GBBC
Global Blockchain Business Council

SPECIAL REPORT

BLOCKCHAIN TECHNOLOGY FOR THE ENERGY SECTOR

Powerledger | GBBC

TABLE OF CONTENTS

1. INTRODUCTION

The rise of blockchain and its applications is one of the most striking innovations of the last 10 years. This paper introduces the ideas and concepts of blockchain technology in the context of upholding trust for human civilization, especially as a ledger for commercial transactions, which are a key component of decentralized energy and grid systems. The main focus is on blockchain's use cases in the energy sector, showcasing how a lower carbon energy system can operate using distributed technology underpinned by a blockchain-based accounting system.

2. THE NEED FOR TRUST

Blockchain is a revolutionary technology that solves an ancient business and economic problem in a new way. How can we trust the other side when we do business with it? To really understand that problem, we have to first understand the role that trust plays in our society, and the way trust has been maintained across societies throughout human history.

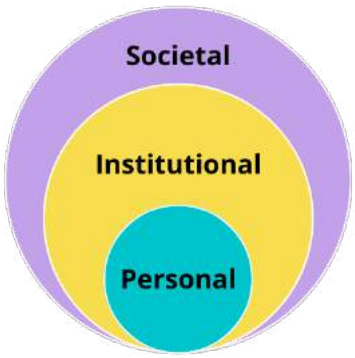
Trust is a crucial component of every healthy society. Without trust, it is impossible for people to cooperate with one another, or engage in meaningful social and economic exchanges. Trust is a vital growth ingredient for any group of humans. Without trust, a society cannot accumulate wealth, and in the extreme case of absence of trust, a society descends into chaos which becomes an existential threat to the community as a whole.

Trust allows us to rely on each other to uphold our collective best interests. When we trust someone, we believe that they will do as they promised, and that they will be fair and honest. This is particularly important when we need to rely on others to perform a task or deliver a service, especially when we are dealing with strangers. Trust enables people to cooperate effectively, guiding social and economic structures toward growth and human flourishing. When we trust our colleagues, we can collaborate more easily by dividing tasks, sharing information more freely, and relying on them to support us when needed. Trust is fundamental for protecting a community's collective best interests as a greater good within which individuals can pursue their own best interests safely. In cases where trust is broken, where we may not trust our government official or neighbors, we have a penal system that ensures serious consequences for breaking trust.

Finally, *trust is based on a shared sense of justice and order, such that no abuse of misuse of information asymmetries would lead to harm and conflict.* If such abuse were to arise, even in the case of unintended wrongdoing, trust ensures a system of accountability to provide relief for affected parties. Societies have developed deeply rooted ways of ensuring trust that tied to human conscience, through religious and cultural prohibitions on acts of untrustworthiness, with variations on social and economic incentives, and even the promise of heaven and hell as carrot and stick. Beyond the spiritual, physical retribution for untrustworthy behavior could also take the form of trial by fire or water, even death or exclusion from a community by being placed in the stocks or being transported to penal colonies or prison.

Historically there have been three manifestations of trust:

- Personal reputation: If someone has a reputation for being honest and fair, others may be more likely to trust them.
- Institutions: Institutions such as businesses and governments can also create and sustain trust in society by consistently acting in a trustworthy manner. In doing so they uphold key functions necessary for human civilization and set standards for ethical behavior.
- Social norms and values: Social norms and values establish expectations for how people should behave, and thus sustain trust in society.



3. TECHNOLOGY AS A TOOL TO PRESERVE TRUST

On the one hand, it is well understood that social norms and values - shared expectations, rules, and guidelines – govern the behavior of people within a society. These norms and values are expressed through family, culture, education, religion, and the law. They have provided ways to ensure violations of trust are kept under control. In addition to this sociological lens, humans have developed technological tools to preserve trust. Technology has also contributed to the format in which trust is cultivated in our society. Technology provides a means to record and validate information. Civilization relies on commonly accepted information in order to operate and progress. Historically, written language enabled contracts to be written down, committing agreements to stone, parchment or paper to preserve them and present them as evidence when needed.

Ledgers became a valuable tool to record data. Double entry bookkeeping allowed for accounts to be verified. Government registries, for instance, came to record ownership of valuable assets such as land and housing, allowing individuals other than the king to be considered legitimate owners. Registries enable a range of economic activities in an orderly manner based on trust. Ultimately, trust in a record system is necessary for individuals to provide their data as documentation, and on the other hand, quality data records are necessary for ledgers to be trusted.

Ledgers like the one above have been found in Mesopotamia dating back 7000 years, where clay tablets recorded important data. These clay tablets were kept in temples by trusted members of a tribe. This Sumerian cuneiform tablet is probably from Erech (Uruk), Mesopotamia, c. 3100–2900 BCE; in the Metropolitan Museum of Art, New York City. Purchase, Raymond and Beverly Sackler Gift, 1988, 1988.433.1.

Money, whose function is based on trust, also became used as a widely accepted representation of value. For instance, medieval English wooden tally sticks served as an early proof of settlement to legitimize agreements and trade. On the Micronesian island of Yap, money took the form of massive stone discs – some up to 2,000 years old and still standing today – their sheer weight and size having given them a form of permanence.

4. TRUST-BASED TO TRUSTLESS SYSTEMS

The varied forms of record keeping tools described above could be lost, broken, or tampered with. Eventually, centralized institutions took on the burden of ensuring trust and standardizing trust systems. Institutions came to store and validate data records, and in doing so, maintain society's expectations of trust. People chose to trust centralized intermediaries, forming the foundation of a "trust-based" society. For instance, trusted institutions like central banks provide their full faith and credit to legitimize the national currency they provide for their respective domestic and international economies.

However, even institutions are not infallible, and every industry has experienced trust problems over time. As important as trust is, it can be subverted and break down. History is littered with examples where trust-based relationships have broken down. Lack of transparency, data silos, and information asymmetries increase risks of misleading advertising and fraud. Even in an everyday example, a second hand car dealer may have access to information about a car that isn't shared with the customer, Business models based on controlling access to data have enabled misuse of data and unintended consequences.

In recent years there have been a number of breaches of trust on the part of institutions, which are coming under increasing scrutiny for their trustworthiness. One example of this is the Barclays LIBOR scandal, where a group of individuals in a large organisation conspired to manipulate the base interest rate. The victims were almost everyone in the UK and beyond, the beneficiaries were the bankers controlling the rate.

In the airline industry, Airbus was fined $4 billion in 2020 for a global bribery scandal. In 2022, its main rival, Boeing was fined $2.5 billion for fraud for knowingly covering up a fault with its 737 Max aircraft and still allowing it to be flown, leading to the loss of 346 lives. These fines could be seen as penalties for loss of trust in these companies. Furthermore, the integrity issues were so far reaching that even the Federal Aviation Administration (FAA) itself lost trust, as the regulator responsible for Boeing's oversight and ensuring flight safety in US and joint global airspace.

The issue was escalated to the very president of the United States. Boeing had important information it chose not to share with passengers, pilots, and crucially, the FAA, for the purpose of its own economic advantage. Instances of untrustworthy behavior on the part of institutions, especially abuses of information asymmetries with respect to the public, have led society to question the unequivocal trust placed on them. There arises an additional risk with centralization, where one institution, such as the FAA in the example above, becomes a single source of trust. Creating trust via centralization can be cost-effective, but it also constitutes a single point of failure. The Edelman Trust Barometer has shown a consistent decline in trust toward centralized institutions – a trend seen particularly in financial services after the financial crisis of 2008, and again with the current turmoil affecting the banking system - which may undermine their significance in society without innovation and change for the better.

Trust is also expensive to sustain and can break down. Over time humans have been very innovative at creating new forms of trust. The value of trust to society is paramount yet difficult to quantify - one study estimates that 35% of all jobs in the US are related to creating and maintaining trust. If one is to consider the direct and indirect dependence on trust for every economic transaction to occur, this number may be even higher. There is a clear correlation between trust and the growth of a capitalist economy. As Professor Arun Sundarajaran at New York University observes, 'If you look back at history, every time there was a big expansion in the world's economic activity, it was generally induced by the creation of a new form of trust'.

There is opportunity in open data records to enable transparency and accountability, as those enabled by blockchain. In an era where technology has been used to achieve tasks that were previously exclusively performed by humans, it's perhaps not surprising that blockchain technology is making its presence felt. A "trustless" system enabled by open data can uphold the same norms behind our civilization's need for orderly functioning, without the need to depend on centralized third parties. This doesn't automatically mean to do away with our institutions, but that the burden of trust is no longer tied to their ability to hold records. Instead, it is transferred to an open and immutable data repository that increases transparency and accountability for all actors. Privacy enhancing mechanisms can also make data permissioned and available to authorized parties (e.g., only doctors having access to medical records on a blockchain and not the general public).

This can foster a new generation of social and economic interactions, give voice to individuals and underrepresented communities in governance structures, in unprecedented ways. Rather than relying on a large number of employees, who are themselves audited by other institutions with large numbers of employees, a trustless system is designed to use multiple distributed network participants to validate each other and the data records. Over the coming years, it's widely expected that numerous blockchain applications will replace traditional processes where trust is central to the stability of the process.

5. TRUST IN COMMERCIAL TRANSACTIONS

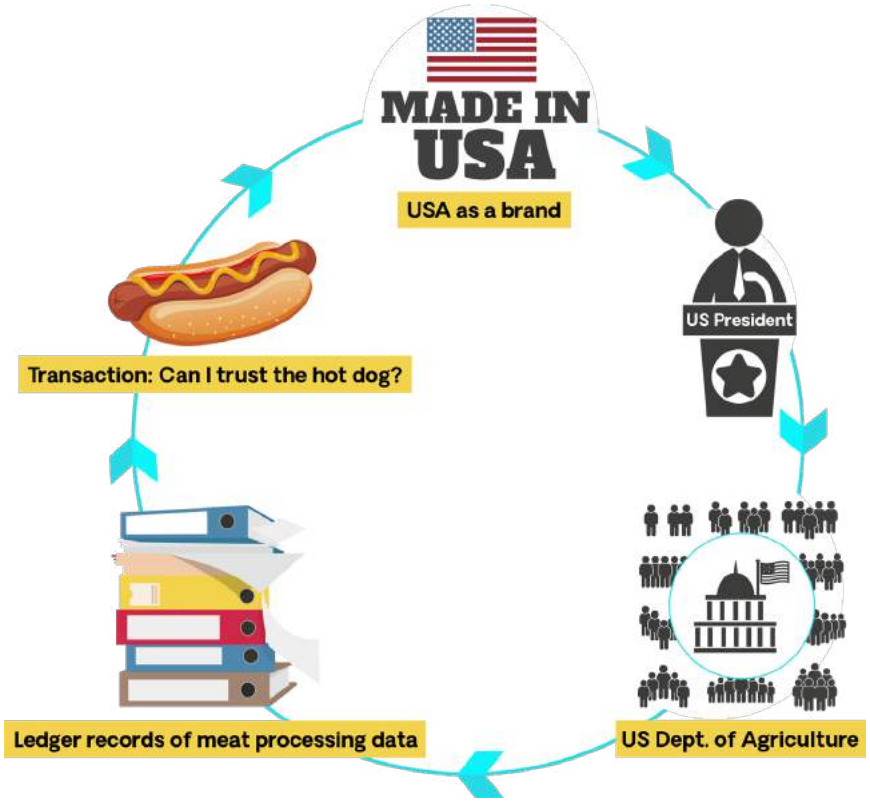
One major example of a transition from a trust-based to a trustless system is in the realm of exchanging value. The need for trust underpins all commercial transactions in an economy, and credibility is a backbone of consumer protection. A buyer must trust that the seller has the desired product or service in an adequate form, and the seller must trust that the buyer has the adequate funds to pay for it. Therefore, a market economy cannot function outside of a framework of order and justice , even if at times it must be imposed by a formalized justice system to address bad actors seeking opportunities for personal benefit at the expense of others. As expanded further below, a system of trusted transactions is fundamental for a well functioning energy system, especially for a new decentralized model that can facilitate individuals purchasing, trading, and transitioning toward clean energies. This section introduces a simpler example of an everyday food purchase to illustrate key concepts.

5. 1 EXAMPLE: EVERYDAY FOOD PURCHASE

Consider a transaction as simple as buying a hot dog from a street food vendor. The consumer trusts that the hot dog is safe to eat. The vendor trusts that the money paid for the hot dog isn't counterfeit. That trust is so implicit that few people even think about those risks when buying and selling hot dogs. Yet they are real.

In this example, risks are managed by the government through designated regulators. Every government issues its own currency (considered legal tender) and ensures that the currency is not being counterfeited. There are many technological innovations that work to prevent and detect counterfeiting, and the crime of counterfeiting is considered serious.

What about the food? In the United States, the Food Safety and Inspection Service (FSIS) of the Department of Agriculture, the Food and Drug Administration (FDA), and the Centers for Disease Control and Prevention are involved in food safety regulation. These federal agencies form part of the executive government, and their heads are appointed by the US President. Accountability goes all the way to the top.



Closely related to a trustworthy item or service is the documentation around it – hence the need for a ledger. In the hotdog example, the types of meat, as well as sanitation levels of the equipment used, are monitored and dated as records on a ledger. It is important to recognize, nevertheless, that there is still a need for expert individuals to check the meat and verify that quality data gets recorded on the ledger. Ultimately, individuals recording quality data are key to preserving the integrity of the ledger.

The ledger becomes a key instrument of trust, and maintaining the ledger properly also maintains its trustworthiness. If someone were to become sick from foul meat, it may indicate that somewhere in the documentation about standards, something was altered, misrepresented or left incomplete. If this issue were widespread, the US Department of Agriculture should theoretically launch an investigation. Trust is implied with the top of the hierarchy supervising all activities beneath it.

Therefore, one could say that protecting a hot dog transaction is a trio of elements. A set of data recorded on a ledger, a large number of people in an institution, and a high status individual whose probity is beyond question. Even this trust-based system is not infallible. A 2013 beef scandal across the European Union involved the unethical sourcing of horse meat for lasagnes sold at grocery stores, which had gone undetected by the Food Standards Agency (FSA). Even a decade later, UK grocery stores were still investigated for food fraud after selling South American beef branded as British beef.

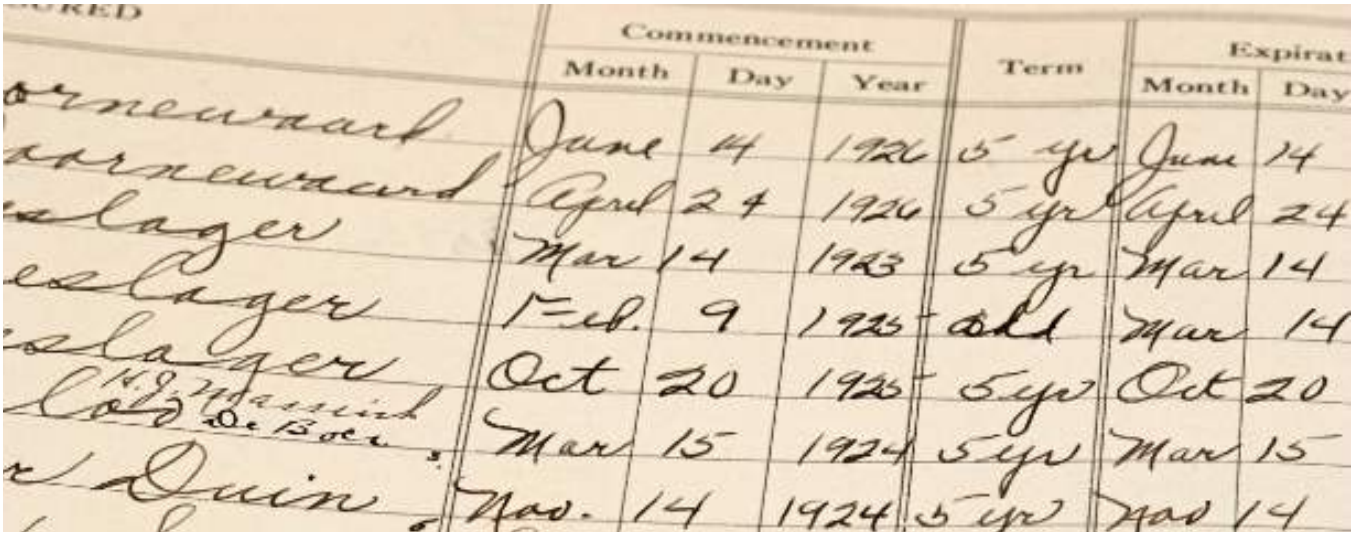
These components could look different in a trustless environment with blockchain technology as a ledger to record the data in a way that is openly available, while preserving individual privacy. For instance, individual consumers could provide data, such as DNA samples of the food they purchase, to be verified and recorded on the distributed ledger. Meat, such as that sourced illegally from racehorses back in 2013 as referenced above, would soon show up as the wrong sort of DNA

6. BLOCKCHAIN AS AN ENHANCED TRUSTED LEDGER FOR TRANSACTIONS

In a digital world where commercial transactions are increasingly taking place through digital means, how would one send money electronically to someone else using computers over the internet? Assuming a trusted central authority such as a bank, that would be easy. One gives the money to one's bank, which notifies the other person's bank, which in turn gives the other person the money. Yet how could this occur if for any reason one couldn't trust centralized parties or intermediary banks?

Blockchain was first envisioned as a tool to do precisely this. This technology was first created as a ledger of transactions in the form of cryptocurrency, the electronic cash designed to operate in a decentralized network. The ledger contains a historical record of every coin ever minted and spent. As a new form of decentralized digital ledger, blockchain technology records transactions across a network of computers.

In order to understand blockchain as this tool, it is helpful to first appreciate the ledgers it can replace. It's worth considering in greater depth how classical ledger technology works, starting from when someone writes an entry into a book with a pen and paper, and implications on the permanence of records.



Records on a ledger

When a pen writes on paper to make an entry, millions of paper fibers and fiber molecules become coated with ink. To rub that ink out requires certain skill and effort. Indeed, any attempt at rubbing out an entry will almost certainly destroy or blemish the top layer of paper and reveal the alteration attempt, obvious to the naked eye and certainly with a microscope. This indication will betray the nature of the fraud. If the ledger were in a safe, one would have to blow the safe open.

Therefore, in an ideal ledger, any attempt to alter it after an entry is recorded creates a catastrophically observable event. Physicists would recognise the concept of entropy as a theme running through this but it's not essential to understand entropy to understand blockchain.

However, in a digital world, when one deletes an electronic record, there is no layer of paper that gets blemished, nor any cluster of molecules or fibers that become altered. Only a few bytes of random-access memory are changed with the deletion. This could make a case that computers aren't inherently a good tool for acting as ledgers. So how does one meet the challenge of creating a digital substitute for the leather-bound ledger guarded in a safe?

Blockchain not only records data transparently but also immutably. Records are made not only in a way that is openly available, but also in a distributed manner, such that there is no centralized repository of the latest master version of the ledger that can tamper with the data. Once a record is validated and entered, it is considered immutable. Moreover, blockchain employs cryptography to ensure privacy and security, such that only legitimate owners of funds can authorize transactions with them. (see Annex for blockchain basics).

Every participant in the network has access to the latest version of the ledger simultaneously. If any single entity were to shut down, the network would continue to operate resiliently, adding new records to the ledger. As soon as an entity were to re-join the network or join for the first time, it would automatically have access to the latest ledger. Therefore, if bad actors were to attempt to change a past record, they would have to re-do all the work put into generating the ledger entries, compromise a majority of the computing power of the network and undergo a consensus-driven validation process for each. This is very difficult, impractical, and therefore unlikely enough to be considered virtually impossible.

6.1 EXAMPLE: TOKENIZATION AND SENDING MONEY OVER THE INTERNET

The ability to exchange data over the internet through blockchain records also allows efficient transfers of value in a trustworthy manner. Blockchain technology is a promising tool to control consumption and trade of energy in a peer-to-peer manner, with the novel opportunity to fractionalize ownership. Tokenization enables the representation of any form of value as a record on the blockchain that can be exchanged and traded.

Tokenization enables efficient management of small amounts of energy and small monetary transactions, alongside added liquidity and monetary benefits for owners. Tokens on a blockchain representing energy assets can provide owners with a fractional claim to a solar panel, for instance, in addition to its corresponding offtake revenue. Fractional amounts of money can be exchanged and accounted for effectively, with close to immediate clearing and settlement, which further reduces risks with more accurate tracking of ownership of funds. This can be a gamechanger for energy systems and other industries.

Decades after the early incarnation of the internet, people started to wonder how one could use the internet to send money in a trustworthy, dependable way. If one could use the Internet to send scripts and images, even pets doing funny things over social media, it could be much more socially beneficial, though complex, to send money.

Sending money is different from sending pictures or text. One can't simply photograph and send a $10 note because the moment the photograph is taken, this can create a duplicate version of the note and the possibility of a double spend. This would require destroying the $10 note being photographed and only sending the picture of it, while also stopping others from duplicating that image. The picture of the $10 note must be unique and impossible to copy. Hence, producing a unique and inviolable token, ensuring it can't be spent twice, becomes the dual problem that must be addressed.

This became the foundation of cryptocurrency, which used blockchain to prevent double spending. In fact, blockchain technology, digital assets, and cryptocurrency are related technologies that often depend on each other to operate properly.

6.2 EXAMPLE: SMART CONTRACTS AND INSURANCE

Finally, blockchain technology also has the ability to support automated transactions through smart contracts. These transactions can be programmed to take place upon the occurrence of predetermined conditions, greatly improving efficiencies and reducing costs for processes that may otherwise involve burdensome manual processing and data silos. Across all industries – from registries, to insurance, payroll, banking operations, and deals of all types – there is a wide range of applications that can benefit from automated transactions. Smart contracts are ideal for highly automated processes like insurance.

If a car accident were to occur under a previous model of operations, one would begin a process with a trusted authority to call upon one's insurance. The insurance company would send an independent assessor, who would take photographs, write a report, and begin a process whereby one may receive compensation or a bill for an amount of money.

This entire process can change with digitization, and it can further evolve with blockchain and cryptocurrency innovations in convergence with already widely used technologies such as smart phones and artificial intelligence (AI).

In a digitized system if one has an accident with another car, one can take out one's mobile phone, make a series of photo snaps and video sequences of the car's exterior, and also take footage of the car one has collided with. Most of the rest of the process is automated. Existing technology can recognize the car's make and model and start assessing the damage, location, lighting conditions, and relevant regulations. The software can then begin chaining in spare parts via the delivery system, estimating costs, making payments and transfers of cash, etc.

Automation in this manner achieves a number of efficiencies. The opportunity for fraud can be reduced by minimizing instances of irregular patterns of activity, as is the number of days needed to pay for a courtesy car for those who would otherwise remain without transport. The number of employees required to make assessments, checks, and audits of the process is also drastically reduced. It's no wonder that systems like this are establishing themselves in this space. This highly automated claims process and overall insurance system presents a scenario that is very compatible with smart contracts.

It is important to note, however, that smart contracts still have limitations and vulnerabilities that may still require human intervention and expertise to ensure proper functioning. For instance, an infinity of future possibilities makes it very likely that transactions undergo scenarios that are not predicted, and thus unforeseen by the code. Unforeseen eventualities may require authorized humans to act as nodes to override the system.

In the context of peer-to-peer trading of renewable energy as illustrated further below, where transactions would be automated by smart contracts, the predetermined terms of the trades established by the code may not fully capture all the circumstances in which buyers and sellers may agree on a price.

7. TRUST IN OUR USE OF ENERGY RESOURCES: BLOCKCHAIN USE CASES IN THE ENERGY SECTOR

All of society's functions run on energy use. Basic laws of thermodynamics state that every activity requires energy in some form. Cooking, moving, heating, cleaning, even the simple act of thinking requires energy, whether one is an animal or a computer. Energy has long been a limiting resource for societies, with an ever-present pressure to increase its supply to support any expansion of human society and its activities. With increasing energy use, a significant portion of commercial transactions in the global economy is also devoted to buying, selling, and tracking data related to energy resources. The last few years have seen energy companies make record profits, as if to underline their importance.

The Industrial Revolution began by finding industrial-scale sources of energy, initially with the fast flowing waterways in England for mass production through mills, and then shifting to coal-powered steam engines. Heavy reliance on coal and fossil fuels led to a search for cheap and widely available energy sources, and nuclear power at one point garnered significant interest and a notion of unlimited energy. Yet in the last century, nuclear research programs proved not to meet expectations - hence a continued dependence on oil. The ensuing oil crisis of the mid 1970s, which involved petroleum shortages and sky-high prices in the Western world as a result of an embargo imposed by members of the Organization of Arab Petroleum Exporting Countries (OAPEC), and today's greenhouse gas crisis, have shown how energy resources must be adequately managed.

Global energy consumption annually amounts to approximately 580 million terajoules – that is, 580 million trillion joules, which would require 13,865 million tons of oil equivalents. Energy consumption is also going up, having increased by one third since 2000, and projected to reach 740 million terajoules by 2040 for another 30% increase. Over 80% of energy used today still comes from fossil fuels, which could mean enormous amounts of greenhouse gas emissions to aggravate global warming if we don't shift the energy supply mix toward renewables. In this context arises our shared responsibility to our environment, as stewards of our planet, to avoid depletion of natural resources and maintain ecological balance that will ensure our long-term coexistence as a society.

According to a global survey led by the University of Bath, the threat of climate change and dissatisfaction with government responses is causing distress in youth aged 25 and under, impacting their daily functioning. Climate anxiety was revealed in 59% of respondents, who reported to be very or extremely worried, while 84% reported to be at least moderately worried.

Accountability in the management and distribution of clean energy resources is facilitated through technology and open data, especially as demand for renewables and decarbonization initiatives is becoming front and center. Blockchain technology can lower costs and improve efficiencies, improving access to low carbon sources of energy at low costs for individuals and communities. Blockchain technology also brings transparency to supply chains, ensuring ethical sourcing and consumption of clean energy, and also tracing greenhouse gas emissions. This will foster clean energy adoption, helping address the conflict between the need to heat our homes and conduct our basic activities, while doing so in a sustainable manner.

The emergence of blockchain in electrical utilities can be a game changer toward meeting the commitments required by the Paris Agreement. Like the accident insurance industry described above, the energy space comprises a trio of elements that make it a likely beneficiary of smart contracts: AI, blockchain, and cryptocurrency. According to a report from the International Council on Large Electric Systems (CIGRE), “Blockchain technology has given rise to many technological frameworks, key among them being Powerledger and Ethereum.” As of today, these two primary frameworks have largely set the stage for blockchain use cases to be deployed in the energy sector.

A transparent and enhanced ledger undergirded by blockchain technology can facilitate a broader range of transactions supporting energy distribution and trade, improving access to clean energy and accountability in the process. Democratization can also put individuals at the center of the energy transition, allocating incentives and economic benefits to individuals and underrepresented communities by enabling fractional ownership of energy assets, empowering individuals in their energy consumption choices, peer-to-peer trading, and energy investment opportunities at the retail level.

7.1 PEER-2-PEER (P2P) TRADING OF DECENTRALIZED ENERGY (DE)

Fossil fuels, nuclear, and hydro, which provide a very stable power output, fit well with the classical centralized grid model that incorporates fixed energy pricing. On the other hand, renewable energy resources (RE) like solar and wind provide highly variable power, delivered in spurts that are difficult to predict, from often remote locations that can wreak havoc on a centralized system.

When wind and solar began to emerge as energy sources capable of producing power for the grid, it became apparent that these energy sources would be in numerous locations that weren't generally co located with major power stations. Wind and solar farms would typically be built in places where there was no major connector to the grid, and therefore their energy output would be essentially stranded. While states could invest in beefing up the grid at that point, doing so could make these projects uneconomical.

In addition to this geographical problem was a challenge of timing, where the intermittent nature of solar and wind power required significant additional investments in battery energy storage systems (BESS). This would also be uneconomical. Therefore, the twin problems of place and time reflect the unique nature of renewable energy relative to traditional energy, and demonstrate why supporting its scale demands a different approach.

In this context, the energy market came to a new realization: that owners of even relatively small-scale power sources could trade power with each other. They could agree on a price and transact a certain amount of power at a time and place of their mutual choosing. As these localized new market's development could drive efficiencies, more battery solutions would get incorporated into the system, enabling peak demand and curtailment periods to become better managed, at better pricing, and accelerating the green energy transition.

This formed the basis for peer-to-peer power trading, which inherently became a natural fit for a decentralized energy model, where blockchain technology is used to track all the underlying financial transactions. If the paradigm shifts to distributed rather than central distribution, the contributions of renewables can much better assimilate to energy grids. Localized and agile pricing works well with a distributed approach, and flexibility of pricing helps balance a system characterized by variability of supply and congestion in the network at intervals, to facilitate efficient distribution of energy.

The Role of Blockchain in Decentralized Systems

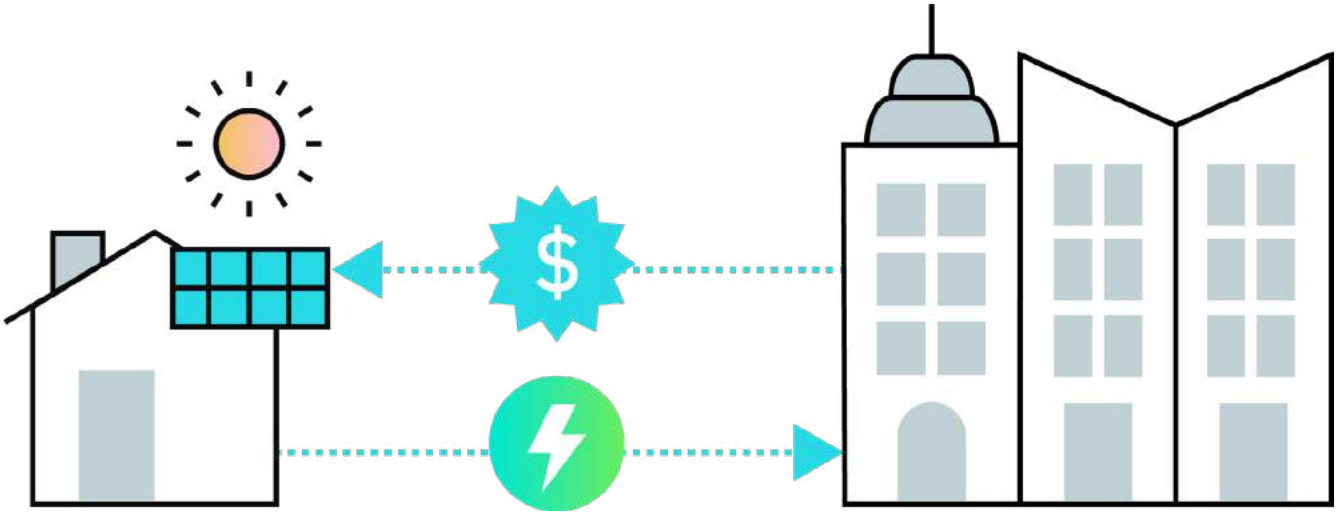
In the new peer-to-peer paradigm where numerous players can trade energy with each other, there are also numerous transactions to keep track of. Energy customers now interact as peers or equals, rather than customers or subordinates of a centralized organization, with this approach opening the market for smaller energy producers to contribute to the energy supply.

What is the best approach to billing in a distributed environment, where transactions are frequent and low margin, and where there is a flat hierarchy in need of security? Blockchain, as described earlier, presents an immutable and trustless way to manage a database (ledger). It also integrates well with smart contracts which suits peer-to-peer trading. Smart contracts use computerized embedded code which defines the terms, rules, and conditions of bilateral trading agreements.

Once peer-to-peer trading contracts are written on the blockchain platform, where tokens on a blockchain represent energy amounts and currency utilized to buy and sell them, transactions are stored permanently and cannot generally be altered or removed. Settlement occurs seamlessly among peer-to-peer traders, based on real time data even before billing cycle reconciliation, and keeping margins of energy retailers and network operators unaffected.

Confidentiality and privacy are also guaranteed through symmetric and asymmetric encryption and anonymous signatures. At the end of each billing cycle, blockchain-stored peer-to-peer transaction data is sent to energy retailers and network operators to finalise the transactions. As the entire process is handled by smart contracts, the model of energy retailers as we know it changes significantly.

Here is an illustrative transaction: Customer A produces 150 kWh in September and, after peer-to-peer trading settlements of 100 kWh, sells the excess 50 kWh to an energy retailer in exchange for cryptocurrency tokens, or their fiat currency equivalent. Customer A's account receives a specified payment amount, which Customer A can then spend on charging an electric vehicle, in any charging-covered network locations of the energy retailer. The energy retailer can then charge transaction fees and benefit from this process.



Above: Customer A trading excess energy to the energy retailer in exchange for crypto or fiat currency

In the current model as shown in the diagram above, individuals consume energy directly from power sources. In a decentralized model, individuals can consume energy, as well as produce energy, by owning fractional amounts of energy producing assets such as solar panels, becoming "prosumers" – that is, producers and consumers. They can sell their excess energy to other individuals for a profit, and even back to the grid. This flexibility and monetary incentives would attract the individual energy consumers operating on a traditional centralized model to take part in a decentralized model.

At scale, peer-to-peer energy trading, which can incorporate features like dynamic pricing, preferential trading, and gifting/donating, empowers consumers to manage their excess energy in a manner that would not have been possible without blockchain applications. This new role that consumers can take on becomes a market-driven incentive to accelerate the deployment of distributed energy resources, in ways that can save communities around the world from the need to rely on other financial incentives and government subsidies to support renewable energies (e.g., feed-in tariffs or net metering to achieve deployment targets).

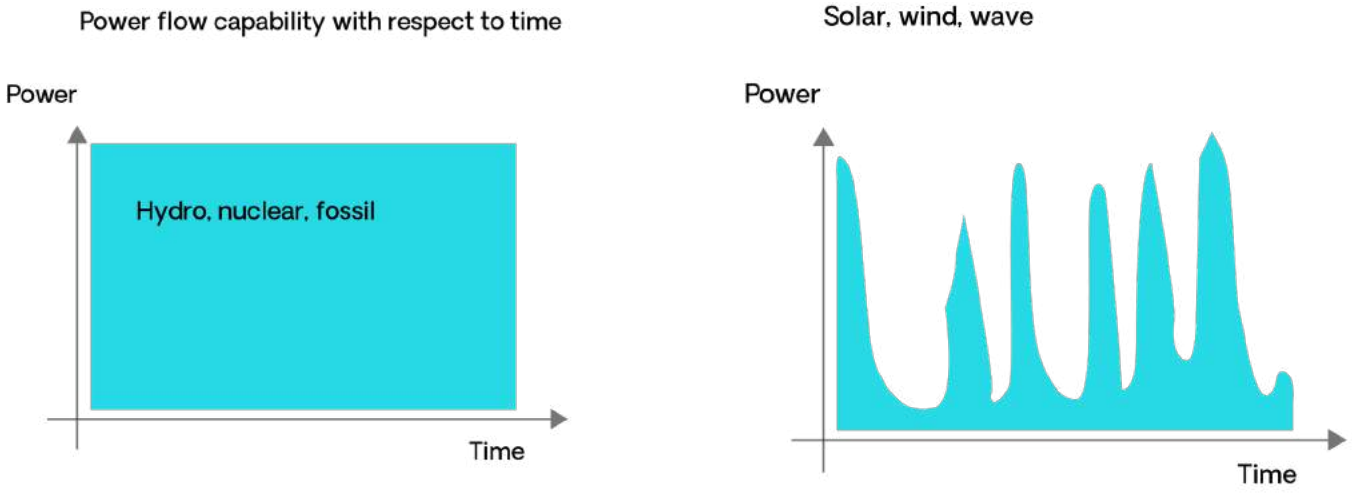
Ultimately, while both blockchain and crypto can provide significant benefits to peer-to-peer trading, collaboration with energy retailers to become key stakeholders as part of the process illustrated above is key to foster adoption.

7.2 LOCAL ENERGY MARKETS (LEM)

A local energy market (LEM) is essentially a community of people creating a sub-market of electricity for each other. It could entail any region or district where electricity is traded between players, allowing energy users to negotiate and decide on energy quantities and prices for each transaction. This flexibility facilitates clean energy integration by helping to manage the shortages and surpluses of an electricity market when they occur. Much like seasonal vegetables, where prices adjust to their supply throughout the year, energy prices at a local level also adjust to seasonal changes in supply that are natural for renewables.

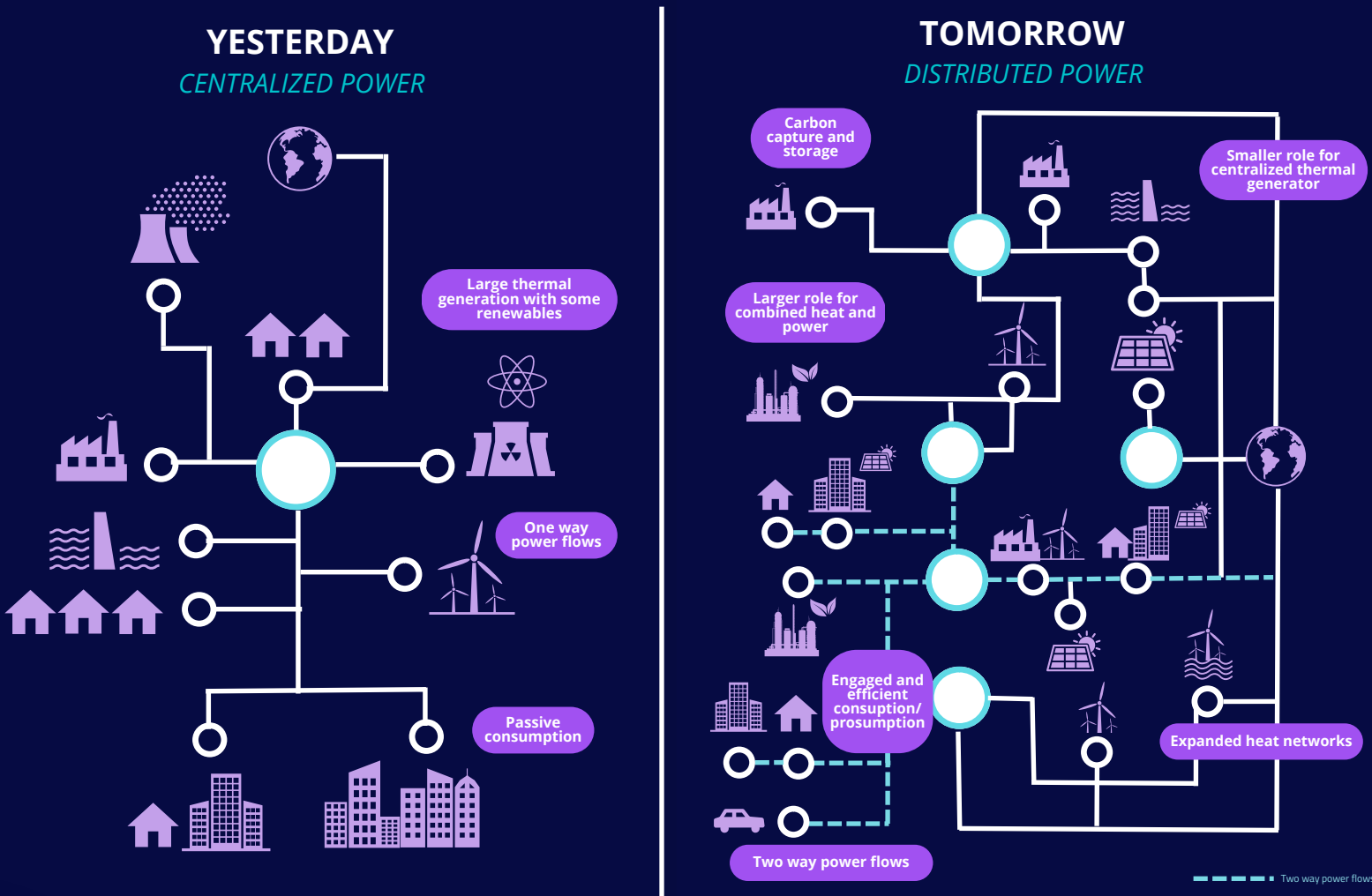
In any LEM, the supply of clean energy is matched with energy demand at the appropriate price by adopting advanced optimization techniques and constraint management. Any mismatch can be traded with the power grid as per business-as-usual (BAU), i.e., surplus local energy is fed back into the power grid at the feed-in-tariff (FiT) rate, while unmet demand is purchased at the time-of-use (ToU) prices. Distributed energy models with underlying blockchain technology for data records, as opposed to centralized energy models, are best suited to manage energy distribution and underlying transactions. Typically centralized energy sources are steady, as opposed to decentralized energy sources which are intermittent, as shown in the figures below.

Centralized energy (left): Steady power capability supports a centralized structure and fixed pricing.
Distributed Energy (DE) (right): Intermittent energy works well with a local energy market and dynamic, agile pricing.



Just as the physical topology layout of a city like Los Angeles is determined by the use of cars, and is different from that of small medieval villages in the south of France, so too is it with the energy grid. The difference in physical structure of a grid reflects the difference in technology behind it, as shown in the physical representations of energy flows below. The ideal grid for a future blockchain-based system will be designed for a decentralized flow of variable energy.

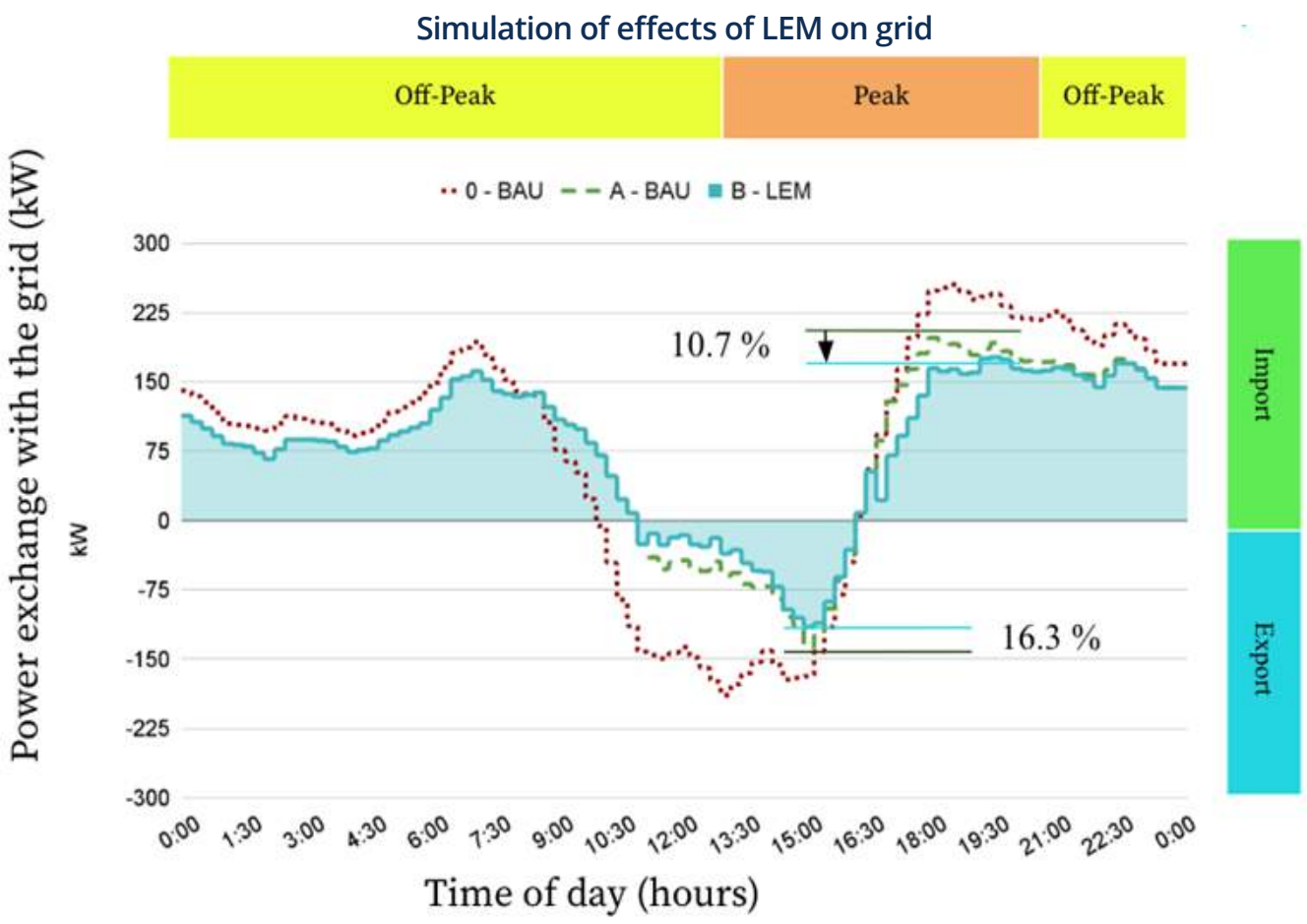
Energy flow with respect to space in a centralized form (left) vs. distributed form (right)



A number of studies have trialled local energy markets, with promising results. Probably the most notable example is called Pebbles, a demonstration and research project by Allgäu Netz, Allgäu Überlandwerk, Siemens, Hochschule Kempten, and Fraunhofer FIT. Pebbles led to increased self-consumption and reduction in congestion of the grid in the vicinity. The project also enabled day ahead and intraday trading, so that the local market can provide flexibility for the larger grid, a significant benefit.

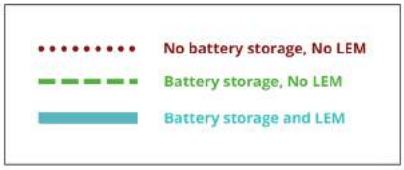
While Pebbles itself does not use blockchain technology, blockchain would be an appropriate technology to help it scale by allowing market rules to be encoded transparently using smart contracts. This would allow real time peer to peer trading of energy with the security and auditability, allowing untrusted actors to collaborate and interact with each other securely, rather than relying on a centralized institution to accurately maintain these markets without manipulation.

As demonstrated in the diagram below, local energy markets flatten the troughs of power availability, promoting a more balanced and efficient market. This is further supported by battery storage to promote energy trading.



Assumptions

- Minimizing the electricity bill cost for 300 participants.
- Minimizing the grid import and export peaks of whole LEM trading trading group
- Analysis is based on AusGrid data of 180 consumers, 60 prosumers with solar PV and 60 prosumers with solar PV and BESS.
- ToU: Peak hours 3pm to 9pm, off-peak hours 9pm to 3pm.
- P2P_selling_price: >5.3 c/kWh and <10.8 c/kWh (excl. network fees (paid by buyer));
- P2P_buying_price: >12.6 c/kWh and <30.7 c/kWh (incl. 4.0 c/kWh (off-peak) to 16.2 c/kWh (peak) network fees);
- FiT: 5.2 c/kWh; Grid_electricty_price: 17.8 c/kWh (off-peak), 31.4 c/kWh (peak)



7.3 DEMAND RESPONSE (DR) AND WHOLESALE ENERGY MARKET (WEM)

Demand response (DR) deals with managing the demand side of energy rather than the supply. This often means rescheduling activities of the energy users, which is exclusively handled by power grid operators — either retailers, network operators, or both. A classic demand response candidate might be an aluminum smelting works, which can save megawatts by operating under a"switch off" setting for a few hours at a time, during which the material remains hot enough for continued processing without affecting the finished product. Aluminum production consumes massive amounts of electricity, which has contributed to major strategic challenges in the context of rising energy prices. In Australia, which is among the top 10 aluminum producers globally, energy and cost savings for smelters can be key for navigating the current environment.

There are several additional examples of smaller-scale demand response initiatives. Supermarket refrigeration, for instance, can be lowered in strength by a few degrees at certain controlled times without affecting the quality of food. In Texas, an energy company ran a program where it could control the thermostat of households. At a household level, individuals can optimize their own energy usage by performing tasks that consume more energy during times of high supply and low price (e.g., using laundry machines and other appliances). Moving forward, developments in batteries and connected smart devices can also be programmed to optimize energy usage in households, with blockchain providing the decentralized computer power, leading to less grid consumption and supported by additional battery storage capacity.

As artificial intelligence plays a large role drawing patterns of energy demand to make informed predictions, it will be possible to foresee demand response reacting to these predictions to balance the grid. This is made possible by algorithms analyzing recent data.

Wholesale energy market (WEM) is a pool-based electricity market, which controls the supply and trading of electricity at a wholesale rate between energy retailers and upstream generators. In Western Australia (WA), it is operated by the Australian energy market operator (AEMO) following WEM rules.

The main objectives are to:

1) lower electricity supply cost in long-term

2) manage the efficient usage of electricity

3) encourage price competition between energy retailers and upstream generators

4) boost reliable and safe electricity generation and distribution

In general, WEM operates involving three processes. The first process comprises pre-market clearing inputs, such as contracts, trade executions, regulations, and logistics. The second process consists of optimization, economic dispatch, and contingency (all or some of them depending on the jurisdiction). The third process includes settlement, billing, and reporting.

Blockchain technology can also be used to store WEM rules, regulations, and analysis using smart contracts. Financial trading to clear the WEM via market clearing price (MCP) can also be performed on a blockchain platform using digital assets. Executed trading information and subsequent billing settlements can also be recorded permanently on the blockchain ledger.

7.4 RENEWABLE ENERGY CERTIFICATES (RECs)

Renewable energy certificates (RECs) are market-based instruments that certify the bearer owns one megawatt-hour (MWh) of electricity generated from a renewable energy (RE) resource. They are not utilities and function as a form of tax break. A REC can be sold for profit as an energy commodity, such as a carbon credit, to other entities seeking to offset their Scope 2 emissions or to REC brokers or Marketers, who will then onsell the energy credits in a secondary market at an increased price or commission. In different markets this certificate may also be known as a green tag, tradable renewable certificate, renewable electricity certificate, or renewable energy credit.

These credits allow the renewable part of the certificate to be traded independently from the underlying electricity, effectively supporting the funding of new renewable sources by increasing the price of the electricity being sold by then. This is a fundamental part of a book-and-claim system and is the cornerstone of Energy Attribute Certificates (EACs) worldwide, which provide proof of electricity produced by renewable sources and of which RECs are a subset.

The REC lifecycle starts at the point of renewable generation asset registration, during which time a third party verifies the validity of the renewable energy generation device capacity, fuel source, and location. Once verified and approved, the renewable energy producer can submit monthly generation data and request the issuance of the corresponding value in RECs for each megawatt hour (MWh) of renewable energy generated. In order to make this possible, the local REC issuer would have reviewed its generation data and then issued the equivalent amount of RECs directly to the corresponding registry account.

These registries, or tracking systems as they can also be known, are meant to establish, manage, and oversee the process of device registration, REC issuance, ownership transfers, and retirement of RECs. Until the REC is redeemed, canceled, or retired, REC marketers or brokers can act on behalf of renewable energy producers to sell their RECs to energy retailers or large corporate customers. Energy retailers can purchase RECs and retire them on behalf of their customers under a “green energy tariff” or “green pricing program,” optional programs offered by public utilities for regulated electricity markets, with state approved electricity pricing structures that allow customers to source their electricity consumption from renewables. Energy retailers can also utilize RECs to meet state or national regulatory requirements. Large corporations, in addition, can purchase and retire RECs to meet their voluntary environmental, social, and governance (ESG) goals. As both regulatory and voluntary targets are set and measured annually, there is a final annual audit stage for all retired, redeemed, and canceled RECs to check if the voluntary or regulatory targets have been met.

All this accounting work traditionally brings a host of potential difficulties which may surface from time to time. These include double counting or selling, mistakes around manual operational processes, system inefficiencies, market inefficiencies, transaction costs, and lack of transparency.

RECs are therefore another promising use case for the application of blockchain technology, and many REC markets around the world are already experimenting with it. Blockchain-based REC issuance also facilitates instantaneous REC ownership transfer and settlement, which minimizes counterparty risks. Blockchain also creates an immutable audit trail of REC ownership, from issuance to retirement. This can effectively address the trust issue facing carbon credit markets, where double counting instances have affected their credibility as reliable markets. Blockchain-based accounting systems can provide transparency to the supply chain, so as to restore the reputation and integrity of these markets.

A blockchain-based REC marketplace can function as described below:

1. **Smart meters post generation data to the smart contract, which mints a REC and assigns it to the asset owner's wallet for each MWh, or at a granular time-scale. Alternatively, smart meters can send this data to a registry that controls the minting of RECs on the blockchain through a smart contract.**
2. **All instances of trading are recorded on the blockchain, providing for a strong audit trail.**
3. **Settlement can occur instantaneously, through the use of cryptocurrencies, or through traditional means (bank transfers) that can be recorded and then added onto the chain.**
4. **Retirements burn REC tokens on the blockchain, destroying them permanently. When a new REC is minted on the chain that contains the generation data present on a retired REC, the registry can be alerted to investigate possible double issuance.**
5. **Beneficiaries of retirement can also be provided with a non-fungible token (NFT) that attests to their consumption of RECs, providing added value.**

7.5 24/7 CARBON-FREE ENERGY

The concept of 24/7 carbon-free energy (CFE) is distinct from 100% carbon free energy, or 100% renewable energy.

The term "100% renewable energy" refers to a company or organization buying renewable energy which doesn't always incentivize the most environmentally sustainable form of renewable energy. The energy that the company is buying may be fossil fuel energy with a REC certificate behind it. Effectively, incentive structures toward 100% renewable energy can result in the production of wasted renewable energy.

On the other hand, 24/7 CFE is a more environmentally sustainable concept. Here, the use and generation of electricity are closely linked, which means that down to 15-minute periods of time, these two are matched. This also enables the premium attached to buying renewable energy to get channeled to sources that are relevant to adequate energy needs. Therefore, this approach reduces the amount of fossil energy being consumed.

Compared to other processes, 24/7 CFE is a more accounting intensive activity. It requires linking up certificates with timelines and generates significant back-office work, all of which can be handled by computers. Blockchain technology coupled with smart contracts can provide both the decentralized computer power to enable the massive computation and also the assurances that the back-office processes are done correctly, which in addition reduces vulnerability to fraud.

7.6 METERING, BILLING AND SECURITY

Traditionally, energy metering has been performed manually, and often estimated, but as the need for more fine-grained energy monitoring has risen, smart energy meters have become increasingly common as the need to track real time energy consumption has risen. By combining smart energy meter readings with the immutable data storage enabled by blockchain, users can not only have increased confidence in real-time electricity billing, but doors open for them to also adjust their usage based on current energy prices, interacting with local energy markets in a transparent and secure manner.

Blockchain technology throughout this process greatly facilitates electronic billing systems through seamless payment processing and trusted data records, so all transactions can be made automatically and without a centralized party in control. The producers of the meter data can finally own their data and share with their counterparty for settlement These transactions are also easy to track and monitor. Further, the entire exchange history can be downloaded from the blockchain platform and can be used for periodical bill settlements.

7.7 GRID MANAGEMENT

Grid management sets the rules for managing several services of the power grid, such as capacity, direction of flow, flexibility services, and security. The aim is to provide an effective solution to address a progressively complex distribution environment. The grid management system features a flexible, interoperable, cyber-secure, and highly resilient design with options to upgrade to the best possible solution in the future.

The grid management system replaces the existing outage management system (OMS) and obsolete legacy distribution management system (DMS). It is composed of an advanced distribution management system (ADMS) and distributed energy resource management system (DERMS).

An ADMS retrieves, handles, and updates the power grid model to the power sub-transmission level. It assists in self-healing circuit functionality, real-time power grid studies, electrical system optimization, reporting capabilities, switching for planned and unplanned outages, and supervisory control and data acquisition (SCADA) controls. It has another important capability, known as mobile grid operation, which enables field personnel to access power grid data and update the information whenever necessary.

A DERMS maintains and dispatches distributed energies (DEs) optimally to cater to power grid services, facilitates DEs to take part in markets, manages distribution deferral resources cost-effectively, and provides non-wire alternatives. It also enhances the power grid's reliability services, DE constraint management, DE utilization by rendering DE communication and forecasting, and situational awareness under rising DE penetration.

Blockchain technology can bring additional insights into the grid management system, as it breaks down the centralized architecture and operates on a distributed platform, resulting in no single point of failure and providing trusted data to drive value in the market. It can allow consensus-based negotiations to procure grid management services using smart contracts. In particular, blockchain technology can assist in faster tracking of generation, consumption, and network data, along with proper and real-time coordination between these factors to stabilize the power grid. This can significantly contribute to avoiding flexibility services required for power grid management. In other words, reliability is enhanced and thus, flexibility service charges can be scaled down.

Another advantage of blockchain technology applied to grid management is its open and verified data records feature, which can permit authorized personnel to access power grid data whenever necessary to execute grid operations in real-time. This technology enables new possibilities to verify, secure, and improve energy flows between energy generators and users.

The security and privacy of such a blockchain-assisted power grid can also be confirmed by ensuring encrypted and public/private key cryptography and anonymous signatures. Security of grid systems is paramount today, especially with increasing cybersecurity risks that accompany increasing digitization. In a world of centralized data repositories, the risk of compromising or hacking public utilities' data systems can have catastrophic consequences that can endanger the availability of basic services to entire communities. Blockchain's security features can ensure resiliency of information systems, trusted data, and transparency.

7.8 ELECTRONIC VEHICLES (EVs)

Electric Vehicles include battery units and have the potential to smooth out the energy disparity between peaks and troughs in the renewable energy supply, in terms of both place and time. Practically, this allows energy resources in the form of batteries and vehicles to participate in the energy market by purchasing and storing energy when and where it is abundant and cheap, and then selling this energy back to the grid when the opposite is the case. This also provides the individual owner of these energy resources with a faster return on investment.

As more EV charging infrastructure is rolled out and cheaper EV models are introduced, the number of EVs is expected to grow significantly. This is where blockchain offers a promising application: to organize EV charging transactions handled by energy retailers. This technology has the capability to store financial information permanently in its ledger, while privacy and security are maintained via advanced algorithms.

EVs can be charged/discharged at home or in public stations, either from the power grid or guaranteed green sources. Blockchain can manage the underlying energy transactions, ensuring transparent and accurate accounting of all energy produced and sold in local energy markets or peer to peer trading.

8. CONCLUSION

Commitments to meet the Paris Agreement are highlighting the need for new business models in the energy market, where blockchain technology can greatly facilitate real-time data management and verify the authenticity of decarbonization claims. Once verified, blockchain technology also ensures that unauthorized changes are not made. In order to meet increasing demands for green energy from retail and commercial customers, utility companies also face pressure to provide evidence of how and where electricity was generated. In the context of rising energy prices, innovations that benefit users are fundamental to preserve fair access to basic resources, especially at the bottom of the economic pyramid.

The green energy transition will benefit from a predictable source of clean energy that is transparently accounted for and easy to manage. A transparent platform is key to manage the grid securely and effectively. Precise data from IoT sensors on devices such as solar panels, recorded on a blockchain, and fed into AI algorithms to make predictions and informed decisions, can transform the current energy landscape toward more sustainable models that better meet the needs of users.

Looking forward, one interesting question that arises regarding decentralized financial models around energy consumption is the responsibility of individuals to look after their own housekeeping. If a customer of a centralized bank loses a credit card, the bank can reissue it upon request. If unauthorized activity is detected on a customer's balance, a bank employee with authorized privileges can be contacted to make amends.[1]

1 With increasing digitization, only recently have phones become part of our payment rituals, as credit cards and cash are gradually being jettisoned. The notion of building physical tools into phones as virtual cards and certificates is fundamental to the concept of a virtual wallet, which is now an everyday concept for many people especially those underthose the under the age of forty. Covid vaccination certificates, rail passes, and credit cards for payment by wireless all received a huge boost during the Covid years while physical objects came under suspicion as 'vectors' for the transmission of viruses.

With decentralized finance and cryptocurrency, the responsibility for custody and safekeeping using virtual wallets lies on the individual. If a legitimate owner loses access to a non-fungible token representing an energy asset, for instance, there is no third party to make amends and it is possible to lose access to the item represented completely. Ensuring security is likely to shift to individual customers and the digital wallets they utilize to make transactions – likely as apps on their phones, linked to sensors on solar panels or other physical equipment. This creates a novel predicament for phone companies and other key infrastructure suppliers because the architecture of these devices was not designed for blockchain technology. While companies can create fixes and workarounds temporarily, it is likely that new hardware and software will be designed around the security and architecture necessary to prevent hacking and vulnerabilities specific to decentralized energy models.

It may be the case that blockchain companies would attempt to create their own hardware. For instance, Google was very successful building a phone based on the needs of the corporation, with its Samsung operating system. According to John Bulich of Powerledger, the future could already be here with Solana's imminent release of their Android Web 3-enabled SAGA mobile device, including Solana blockchain integration. As the virtualization trend is set to continue, individuals are becoming owners of their own data. Electrical energy and water data, and all other facets of human life (e.g., medical records), may become decentralized in the coming years. This trend will demand both software and hardware (e.g., phones) with the highest level of security and reliability. In this context, a race to create phones and other necessary equipment to facilitate web 3.0 will be inevitable.

Finally, blockchain technology can also help scale and pool together small projects to collectively attain the size required to attract major energy investments. This can democratize access to opportunities to participate in project finance and other investment models for renewable assets at a retail level. Decentralized energy systems enable energy investments at a localized city, village, and individual level. This can be a gamechanger for constrained grids, remote areas, low-income communities, and developing countries. New financing networks can facilitate these new energy networks, enabling new forms of bankability that relies on trusted networks and transparency.

9. ANNEX: BLOCKCHAIN BASICS

9.1 BLOCKCHAIN ORIGINS

Blockchain was envisioned to address the problem of not knowing whether a party one is transacting with, particularly when it is an intermediary, is trustworthy. The pseudonymous person, or group of persons, Satoshi Nakamoto set out to solve this issue when publishing the famous white paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” in 2008. In doing so, this also created the very first cryptocurrency.

This technology was developed to securely record and verify transactions, and in doing so track ownership of the digital currency Bitcoin. This combined a number of pre-existing technologies to envision the concept of a blockchain. These technologies include distributed ledger technology, cryptography, peer-to-peer networking, consensus mechanisms, and smart contracts.

9.2 TIME-STAMPING A DIGITAL DOCUMENT

In 1991 Stuart Haber, an American cryptographer, and Scot Stornetta, an American physicist, were working on a related problem. Together, the pair wrote a paper “How to Time-Stamp a Digital Document,” which was to start a revolution in record verification that was adopted by blockchain technology.

The original problem Stornetta and Haber set out to solve was how do you create a timestamp that is fraud proof? A simple example where this might be useful would be the following: A talented screenwriter comes up with a brilliant screenplay idea - something akin to The Maverick concept in Top Gun. Let’s assume the screenwriter wants to show the screen material was written on or before 1983, such that anyone it gets sent to might have been aware of it from that point in time. In other words, can writers prove any counterfeit version of their work has been copied from their own earlier original work?

The standard procedure advised by the Writers Guild of America in the 1980s was for writers to post themselves a dated copy of a complete manuscript in an envelope and leave it closed. That way, anyone could see the script was dated on a certain date. In the case of a lawsuit filed for copyright infringement, the sealed envelope could be opened in front of numerous legal witnesses who could read a script, determine if it had been copied in subsequent works, and the matter could thus be resolved.

While not a very digital approach, this leverages a centralized agency (the mail service) and numerous high status witnesses (intellectual property lawyers) to create a validation of the timing of a given material.

Stornetta and Haber propose a digital incarnation of this concept, allowing one to put an entire screenplay, which could be made up of half a million words, as an input into a hash function. A hash function takes a series of words and numbers as an input and produces exactly 60 letters and numbers as an output.

When using a hash function, the same input will always give the same output, but one can never find a reverse or inverse function that will turn one’s output back into one’s input. For this reason, a hash function is also known as a one-way function.

Let's say one takes the Top Gun screenplay and puts it through the SHA 256 hash function (or others with similar effect). Outcome could be 60 characters as follows:

c308b46a840689476fd642947b5415197c41add4f2a53c462dc747813352

One could now send it to oneself and others as an email. They would not be able to decode it or read it. If anyone doubted the legitimacy of the author, the author could publicly show the screenplay as a word document, put it through the hash function, and come out with exactly the same hash sequence, or value. The fact that an author could prove having sent onerself or someone else exactly that hash function would serve as a timestamp for the original work.

The one-way property of a hash function is somewhat analogous to the screenplay in a mailed stamped envelope. One can have the screenplay but not read it while it's in its envelope, just like no one can work out what the screenplay is from looking at the hash function of that screenplay.

HOW MANY WITNESSES ARE ENOUGH?

Another issue that Haber and Stornetta identified was that there always needed to be an independent person or body to verify authenticity—yet what if they were also part of a collusion?

If one needed to keep adding trusted parties to vouch for the honesty of existing players, the list could expand infinitely until the whole world was required. And that still wouldn't be enough.

Stornetta explains his insight: "I realized that if you turn that upside down and created a system of interlinked documents with essentially everyone as a witness, then you had, in fact, solved the problem." In other words, any attempt to change an entry earlier in the document would also now create a catastrophically observable event that many could notice.The Haber Stornetta approach to witnessing can best be understood by the way hashing is used to include not just any given entry, but also everything that came before it.

9.2.1 EXAMPLE: STORING DATA WHERE EVERYONE IS A WITNESS

Let us imagine Adam, Betty, Charlie, Dan, Eleanor and Freddie represent the community that uses a simplified blockchain.

Their ledger needs to include the following entries: Adam owes Betty $10, Charlie owes Dan $17, and Eleanor owes Freddie $14. The hash function enables a joint verification for all these entries to be hashed together. This means that changing one entry afterwards would change all of them.

First, when Adam owes Betty $10, this amount is written into the ledger and is run through a hash function which comes out as:

7896fe1174a172c47d33270d0216e6eb8bccac04a3ab0a5a60230ded9b1e

Then, when Charlie and Dan input their line in the ledger, they include the previous hash in their line, so they hash:

7896fe1174a172c47d33270d0216e6eb8bccac04a3ab0a5a60230ded9b1e

The new hash of these records is now:

5d9a3d9fbbbef3b5fdb70f78b78b653c31005f8049ce707d99a65bc1d7e9

Because a hash only ever returns 60 characters, the result of adding 21 extra characters with the phrase " Charlie owes Dan $17" is still only 60 characters long.

Then Eleanor and Freddie write their entry, appending it to the one above so as to hash:

5d9a3d9fbbbef3b5fdb70f78b78b653c31005f8049ce707d99a65bc1d7e9

Eleanor owes Freddie $14. This gives yet another new hash as an output:

86f74e2001e0461d06fde364b89f753342eaf81c2593789eedd7661f0f04

And so on. This system brings the entire community in the network, in this case comprised of Adam, Betty, Charlie, Dan, Eleanor, and Freddie, to observe every entry, without actually knowing anyone's personal information.

If anyone in this community tries to change their own entry, they will mess up the entire blockchain integrity for each and every other participant. In a way, this is analogous to putting a big scratch out mark or scribble on a paper ledger, in an attempt to rewrite a single entry.

Another analogy of tampering with hashed records would be taking a photocopy of the last page of a leather-bound ledger and sticking it to the current page and doing so for every page. This would mean that all the previous histories of records are present on every page. In all these scenarios, any attempt to change a single line of a ledger recorded in the past would become apparent to all in the present. Therefore, it also means it's in everybody's interest to pay attention to keeping it free from tampering.

Ultimately, hashing is an important feature that makes blockchain as secure as it is.

It also leverages numerous different computers distributed across many different places. A fraudster would have to attack each and every computer in the system to be successful; otherwise the system would detect that something is out of check.

9.3 PROOF OF WORK

There is one further refinement that helps prevent fraud. By requiring everyone, from Adam and Betty to Zita, to race to solve a problem before they admit a new block of information on the blockchain, you can make it even harder to cheat the system, and also unprofitable to do so. In a proof of work scenario, a number of specified network participants take on the role of miners in order to verify the latest transactions on the blockchain by solving hash puzzles.

The unique mathematical problem to arrive at the latest hash requires essentially a race between various miners who will, in the process of competing to solve the problem, give it a timestamp with multiple witnesses.

Because everyone knows who wins a race, and there can only be one winner, there can only be one source of truth for the information that gets laid down on the blockchain.

Moreover, any miner who joins the network afterward hasn't competed in the race and will have to solve all the subsequent problems too. This means that when one makes a mistake in a ledger at the start, all the numbers have to be adjusted afterwards. In computing and energy terms, this is eye wateringly and prohibitively expensive.

The Bitcoin blockchain has adopted this system. Because no bank was involved in the first Bitcoin transaction, but rather only a group of miners, this was the first decentralised currency and the first natively digital currency. The Nakamoto paper showed how to use Haber and Stornetta's work to keep a historical record of every Bitcoin that was ever minted and spent. If a miner, whose role is to validate transactions by solving problems in this way, attempts to alter a past block, it would take a very large amount of electricity and specialized hardware to do so.

An attack of this sort is not only practically impossible, but would also require vast amounts of capital investment that would have a better return by simply acting honestly and playing by the Bitcoin network's rules. This creates a situation where the most profitable strategy is to play by the protocol's rules, a game theory concept called a "Nash Equilibrium" that is a vital component of how the Bitcoin network has remained functional, even in an adversarial environment.

9.4 PROOF OF STAKE

As blockchain adoption continues to expand in a world which is increasingly carbon conscious, the proof of work consensus algorithm is now no longer regarded as the state-of-the-art approach. A number of other consensus mechanisms have emerged to validate records, with the most popular being proof of stake and its variants.

Proof of stake requires all participants to put up blockchain tokens as stake, and allow them to have a share in its maintenance, validation rights, and reward distribution. In our simple hypothetical example Adam, Betty, Charlie Dan, Eleanor and Freddie, all the way to Zita and beyond, own part of the blockchain.

In a proof of stake chain, we do not have 'miners' but rather 'validators'. Validator nodes are designated to actively validate records, and there may be delegation mechanisms by which other participants may choose to delegate their "stake" in the network to validator nodes. There is an optimum number of validator nodes, linked to the volume of transactions and number of participants, which in the future would point to the millions.

Validators are required to hold and 'stake' tokens, and if they are discovered to have made an error in the validation of blocks, then they are penalized by having all or a portion of their stake 'slashed' (i.e. removed) and lose the ability to remain validators. In the case of Ethereum, which recently transitioned from being a proof of work chain to a proof of stake chain, validators are required to stake 32 ETH. On this form of proof of stake chain, validators are randomly selected to add the next block and earn transaction fees.

9.5 PUBLIC AND PRIVATE KEYS

Users of blockchains also need to have keys to partake in the system. Users each have both a public key and a private key. The public key is a unique identifier that can be known publicly. It functions as an address – if someone wants to send you money, they send it to your public address. If, however, you want to access that money (Bitcoin for example) that has been sent to you, you need to provide your private key, which is not known publicly. A private key's function is similar to the key to one's safety deposit box, or the PIN to one's bank account. A very important difference, however, is that if your private key is lost, your money is inaccessible forever.

9.6 PUBLIC AND PRIVATE BLOCKCHAINS

We also need to be aware of the difference between public and private blockchains. A public blockchain is said to be 'permissionless'. Anyone can use it or build applications on it. Private blockchains, however, are just that. They are permissioned chains and can only be used with the permission of the owner.

9.7 SMART CONTRACTS

Smart contracts are lines of self-executing code that can automate transactions, even several at a time. They operate based on an 'if this, then that' basis. One can think of smart contracts as akin to vending machines. For a specific range of transactions, they serve to automate an entire process. Web 30 technology ultimately refers to the application of blockchain to smart contracts, performing transactions using cryptocurrency.

There are two schools of thought regarding the extent of smart contract applications. On the one hand, the breadth of applications is only limited by the sophistication of computing power. On the other hand, there will always be a human creative intelligence that may raise scenarios in addition to where smart contract technology alone is not sufficient, and a combination of traditional web technologies must be employed in conjunction with blockchain technology.