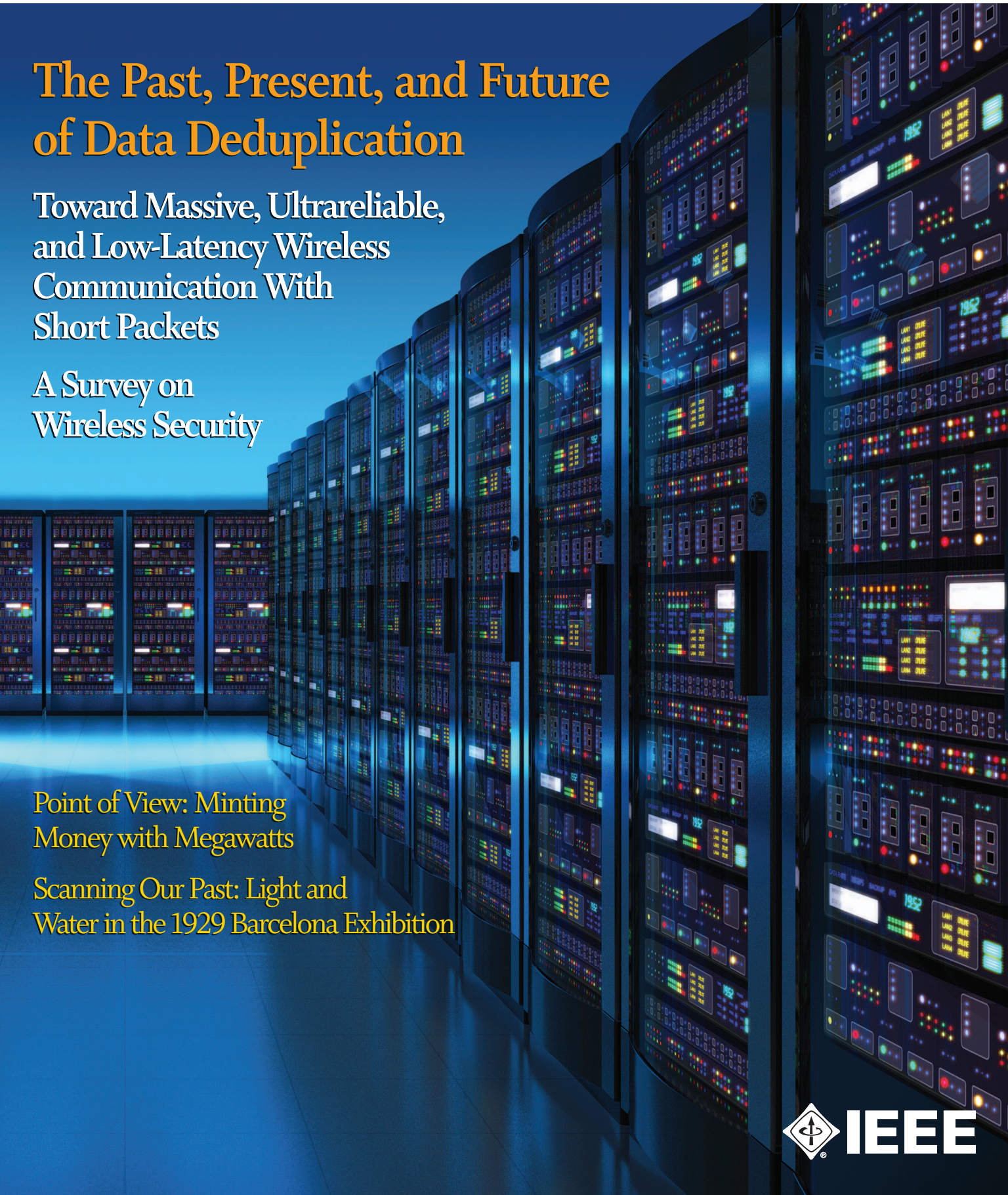
September 2016 | Volume 104 | Number 9

Proceedings of the IEEE



The Past, Present, and Future of Data Deduplication

Toward Massive, Ultrareliable, and Low-Latency Wireless Communication With Short Packets

A Survey on Wireless Security

Point of View: Minting Money with Megawatts

Scanning Our Past: Light and Water in the 1929 Barcelona Exhibition

IEEE

Minting Money With Megawatts

BY SVEINN VALFELLS
Flux, Ltd.

JÓN HELGI EGILSSON
Faculty of Economics,
University of Iceland

I. INTRODUCTION

Launched in January of 2009, Bitcoin is a rapidly growing peer-to-peer (P2P) online payment network with an annual transaction volume of $45.4 billion. The market cap of the bitcoin digital currency (BTC) is currently $10.2 billion.[1] For comparison, PayPal, which was founded nine years before Bitcoin was launched, had payment volume of $282 billion in 2015 and a market cap of $45 billion at the end of last year. PayPal's volume is still growing at an impressive 27% per annum, but the value and number of bitcoin transactions have, on average, more than doubled every year since inception, a strong indication that this new payment network is on a fast trajectory toward mainstream adoption (Fig. 1).

Unlike PayPal and other traditional payment services, however, Bitcoin payments do not go through financial institutions. Instead, the open architecture first described by the unknown founder, Satoshi Nakamoto, allows users and other participants to join the Bitcoin payment network freely without going through traditional banks or payment providers [1]. Through a judicious selection of technologies and incentives, Satoshi's architecture has given rise to a new payment network and digital currency independent of existing financial service providers and central banks.

II. BITCOIN MINING

A crucial part of this new financial network is a computational process known as mining. The Bitcoin transaction ledger is distributed, and there are no central copies

[1]When capitalized, Bitcoin refers to the entire Bitcoin network and protocol; when not capitalized, bitcoin refers to the digital currency used on the Bitcoin network. The currency is also often abbreviated as BTC or XBT.

Digital Object Identifier: 10.1109/JPROC.2016.2594558

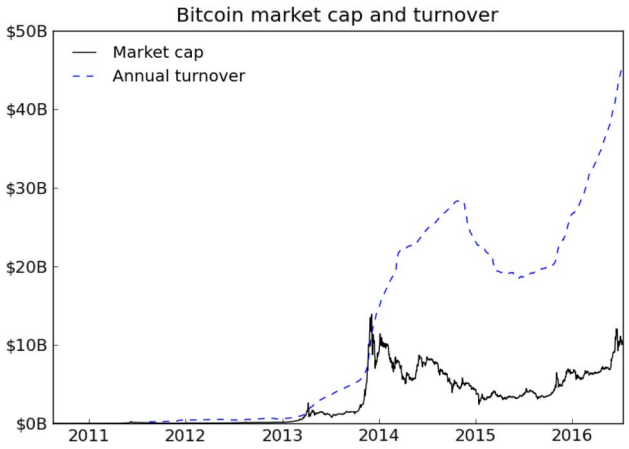


Fig. 1. ***Bitcoin market cap and trailing 365 day turnover (in billions of dollars).***[2]

maintained by trusted institutions. The ledger consists of a chain of timestamped transaction blocks, the blockchain. The integrity of the blockchain is secured by cryptographic hashes of the transaction blocks with each block referencing the hash of the previous block. Miners compete to calculate or "mine" valid hashes and are rewarded with new bitcoins and transaction fees. The miners consume hundreds of megawatts of power minting bitcoins worth billions of dollars.

In technical terms, the cryptographic hash which Bitcoin uses is a one-way transformation of an input string, the transaction block header, into a highly garbled output string. The block header consists of several data fields, including a signature of the enclosed transactions, the hash of the previous block, a timestamp, and a random data field called "nonce." A valid output of the block header hash must belong to the subset of outputs which have a certain number of leading zeros. More zeros indicate a smaller subset and greater difficulty of finding a valid hash. The hash is computed repeatedly varying the nonce until a nonce is discovered which produces a valid block header hash. The target difficulty is adjusted every 2016 blocks to make new blocks appear every 10 min, on average.

The block header hashes serve as digital watermarks which are easy to authenticate but difficult to reproduce. They remove the need for a central authority to maintain an official copy of the blockchain. The miners compete in computing the hashes. Successful miners claim the new block reward which now stands at 12.5 BTC for each block. User transaction fees are elective and currently average less than 1 BTC per block.

Miners' annual revenues have reached over $545 million. Fierce competition has ensued, with miners moving from central and graphical processing units in desktops and servers to application-specific processors and systems deployed in custom data centers. The largest five mining pools and companies control over 75% of the total mining capacity which now stands at 1517 petahash per second (Fig. 2). The network hashrate corresponds to power consumption of 160 MW if mined with the latest processors and data centers, but the actual consumption is probably somewhat higher because of older systems still in use. The estimated replacement cost of the network is $800 million (Table 1).

Each miner's share of total mining revenues is diluted when new capacity is added. Consequently, miner profits drop as the network grows. Additionally, the new block reward halves every 210 000 blocks, or approximately every four years. Because transaction fees are currently about 50 times smaller than the block reward, halving the block reward effectively halves total mining revenues if bitcoin price or transaction fees remain unchanged.

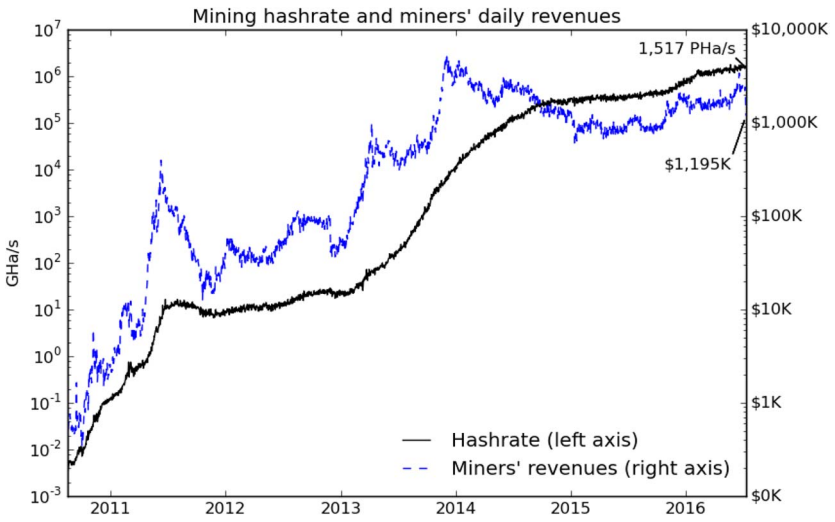


Fig. 2. ***The total hashrate of Bitcoin mining (in gigahash per second) has increased with mining revenues (in thousands of dollars). The current hashrate is 1517 petahash per second (peta denotes 10^{15}).***

[2]Based on data from blockchain.info, Jul. 2016. All calculations performed by the authors.

Table 1 Price and Performance Data of Recent Mining Systems and Deployment Environments[3]

Factor	Value	Units
Non-recurring engineering costs	8M	$
Variable investment cost	0.5M	$/PHa/s
Power consumption	0.1	W/GHa/s
Co-location costs	50	$/kW/month
Power Usage Efficiency	1.03	None
Availability	0.99999	None

Several miners have run into difficulties, for example KnCMiner which declared bankruptcy in May citing the drop in transaction block reward from 25 BTC to 12.5 BTC which took place on July 9. Capital costs of the latest systems and facilities are high which presents a barrier to entry to new miners. Consolidation in mining raises concerns about the integrity of Bitcoin: the greater the concentration of mining capacity, the greater opportunity the miners have of colluding to attack the blockchain. If any entity or group were to gain control over 51% or more of the mining capacity, they would effectively control the transaction history of the blockchain, and the decentralized, trustless quality of Bitcoin would be destroyed.

III. HOW TO MINE PROFITABLY

The evolution of mining is determined by economic incentives and the cost and performance of technology. In order to analyze the market structure we construct a simple economic model which captures the key factors influencing miners' profit and loss: revenues, operational costs, and investment costs [see (1) in box].

As shown in Fig. 3, under the right circumstances new capacity can be profitably added to the mining network. Given market data, it is possible to determine whether new entrants can profitably add capacity, how much, and the minimum cost of profitable entry. The shortest payback period can also be computed.

[3]Based on information from miners, colocation centers, and power utilities.

Using recent cost and performance numbers of mining systems and deployment environments (Table 1), we can map out the breakeven zone within which new miners can profitably add new capacity (Fig. 4). We choose an amortization period of three years which reflects the fact

BITCOIN MINING PROFIT FUNCTION

The profit $\pi(X)$ generated by new Bitcoin mining capacity X is defined as

$$\pi(X) = \frac{X}{h_0 + X} B(S+F) - XC - \frac{1}{T}\left(\frac{X}{z} + \text{NRE}\right). \quad (1)$$

Here h_0 is the preexisting hashrate, B is bitcoin price, S is supply, F is transaction fees, C is the operational cost, T is the amortization period, $(1/z)$ is the variable investment cost, and NRE equals the nonrecurring engineering cost of investment. Under the right conditions, capacity can be profitably added within a range defined by the two breakeven points (Fig. 3). A detailed discussion of the profit function is available on Github, including derivations of the breakeven points, the point of maximum profitability, and the payback period [2].

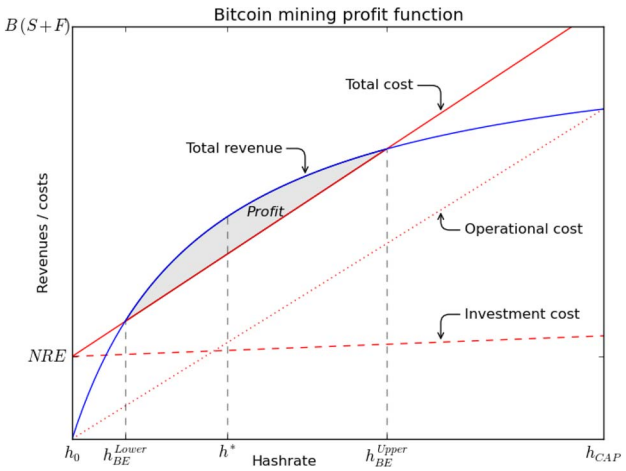


Fig. 3. *Miners compete to collect new supply and transaction fees. In dollar terms, their total revenues are $B(S+F)$ where B is bitcoin price, S is supply, and F is transaction fees. With total hashrate at h_0, new capacity added must generate enough profit to cover operational and investment costs within the amortization period T. For the right combination of revenues, costs, performance parameters, and amortization period, capacity can be profitably added within a range bounded by the lower and upper breakeven points h_{BE}^{lower} and h_{BE}^{upper}. The point of maximum profitability h^* lies between the breakeven points. For hashrates greater than h_{CAP}, operational costs exceed revenues, and miners shut off their equipment.*

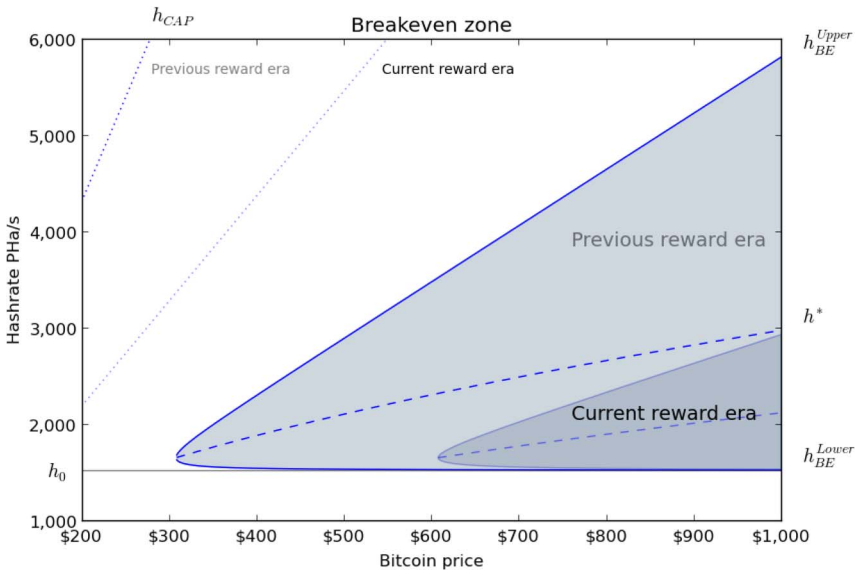


Fig. 4. *In the previous reward era of 25 BTC for each block mined, new miners could profitably add capacity in the breakeven zone between h_{BE}^{lower} and h_{BE}^{upper} at bitcoin prices as low as $300. When the block reward halved to 12.5 BTC, the lowest price point of profitable entry jumped to over $600, and the breakeven zone narrowed considerably. Existing miners will keep their systems running for all values below h_{CAP}. At any given price, h^* represents the most profitable capacity addition.*

that Moore's Law doubles the peak output efficiency of processors roughly every three years [3]. With the previous block reward of 25 BTC and at current network hashrate, the breakeven zone started at just over $300 and fanned out with increasing price. At current price of $648 and hashrate of 1517 petahash, there was room for new entrants to more than double the hashrate. The smallest amount of capacity that could be added profitably was just under 10 petahash. However, when the block reward halved to 12.5 BTC, the lowest price point at which capacity can be profitably added jumped to over $600. Furthermore, the minimum amount of capacity which can be added profitably has risen to over 60 petahash, and the maximum capacity addition has declined to 300 petahash, around 20% of the existing hashrate. A significant barrier has developed for new entrants, and the range of profitable entry has contracted considerably.

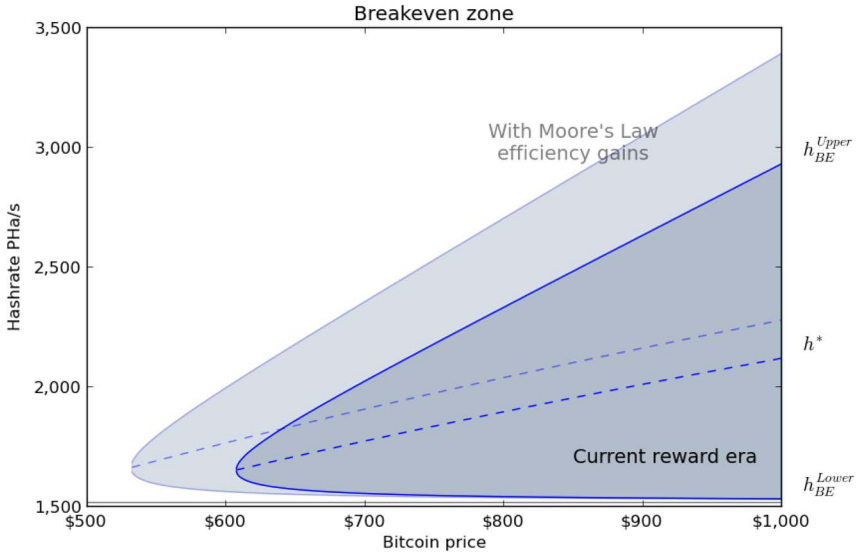


Fig. 5. *Moore's Law partially counteracts the reduced block reward. It expands the breakeven zone for new entrants and reduces the lowest price of profitable entry from $610 to $530.*

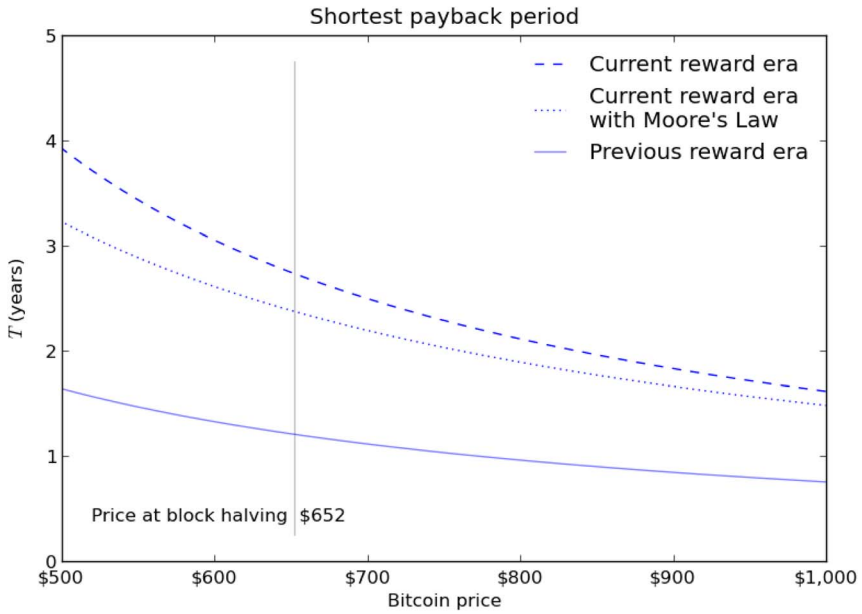


Fig. 6. ***The shortest profitable payback period of new Bitcoin mining capacity increased when the block reward halved, but Moore's Law power efficiency gains will reduce the payback period and partially reverse the effect of the halved block reward.***

Unlike new miners, existing miners with installed capacity are not constrained by the breakeven zone. Having already incurred investment costs, they will continue to operate their capacity until their operational costs exceed revenues, at h_{CAP}. As shown in Fig. 4, h_{CAP} is much higher than the current network hashrate, and existing miners have no reason to turn off their equipment even after the block reward has halved to 12.5 BTC. Because h_{CAP} far exceeds the values of the breakeven zone, incumbents enjoy a clear advantage over new entrants.

While processors continue to advance according to Moore's Law, however, power efficiency will continue to double approximately every three years. As Fig. 5 shows, a new generation of processors with improved efficiency can expand the breakeven zone and bump the lowest profitable price point of new entrants from $610 back to $530, counteracting, in part, the halving of the block reward. As the power efficiency doubles, the smallest amount of capacity that can be added profitably at the current price and hashrate declines to 30 petahash from the current value of 60 petahash, and the maximum profitable capacity addition increases from 300 petahash to 600 petahash.

Finally, we note that halving of the block reward has more than doubled the shortest possible payback period of new entrants from 1.2 years to 2.8 years (Fig. 6). With Moore's Law, the posthalving payback period can reduce back to 2.4 years.

IV. CONCLUSION

Following the recent halving of the Bitcoin block reward, new miners are close to being shut out from Bitcoin mining and unable to add new capacity profitably. The ability of incumbents to continue mining is not substantially affected, however. A rise in bitcoin price, higher transaction fees, or a reduction in existing mining capacity may improve the opportunity for new miners to enter the market, but each future halving of the Bitcoin block reward will narrow the range of profitable entry for new Bitcoin miners considerably. The stronger relative position of incumbents compared to that of new entrants supports further consolidation of Bitcoin mining. Consequently, the distributed Bitcoin ledger, the blockchain, may become more vulnerable to attack, and its trustless nature may ultimately even be destroyed.

Continued improvement in microprocessor efficiency will counteract mining consolidation. While Moore's Law remains valid, new generations of processors will from time to time open a window of entry into the mining marketplace. Ultimately, the greatest disruption to the current market structure may come through adoption of new computing technologies, such as graphene processors or quantum computers. ■

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] S. Valfells and J. H. Egilsson, "Bitcoin mining profitability," [Online]. Available: http://www.github/sweyn

[3] J. Koomey and S. Naffziger, "Moore's Law might be slowing down, but not energy efficiency," *IEEE Spectrum*, Mar. 31 2015.