Written Testimony

Hearing of the U.S. Senate Energy and Natural Resources Committee

Thomas A Golden
Program Manager, Technology Innovation
Electric Power Research Institute

“*The purpose of the hearing is to consider the energy efficiency of blockchain and similar technologies and the cybersecurity possibilities of such technologies for energy industry applications.*”

August 21, 2018

Chair Murkowski, Ranking Member Cantwell, Members of the Committee – thank you for inviting me to discuss the energy efficiency of blockchain and similar technologies as well as the cybersecurity possibilities of such technologies for energy industry applications.

The Electric Power Research Institute (EPRI) conducts research and development relating to the generation, delivery, and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers, as well as experts from academia, government, and industry, to help address challenges in electricity, including reliability, efficiency, affordability, health, safety, and the environment. EPRI’s members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries.

EPRI’s research into blockchain and its capabilities began recently (2016) as early interest in bitcoin led to questions on bitcoin mining energy usage and how other blockchain enabled technologies could impact energy industry processes and operations. EPRI’s early research efforts related to blockchain technology in the energy sector have revealed several pilots that have shown potential promise in the use of blockchain to enable transactive energy. The GridWise Architecture Council’s (GWAC) Transactive Energy Framework defines transactive energy as techniques for managing the generation, consumption or flow of electric power within an electric power system through the use of economic or market-based constructs while considering grid reliability constraints. The term “transactive” comes from considering that decisions are made based on a value. These decisions may be analogous to or literally economic transactions.

While innovation in the blockchain space is rapidly expanding blockchain capabilities, questions remain as to the standards, scalability, energy usage, and potential return on investment related to deploying blockchain-enabled technology into distribution and transmission networks. EPRI has helped to raise awareness and provide information to the energy industry via our Technology Innovation research program and EPRI's Utility Blockchain Interest Group (UBIG). This UBIG is comprised of nearly forty energy companies and growing as the technology continues to generate great interest within the industry. EPRI has also begun developing a blockchain-based energy market simulator to explore how loads and renewable resources could work together using more granular market information.

Information & Insights

EPRI has published a whitepaper (attached) and what we term "Quick Insights" (*Blockchain: Early Activity for Utilities; Bitcoin Mining, Blockchain, and Energy Consumption* attached) to provide the public and energy industry with a high-level view of blockchain basics and potential impacts on industry capabilities if blockchain technology were to be adopted. These two documents provided much needed education to counter some hype that often surrounds emerging technologies. In addition to these early education efforts, EPRI's UBIG holds regular webcasts to share experiences and applications of blockchain among supporting members.

Blockchain and Energy Use

In response to questions around blockchain and energy use, EPRI published *Quick Insights: Bitcoin Mining, Blockchain, and Electricity Consumption*. Questions have been raised about data mining operations. These operations often seek out locations with a cool, dry climate, which reduce HVAC expenses and lower energy costs. The concern is that these operations may shutter if cryptocurrency mining becomes less profitable. The price of Bitcoin, one 'cryptocurrency', has seen a decline in recent months from a high of ~$19,000 in December of 2017 to roughly ~$6,000 today as shown in the figure below.

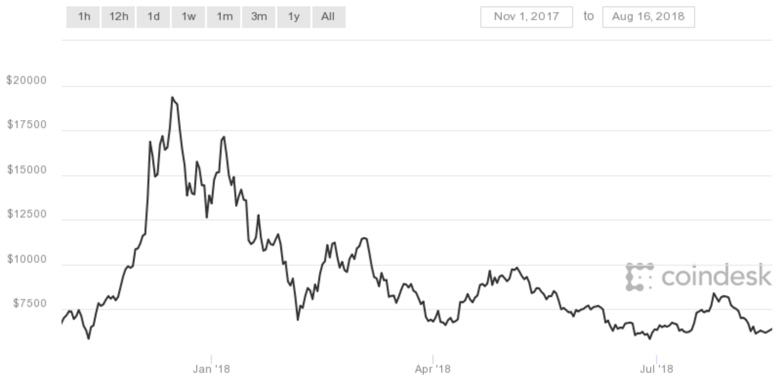


Figure 1 Bitcoin price from Nov 1, 2017 to August 16, 2018 Source: Coindesk

Blockchain Architecture

Blockchain is as an append-only file; data can only be added and verified. Once added, data cannot be changed or deleted. The various blockchain architectures of Proof-of-Work, Proof-of-Stake, Proof-of-Authority, and tangle all make different design trade-offs and hence, use different amounts of energy, have different security requirements, and differing performance characteristics. A blockchain company called Ethereum is already experimenting with using Proof-of-Stake[1] for some blocks in its chain to counter scalability and energy use issues.

The three primary characteristics that collectively make blockchain interesting -- security, transparency, and immutability -- don't fit all types of transactions. Security and control requirements vary due to design trade-offs inherent in the technology. It is important to find processes where these three characteristics add value. Some of the early uses EPRI is exploring in addition to transactive energy involve applications that may be subject to audits and safety checklists. For customer-facing applications the main value may be in increasing trust for those customers who would prefer an independent system capturing energy usage.

Transactive Energy

Blockchain is seen as an enabler for Transactive Energy. The challenge facing any transactive energy system is that it must run on disparate devices, through many levels of the grid; consumer, microgrid, feeder, distribution system operator, and transmission system operator to enable transactions. These transactions will be between the customer and the utility, as well as any willing buyer and seller (prosumer). Blockchain could potentially solve this challenge and provide a platform that handles exactly what is described above. Regardless of the type of device, if the market constructs are standardized, then the device would only need to be able to exchange price/energy data with the blockchain being used to enable the market. In the energy sector, nearly all the attention has been on blockchain's enabling capability for transactive energy or eMobility (e.g., payment platform for electric vehicle payments). However, there are regulatory barriers that currently restrict transactions to being between a customer and their local utility and questions about the cost, return on investment, and capability of the devices required to enable this infrastructure. Also, as in traditional smart metering, there are differences in geography and topology that impact the design of the required communication networks. What may be feasible in downtown New York with ubiquitous broadband connectivity, may not work in rural areas that are usually more limited to Power Line Carrier (PLC) or intermittent communication.

To better understand this environment EPRI has created an initial version of a blockchain energy market simulator. This platform was developed as part of the Information Communication Technology Security Architecture for DER research program. This platform will be expanded to simulate many more nodes, loads types, and combined with the EPRI smart inverter simulator,

[1] https://www.coindesk.com/bitcoins-taproot-privacy-tech-is-ready-but-one-things-standing-in-the-way/

and should provide robust simulation capabilities for loads, generation, and energy from solar panels. This simulation capability, built on an open platform, coupled with the projected deployment cost, may finally give some insight into the total cost of ownership required to enable transactive energy.

Concluding Remarks

Working collaboratively with other stakeholders, EPRI will continue to explore energy efficiency of blockchain and similar technologies as well as their cybersecurity implications.

EPRI is committed to developing science-based solutions to these difficult problems, and offers technical leadership and support to the electricity sector, public policymakers, and other stakeholders to enable safe, reliable, affordable, and environmentally responsible electricity.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Quick Insights

Blockchain: Early Activity for Utilities

RESEARCH QUESTION

What is blockchain and its associated capabilities and applications in the utility industry?

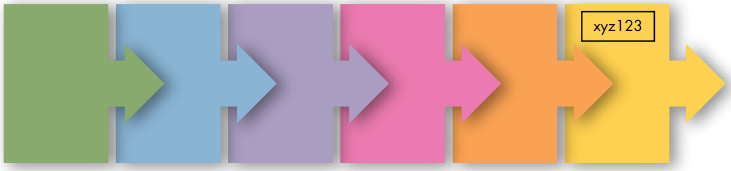
KEY POINTS

- Blockchain is an emerging digital technology acting as a distributed ledger to record transactions.
- The technology removes the need for centralized third-party intermediaries and supports cryptocurrencies that function similar to cash, which are exchanged immediately with no provision for money being returned.
- As the energy internet of things (eIoT) evolves and connected devices proliferate, blockchain may facilitate payments and other information exchanges among an exponentially increasing volume of customers and service providers.
- The technology is in its early stages of development, with only a couple of utility-related proof-of-concept implementations, though engagement is starting to increase with companies developing the technology for various use-cases.

INTRODUCTION TO BLOCKCHAIN

Blockchain is a "distributed ledger" technology. Like a traditional ledger, it keeps a record of every transaction in a system. Unlike centralized ledgers, it is considered transparent because every participant in the peer-to-peer network has a copy of the ledger and can see the contents of every transaction. Blockchain is currently most closely associated with enabling cryptocurrencies such as Bitcoin, Ethereum, or zCash, but in addition to its uses as a currency, hundreds of use cases are being explored; everything from games to contracts.

Blockchain gets its name because it is a chain of data blocks, each containing a given set of transactions. Additionally, each block contains a mathematical algorithm called a *cryptographic hash* which is based on all the content of all the blocks in the chain to that point including a timestamp based upon the time of creation.



Each block has a "hash" that is based on the contents of all prior blocks, creating a chain.

While there are a number of kinds of cryptographic hashes, they all share the property that it is relatively easy to verify that a particular block of data matches a given cryptographic hash, but that the reverse operation of creating a block of data that matches a particular hash is very difficult. This computationally difficult verification is called a *proof of work* in blockchain parlance. In Bitcoin, one of the more well-known cryptocurrencies based on blockchain technology, the "miners" (the entities that create a new block) are rewarded with bitcoins for performing this task. Other entities also exist in the cryptocurrency ecosystem, such as exchanges, which will exchange the cryptocurrency for something else (dollars, euros, etc.), and wallets, a mechanism that allows one to buy or sell using the cryptocurrency, without the energy or computational overhead of the entities that maintain the blockchain.

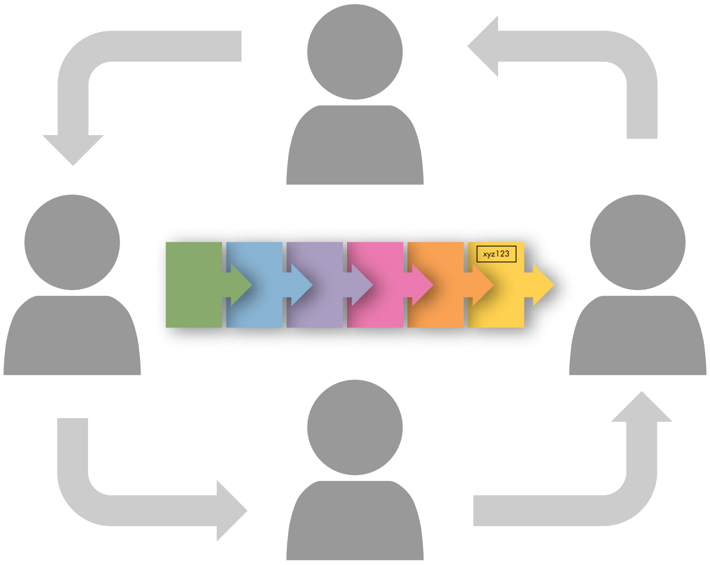
There are tradeoffs made with the distributed ledger design choice. For example, with Bitcoin, the blockchain is computationally expensive, and for Bitcoin miners (the entities that create the proof-of-work), only the largest organizations can afford to pay for the energy required to run the computers, whereas smaller entities may pool their resources and share the rewards. The size of the blockchain is also a challenge. It is estimated that for a Visa-scale transactional system (~3000 per second) the blockchain would grow at the rate of approximately 25 terabytes per month.

While a blockchain is inherently secure due to how blocks are created and the use of cryptographic keys, it is not without its challenges. While the chain is secure, the computers and devices that would participate are still vulnerable to hacking. However, to compromise the blockchain, a hostile entity would need to control more than half of the participating devices due to the nature of how participants need to "agree" on each block that is added to the chain; the majority "wins".

PERMISSIONED VS PERMISSIONLESS BLOCKCHAINS: A MATTER OF TRUST

The Bitcoin implementation of blockchain is permissionless; that is, anyone can choose to participate and decide how much information they wish to reveal about their identity. In this way Bitcoin is "pseudo anonymous"—while identities may be hidden, some companies now offer services that perform analysis on the blockchain in an attempt to reveal participant identities. However, in a permissioned blockchain, entities are only allowed to participate if their identity has been verified.

There are cryptocurrencies such as zCash that allow complete anonymity using what is called a "zero knowledge proof", where a verifier can validate that the user knows something to a third-party without revealing the actual item in question. Zero knowledge proofs are probabilistic proofs rather than deterministic proofs. The cheater has some chance, albeit small, to make the verified believe they satisfy the proof.



The blockchain is distributed to all participants on the peer-to-peer network

Due to current and potential emerging regulatory requirements, blockchains applied in the utility industry will likely be the permissioned variety.

APPLICATIONS OF BLOCKCHAIN

There are hundreds of use cases for blockchains in various stages of development (a list can be found at http://dapps.ethercasts.com). These applications run the gamut from smart contracts (insurance, ticket purchasing) and keeping personal data or identity records, to unalterable constitutions or governance—now enforced by algorithm rather than humans.

Nominally, any transaction that the utility participates in that requires an exchange of currency or of paper could use a blockchain. When all parties can verify a transaction without requiring a third party for validation or confirmation to process or hold information, the cost and speed of transactions is improved, potentially reducing costs and benefitting society. EPRI's investigation of blockchain as well, aligns with its public benefit mission. This may also be the answer to facilitating the transactions required to enable transactive energy. This concept changes the relationship of customer and utility to one of prosumers. A prosumer can buy or sell, not just to the utility, but to any willing participant.

INDUSTRY ACTIVITY

The Cleantech Forum Conference (January 23-25, 2017) offered a panel discussion on blockchain technology which brought together international representatives from the utility, vendor, and startup communities. The startup companies see, and are pursuing, clear opportunities in the financial industry. They were looking to the utilities to outline potential use cases for blockchain in the energy sector, while the utility attendees were interested in potential applications and impact on their businesses.

There is a clear knowledge gap between technology developers and existing market participants, as well as legal, regulatory, and technical issues which will need to be addressed. However, three use cases were mentioned that may demand closer inspection:

- Transactive energy to support DER and their interaction with DER management systems (DERMS)
- eMobility – the ability to transact energy charging at stations in multiple service territories
- Customer contracts – removing the middleman from the retail energy market

NEXT STEPS/ONGOING EPRI RESEARCH

EPRI will continue to survey new technologies and the marketplace for blockchain-related capabilities and use cases that would present opportunities in the utility industry. EPRI will also engage utility leadership and thought leaders in this emerging industry to provide information and assess potential impact to the energy industry, and to inform related research activities.

CONTACT INFORMATION

For inquiries regarding the technical content of this brief or for general inquiries about EPRI's Quick Insight Briefs, please send an email to QuickInsights@epri.com.

Quick Insights are developed by EPRI to provide insights into strategic energy sector questions. While based on sound expert knowledge, they should be used for general information purposes only. Quick Insights do not represent a position from EPRI.

3002009889 February 2017

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA • 800.313.3774
• 650.855.2121 • askepri@epri.com • www.epri.com

ELECTRIC POWER RESEARCH INSTITUTE

Quick Insights

Bitcoin Mining, Blockchain, and Electricity Consumption

RESEARCH QUESTION

What is the energy consumption of mining cryptocurrencies such as Bitcoin, and how can utilities best interact with these customers?

INTRODUCTION

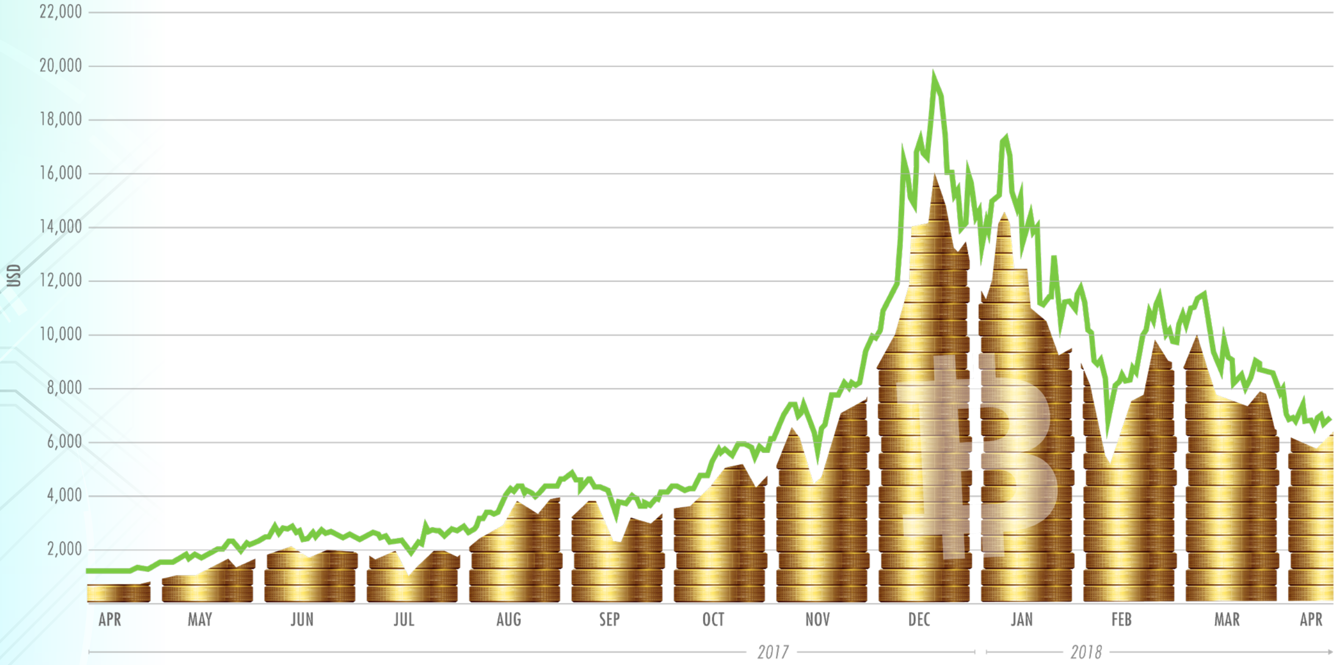
In 2009, Bitcoin became the first digital currency based on cryptography—creating what has become broadly known as *cryptocurrencies*—to provide a medium of currency exchange without a central authority and without backing by a physical commodity or nation-state. There are currently more than 1,300 similar cryptocurrencies using cryptography to secure transactions, control the creation of new currency, and validate the transfer of value. Cryptocurrencies are backed by blockchain technology, which employs cryptography to validate each transaction and create a permanent public record. Bitcoin mining requires large amounts of electricity, but its inherent volatility, decentralized operations, and uncertain future create challenges for electric utilities engaged in long-term resource planning.

KEY POINTS

- Bitcoin mining requires an estimated 1 to 3 GW of continuous electricity demand—representing less than 0.1% of global electricity generation capacity.
- It is difficult to determine the actual electricity use for mining Bitcoin at any given time because there is no central registry of miners. Similarly, it is virtually impossible to accurately predict future growth because the efficiency of mining equipment is changing rapidly, the difficulty of mining varies, and the revenue paid to miners is highly volatile.
- Given that the values of many cryptocurrencies have recently skyrocketed, any reporting that extrapolates current growth rates to project future electricity demand will likely inflate future predictions of consumption.
- The potential boom-bust nature of cryptocurrency mining and the risk of failure for this emerging industry may present a risk to electric utility cost-recovery or lead to stranded assets.
- Amid rapid Bitcoin mining growth in U.S. regions where electricity is inexpensive, local utilities have grappled with accommodating or banning this type of electricity load.
- The blockchain technology that underpins cryptocurrencies could eventually streamline the management of other transactive processes, but it is too soon to determine its ultimate impact.

BITCOIN MARKET PRICE

source: blockchain.info



WHAT IS BLOCKCHAIN?

Fundamentally, a blockchain is a series of digital blocks, each of which contains a set of transactions. A unique identifier represents the contents of each block and the combined value of all prior blocks in the chain. This linkage of unique identifiers, called a "cryptographic hash," ties the blocks together in the chain. Rather than having a centrally stored and controlled ledger like a traditional accounting system, the blockchain's "ledger" is distributed, with each participant in the peer-to-peer network holding a copy of the "distributed ledger."

Each *block* of transactions recorded in a blockchain requires a proof of work (PoW) to validate the block and securely append (and timestamp) it to the ledger. This creates a chain of blocks, hence the name blockchain.

A PoW is a cryptographic hash discovered by performing a computationally intense algorithm called *mining*. A hash function is simple to compute given an input value, but the inverse function—i.e. solving for an input given the output—can only be determined through brute-force trial and error. Because a PoW is required to validate each block of transactions that is added to the ledger, mining is necessary to support the use of the currency. In exchange for computing the hash, a miner earns a reward (typically a small amount of the cryptocurrency).

For more information on potential applications for blockchain technology, see EPRI Quick Insight 3002009889 *[1] and EPRI white paper* 3002010242 *[2], which explain how blockchain technology could be applied to other utility transactional business operations.*

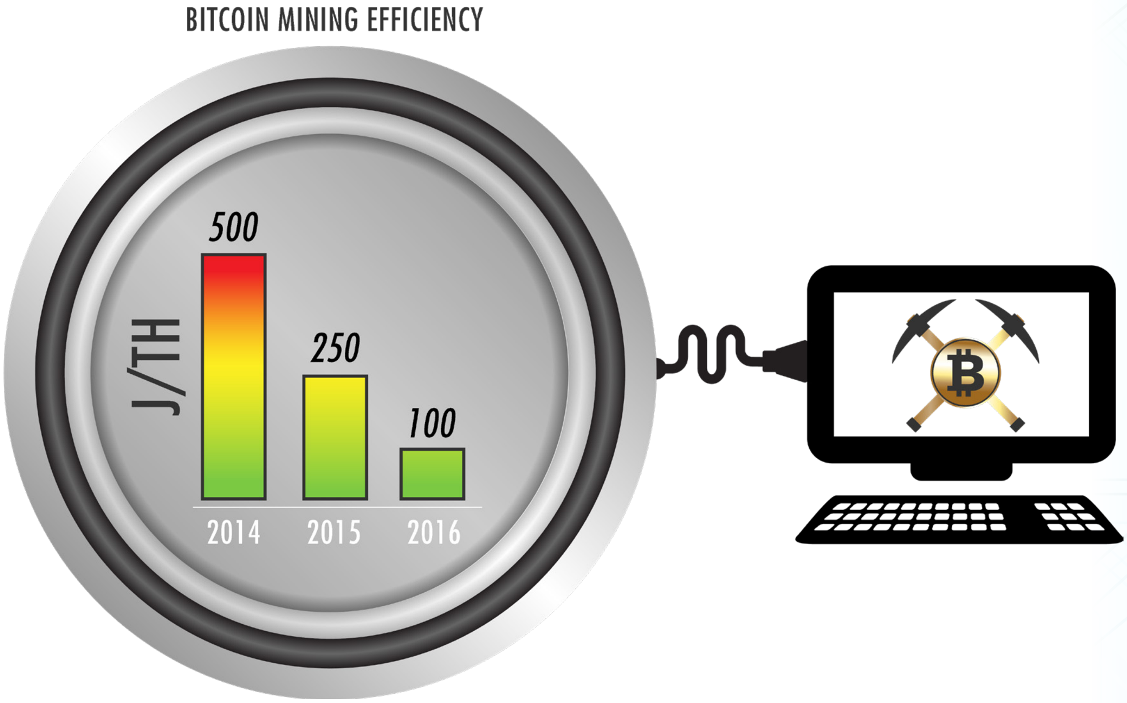
MINING FOR CRYPTOCURRENCY

When Bitcoin was first established, mining was possible using the CPU of a standard desktop PC. As more miners have joined the Bitcoin network, the global *hash rate* (overall number of hash functions that are solved by all miners on the network, now represented by exa hashes per second [EH/s, 10^{18} H/s]) has risen exponentially, to as high as 26 EH/s in March 2018.

The difficulty of the mining algorithm is adjusted roughly every 10 days to maintain an average creation of one block every 10 minutes. With the mining reward set to be halved about every four years, mining will become less profitable over time. As a result of continuously growing resource requirements—particularly the amount of electricity needed for processing and cooling—CPUs are no longer cost-competitive for Bitcoin mining. To improve efficiency, miners initially shifted from CPUs to graphics processing units (GPUs), which offer about an order of magnitude superior mining performance over standard CPUs.

Today's best-in-class mining hardware—which employs an application-specific integrated circuit (ASIC) specially designed for mining Bitcoin—performs two orders of magnitude better than GPUs. Due to advances in chip technology, reported mining efficiencies have roughly doubled every 12 months, from about 500 J/TH (joules per terahash, equivalent to watts per trillion hashes per second) in late 2014, to 250 J/TH in late 2015, to 100 J/TH in mid-2016. Recognizing that one of the largest manufacturers of mining hardware also operates one of the world's largest mining facilities, there may be preproduction mining machines in operation that surpass the commercially available 100 J/TH efficiency level.

Serious Bitcoin mining operations are not expected to reside in conventional data centers because the core business of data centers that house mining operations is to maximize the number of hashes computed for the lowest operating cost. With little concern for equipment availability, mining facilities do not employ the redundancy, fault-tolerance, or power conditioning equipment used in conventional data centers. In addition, many miners use "free cooling," relying on evaporative "swamp" cooling rather than mechanical (vapor compression) cooling. Some mining facilities have no mechanical cooling aside from fans that bring in outdoor air.

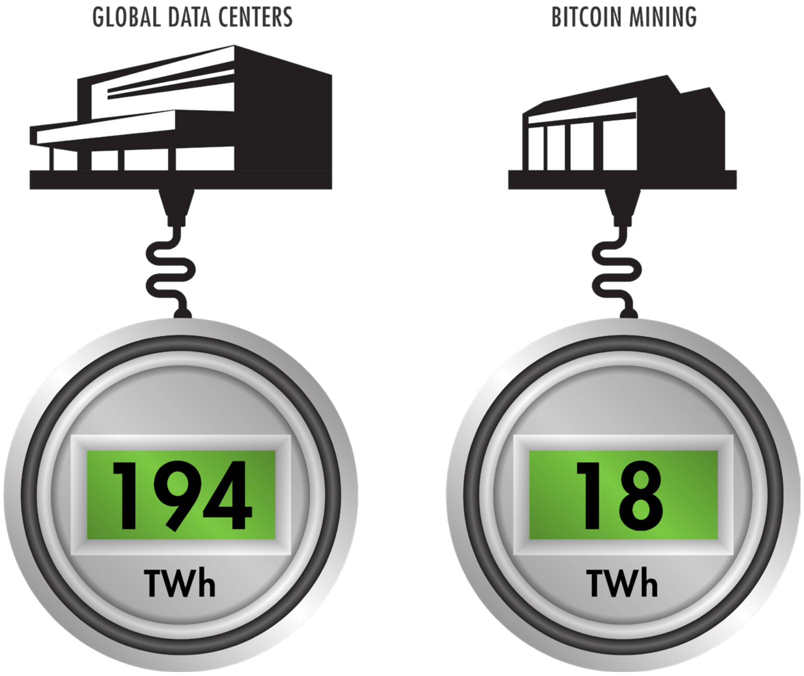


INDUSTRY ENERGY CONSUMPTION

Since December 2017, when the value of Bitcoin reached an all-time high of $20,000 per bitcoin, numerous media outlets have reported on the growing energy consumption of the Bitcoin network. These reports cite the Bitcoin Energy Consumption Index (BECI) published on Digiconomist.net [3] which uses an economic approach to estimate the annual energy consumption of Bitcoin (more than 50 TWh as of March 2018). Note that any estimate of overall energy consumption must make numerous assumptions because there is no central registry of all active Bitcoin mining machines. Moreover, there is neither published data on the efficiency of mining machines in real-world applications, nor data on the number of machines in operation.

However, this widely cited estimate is fundamentally flawed; it assumes that 60% of mining revenue is spent on electricity, without providing a citation. One critic of this approach [5] suggests that the actual percentage of mining revenue spent on electricity may range from 6% to 32%, when accounting for capital recovery. In addition, the author of the BECI estimate presents a case study from an operating mining facility that found that the real-world efficiency of mining machines was less than rated efficiency—a finding attributed to the elevated operating temperature and failure rates seen in the real-world application.

Marc Bevand, a cryptocurrency researcher and entrepreneur, makes a more detailed evaluation of hardware efficiency on his website [4]. This approach took an in-depth look at the evolution of mining hardware efficiency over time, estimating the number of machines added in each hardware generation as a function of the increasing global hash rate. It makes the conservative estimate that only the least-efficient hardware available in each generation was added, so long as it was profitable to operate at $0.05/kWh. On January 11, 2018, Bevand updated his estimate of the global Bitcoin mining network to be 2.1 GW of demand (upper and lower bounds of 1.6 and 3.1 GW) and 18 TWh of annual consumption (bounded by 14 and 27 TWh).



The results of this estimate and others suggest that Bitcoin mining worldwide is on the order of 2 to 3 GW. With global installed generating capacity totaling more than 6,200 GW as of 2015 [6], Bitcoin mining represents less than 0.1% of world generating capacity. In 2014, the annual energy consumption of data centers worldwide was estimated to be 194 TWh [7], roughly 10 times the annual consumption of Bitcoin mining estimated by Bevand [4].

There may be valid concerns as to how the energy intensity of cryptocurrencies would scale if they were to handle the number of transactions supported by credit cards each year (roughly two orders of magnitude more). Any reporting that extrapolates current growth rates—when the value of the currency has recently skyrocketed—will likely inflate future predictions of energy consumption. It is virtually impossible to make an accurate prediction of growth in mining demand due to the number of unknown variables, including:

- Mining difficulty depends on the number of miners connected;
- The real-world efficiency of mining hardware is unknown, and reported hardware efficiency has improved at an unprecedented rate;
- The revenue paid to miners is highly unpredictable because it is determined by the value of the cryptocurrency, which has been highly volatile.

EVOLVING INDUSTRY

While it is impossible to predict the rate of future mining growth, there is evidence that this industry may continue to expand in the near future. First, demand for mining equipment has created a scarcity of best-in-class hardware, and prices have risen significantly. In addition, anecdotal reports from mining operations and utilities indicate that it is growing rapidly in certain parts of the United States.

Previously, the majority of commercial Bitcoin mining operations have been located in China—specifically, Inner Mongolia—due to its cool, dry climate and reportedly low cost of electricity. In January 2018, the Chinese government began to curb mining, in part due to its impact on demand for electricity. Since then, there have been several reports on mining operations seeking to make significant expansions in areas of North America where electricity and land prices are modest and the climate favors free cooling. For example, mining operations in Wenatchee, WA have been able to take advantage of low-cost electricity and unused distribution capacity left by shuttered industries (namely aluminum and logging). On the other hand, Plattsburgh, NY has banned any additional mining operations from locating there for 18 months due to the impact that these facilities may have on local electricity prices.

Even with low-cost electricity, the volatility of mining revenues may drive some mining companies to cease operations before electric utilities fully recover the costs of delivering service. With so much uncertainty in the longevity of this market, utilities may best consider these customers cautiously. Yet given the high load factor of these facilities, some utilities might consider them very attractive customers, if only for a limited time.

One aspect largely missed in the discussion of blockchain efficiency is the potential for the technology to make other transactive processes more efficient. Because blockchain eliminates the need for a central database manager or independent transaction validator, it could streamline transaction management in areas other than cryptocurrency. If used for transactional databases in other industries (e.g. the insurance, medical, real estate, and banking sectors), Blockchain technology has the potential to offer global (societal) efficiency gains (i.e. digitizing and streamlining the management of verified transactions) while increasing electricity use to validate the transactions. However, it is too early in the maturity of this technology and its deployment to predict the potential efficiency gains. This is an area of continuing research that EPRI is conducting under its Information and Communications Technology for Integration of Distributed Energy Resources program [8].

RESEARCH GAPS

- Can the actual energy consumption of cryptocurrency mining be more accurately estimated? What is the real-world efficiency of deployed mining machines?
- What is the risk to an electric utility of stranded assets or failure to recover costs?
- Can a mining operation follow time-of-use rates and only be active during periods of low electricity prices?
- Are there methods for making cryptocurrencies more efficient while maintaining security and validity?
- Can blockchain technology offer global (societal) efficiency gains (i.e. digitizing and streamlining the management of verified transactions)?
- What electric utility or other industry processes are best suited to blockchain technology?

REFERENCES

1. *Quick Insights – Blockchain: Early Activity for Utilities*, Electric Power Research Institute, Palo Alto, CA. Product ID: 3002009889, February 2017. https://www.epri.com/#/pages/product/3002009889/

2. *Blockchain: Technology Risk and Rewards for Utilities*, Electric Power Research Institute, Palo Alto, CA. Product ID: 3002010242, October 2017. https://www.epri.com/#/pages/product/3002010242/

3. A. de Vries, "Bitcoin Energy Consumption Index." [Online], (Accessed: 15 March 2018). https://digiconomist.net/bitcoin-energy-consumption

4. M. Bevand, (2017, 10 March). "Electricity consumption of Bitcoin: a market-based and technical analysis," [Online] http://blog.zorinaq.com/bitcoin-electricity-consumption/

5. M. Bevand, (2017, 1 February). "Serious faults in Digiconomist's Bitcoin Energy Consumption Index," [Online] http://blog.zorinaq.com/serious-faults-in-beci/

6. U.S. Energy Information Agency. http://www.eia.gov

7. *Digitalization & Energy*, International Energy Agency, Paris, France, 2017.

8. *Information and Communications Technology and Security Architecture for Distributed Energy Resources Integration*, Electric Power Research Institute, Palo Alto, CA. Product ID: 3002009694, January 2017. https://www.epri.com/#/pages/product/000000003002009694/

CONTACT INFORMATION

For inquiries regarding the technical content of this brief or for general inquiries about EPRI's Quick Insight Briefs, please send an email to QuickInsights@epri.com.

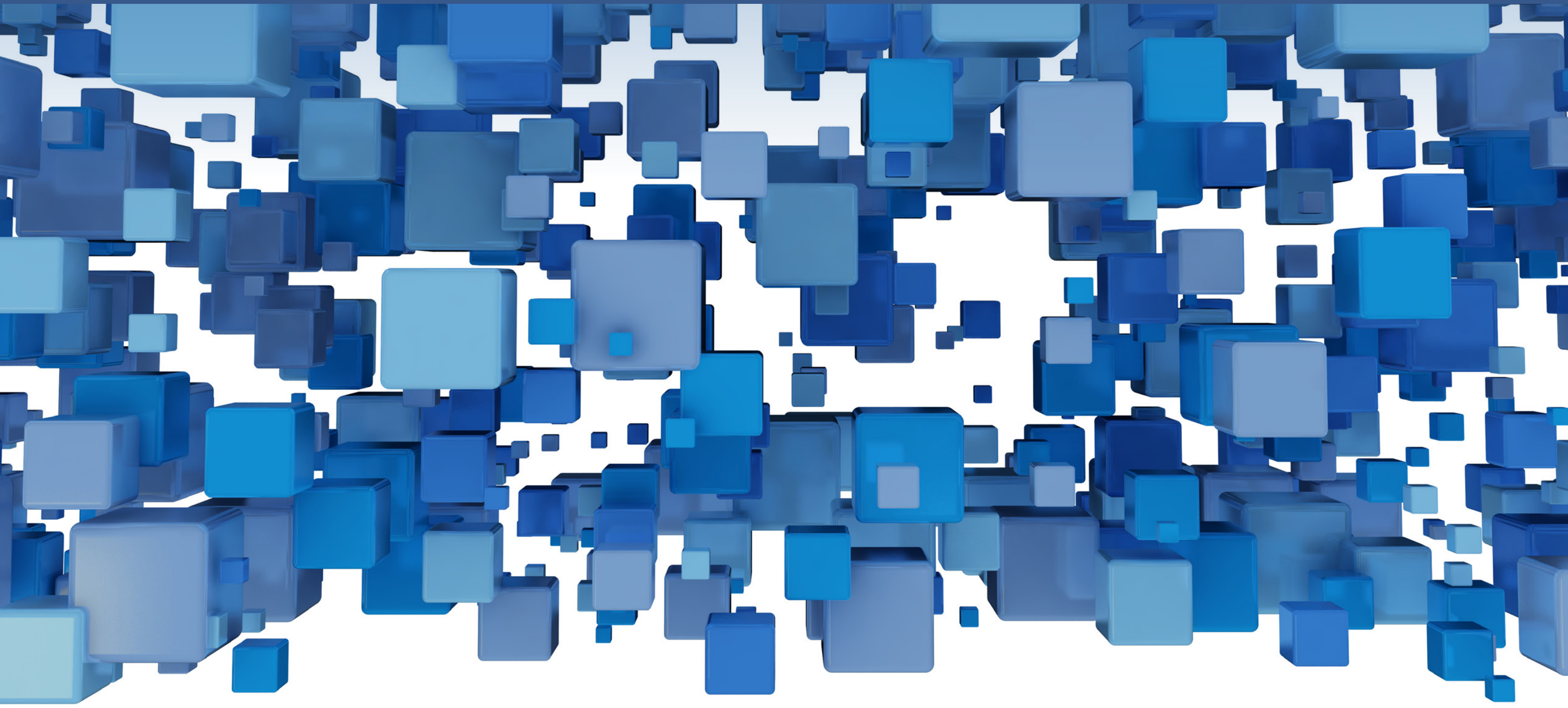
Quick Insights are developed by EPRI to provide insights into strategic energy sector questions. While based on sound expert knowledge, they should be used for general information purposes only. Quick Insights do not represent a position from EPRI.

3002013910 April 2018

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA • 800.313.3774
• 650.855.2121 • askepri@epri.com • www.epri.com

ELECTRIC POWER
RESEARCH INSTITUTE

BLOCKCHAIN: TECHNOLOGY RISK AND REWARDS FOR UTILITIES



Abstract

Blockchain is a potentially disruptive technology that will impact the way in which many business transactions are conducted in the future, including those used by the utility industry and its trading partners. While it is most commonly known as the technology behind cryptocurrencies such as Bitcoin, the greater impact will likely be with the implementation and automation of "smart" contracts that reduce costs by eliminating intermediaries. In this white paper, the characteristics of blockchain will be explored, providing insight into why this is a disruptive technology, the places blockchain is being used today, some of the potential applications of this technology in the utility industry, and the current challenges and limitations of the technology of which utilities need to be aware.

WHAT IS BLOCKCHAIN?

Fundamentally, a *blockchain* is simply a chain of blocks (hence the name), with each block containing a set of transactions. Within each block, a unique identifier is generated that represents the contents of that block, and additionally, the value of all the prior blocks in the chain. This linkage of unique identifiers, called a "cryptographic hash", is what ties the blocks together in the chain. Additionally, rather than being centrally located like a traditional accounting system, with a ledger stored and controlled in a central database, the blockchain's "ledger" is distributed, with each participant in the peer-to-peer network holding a copy, hence the term "distributed ledger".

How Blockchain Works

In addition to the cryptographic hash, each block contains other data as well. In the case of cryptocurrencies such as Bitcoin, the block contains a list of *transactions* and the entire blockchain functions as a distributed ledger, which means that all the participants on the blockchain network have, and can verify, the contents of the blockchain. This transparency is an important feature of blockchain.

Whenever a node wishes to create a new transaction, for example, a customer wants to buy a hat, or two financial institutions want to exchange currency, this transaction is sent to neighboring nodes in the blockchain network. Because each transaction is digitally signed, each receiving node verifies the signature. Each receiving node propagates signed transactions, discarding any that cannot be verified. Collections of transactions are packaged into a *candidate block* by nodes in the peer-to-peer (P2P) network. This packaging and linking is called *mining* and has several different forms, depending on the type of blockchain mechanism used. The *miners* receive a "proof of work" for solving the puzzle (the hash of the prior blocks in the chain plus the new transactions). Receiving nodes verify the validity of these candidate blocks and accept them, adding them to their own blockchain. As candidate blocks are propagated and accepted by other nodes, the network arrives at *consensus* on the current state of the blockchain.

For a high-level view, Figure 1 below, illustrates the steps in the blockchain process.

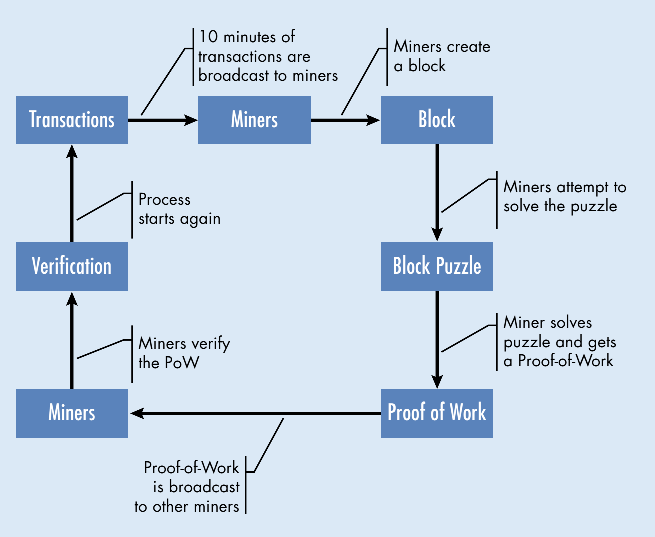

10 minutes of transactions are broadcast to miners
Miners create a block
Transactions
Miners
Block
Process starts again
Miners attempt to solve the puzzle
Verification
Block Puzzle
Miners verify the PoW
Miner solves puzzle and gets a Proof-of-Work
Miners
Proof of Work
Proof-of-Work is broadcast to other miners

Figure 1. Blockchain process (adapted from Napkin Finance[1])

Transaction Basics: "I want to buy a hat"

Assume for a moment that a customer wants to buy an item using a cryptocurrency such as Bitcoin (see Figure 2). The customer needs to send the merchant ("Hats R' Us"), a bitcoin for payment (based on the current valuation, a very expensive hat!). The merchant generates an address[2] and sends it to the customer. The customer forms a transaction to transfer from their address to the address of the merchant. The transaction record contains a unique address and all the details of the sale. This transaction is then broadcast to all the miners on the P2P Bitcoin network. The miner takes this transaction (and all the others it has received) and puts it into the next block in the chain (per Figure 1). The merchant will either wait for notification (approximately 10 minutes for the miners to verify the transaction), or for low value transactions, simply assume the transaction is accepted so that the customer does not need to wait.

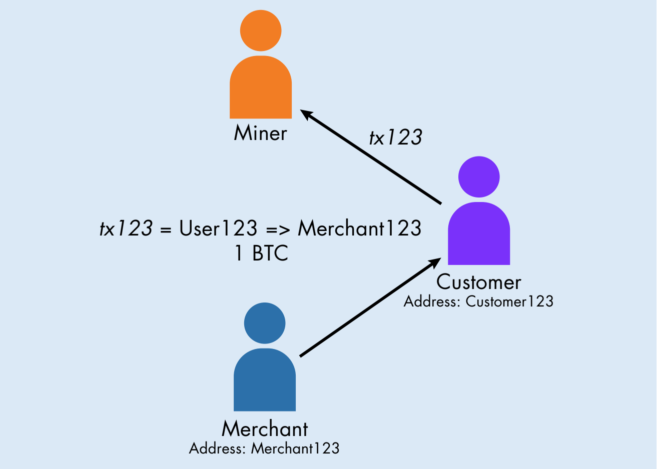


Figure 2. Simplified blockchain transaction sequence

Bitcoin Ecosystem

While the Bitcoin ecosystem [1] is not definitive for all blockchain, other blockchains will have similar actors participating in whatever ecosystem evolves relative to a given blockchain. Bitcoin is the most established of the cryptocurrencies, so this discussion starts there.

Code base / Developers – Each blockchain, while using the fundamentals of the distributed ledger, may have attributes that are unique to its design, for example, how many tokens can be created or what the token is (Bitcoins in the case of Bitcoin, Ether in the case of Ethereum), that distinguish it from other blockchains. For each code base, (the software) upon which a blockchain is based, a community of developers has control to limit changes that would split

[1] https://napkinfinance.com/napkin/bitcoin-blockchain/

[2] Addresses are generated within the Bitcoin core software, is an identifier of 26-35 alphanumeric characters, https://en.bitcoin.it/wiki/Address

the community, such as different miners running different versions of the code. This protects the community by helping to ensure that each node in the blockchain P2P network runs the same version of the software. This prevents challenges such as differences in determining how consensus is reached and, hence, which are the valid blocks in the chain.

Large miners / Pool operators – In the Bitcoin ecosystem, miners are rewarded for generating a key and establishing a proof-of-work with bitcoins. In the early days of Bitcoin, a person with a single desktop computer had a reasonable chance to get such a reward. However, as the number of participants has increased, the reward for generating the proof-of-work has been outstripped by the energy costs to run the computer system. Only the largest miners, with the latest technology, optimized for mining and energy costs, can now reasonably expect to be rewarded with bitcoins. An individual operator has an increasingly smaller chance of getting such a reward. Hence, the evolution of pool operators. A smaller miner can join this pool, increasing the chance of a reward being earned by this group, and the rewards are spread across all the participants in the pool.

Users / Wallet providers – Users or customers, create new transaction requests, for example, maybe they would like to buy a hat. Software, called a wallet, passes requests to the P2P network, and these transactions are then packaged into blocks. A wallet allows a person or entity to generate a transaction without having to do the mining.

Payment processors – This software allows organizations the ability to offer payment services in Bitcoin, but then pay their clients in non-digital currencies.

Exchanges – Just like traditional currency exchanges, this allows bitcoin to be exchanged with other currencies.

BLOCKCHAIN AND THE DISRUPTION CURVE

The disruption curve [Figure 3 below] illustrates how new technology can destroy incumbent players in established markets. Based on the work of Clayton Christensen, who discovered the phenomenon while investigating architectural changes in the hard drive industry and found that the curve repeated itself across many industries and technologies. Christensen makes the distinction between "sustaining innovation" versus "disruptive innovation". This finding dispelled the notion that perhaps companies were not listening to their customers or investing in their product lines. Quite the contrary. They often did, but the investment in existing products and listening to customers led to only changes in existing technology.

Disruptive technology is often not recognized when it emerges. It often underperforms existing technology. However, disruptive technology presents certain attributes that new customers prefer, and in fact, disruptive technology often must identify new customer to be successful. When the new technology matures, and begins to outperform the incumbent technology, then it begins stealing customers from the incumbent (Figure 3 below).

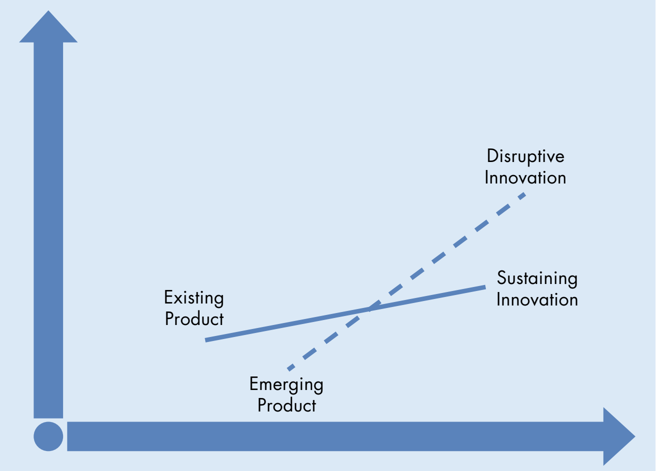


Figure 3. Disruptive innovation curve

It remains to be seen if blockchain's distributed ledger technology appears to be just such a disruptive technology.

Blockchain emerged in response to the financial crisis in the hopes of increasing transparency and to create a currency with specific attributes such as immutability, and limited supply (much like gold). At the time, these attributes were attractive to a small audience. As Bitcoin demonstrated the capability of the technology and became more accepted, innovators began exploring how distributed ledger technology could be employed in other types of transactions. While there are challenges with Bitcoin itself when it comes to issues such as scalability, the technology is being applied to a host of "smart contracts" and distributed applications. While any new technology must answer the question of, "How does this technology do something better than the existing technology?" to justify investment, it appears that it may be applicable anywhere contracts or exchanges are used today, with the added benefit of eliminating third parties to the transaction, which lowers costs [4].

The attractive advantages for new customers are reduced transaction costs, anonymity (to a greater or lesser degree), and immutability of the transaction. In this regard blockchain has been creating a new set of customers; however, the destruction of incumbents, the key hallmark of disruptive technology, has not been observed yet.

Blockchain and Distributed Applications

While blockchain is more well known as the technology behind cryptocurrencies, its greater potential is in the use of distributed applications, or in blockchain vernacular, "dapps". There are hundreds of dapps that cover everything from games, to insurance, to unalterable constitutions. Anything that can be contracted (essentially, any exchange), can be codified in a distributed ledger. The value-add of dapps is that they leverage the transparent quality of distributed ledger and payment is typically immediate. This immediacy of payment, which functions essentially like cash, is one of the other benefits of blockchain.

BLOCKCHAIN CHALLENGES

Like any technology, there are tradeoffs intentionally made in the design to favor certain characteristics over others. Looking at the Bitcoin implementation, there have been challenges with scalability, anonymity, and hacking [4][5][6], albeit with some interesting twists.

Scalability – The Bitcoin blockchain is now 149 GB[3]. This is easily handled by computers of the scale that are typical in utility data centers. However, it is estimated that a "Visa scale" global network (~2000 transaction per second) would grow at a rate of 2.5 terabytes (TB) per month [7], which requires planning to accommodate such a file, and would, of course, outpace the ability of utility grid edge devices to be a peer on the Bitcoin blockchain network (although edge devices could run a wallet and transact with a peer). As it related to the Internet of Things (IoT) there are questions about the ability of cryptocurrencies to support the micro transactions that these devices might employ as they exchange services.

Anonymity – As discussed in the "Getting Technical" section, blockchains can be permissionless (anyone can join) or permissioned (only authorized entities may join). It is often assumed that Bitcoin is anonymous, when it is technically *pseudo-anonymous*. Parties to transactions do not have to give identifying information beyond their public key, but there are methods available to determine a given party's identity (for example, some companies offer services wherein they examine the Bitcoin transaction to deduce a party's identity). Alternatives to Bitcoin, such as zCash [8] and Monero[4], promise complete privacy for those engaging in transactions. There is an interesting dichotomy at play when Bitcoin's acceptance has been reflected in increasing regulation. [9][10][11] Blockchains that are completely anonymous not only disrupt markets, but disrupt regulation as well (if you're using it, no one can tell). Also, when the particulars of a transaction are stored or controlled by a "smart contract" [12], this requires less need for oversight because the "oversight" is encoded in the contract to which the parties agree.

Security and Control – Those that control the nodes, control the contents of the blockchain. This goes back to how consensus is reached on the blockchain. The nodes "vote" on the longest chain. If a single entity controls more than 50% of the nodes, then that entity can determine which block "wins". This has implications for both permissionless and permissioned blockchains, where a consortium controls the nodes; participants need to be mindful of the 50% rule. This also has implications for claims that blockchain will solve IoT security challenges. This is because the devices themselves are still vulnerable. If more than 50% of the IoT devices are compromised, then the blockchain they transact on can also be compromised.

An IoT consortium, led by CISCO, Bosch, and others, is working to leverage blockchain to "secure and improve" IoT applications [13]. However, while the blockchain itself is secure due to the nature of the security employed to encrypt the transactions, this does not inherently secure the IoT devices themselves. For example, traditional device issues, such as not changing the manufacturers default password or inappropriately applying vulnerability patches, could allow bad actors to launch a distributed denial of service attack (DDoS) from these vulnerable devices [14]. If the devices are compromised, then these devices could flood an IoT-based blockchain with bogus transactions.

While blockchain technology has some technology challenges that need to be addressed as it matures, it still bears the hallmarks of a disruptive technology.

The Ethereum Hard Fork – One demonstration that blockchain technology is still maturing, was the "hard fork" (a change in the software that runs Ethereum) that was used to restore stolen funds [15]. This change to the software was required to return roughly $40 million worth of ether that had been stolen from an account owned by an unknown

[3] https://bitinfocharts.com

[4] https://getmonero.org/home

hacker. While the hack was remediated, the act of remediation raises questions about the supposedly immutable blockchain and the finality of any contracts based on said blockchain.

APPLICATIONS IN THE UTILITY INDUSTRY

Outside the exchange of Bitcoins used with financial applications, there have been few implementations of blockchain in the utility industry. In terms of simply enabling financial transactions via electronic data interchange (EDI), automated clearing house (ACH), or other means, Bitcoin is simply another currency that could be enabled to be used for payment just as dollars or Euros are used. However, there are several other applications in the utility industry that could also implement blockchain.

Transactive Energy

Transactive energy is a concept that refers to the "economic and control techniques used to manage the flow or exchange of energy within a power system"[5]. The example of transactive energy exchange is a bit more complicated because transactions are not limited to being between a utility and their direct customers. Customers can also sell to their neighbor – the "prosumer" concept, which is the notion that a customer might be both a buyer and seller of energy.

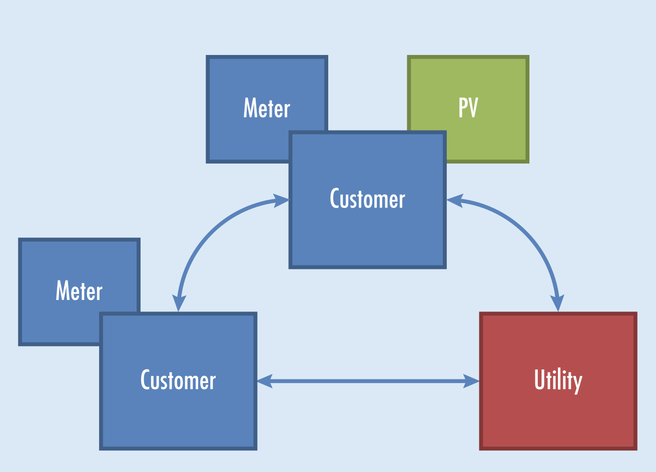


Figure 4. Simplified transactive energy exchange

For example, in Figure 4, suppose the customer with the PV generates more energy than they need and offers to sell it to the other utility customer. In this future looking scenario, a meter still provides the measurement and verification (one wants confirmation that what one is paying for has been produced). The utility, in this scenario, is the distribution system operator and provides the wires for the energy exchange to take place, and one or both parties would have a transaction fee to the utility that pays maintenance overhead on this operation, in addition to the transaction fee that would be associated with the blockchain in use. Again, blockchain computational requirements exceed the capability of residential meters, so another platform would need to be provided to manage the peer-to-peer network, perhaps an additional meter behind the utility meter as we see in the LO3 configuration of the Brooklyn microgrid, or a device that can run a blockchain wallet, or there may be a distributed peer on the circuit run by the utility, e.g. a distributed DMS or DERMS that in addition to providing control function could also provide the mechanism for the blockchain transaction. Contrast this with how transactive energy is provided in the United Kingdom.

P2P Energy in the UK

The United Kingdom already supports a P2P energy trading program, albeit a traditional one. Good Energy[6] allows customers to sign up to purchase power from renewable energy suppliers that come in two categories: a 10 kW – 100 kW provider with a pay in tariff (PIT) tariff, or for >100 kW suppliers, power purchase agreements (fixed, variable, and "cost for difference"). Buyers can choose from whom they wish to purchase and sellers get a predictable income.

> Customers who sign up to the service are given access to an online portal where they can set preferences and priorities for their energy supply at certain points throughout the day. If a generator is available, the two parties are matched and the business will effectively pay that generator for the electricity it consumes. [1]

The difference is that Good Energy appears to be the normal third party handling the arrangements. In a blockchain-based P2P, once contract terms are met, buyers and sellers trade; there is no third party setting the market.

Metering

While blockchain could be used to secure transactions, there are some facets of smart metering today that do not lend itself to this application. Metering actors include the meter, the AMI Head-End, optionally a Meter Data Management System (MDMS) that may serve as a data ware-

[5] http://www.gridwiseac.org/about/transactive_energy.aspx
[6] https://www.goodenergy.co.uk/business/our-generators/power-purchase-agreements-ppas/

house for metering data, and the Customer Information System (CIS) which ties meters to customers and generates the bill. In traditional metering, there does not appear to be much place for blockchain to provide a "better" story.

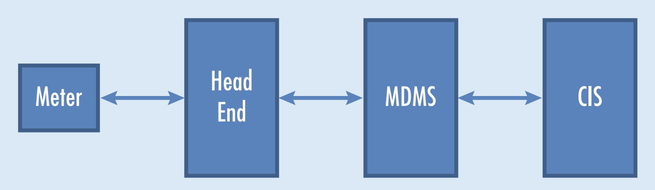


Figure 5. Simplified AMI metering data flow

The data flow for AMI metering is already secured, so there is not a value proposition for blockchain relative to that. In this case, the data exchange is only between the utility customer and the utility. There is no third party involved. Also, blockchain as currently available outstrips the ability of a standard residential meter's computational capability.

Move-in / Move-out / New Service / Prepaid metering

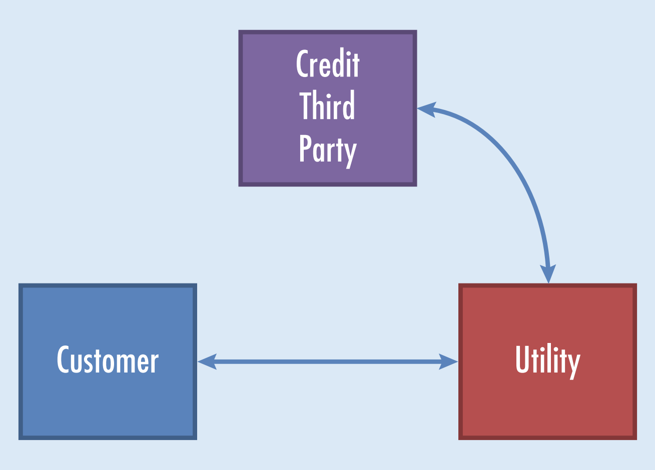


Figure 6. Simplified customer engagement process

Where there might be a place for blockchain in this scenario is for the move-in/move-out process or to setup pre-paid metering. This is not the metering information path, but rather the "out of band" communications that goes on between a potential customer, the utility, and third parties that may confirm the creditworthiness of a customer. In this scenario, the customer indicates a desire to become a utility customer. The utility uses a third party to confirm the creditworthiness of a customer and may require the customer to provide a deposit before engaging in a service contract.

Now consider using blockchain in this scenario. The tokens used by blockchain such as Bitcoin function like cash. If the customer wants to engage in business, blockchain assures the merchant, in this case, the utility, that the cash (tokens) are on hand before entering into a contract. The credit third party can be eliminated (saving the utility money) and speeding the execution of the transaction. The customer and utility agree to pay via a blockchain currency, with the costs limited to the transaction fee of the blockchain in use. If the utility and customer use a permissioned blockchain, the transaction has the added benefit that the customer identity is verified before the parties enter into the transaction.

Mobile Payments

Even as early as some of the first requirements gathering efforts were occurring for Home Area Networking (HAN), vehicle charging and the payment for those services had been considered as part of that development. If a customer has an electric or plug-in hybrid electric vehicle, this process is straightforward. One adds electric vehicle supply equipment (EVSE) to their premise, contacts their utility if there is an applicable tariff or program, and they can charge their vehicle.

The problem gets a bit more complex if the vehicle owner drive the vehicle to a different location and charges their vehicle there. If the location is in the same utility service territory, the driver simply needs to pay for the service locally, and if they wish to get credit within the utility program, then they need to identify themselves at that location.

It gets more complex when the electric vehicle user crosses territory. Potentially this customer would need to create an identity with every utility with which it desired to charge from. In the early days of HAN requirements, it was supposed that a national clearinghouse would emerge much like a VISA or American Express that would handle these transactions. But these clearinghouses operate on a per-

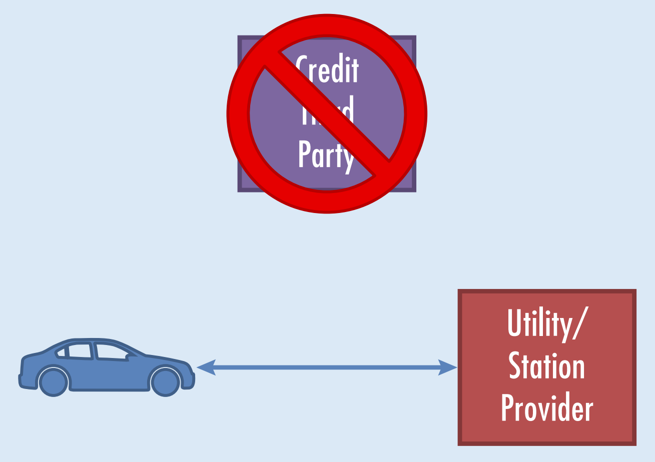


Figure 7. Simplified charging diagram with third party credit handlers eliminated

centage of the transaction, 3% and 5% respectively. Given the low transaction amount for vehicle charging this does not provide much of an incentive to enter this market.

Now imagine that one is not only crossing utility service territory, but national boundaries as well. This is the situation with electric vehicles in Europe and the Ethan BIoT charging stations. The Ethan BIoT stations accept cryptocurrencies that can be paid via a blockchain wallet so the fees associated with the transaction are very low and no registration with a local charging provider is required because the identities and transactions are managed by the blockchain, and if the underlying infrastructure is used, it does not matter what local entity (utility, government, private) operates the charging station. For a similar case to work without blockchain, the existing charging station providers would need to agree to a common messaging infrastructure between all of the potential transaction participants, secure it, and then provide a mechanism to ensure transparency (or be audited), all of which would increase the operating costs. While the market is small today, the value proposition will increase as the numbers of electric vehicles and charging stations increase.

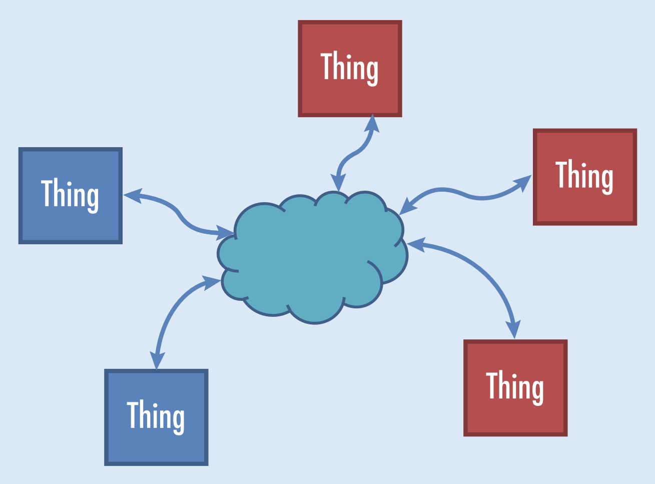


Figure 8. Simplified IoT with the majority of devices compromised

Internet of Things

One of the promised benefits of blockchain is that it will make IoT more secure. But again, there are two problems: 1) the computational capability of the device and 2) blockchain might secure the *message*, but it does not inherently secure the device. The promise of IoT as it relates to utilities (sometimes referred to as energy IoT or "eIoT") is that as more devices are deployed into the grid it gives utilities greater visibility and control.

When the home security cameras were compromised, the issue was not with the messages per se, it is that the devices were compromised in the first place, allowing the devices to participate in the distributed denial of service attack. With IoT, the messages might be secured and properly formatted, but if the devices themselves are compromised, if an entity gets control of the majority of devices, then that entity will determine the content of the blockchain. When a device uses a low-power protocol such as CoAP that is designed to run in as little as 10 KB RAM, that suggests it may not have the processing power to support blockchain, even if it is only the wallet (allowing the device to transact) and not a peer. Again, there are various strategies in place today to secure IoT messages (TLS/SLS, DTLS, depending on the messaging protocol), but the challenge is securing the devices. It remains to be seen if the design compromises required to get an IoT device to support blockchain would be more or less secure than the security protocols current supported for the messages; device security remains a separate issue.

Asset Management

The story of the "lost" transformer is an issue as old as transformers themselves. (Transformer in this case is a surrogate for any asset deployed in the field). The utility orders a transformer; it arrives and is scanned into the system. When it is needed for a job, the transformer is scanned, removed from inventory, and loaded onto the truck. The transformer is deployed in the field, with its location theoretically noted by the crew. However, in the past days of paper-based paperwork, it was not uncommon for the paperwork to be lost or incomplete. As systems have been automated and barcodes or RFID employed to tag assets with tablets, laptops, and scanners employed to automate the transfer of custody, the barriers to adopting these leading practices have been reduced, though perhaps not eliminated, as the process still relies on a human to perform these functions.

The benefit that blockchain brings to this situation is that the record is immutable. It cannot be changed or forged (assuming some nefarious intent and not just "I forgot to scan the asset"). Although an asset still relies on a human actor for transfer, one thing will be known for certain, who the last person was to "touch" it.

“Smart” Contracts: Appliance Service Plan example

Another area where a smart contract might be employed is with Appliance Service Plans. Often utilities offer this service themselves or via a contractor. Customers typically sign up via a web site and the work is contracted to annually inspect and service equipment, and in the case of a failure, replace or repair the equipment that is included in the plan. One of the benefits of a smart contract is that it is executed once the terms of the contract are met. Again, assuming a known entity via a permissioned blockchain and tokens that are treated as cash (no need for a credit check or if funds are available), the contract could be executed immediately. Compare this experience to banking or real estate (or utilities) where signed paperwork still needs to be faxed before an agreement can be executed[7].

European Utilities Get Involved

Other utilities in Europe investigating blockchain technology include: ENEL, EON, EDF, Innogy, CEZ, Fortum, Vattenfall, Iberdrola, EDP, BSE, Eandis, ACEA and Alliander, as well as the British TSO National Grid and Eurelectric [21] that participated in a two-day workshop in Amsterdam. ENEL indicated that they see a need to review architecture impacts and the primary area of focus for them is low-medium voltage grid management, trading on the energy and commodities markets, and renewable energy, for facilitating payments within microgrids[25].

LOOKING FORWARD

Bitcoin has moved from nascent technology to being accepted, albeit with at times dramatic fluctuations, as a currency that is used on world markets. But the disruption associated with blockchain distributed ledger technology is not with the emergence of this cryptocurrency, but with dapps, the distributed applications that will replace how any exchange based on a contract (buyer, seller, consideration, and terms) are executed. Realizing this, several consortiums have formed to address the financial sector [22], IoT, Logistics, and a coalition in the energy sector called the “Energy Web Foundation”[8]. EPRI will also be exploring how blockchain may impact different facets of the utility business, with emphasis on cyber security in the supply chain within the Information Communication and Cyber Security Program 183, and the *Information and Communications Technology and Security Architecture for Distributed Energy Resources Integration.*[9]

We have only touched upon a small sample of use cases here. While these show some promise, the “killer app” for distributed ledgers has yet to be identified. For those looking for potential applications of distributed ledger technology in the utility industry, there are two sources one might start with, either the American Productivity and Quality Center (APQC)[10] Process Classification Framework (PCF) utility specific model, or the EPRI Business Architecture Service Repository[11]. Both list hundreds of business processes that exist within utilities. These lists of processes and services could be reviewed for how distributed ledger technology either makes the process better (using the unique distributed ledger characteristics of immutability ad transparency), or faster, by eliminating intermediaries.

In addition to utilities, it seems all the well-known technology companies, IBM, Google, Microsoft, in addition to a plethora of start-ups are emerging, all to create new blockchain applications. EnergyBiz cited a Navigant estimate that the spending to support these related technologies “will be about $182.6 million in 2016, growing to around $2.1 billion by 2025” [23].

Keep an eye on incumbent players. For example, while big banks are investing in blockchain applications because of the reduction in transaction costs, there will be emerging companies trying to displace banks for the very same reason.

Similar issues revolve around regulation. There are emerging attempts to regulate cryptocurrencies, but a permissionless blockchain where all the participants are completely anonymous has the ability to sidestep regulatory frameworks. Utilities will not want to be caught up in such schemes, but the potential disruption to regulatory agencies and their attempts to deal with this will bear watching.

As with any emerging technology, utilities should continue to monitor the capabilities as they evolve, but be wary of

[7] Stoker, L. (2016). Good Energy formally launches peer-to-peer renewables trading service Selectricity. Available [Online]: http://www.cleanenergynews.co.uk/news/solar/good-energy-formally-launches-peer-to-peer-renewables-trading-service-5133

[8] www.energyweb.org

[9] https://www.epri.com/#/pages/product/000000003002009694/

[10] https://www.apqc.org/pcf

[11] https://www.epri.com/#/pages/product/000000003002011054/

start-ups that are not familiar with the utility business. Expect to see smaller companies go out of business, be acquired, or exit the space where they cannot compete. As the many pilots begin to emerge, it will also be important to be wary of products that might still be in beta, or otherwise not ready for full production mode, or companies that may outgrow their ability to support the customers they do gain. Gartner has blockchain at or near the peak of the hype cycle [24]. Be prepared for a shaking out period as blockchain enters what Gartner refers to as the "trough of disillusionment". Cryptocurrencies such as Bitcoin and Ethereum seem to have established themselves, but other applications of the technology have yet to do so and no "killer app" outside of these cryptocurrencies has really emerged.

Utilities should also be wary of pilots or applications that do not have a clear story of how blockchain technology improves or eliminates redundant processes, improves speed of delivery, or provides some other operational benefit. History has shown that in the IoT space, there have been overstated claims of how simply using blockchain solves the security issues related to the devices themselves, so utilities will need to dig into benefit claims and ask for demonstrated capability of blockchain related products and not chase blockchain because it is the latest silver bullet to hit the industry. There will be cases where blockchain provides a clear benefit, but these "can't miss" use cases are still in the process of being determined.

For more information

Please contact Dr. Gerald R. Gray, ggray@epri.com, +1.865.218.8113

GETTING TECHNICAL: THE DISTRIBUTED LEDGER

Blockchain is more than the technology behind cryptocurrencies such as Bitcoin. Due to the nature of distributed ledger technology that blockchain supports, the capabilities of smart contracts is likely to be the most disruptive feature of the technology. But first, readers will need to get technical for a moment while some of the pieces that make this technology work are explored to have a better understanding of the potential impacts. Also, when vendors come calling, it is important to be able to understand the basics of the technology so as to be able to validate any vendor claims about their products capabilities.

Public Key Cryptography

An important mechanism employed in blockchain is *public key cryptography* which is also known as *asymmetric key cryptography* to contrast it with *symmetric key cryptography*. With any symmetric encryption mechanism, the two fundamental operations are *encryption* and *decryption*. With encryption, an input message is rendered, often called the *plaintext*, into an equivalent message called the *ciphertext* which, ideally, is completely unintelligible. In symmetric key cryptography, which includes the well-known and widely used Advanced Encryption Standard (AES), the same key is used for both encryption and decryption. It is important to note that the security of such encryption is solely dependent on keeping the key secret. The fact that the algorithm is well known does not adversely affect the security of messages encrypted with such algorithms.

By contrast, public key cryptography employs key pairs. The pair of keys are related mathematically by one of a few so-called *trapdoor* or *one-way functions* in which is relatively computationally easy to compute a function, but for which the inverse function has no such algorithm. Of these key pairs, one must be kept secret and is therefore called the *private key*, but the other related key may be freely shared without compromising security and is therefore called the *public key*. The only difference between the keys is that one is kept secret. Mathematically there is no distinguishing characteristic to determine which is which, so for a given key pair, which one is made public and which one is kept private is an arbitrary choice. This feature allows some interesting uses that are much easier to accomplish with public key cryptography than with symmetric key cryptography.

Digital Signature

One such use is the *digital signature*. A digital signature is a way of associating a message with a private/public key pair without revealing the private key. The usual way that a digital signature is created for some message is to follow these steps:

1. Calculate the cryptographic hash of the message, called a message digest
2. Use the private key to generate a digital signature over the message
3. Transmit both the encrypted hash and the message

Using this, a receiver who knows the associated public key can verify the message by these steps:

1. Calculate the message digest of the message
2. Perform signature verification on the digital signature, resulting in a message digest
3. If the two message digests match, accept the signature.

There are two reasons that a cryptographic hash is used here. First, asymmetric cryptography tends to be much more computationally intensive (and therefore slower) than the correspondingly secure symmetric key encryption, so it is faster to encrypt a small digest than a large message. Second, the use of a hash enhances the security of the scheme for reasons not explained here.

Using these mechanisms provides the features of *authentication*, *integrity* and *non-repudiation*, but not *confidentiality*. Simply explained:

- Confidentiality means that only authorized parties may read the message
- Integrity means that one can verify that the message has not been altered either accidentally or maliciously
- Authentication, in this context, means that if the digital signature of a message is verified, the message was created by the entity possessing the corresponding private key
- Non-repudiation means that an entity cannot plausibly deny creating a verified digitally signed message

Note again, that these features require that the private key remains secret.

The Cryptographic Hash

A cryptographic hash is a mathematical algorithm that reduces an arbitrarily-sized block of data called the *message* into a shorter, fixed-size sequence of bits that is often called a *digest*. There are several kinds of cryptographic hashes, but they all share the property that it is relatively easy to verify that a block of data matches a given digest, but that the reverse operation of creating a block of data that matches a digest is very difficult. This property allows for a simple method of verifying that the contents of a message match a given digest. One commonly used cryptographic hash function is called SHA-256. SHA256 is endorsed and used by the US Government and is standardized; FIPS180-3 Secure Hash Standard. It should be noted that the NSA plans to retire current cryptography standards and already recommends using at least SHA-384[12]. Ensuring the cryptography standards stay ahead of hacker capabilities is an important facet of ensuring financial transaction security. The cryptographic hash is what ties the blocks in a blockchain together.

Wallets

A wallet is software that allows a user to transact with the blockchain P2P network, without the requirement of being a peer or doing a mining activity. When it is created, there is a seed function that will create an account and manage the secure keys that a user needs to transact with a blockchain. Additionally, the wallet is encrypted upon whatever device runs the software and the user's password for the wallet is used to both encrypt and decrypt the contents[13]. As noted in the "Transaction Basics" section, when a customer wants to buy a hat, it is the wallet software that connects with merchant system and a peer on the P2P network, authorizing the transaction (via the user) and sends the appropriate number of tokens for the transaction.

Smart Contracts

A smart contract is not the same as a legal contract, although the same parameters one would use in a legal contract can also be used in a smart contract. A smart contract is simply a digital conditional trigger that is configured and embedded in the blockchain coding, that then executes when the conditions are met. In fact, a smart contract does not require the use of a blockchain, it is that simply a smart contract, in conjunction with the blockchain, takes on the attributes that make the blockchain attractive in the first place: security and transparency.

DESIGNING A BLOCKCHAIN

If an organization did not want to use an existing blockchain but rather design a blockchain for a specific purpose or industry, there are several choices that need to be made. Each choice is briefly described below.

Who can access the network?

In cryptocurrency systems, such as Bitcoin, literally anyone can participate on the network (*permissionless*) [3]. All nodes can see the entire contents of the blockchain (which functions as a distributed ledger) and can participate in creating and verifying new transactions. However, there are other possible models. For instance, it is possible to create a private blockchain system in which only certain qualified nodes may participate (*permissioned*). It is also possible for different nodes to have different roles as further described below.

How are tokens created?

In some systems, including Bitcoin, tokens are created via a special "genesis block" (the first block of the blockchain) and then further tokens are generated during the process of mining. With Bitcoin, miners are incentivized to mine by being rewarded with Bitcoin. Eventually all Bitcoins will be mined and no further ones can be created (the design of Bitcoin is such that the limit of generated tokens will be ~21 million) although fractions of Bitcoins will continue to be used in transactions

An alternative scheme is to give some nodes the ability to create digital tokens that are then used by the system. A genesis block is still required, but need not actually contain any tokens. Similarly, there may be a mechanism for destroying or "retiring" tokens.

How are transactions validated?

In the case of Bitcoin, a message is at least potentially valid if the digital signature of a transaction is verified. To prevent "double spending" of Bitcoin, the network must arrive at a new consensus view before the transaction is verified.

Alternatives could include matching the public key to an authorized list of nodes who can initiate that kind of transaction, though in this case, a mechanism would need to provide for a means to verify the identity of such a node.

[12] http://blog.bettercrypto.com/?p=1917
[13] https://blockchain.info/wallet/how-it-works

How does the network arrive at consensus?

Within blockchain, the mechanism for the nodes to agree on a valid block is referred to as consensus. There are several ways that the network might arrive at consensus. Bitcoin uses a "proof-of-work" (PoW) scheme that involves solving a mathematical puzzle involving a cryptographic hash of the block content. Because it is computationally expensive to solve this puzzle, the first mining entity to solve the puzzle presents it to the network and other nodes may easily verify it. In the case that two nodes solve the puzzle nearly simultaneously, there are temporarily two versions of the blockchain on the network, but this is generally resolved when the first solution to the next block is propagated; the network only accepts the longest chain as the correct one.

Another scheme is called Proof-of-Stake (PoS) which is less computationally expensive and uses significantly less energy. In this mechanism, nodes which have a larger balance have a higher probability of creating the next block. The cost to mine is significantly lower, and transaction throughput is increased and energy use is reduced versus PoW schemes. Lower mining costs, however, benefit both legitimate and malicious entities so the rate of introduction of fake blocks could be higher. There is also the potential that the entity with the largest stake might also be malicious. Various alternatives have been introduced to attempt to mitigate this risk including randomization and delegated PoS (DPoS) systems.

A class of algorithms generally called Byzantine Fault Tolerant (BFT) algorithms is also an alternative approach. It was originally described in terms of what is called the Byzantine Generals Problem[14]. Several Byzantine generals have, with their armies, surrounded a city. Some of them, but a minority, may be traitors. The problem is to find a way in which the generals may arrive at a plan of attack using only messengers between them such that all loyal generals agree on the same plan. There are a few variants, but essentially all of them have a maximum threshold of disloyal generals. The algorithm works if the actual number of disloyal generals does not exceed this threshold.

The Byzantine Generals problem applies to blockchain because one cannot assume that there are no malicious nodes in the network. In fact, if a malicious entity gains control of more than half of the nodes on a given network, that entity determines what block, and its contents, achieve consensus.

[14] Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem" (PDF). ACM Transactions on Programming Languages and Systems. 4 (3): 382–401. doi:10.1145/357172.357176.

REFERENCES

1. Peck, M. E. (2015, November). Bitcoin needs to get its act together. IEEE Spectrum. Available [Online]: http://ieeexplore.ieee.org/document/7335883/

2. Christensen, Clayton M. (1997), The innovator's dilemma: when new technologies cause great firms to fail, Boston, Massachusetts, USA: Harvard Business School Press, ISBN 978-0-87584-585-2.

3. Allaby, D. (2016, October, 27). The Trust Trade-off: Permissioned vs Permissionless Blockchains. www.fjordnet.com. Available [Online]: https://www.fjordnet.com/conversations/the-trust-trade-off-permissioned-vs-permissionless-blockchains/

4. IEEE (2016, June). The blockchain has a dark side. IEEE Spectrum. Volume 53, Issue 6, p. 12 – 13. Available [Online]: http://ieeexplore.ieee.org/document/7473136/

5. Underwood, S. (2016, November). Blockchain beyond Bitcoin. Communications of the ACM. Vol. 59, No. 11, P 15 – 17. Available [Online]: http://cacm.acm.org/magazines/2016/11/209132-blockchain-beyond-bitcoin/fulltext

6. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., and Savage, S. (2016, April). A fistful of Bitcoins: Characterizing payments among men with no names. Communications of the ACM. Vol. 59. No. 04. P. 127 – 140. Available [Online]: http://dl.acm.org/citation.cfm?id=2504747

7. Zohar, A. (2015, September). Bitcoin: Under the hood. Communications of the ACM. Vol. 58. No. 9. P. 104-113. Available [Online]: http://cacm.acm.org/magazines/2015/9/191170-bitcoin/abstract

8. Peck, M. (2016, November 18). A blockchain currency that beats Bitcoin on privacy. IEEE Spectrum. Available [Online]: http://spectrum.ieee.org/computing/networks/a-blockchain-currency-that-beats-bitcoin-on-privacy

9. Ito, J., Narula, N., and Ali, R. (2017, March). The blockchain will do to the financial system what the internet did to media. Harvard Business Review. Available [Online]: https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

10. New York State Department of Financial Services. Part 200. Virtual Currencies.

11. Regulation (EU). No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the intermarket and repealing Directive 1999/93/EC. Available [Online]: https://www.anacom.pt/render.jsp?contentId=985913#.WI-0Rn85UvU

12. Kouzmanoff, J. (2017, January, 19). Blockchain technology: a hidden gem of innovation for the solar industry. Solarplaza.com. Available [Online]: http://www.solarplaza.com/channels/finance/11648/blockchain-technology-hidden-gem-innovation-solar-industry/

13. Irrera, I. (2017, March 29). Bosch, CISCO, BNY Mellon, others launch new blockchain consortium. Rueters. Available [Online]: http://www.reuters.com/article/us-blockchain-iot-idUSKBN15B2D7

14. Smith (2016, June 8). IoT botnet: 25,513 CCTV cameras used in crushing DDoS attacks. NetworkWorld. Available [Online]: http://www.networkworld.com/article/3089298/security/iot-botnet-25-513-cctv-cameras-used-in-crushing-ddos-attacks.html

15. Castillo, M. (2016, July 20). Ethereum Executes Blockchain Hard Fork to Return DAO Funds. Available [Online]: http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/

16. Besnainou, J. (2017, February). Blockchain meets Energy: State of the Market. Cleantech Group. Available [Online]: http://www.cleantech.com/blockchain-meets-energy-state-of-the-market/

17. Higgins, S. (2016, November, 1). Ethereum Energy startup awarded blockchain patent. Coindesk. Available [Online]: http://www.coindesk.com/blockchain-energy-startup-patent/

18. Blockchainfirst. (2017, January 18). The first Multipurpose Blockchain enabled EV Charging Station. Available [Online]: https://medium.com/@blockchainfirst/the-first-multipurpose-blockchain-enabled-ev-charging-station-d8265c1bcb38

19. Engerati (2016, April, 11). Blockchain transactive grid set to disrupt energy trading market. Available [Online]: https://www.engerati.com/article/block-

chain-transactive-grid-set-disrupt-energy-trading-market

20. Engerati (2017, January, 10). Australia – land of blockchain opportunity. Available [Online]: https://www.engerati.com/article/blockchain-transactive-grid-set-disrupt-energy-trading-market

21. Burger, A. (2017, February 27). More than Half German Utilities Carrying Out or Planning Blockchain Pilots. Energy Central. Available [Online]: http://www.energycentral.com/c/pip/more-half-german-utilities-carrying-out-or-planning-blockchain-pilots

22. Clancy, H. (2016, October 3). How the blockchain will disrupt energy markets. EnergyBiz. Available [Online]: https://www.greenbiz.com/article/how-blockchain-will-disrupt-energy-markets

23. Khyati, K. (2015, September 17). World's 9 Biggest Banks to adopt Bitcoin's Blockchain, The Hacker News. Available [Online]: http://thehackernews.com/2015/09/bitcoin-blockchain.html

24. Hype Cycle for Blockchain Technologies and the Programmable Economy, 2016, (2016, July 27). Gartner Research. ID: G00308190. Available [Online]: https://www.gartner.com/doc/3392717/hype-cycle-blockchain-technologies-programmable

25. ENEL (2017, February 10). ENEL to the discovery of the blockchain. ENEL. Available [Online]: https://www.enel.com/en/media/news/d201702-enel-to-the-discovery-of-the-blockchain.html

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together . . . Shaping the Future of Electricity

3002010242 October 2017

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA • 800.313.3774
• 650.855.2121 • askepri@epri.com • www.epri.com