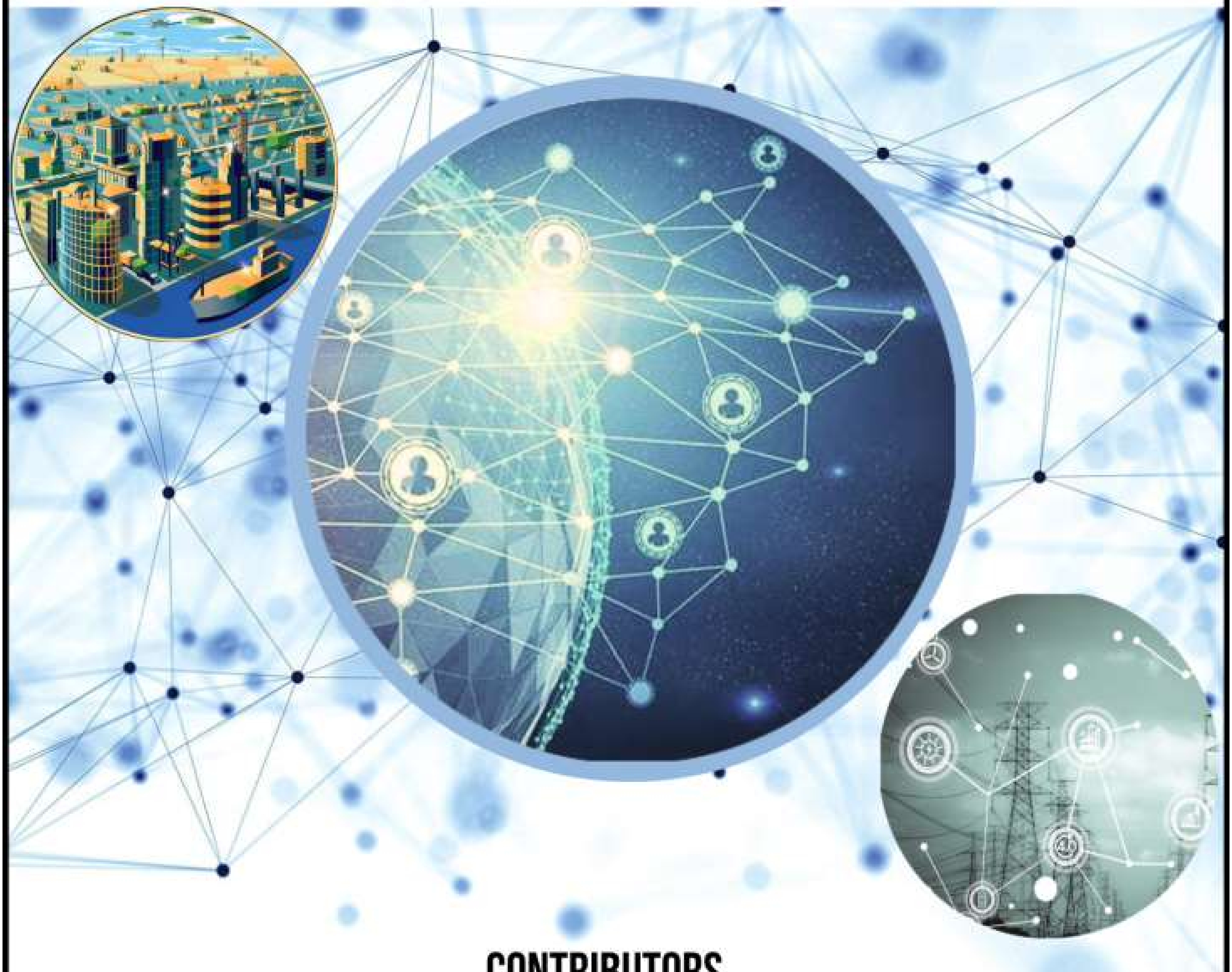
Global Smart Energy Federation

BLOCKCHAIN FOR ELECTRIC UTILITIES: A PATH TO LOW CARBON FUTURE



CONTRIBUTORS

GBBC Global Blockchain Business Council · Powerledger · RMIT UNIVERSITY · FLEXIDAO

July 2023

GLOBAL SMART ENERGY FEDERATION

www.globalsmartenergy.org

Blockchain For Electric Utilities: *A Path to Low Carbon Future*

Synopsis

This whitepaper provides a comprehensive overview of the significance of blockchain technology in the energy sector. Blockchain is not only nice to have, but it is also a necessity if we are to successfully create a distributed agile energy grid. It introduces Gen3 blockchain and argues that such a blockchain will be able to bring down the cost of ancillary services, reduce renewable curtailments, help flatten the duck curve, reduce the cost burden to the end customer, resolve issues with greenwashing and reduce fraud and errors. A detailed primer on Blockchain technology is given as Appendix-II to this paper.

Table of Content

Executive Summary: Why blockchain must be part of any renewable energy platform

Ever since the introduction of renewables onto the grid, there have been associated and anticipated problems: Issues such as intermittency, inertia deficits and transmission/distribution line congestion (also called grid congestion). While the classical response to this is to build bigger and more infrastructure, the cost of this has led many to see a distributed architecture of the grid as the sensible solution. In order for it to work properly, without spending a fortune on unlimited batteries, we need a very agile market. In this future you have distributed energy and decentralised markets that include energy, ancillary and network services.

Although that proposition is not controversial, there are those that say that a conventional system will suffice while we and others argue that only a decentralised blockchain system will prove to be better and efficient. We argue that the rapidly emerging and more complex energy landscape demands a shift from traditional centralised databases to blockchain and the new and decentralised markets they unlock. Realising this is fundamental to saving lots on battery capacity by using the existing resources better.

While we unpack how these issues could be solved by blockchain technology, there is also a stronger claim to be made about the appropriateness of next-generation blockchain to mitigate the problems of the grid. Some commentators see the agile market evolving, becoming more sophisticated and offering significant new functionalities. Not just peer exchanges of electricity in real-time, but also forward booking of electricity slots with the cost depending on how far in the future you are booking. In some ways, much more like an airline ticket than a conventional electricity bill.

In this future of the grid with forward booking, auctioning and re-booking slots with penalty clauses and bonus offers, you will need a real-time high-volume Gen 3 blockchain to manage this market. In this world, the consumer (everyday person who consumes electricity) becomes increasingly responsible, de-facto, for the balancing markets that make a grid work. They will not only consume but also provide services like frequency response, reserve, reactive power, and system restoration. Put another way, the prosumer (everyday person who also generates electricity e.g. using rooftop solar) gets involved with the financial instruments behind the grid. Just as the advent of the smartphone created more than just a camera on a phone, but opened an era of social media, so we can expect a plethora of new services that solve old problems, and blockchain technology is a necessity if we are to successfully create a distributed agile grid.

1.

Problems in power grids caused by the distributed imperative

The enthusiasm to include variable renewable energy (VRE) into the grid has come with some now very well-understood issues. Many of these can be likened to the problems of growing grain in the former Soviet Union. Without proper price signals to communicate the precise need, the planning for renewable energy sources has been inadequate. Just as the Soviet Union had no shortage of fertile soil, arable land, access to agrichemicals, cheap labour, good weather and knowledge of how to run large farms, the centralised planning system resulted in extreme shortages which required urgent intervention in the mid-1980's from the United States of America to survive. It is no exaggeration to say that centralised planning in the USSR meant that US grain donations averted widespread starvation.

In the world of electricity, the situation has many parallels. One might imagine that as solar power becomes better established in the state of California, and as pressure to reduce carbon-sourced energy ramps up, VRE would become better integrated into the California grid and costs of electricity would reduce. However, this does not appear to be the case.

I. Inherent problems with centralised planning

Like with the USSR's central planning, there are inherent problems with the centralised systems and centralised ways of doing things in the electrical grid. Here are a few of them.

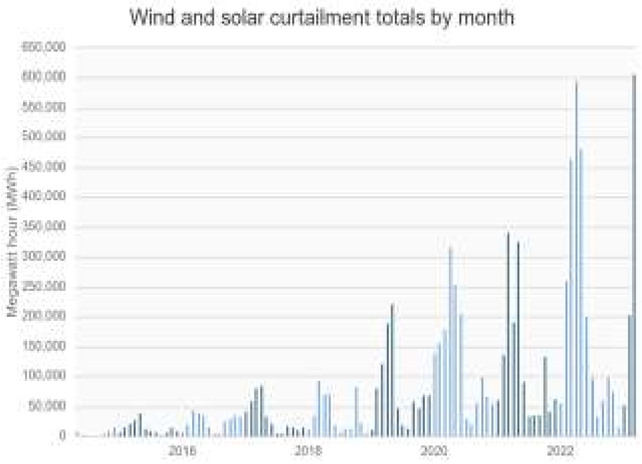


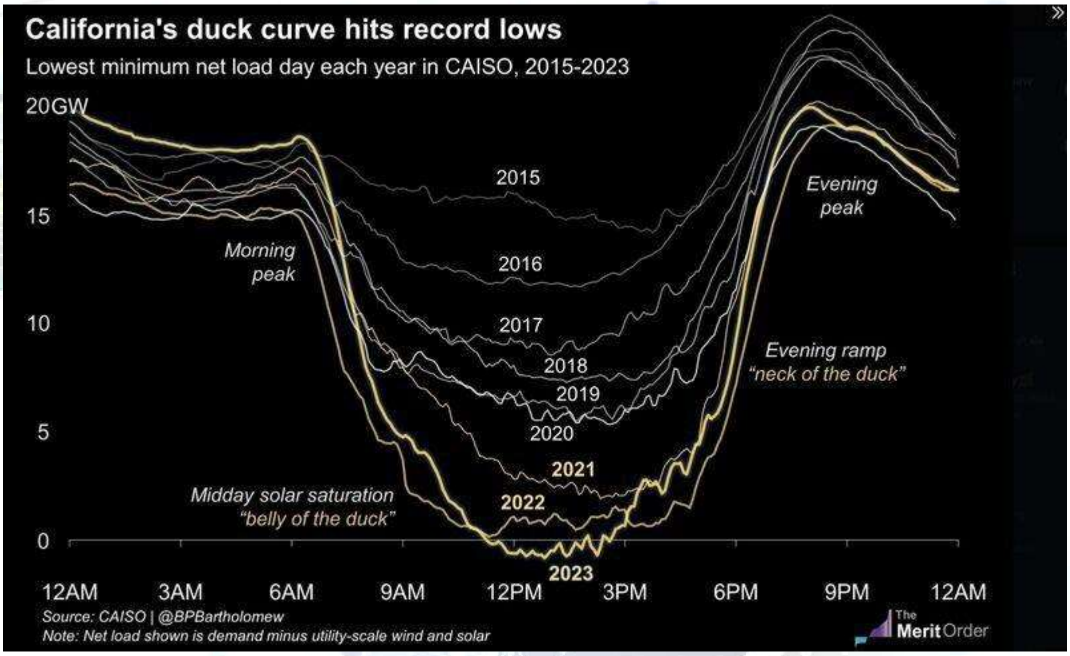
Figure SEQ Figure * ARABIC 1: Wind and solar curtailment totals by month

A. The renewables are increasing but being curtailed

The chart[1] the above shows how curtailment, i.e. switching off renewable energy sources from the grid (or reducing their output), is increasing, year on year, with peaks every spring.

B. Increasingly steeper duck curve

There have been increases in the cost of electricity in California every year and indeed increases in the cost of electricity everywhere in Europe long before the energy crisis struck. Similarly, the



duck curve,[2]which details the problems of uneven solar energy production over the daily cycle has become increasingly deep.

These problems speak of a challenge in integrating renewable electricity onto the grid. These issues can be traced back to two more fundamental ones: Problems to do with intermittency (time) and problems of place (spatial). Both, the difficulties of balancing a grid where the urge to place renewable sources has overwhelmed the system's ability to plan for them correctly. There is a third problem that arises from increased usage of VRE, and the loss of inertia, but that has yet to become critical in many parts of the world.

C. Increased costs burden to the customers by just increasing CAPEX spend

Blunt price signals caused by subsidies and high feed-in tariff rates have resulted in an indiscriminate building of VRE at locations unsuitable from a power system perspective as they are spatially far away from load centres. This has in turn led to high expenditure for networks to bring the electricity to market. Additionally, balancing supply and demand on the grid, via ancillary services is costly. The subsidies and capital expenditure on networks result in expensive

---

1 https://www.linkedin.com/pulse/electric-production-consumption-california-between-matteo-putzulu/

2 https://www.linkedin.com/pulse/electric-production-consumption-california-between-matteo-putzulu/

electricity, leading to higher energy tariffs passed over to the end customers, as seen in the figure below.

We will not be wrong in saying that such an expenditure has even created generational debt and disproportionately provided benefits to the high-income people (affluent population who make best use of early subsidies).

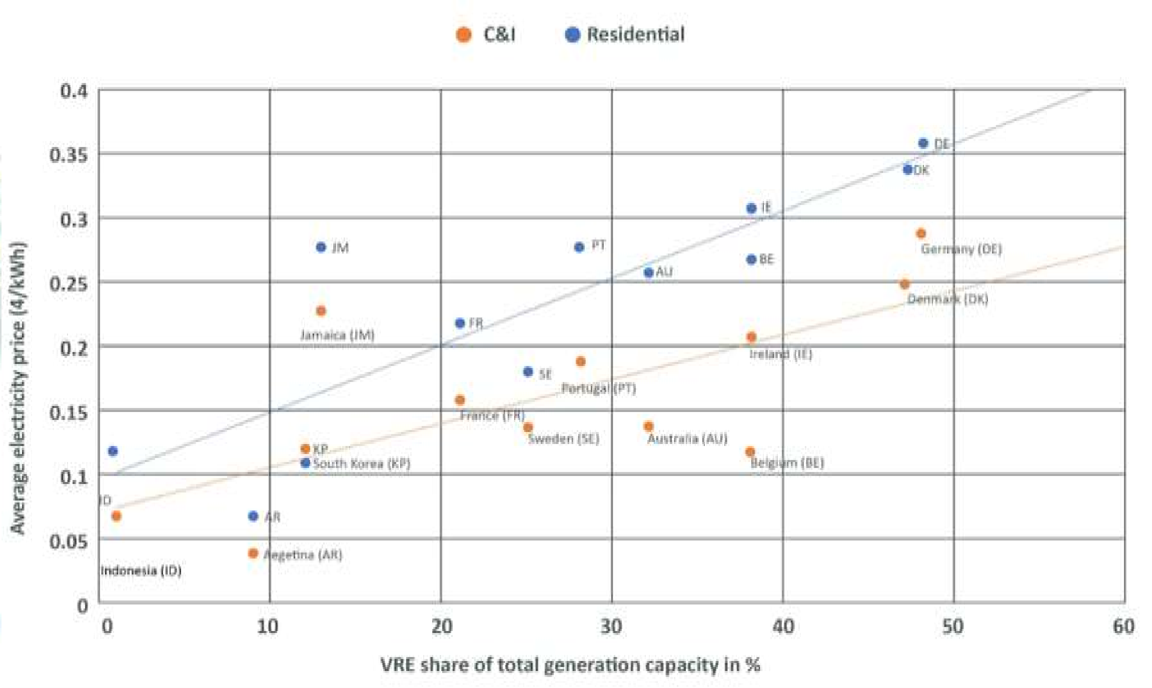


Figure 3: Average electricity price in $/kWh vs the VRE share of total generation capacity in %, authors

D. Problems with more peaking power plants and grid congestion: The cost of solving the above with the classical solution

Ancillary services refer to functions that help grid operators maintain a reliable electricity system and address the real time imbalances between supply and demand. The elaborate market mechanisms that we have today were engineered for a world some 50 years ago when energy was cheap and solar and wind generation were non-existent. In systems with significant variable renewable energy (RE) penetration, additional ancillary services such as “flexibility reserves” would be required to manage increased variability and uncertainty on timescales longer than contingency and regulating reserves.

Apart from more accurate forecasting to anticipate ancillary service needs by the system operator, new ancillary services such as “following reserves,” and “frequency and inertial response reserves” would have to be called upon to maintain a reliable and secure power system. “Following reserves” would need faster-ramping resources while the limited availability of large synchronous generators reduces the ability of the generation fleet to supply “frequency and inertial response“ services. In some countries, to meet peak demand, capacity markets are used in wholesale energy markets to pay for resources to be made available. All this has resulted in increasing the cost of electricity that is passed over to the end customers.

For example, in the UK, during the Covid-19 lockdown, the periods of very low net demand combined with high nuclear output increased the need for ancillary services implying additional costs. Ancillary services costs were 3 times higher in the period May to July 2020 compared to the same months in 2019: £302m in 2020 compared to £101m in 2019.

This sets the stage for what we are going to witness in the near future. Even though electricity demand is expected to increase over the coming decades due to the electrification of heat and transport, net demand is expected to further decrease due to an even higher rate of increase of variable renewable penetration to meet the emission targets. The costs of ancillary services[3] to cater to this level of renewable energy in the UK are estimated to reach 15% of total system operating costs by 2030 compared to 2% in 2015.

According to data from the California Independent System Operator (CAISO), the grid operator for most of California, the costs of ancillary services have been increasing as renewable energy penetration grows. For instance, the cost of regulation requirements rose more than 34% in 2021[4].

These examples highlight the general trend of increasing ancillary service costs associated with grids incorporating renewable energy sources. However, it is important to consult up-to-date and region-specific data for a more accurate assessment of the current costs and trends in ancillary services.

E. Greenwashing: An emerging crisis

Greenwashing is a pervasive issue today, as companies and organizations attempt to portray themselves as environmentally responsible without making substantial changes to their practices. Greenwashing involves the deceptive marketing tactics employed to create a false perception of environmental stewardship, leading consumers to believe that a product or service is more sustainable than it actually is. Some recent examples are Volkswagen AG, BP, Mitsubishi Motors Australia, Woolworths, Tlou Energy[5] and more[6].

By presenting a misleading image of sustainability, greenwashing not only misleads consumers but also undermines genuine efforts to address environmental concerns, making it imperative for individuals to be critical and discerning in their evaluation of eco-friendly claims.

---

3 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9759740/#sec3title

4 http://www.caiso.com/Documents/2021-Annual-Report-on-Market-Issues-Performance.pdf

5 https://www.wolterskluwer.com/en-au/expert-insights/asic-first-greenwashing-court-case-and-7-other-greenwashing-cases

6 https://earth.org/greenwashing-companies-corporations/

F. Fraud and error: From billing to phantom credits

In the Dole Food share issuance scandal[7], shareholders owned 30% more shares than were actually issued. This occurred because 2.9 million shares were bought from short sellers on the last day of trade, however, the centralised institution providing clearing and settlement services to the US stock market, the Depository Trust Company, generally stops tracking shares 3 days prior to a merger. Resolving the issue and compensating shareholders requires holding the short sellers accountable, which is challenging with the current share accounting system. Implementing blockchain technology could have addressed this problem.

The utility industry and energy sector experience similar challenges. In the US, Verra's[8] CEO resigned in May 2023 after it was discovered that Verra, a carbon credit standard and registry used by major global organisations, had approved tens of millions of worthless offset credits (known as "phantom credits"), according to a joint Guardian investigation[9].

II. Charting a path forward: Solutions for addressing energy market challenges

While the classical response to the issues with VRE discussed in the previous sections, is to build bigger and more infrastructure, the cost of which along with the lack of scalability has led many to see a *distributed architecture (see figure on the right)* of the grid as the sensible solution as VRE penetration increases.

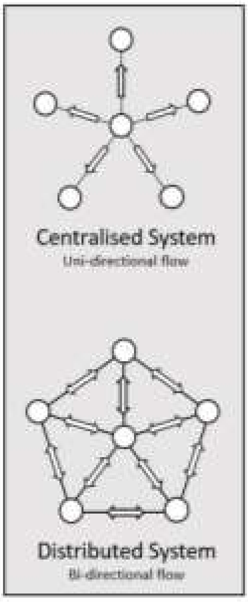


Figure SEQ Figure * ARABIC 4: Distributed architecture of the grid

New ideas can be very confusing. When Einstein's theory of general relativity came out it was said that only three people understood it, but apart from the mathematician involved in supporting Einstein and Einstein himself, no one quite knew who the third person was. However, the verification of relativity made Einstein an instant celebrity; the first celebrity physicist ever. Somehow, the general public immediately grasped the novelty of the new theory; they had a sense of its potential, even if the experts were still catching up on understanding what it really meant. It is possible that the conflicts and upsets around energy that we have described up to now, stem from the fact that many people do not really understand the new grid, distributed architecture and the theory and technology behind it. Turning the centralized scheme on its head and creating a distributed model is not just nice to have, nor a gimmick. The new grid is emerging as perhaps the only way renewable energy can overcome the dispatchability issue and be made to work.

[7]https://www.nytimes.com/2017/03/21/business/dealbook/dole-case-illustrates-problems-in-shareholder-system.html
[8]https://verra.org/
[9]https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe

Because there is such a large number of individual prosumer cells, a market evolves that reflects their state at any one time. This is the essence of the cellular paradigm and how the power part works.

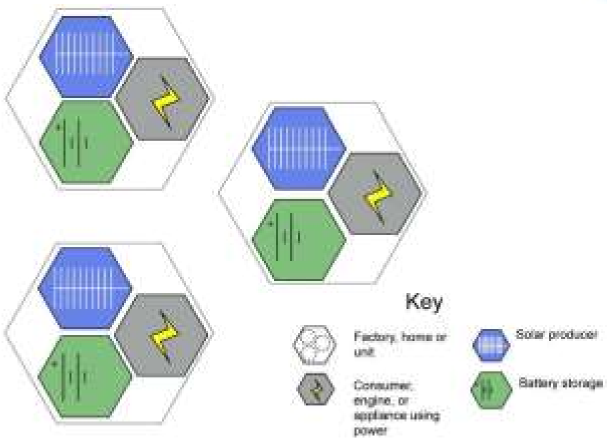
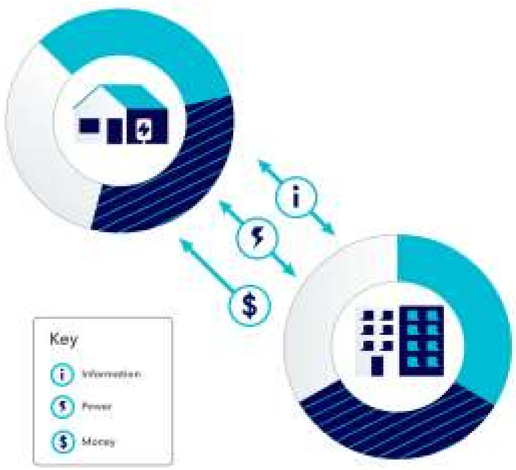


Figure SEQ Figure * ARABIC 5: Cellular energy systems, authors



The difference is that electricity flows are now bi-directional. Whereas in the old system, power flowed from the central generator to the households and factories; now with the cellular system, power can go from any one cell to any other. So too can money and information about price and demand. That means all cellular units are more or less equal in the hierarchy. At the next level, each of these cells has a control function that allows it to interact successfully with the rest of the grid.

The first of these is a kind of artificial intelligence brain that essentially works out the price of electricity at which the household appliance or electric vehicle is willing to buy from or sell to the other cells. It tracks every electron and its attributes like space, time, preferences etc. In the new grid, prices can rise and fall very quickly, for extremely brief intervals of time, because the price is the communication that ensures supply always matches demand. This is the emerging brave new world of energy systems. It requires a completely new way of planning and operations. It needs to be decentralised and needs to use blockchain. This report argues that.

2.

Why hobble your system when you can make it future proof? And it's not that far

In the previous chapter, we examined how many electrical engineers now agree that distributed architecture for the grid is almost a given, if we are to integrate variable renewable energy (VRE) resources successfully. Many of these commentators also can see that increasingly just-in-time pricing and trading of electricity (not just energy but also energy attributes like space and time) will be the obvious way to manage the grid of the future. However, one area of contention is the role that blockchain will play in this distributed grid.

Currently, all the electric utilities run centralized data base systems. However, the electrical system is undergoing a massive change that is going impact the record keeping and other business process in a utility. As countries reach their renewables goals or net zero goals, the grid will need to engage traditional consumers to help balance supply and demand.

Citizens are demanding more choice. They want to sell energy. They want flexibility in selecting the type of energy, over who they trade with, and over when and where they want the trade to happen. In our examination, we delve into the capabilities of centralized systems and uncover their limitations in effectively managing the complexities of the modern electrical world.

I. Myth Busting: Unveiling the True Potential of Blockchain Technology

In this section, we debunk common misconceptions surrounding blockchain and explore its actual capabilities and potential impact on various industries.

A. Scalability and Performance

Blockchain technology is deemed to be limited in scalability due to the consensus mechanisms and the replication of the entire ledger across multiple nodes, which can impact performance when dealing with high transaction volumes. It is also true that the early generation of blockchain systems had limited ability to scale up; this was certainly true for Generation 1 (Gen 1) blockchain systems. But as you might expect, successive generations of technology have eliminated this problem. A fuller discussion about Gen 2 and Gen 3 is available in our Blockchain Guide, but in essence, with the introduction of True Gen 3 blockchains, this argument no longer holds.

B. Speed and efficiency

Blockchain is misunderstood to introduce additional complexity and computational overhead due to the consensus algorithms and cryptographic operations, potentially impacting the system's speed and efficiency.

C. Cost-effectiveness

Blockchain is further misunderstood to be expensive, both in terms of maintenance and gas-fees[10]. On the contrary, several of the blockchains like the Powerledger blockchain are provided as managed services and the gas fee is extremely low. Another example is Solana. As of March 2023, the average gas fee for a simple transaction on the Solana network is around 0.0001 SOL, which is equivalent to two US cents.

D. Compatibility with existing systems

Finally, there is a common misunderstanding that building and operating a blockchain infrastructure requires significant computational resources, energy consumption, and specialized expertise. In contrast, the blockchain by nature, is modular and flexible to interact with the other existing systems.

E. Regulatory compliance

The immutable records of transactions generated on the blockchain network helps in regulatory compliances.

II. Future-proofing and what the system needs?

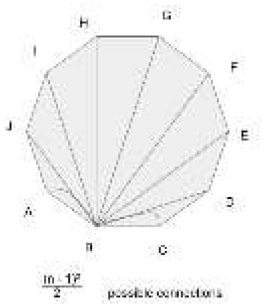


Figure SEQ Figure * ARABIC 7: The relationship between the power of a network and the number of nodes in a network

A. New types of markets

Caters for upcoming massive scales from citizen utilities in multiple forms (energy communities, choose your energy mix etc):

Consider the first point, about scalability. There is no doubt that scalable distributed systems will be needed and that presently distributed electricity trading trials are very limited in size so the big problem has yet to materialise.

However, the scalability argument cuts the opposite way. To understand this, you have to comprehend the underlying maths of peer-to-peer energy trading. If you consider, say, a 10-

[10] https://www.kraken.com/learn/what-is-a-blockchain-gas-fee

player network, each of the prosumers can give their electricity with 9 different neighbour connections, and going around the circle, that would give 9x9 connections each way, which counts each way twice. In general, this becomes $1/2\ (n-1)^2$.

This is if they were selling one attribute, say energy. The complexity further geometrically increases if there are additional attributes (like choosing the location of the trade, choosing the renewable source, preferential trading, buying or selling at a particular location or time) are considered.

Let us take an example. In the distributed paradigm for a region which had 1 million electricity users, there may well be at least over half a trillion transactions to keep. At this point, there is now a scalability problem for traditional database systems rather than blockchain. With half a trillion accounts keeping possibility of a low level of systematic fraud becomes a distinct possibility, because the centralised databases have relatively low levels of immunity to hacking. The paradigm of a low-level, but widespread fraud might be the LIBOR scandal where Barclays Bank manipulated the interbank interest rate by a small amount to gain a large advantage over time.

There is also the possibility of a more gross type of fraud or simply missed billing which has been on the increase for several years. Now consider buying/selling energy and its unlimited attributes. It could become a billing nightmare. Walmart Canada faced a similar issue and resolved[11] it using a decentralised database.

Blockchain, in this case, becomes a hyper scaler database that is well-equipped to handle the new types of markets. This is also illustrated by the theory of Network effects. Network effects[12] are used in technology networks to describe any situation in which the value of a product, service, or platform depends on the number of buyers, sellers, or users who participate in the network. In other words, the greater the number of buyers, sellers, or users, the greater the network effects; the greater the value created by the system.

So, the more the prosumers/consumers and other participants interact creating new types of markets and products, the value of the network increases. Blockchain facilitates this and caters for upcoming massive scales from citizen utilities in multiple forms (energy communities, choose your mix, etc).

B. Data sovereignty to participate in new things or monetize your data

In today's digital landscape, the concept of data sovereignty holds immense potential for individuals seeking to participate in new opportunities or monetize their valuable data. This need will also be soon felt by the participants in the energy sector.

[11] ttps://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges#:~:text=Then%20Walmart%20Canada%20pioneered%20a,70%20third%2Dparty%20freight%20carriers

[12] https://espace.curtin.edu.au/handle/20.500.11937/90269

By leveraging blockchain technology, customers (consumers and prosumers) can regain control over their data and explore innovative avenues for collaboration and economic empowerment. For instance, blockchain-powered decentralised identity systems enable individuals to securely manage and share personal information with the electricity providers (or in fact any other party of their choice), facilitating seamless access to services while maintaining privacy and control over sensitive data.

And this data can be sold in marketplaces that offer individuals the chance to monetize their data in a fair and transparent manner. For instance, individuals can contribute their data to platforms that specialize in gathering consumer insights, and in return, receive tokens or direct compensation based on the value their data brings to businesses. This allows individuals to benefit economically from their data while maintaining ownership and control over its usage, creating a more equitable data economy that empowers individuals to directly participate and reap the rewards of their data contributions.

Embracing data sovereignty through blockchain is a transformative step toward fostering a more inclusive and equitable digital future, where individuals have the power to participate and benefit from their own data. The examples above represent just a glimpse of the potential that lies within blockchain-enabled data sovereignty, opening up new horizons for individuals to engage in various sectors and industries, while ensuring their data is protected and fairly valued.

C. Tokenomics

Tokenomics can be utilized to guide or change behaviour, automate processes, and provide a secure way to interact without intermediaries. Tokenomics is very unique to blockchain. With its unique ability to guide or change behaviour, automate processes, and facilitate secure interactions without intermediaries, it presents a powerful tool that can revolutionize energy systems. By employing tokens within energy ecosystems, various stakeholders can incentivize sustainable practices, streamline transactions, and enhance overall system efficiency. For instance, in a renewable energy marketplace, tokens can be utilized to reward individuals or businesses for generating clean energy and reducing their carbon footprint. By tokenizing the energy produced, consumers can be incentivized to choose renewable sources, fostering a behavioural shift towards sustainable practices, and contributing to the larger goal of combating climate change.

Tokenomics also offers the potential to automate processes within energy systems, reducing administrative complexities and enabling seamless interactions. It eliminates the need for the central actor and their centralised database. Smart contracts powered by tokens can automate and verify energy transactions, ensuring transparency, accuracy, and security. This automation eliminates the need for intermediaries, such as traditional energy brokers or utility companies, streamlining the energy trading process and reducing associated costs. By eliminating intermediaries, tokenized energy systems empower individuals and small-scale producers to directly engage in energy trading, promoting decentralized participation and democratizing the energy market. Tokenomics has the potential to transform energy systems by guiding behaviour, automating processes, and providing secure interactions without intermediaries. This is an integral part of the decentralised future and cannot be realized using a centralised database.

D. Ease of auditability in a rapidly emerging and more complex energy landscape

With issues around false claims, greenwashing, and the need for provenance tracking, the use of blockchain over traditional databases is paramount. The ease of auditability provided by blockchain technology offers a game-changing solution. As energy systems become more decentralised and incorporate diverse sources such as renewables and consumers/prosumers, ensuring transparency and accountability becomes paramount.

Blockchain's immutable and transparent nature allows for seamless tracking and verification of energy transactions, providing a comprehensive audit trail that can be easily accessed by relevant stakeholders. This enables regulators, energy market participants, and consumers to verify the origin, authenticity, and environmental attributes of energy sources, ensuring compliance with regulations, promoting trust, and facilitating the integration of clean energy into the grid.

With blockchain, the once burdensome and time-consuming process of energy auditing, which once required heavy coordination of a central actor, can be streamlined.
Blockchain eliminates duplication of records and other frauds and it reduces administrative complexities and provides a reliable and efficient means of navigating the intricate energy landscape of the future. Blockchain can enable transparent and immutable records of emission reductions, enhancing the credibility of carbon credit certificates. . Through smart contracts and decentralised consensus, it ensures accurate accounting and reduces fraud risks.

III Why limit your system's potential when you can future-proof it? Embrace blockchain technology and unlock a world of possibilities.

The rapidly emerging and more complex energy landscape demands a shift from traditional centralised databases to the blockchain. As the energy sector integrates variable renewable energy resources and adopts distributed architecture, the transparency and accountability offered by blockchain become paramount.

Blockchain technology offers not only the core benefits of centralised database management systems but also future-proofs them. It presents a reliable and efficient means of navigating the intricate energy landscape of the future. So, instead of resisting change and struggling with outdated systems, it's essential to embrace the clear benefits that blockchain brings.

In summary, neglecting to incorporate blockchain in distributed energy markets can hobble your system by impeding transparency, hindering data management, limiting scalability, creating compliance challenges, and stifling innovation. On the other hand, embracing blockchain technology establishes the foundations for a robust and future-proof distributed energy market ecosystem. In the next chapter, we delve into the potential of controlling the decentralised grid with a True Gen 3 blockchain, exploring the advancements and possibilities that this technology brings to the forefront.

3.

Gen 1, 2, and 3 Blockchains

Blockchain offers a decentralised and transparent approach to record keeping, enabling secure and immutable transactions. At the end of this report, readers will find a comprehensive Blockchain Guide that provides fundamental insights into this transformative technology, paving the way for a deeper understanding of its potential applications in solving the problems associated with centralised systems in the energy sector.

The blockchain evolution: Gen 1, 2, and 3 blockchain

The Gen 1 blockchain is Bitcoin. It can just record information and process approximately 7 transactions per second.

The invention of Smart Contracts on Ethereum saw the birth of Gen 2 blockchains. The characteristics of Gen 2 blockchains include that they were:

- Initially secured by proof of work
- Are a Turing complete programming language allowed for custom applications to be built on top of the consensus layer
- Later blockchains improved on speed, efficiency, user experience, and power consumption while allowing general-purpose computation

Gen 3 blockchains, like Cardano, Avalanche, and Algorand, are generally referred to as blockchains that have smart contracting functionality like Ethereum, but with improvements in areas such as**:**

- Transaction processing time
- Lower transaction fees
- Higher limit on the number of transactions per second
- And higher data throughput

Significant advancements have been further made in Gen 3 blockchain technology, particularly with the introduction of parallel block processing. This innovation has led to higher throughput, meaning the ability to handle a larger number of transactions, and lower transaction fees compared to earlier Gen 3 iterations. Solana, in particular, is often referred to as a "***True Gen 3***" blockchain, showcasing its exceptional capabilities and advancements in the field. Another notable example of a *True Gen 3* blockchain is Powerledger Blockchain, which is an adaptation and enhancement of Solana for energy use cases. Such *True Gen 3* blockchains are clearly the winner. It has solved many of the issues that have dogged Gen 1 and Gen 2 such as energy intensiveness and efficiency. For a more complete update on the problems and how they've been solved, see the Blockchain Guide.

Here's a closer look at these aspects:

Speed: True Gen 3 chains that support high throughput and low latency and are capable of processing thousands of transactions per second, enabling near real-time transaction settlement. For example, as of 15 June 2023, the Solana Foundation is reporting 4,000 transactions per second are being processed based on overall activity on the mainnet, with the theoretical processing limit being much higher at 710,000 transactions per second. This speed is crucial for energy applications that require fast and reliable data transmission, such as real-time energy trading, grid management, or supply chain optimisation. The fast transaction processing capability of Gen 3 chains makes it suitable for handling the high volumes of data generated in energy systems.

Energy efficiency: While traditional blockchain networks like Bitcoin and Ethereum rely on energy-intensive consensus mechanisms like Proof of Work (PoW), Gen 3 chains using Proof of History (PoH) and Proof of Stake (PoS) hybrid consensus models with significantly reduced energy consumption. PoS is known for its energy efficiency because it does not require extensive computational work like PoW. By utilising a combination of PoH and PoS, Gen 3 chains aim to minimise their environmental impact and carbon footprint.

Comparing energy consumption, an average Google search transaction requires approximately 1.1 kilojoules (KJ), a single Solana transaction consumes only 0.793 KJ[13], while a Bitcoin transaction is considerably more energy-intensive, requiring a staggering 5 billion joules. For comparison, 3.6 million joules (or 3600 KJ) is equivalent to 1 kWh of electricity.

Gen 3 blockchain’s energy efficiency and speed make them well-suited for integrating with renewable energy systems and managing decentralised energy grids. In the context of energy, they can facilitate P2P transactions, enable efficient coordination of distributed energy resources, and provide a transparent and secure platform for tracking and verifying energy transactions.

I. Examining what’s possible

Features of Gen3 blockchains truly open remarkable and transformative innovations, first by securing data and then building new applications and ecosystems from that data and using a token economy, by harnessing these features and benefits:

- **Transparency**: Since the order book is on the blockchain, all transactions are public. Everyone can view the order book, and all changes to it are publicly visible. This transparency can help to prevent market manipulation.
- **Security**: By using the blockchain's distributed ledger, on-chain order books are highly secure and resilient to attacks. Even if one node is compromised, the other nodes on the network will continue to operate.

[13] https://solanaclimate.com/#

- **Trustless**: The on-chain order book operates in a decentralised way. You do not need to trust a centralised exchange to handle your orders; instead, the orders are directly executed on the blockchain.
- **Decentralised**: As the order book is hosted on the blockchain, it is not controlled by any single entity. This decentralisation ensures that no single entity can monopolise or manipulate the market.

We look at some examples here and later explore the possible similar applications to the energy systems in Chapter 5 The Agile Grid. What it looks like and how it works.

A. Hive Mapper is an innovative protocol designed to foster a decentralised mapping platform by enabling users to contribute valuable data. This protocol operates by incentivising users to enhance the platform's quality and value by offering rewards for providing high-quality mapping images. By actively involving users in the data contribution process, Hive Mapper aims to create a collaborative ecosystem where individuals are motivated to contribute their mapping expertise, thus collectively building a comprehensive and reliable mapping platform. This decentralised approach empowers users to actively participate in shaping and expanding the mapping network while receiving incentives for their valuable contributions.

B. **The Render Network** is a groundbreaking decentralised cloud computing platform that empowers developers to effortlessly deploy and scale web and application services, all while eliminating the complexities associated with managing the underlying infrastructure. Leveraging the power of blockchain technology, this innovative platform creates a trustless network of computing resources contributed by users worldwide, thereby revolutionising the conventional reliance on centralised cloud providers. By harnessing the decentralised nature of the Render Network, developers can unlock unprecedented levels of efficiency, security, and scalability in their computing operations.

C. **The Helium Blockchain Network** is a pioneering solution tailored specifically for Internet of Things (IoT) devices, offering a decentralised wireless network infrastructure. By employing a consensus mechanism known as Proof of Coverage (PoC), the Helium network ensures the validation of wireless coverage and data transmissions. Leveraging the power of LoRaWAN technology, the network enables efficient, low-power, and long-range wireless communication for IoT devices. This innovative approach facilitates seamless connectivity and data transfer, revolutionising the way IoT devices interact and function within a secure and scalable ecosystem.

D. **An on-chain Order Book**[14] **Exchange** is a ledger of buy and sell orders for a particular cryptocurrency asset that is hosted directly on the blockchain. Each transaction or order that takes place is directly recorded on the blockchain, in contrast to off-chain order books, which are hosted on centralised exchanges. Everyone has equal access to orders and can verify. All bids and asks are recorded as entries on the blockchain, not just settlements. There is no waiting room for transactions (via what is called a meme pool) for people (miners/ validators) to see so there cannot be front running , which can occur in centralised stock and commodities exchanges.

[14] https://tabtrader.com/academy/articles/what-is-openbook

These examples serve as powerful illustrations of how innovative technologies can bring about transformative changes across sectors. Drawing inspiration from these advancements, similar possibilities can be envisioned within the energy sector by leveraging blockchain to ensure secure and decentralised data management. This foundational layer of secure data can then unlock a wide range of innovation potential, as demonstrated in the highlighted examples. By embracing blockchain technology in the energy sector, we can lay the groundwork for groundbreaking developments and realise the transformative potential it holds for our industry and empower software developer ecosystems to innovate and create new applications. We discuss energy examples in Chapter 5.

4.

Controlling the decentralised agile grid using blockchain

Blockchain is not just another database. Databases are used to store and manage data and information. Very often, they are centralised. By contrast, blockchains are decentralised and distributed ledgers designed to be secure, transparent, and tamper-proof, that can specifically execute smart contracts, i.e. they can perform a range of complex transactions, which may include physical and financial settlement between counterparties.

Industry and governments have increasingly recognised the role of blockchain technology in the energy sector. Several notable examples of its application include:

- The Government of India public policy think tank NITI Aayog has written about the need for trust and the benefits of blockchain with energy trading as one of the use cases[15]
- The Indian Ministry of Electronics and Information Technology (MeitY) has come out with the National Strategy[16] to implement a National Blockchain Platform and will work with various Government organisations to implement the strategy and realise the advantages of blockchain technology in terms of enhanced security, trust and ability to create tamper-proof transactions.
- Blockchain MRV (measurement, reporting and verification) technology, for certifying green hydrogen and other environmental attributes, has already been developed by industry leaders. The Interwork Alliance, in collaboration with Microsoft, will, in 2023, finalise its Digital MRV Framework[17]. In the first instance, this will be used by issuers of carbon credits.
- Uttar Pradesh[18] & Delhi[19] are two geographies in India that have tried and mandated (or are in the process of mandating) Blockchain-based P2P Local Energy Markets.

Blockchain allows us to revolutionise our activities, to do things differently than before, or even try new things that we could not do before. The creation of local markets, for example, employing

15 https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf

16 https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf

17 https://interwork.org/resources/mrv-framework/

18 https://uperc.org/App_File/P2P-Guidelines_UPERC-pdf416202393822PM.pdf

19 https://cointelegraph.com/news/public-private-actors-in-delhi-trial-blockchain-based-solar-energy-trading

local knowledge and adapting to local conditions could not be done before the advent of blockchain.

Blockchain technology is best suited for environments where trust is especially important, where there is a need for a secure and transparent record-keeping system, supported by the automation of complex transactions through smart contracts. To illustrate this point, we detail a couple of high-profile examples where things have gone wrong, and how blockchain technology could have been used to prevent them.

Given the use cases of blockchain in the energy and attribute certificate trading space, the following are the benefits of using it:

A. **Transparency and traceability:** Blockchain creates an immutable record of every transaction, enabling all parties involved to track the origin, usage, and ownership of energy. This increases transparency and traceability, which can help to prevent both disputes and errors. Traditional energy trading systems can lack transparency, making it difficult to track and verify the origin, usage, and ownership of energy. This can lead to disputes and confusion, especially in complex energy trading networks or when attempting to roll out innovative products and offerings.

B. **Reduced intermediaries and costs**: Traditional energy trading systems often involve intermediaries, such as brokers and clearinghouses, which can add layers of complexity and cost to the process. Intermediaries can slow down settlement times and increase costs for all parties involved. Blockchain databases can remove the need for intermediaries which can reduce costs.

C. **Smart contracts**: Smart contracts are self-executing digital contracts that can automate the negotiation and execution of transactions. By leveraging blockchain, smart contracts can be used to automate energy trading and settlement processes, reducing the need for manual intervention and increasing efficiency.

D. **Security and privacy**: Traditional energy trading systems can experience security breaches and fraud [20], which can lead to significant financial losses and reputational damage. A lack of a secure and tamper-proof record of transactions can make it difficult to prevent or detect fraudulent activities. Blockchain's decentralised, tamper-proof record of transactions can reduce the risk of security breaches and fraud. This provides greater privacy and security for all parties involved, reducing the risk of financial and reputational losses.

The actual and potential application of blockchain to enhance the functioning of the agile grid is described in Chapter 5.

[20] https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/#:~:text=The%20US%20Department%20of%20Energy%20%28DoE%29%20reported%20150,that%20targeted%20systems%20holding%20information%20regarding%20electricity%20grids

5.

The Agile Grid. What it looks like and how it works better with Gen 3 blockchain

I. Shifting the energy paradigm: The evolution of distribution management systems and the rise of flexibilities

Traditionally, SCADA and distribution management systems (DMS) were used for automating the operations and switching management in the electric grid. In other words, when a tree falls on a power line, the DMS will switch off that feeder. Before the advent of DMS, only when a customer report power outage, the utility could dispatch the crew to patrol, find the fault and rectify it. In the recent years, Advanced DMS systems (ADMS) are deployed in utilities which integrated the DMS with the GIS map of the electrical network. This more modern system uses computer modelling to simulate conditions on the network, producing a quicker, better and faster method for restoring power. ADMS has a rich set of functionalities.

But then came the advent of DERs and their associated complexity. Not only were there trees falling on the line to contend with, but there were also intermittent moments of a high generation that were difficult to predict or even monitor. Clearly, a new system was required to manage this and it came with the title of DERMS, or distributed energy resource management system.

A DERMS would try to balance the behind-the-meter generations with load, it could do a few other things besides. Not only could it do the balancing, but it could also aggregate an entire fleet of say rooftop solar, and see it as a virtual power plant (VPP). It could manage the individual units as assets. It could manage Demand Response also.. . But as energy systems evolved and privatisation became a recurrent theme in energy purchase, a market was required. This market would enable a generator to buy the cheapest available energy at any time, while operating within the constraints of the grid. At the wholesale level, the market approach demonstrated real value. For example, in the state of California around 2014, the energy imbalance market was introduced. It has been calculated that this market approach saved the US taxpayer $2 billion by allowing efficient DER participation.

In the last few years, many commentators have sought to bring in a market layer in the Distribution space to procure so-called Flexibilities. That is the layer that guarantees steady frequency, voltage, and other power quality attributes of the power system. Rather than having a man in a white coat physically push a button to switch off excess DER production that is causing voltage and frequency issues, the automatic market-based system does something much more sophisticated. By letting the market set a price within given constraints, the system takes care of itself. This is a new energy paradigm. In the subsequent sections we will discuss how to unleash the full potential of the grid and explore the following blockchain use cases:

a) Energy Tracking and Environmental Attribute Certificates
b) Emissions Tracking
c) 24x7 Carbon Free Energy (CFE)
d) Transactive Energy Applications including P2P and LEMs
e) Demand Response
f) Grid Management
e) Emergence of EVs
f) Metering and Billing

II. Unleashing potential: How the data layer unlocks the new energy paradigm

Similar to how tracking and data layers are crucial for innovations in transportation (e.g., Uber being invented off the back of having a GPS data layer) or earlier discussed Gen 3 blockchain example, Hive Mapper, the energy sector also relies on a robust data layer as the foundation for innovation and progress. In the context of energy, establishing a comprehensive data layer is essential to capture and analyse information related to energy generation, consumption, distribution, and grid operations. This data layer can encompass various elements, including real-time energy production and consumption data, weather patterns, grid infrastructure details, and market dynamics.

A. Empowering energy management: Unlocking the potential of energy tracking as a service

The data layer in the energy sector serves as a crucial foundation for offering "tracking energy as a service" in various forms. This concept involves utilising the data layer to enable accurate and real-time tracking of energy-related parameters and delivering valuable insights and services to users. Here is how the data layer enables tracking energy as a service:

Energy tracking as a service: By leveraging blockchain technology, these systems enable transparent and immutable recording of the origin and attributes of environmental commodities, such as carbon credits or renewable energy certificates. This ensures that the environmental claims made by companies and organizations can be verified independently, mitigating the risk of greenwashing as explained in Chapter 1. Energy markets have their own share of scandals where customers were overcharged erroneously by energy retailers (see Appendix 1). The lack of transparency for consumers can lead to such errors, mostly by omission and, in certain cases by the commission on the part of the retailer or network operator. An example of energy tracking using blockchain is an electricity retailer in France, EkWateur[21], which is using a blockchain-enabled platform that provides provenance tracking of green electricity to its customers in France. EkWateur's customers are able to track the source of every kWh they consume and choose where their next kWh should come from. As another example, in Europe, there is a consortium of European energy transmission companies that wants to bring blockchain-based electricity tracking called Energy Track and Trace[22].

Emissions tracking as a service: Emissions tracking plays a vital role in assessing the environmental impact of industries. However, traditional systems face challenges in data accuracy and transparency. Blockchain technology offers a transformative solution by providing transparency, traceability, and security. Blockchain enables a transparent and traceable ecosystem for emissions tracking. Each emission-related transaction is recorded on the blockchain, ensuring data integrity and transparency. Smart contracts automate verification, calculation, and enforcement processes, streamlining emissions tracking. The tamper-proof nature of blockchain ensures data security, eliminating the risk of manipulation or fraud. As an example, the Climate Chain Coalition[23] brings together organisations utilising blockchain to address climate change issues, focusing on emissions tracking, carbon offset verification, and supply chain transparency. These initiatives highlight the potential of blockchain for accelerating emissions reduction and fostering sustainability. As blockchain can enable transparent and immutable records of emissions reductions, it would enhance the credibility of carbon credit issuance within Verra. Through smart contracts and decentralised consensus, it would ensure accurate accounting and reduce fraud risks. The Verra issue as outlined in Chapter 2, could have been avoided. Another emerging sustainability reporting metric is emissionality. Rather than solely tracking an entity's carbon footprint, emissionality looks at the broader environmental impact of energy consumption and production. It encourages businesses to use more energy when it is greener and drives investment towards carbon-free energy sources and storage solutions in the world's most polluted grids. Emissionality is a global metric, hence requiring a globally verifiable ledger, linking real-time emissions data with energy metering data. The data on this ledger should be tamper-proof, transparent, and accessible to all stakeholders, ranging from businesses, governments, and individuals, in order to ensure mutual trust and the integrity of emissionality reporting. Blockchain technology offers a transformative solution to the challenges of traditional emissions-tracking systems. By providing transparency, traceability, automation, and security, blockchain can enhance the accuracy and reliability of emissions tracking. Integrating blockchain technology holds the potential to accelerate global efforts to reduce greenhouse gas emissions and combat climate change.

Renewable energy integration: Accurate and granular data on renewable energy generation from sources like solar and wind enables grid operators to better manage and integrate these intermittent resources. The data layer allows for optimised scheduling, forecasting, and balancing of renewable energy, leading to increased reliability and improved grid stability.

---

[21] https://www.iotm2mcouncil.org/iot-library/news/smart-energy-news/ekwateur-uses-blockchain-to-give-energy-choice-in-france/

[22] https://energytrackandtrace.com/

[23] https://unfccc.int/news/un-supports-blockchain-technology-for-climate-action

24x7 carbon-free energy tracking as a service: 24x7 carbon-free energy (CFE) means that a customer's electricity consumption is fully matched with carbon-free energy sources at every hour of every day, in every location (see the graph[24] below). It operates under the following principles:

- Principle (1), time-matched carbon-free procurement deals with matching hourly electricity consumption with CFE generation via distributed energy resources (DERs)
- Principle (2), location-matched carbon-free procurement principle refers to buying CFE on the local power grids, where electricity consumers are connected
- Principle (3), the carbon-free technology-inclusive principle recognises the requirement of swift creation of CFE-driven power grids, and that all carbon-free energy technologies — including nuclear energy — can contribute towards creating this future

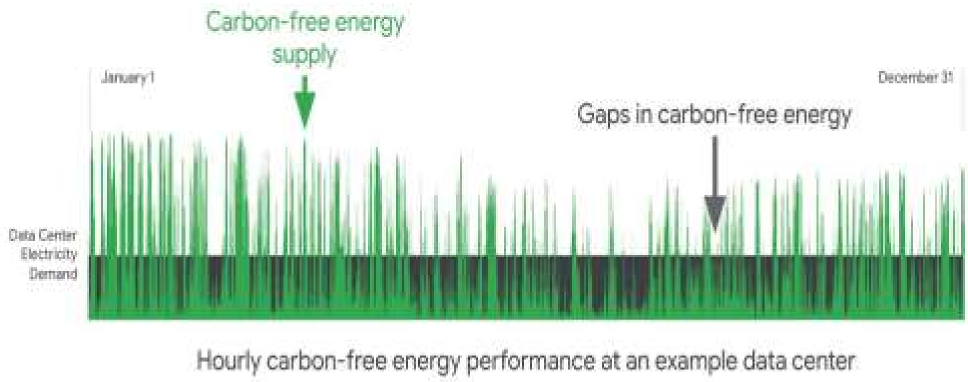


Figure 8: Hourly carbon-free energy performance at an example data cover, Google

- Principle (4), enabling new generation technology, focuses on the development of long-term storage or renewable energy sources such as advanced geothermal or green hydrogen that can provide base load energy. While these technologies are still in the nascent phase of development, 24x7 CFE is intended to drive investment and the rapid scaling of these new technologies
- Principle (5), maximising system impact, focuses on maximising emissions' reduction at a system-wide level, but the correct categorisation of new CFE or the creation of technologies that provide carbon-free energy for the dirtiest energy consumption hours. Example service providers include Powerledger and Flexidao.

B. From data to breakthroughs: Unleashing paradigm-changing energy innovation via the data layer

Once the data layer is in place, it becomes the basis for a wide range of innovations and advancements within the energy sector. Here are six examples:

Transactive Energy: Peer-to-peer (P2P) energy trading refers to the direct exchange of electricity between energy producers and consumers within a decentralised marketplace. In P2P energy trading, participants can generate renewable energy from sources such as solar panels,

[24] https://cloud.google.com/blog/topics/inside-google-cloud/announcing-round-the-clock-clean-energy-for-cloud

wind turbines, or other distributed energy resources. They can then offer their surplus energy for sale on a digital platform.

Image 1: Man installing solar panels on a roof, Pexels

As the energy paradigm shifts to distributed rather than central distribution, the contributions of renewable generation can work much better. Localised and agile pricing works well with a distributed approach, and the flexibility of pricing helps balance a system where there is variability of supply and congestion in the network to move energy around. In this context, blockchain becomes a candidate for keeping track of all financial transactions.

Tata Power, as an example, has piloted the use of a blockchain-based platform for P2P trading and grid management[25]. Commenting on the initiative, Mr. Ganesh Srinivasan, CEO, of Tata Power-DDL, said: "Tata Power-DDL is focused towards building a 'Utility of the Future' and transforming the power distribution space through innovative green technologies, collaborations, and initiatives. We are always looking at how we can increase the services we can offer to our

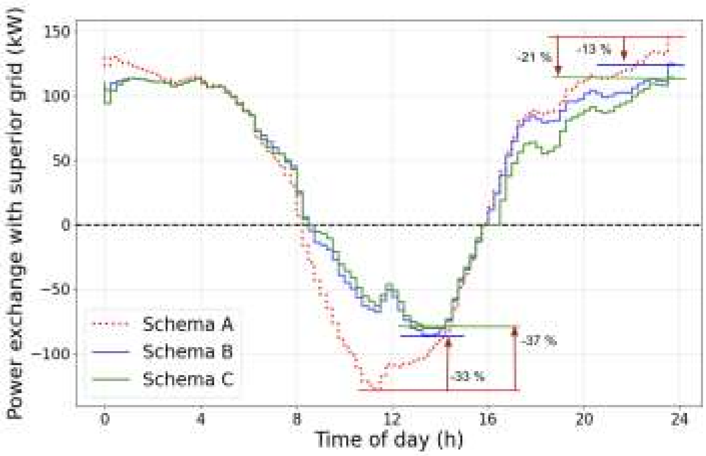
[25] https://www.tatapower-ddl.com/pr-details/199/1658486/tata-power-ddl-rolls-out-live-peer-to-peer-(p2p)-solar-energy-trading,-a-first-of-its-kind-pilot-project-in-delhi

consumers. Today, with growing rooftop solar power being available, we believe that P2P solar power trading can offer customers the flexibility to buy green power from those who have surplus solar power to sell".

A few years ago, when P2P trading was being experimented with; it was discovered that by including batteries, it could reduce troughs/peaks. The Pebbles Project in Germany was one such experiment. Pebbles used P2P trading with batteries to balance the supply and demand of energy at local nodes. P2P energy trading, which includes rooftop solar and batteries, is referred to as local energy markets, or LEMs.

Excess solar energy charges the batteries of peers during sunny hours, which would then be discharged during peak load hours in the evening/night. This reduces the energy transfer to and from the superior grid, and thereby reducing network violations and improving the power quality. The figure on the left represents the impact of LEM trading on the grid exchange with the wider grid. Schema A refers to a l business-as-usual (BAU) scenario with consumers and prosumers with solar PV. Schema B extends Schema A with prosumers owning a battery for self-supply only. In Schema C, the prosumers' batteries are operated by the LEM platform to optimise the balancing of load and supply with P2P trading between consumers and prosumers.

Batteries allow for LEMs to behave akin to wholesale markets. Wholesale markets have a forward-facing aspect in that bids can be placed into the future and then dispatched. In the LEM, battery owners can schedule their charge and dispatch activities for the future. This means that as the market can drive efficiencies, more and more BESS would be added to the system, enabling better management of peak demand, flattening of the duck curve, lowering of capital expenditure and reduction of curtailment periods.



In the LEM, the supply from clean energy is matched with energy demand at the appropriate price by adopting advanced optimisation 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.

A number of studies have tried LEMs and the results have been interesting. Probably the most notable example is called Pebbles[26], a demonstration and research project by Allgäu Netz, Allgäu Überlandwerk, Siemens, Hochschule Kempten, and Fraunhofer FIT. One of the observations of the Pebbles project is that it leads to increased self-consumption and a reduction in congestion

[26] https://pebbles.fit.fraunhofer.de/market/?lang=en

of the grid in the vicinity. The project allows day-ahead and intraday trading so that the local market can provide flexibility for the larger grid, which is a significant benefit. Pebbles also used blockchain by allowing market rules to be encoded transparently as smart contracts.

Demand Response Programs: Leveraging real-time energy data, demand response programs can incentivize consumers to adjust their energy consumption during peak periods or in response to grid conditions. This demand-side management approach helps balance supply and demand, reduces strain on the grid, and avoids costly infrastructure upgrades. Demand response (DR) is another example of grid management. DR deals with managing the demand for energy, rather than the supply of it. This often means rescheduling the activities of energy users, which is exclusively handled by power grid operators — either retailers, network operators or both. A classic demand response candidate might be switching off or reducing the cooling (or heating) load in a large building for few hours during peak demand periods.. But there are examples of more small-scale demand response initiatives like controlling the thermostat of a residential household. Blockchain technology can also be used for DR. As an example, *The Smart Contracts-Based Demand Response Bidding Mechanism to Enhance the Load Aggregator Model in Thailand*[27], looks into the data system owned by an individual load aggregator and cites the lack of transparency and distortion of the facts as a reason to introduce execution of DR based on blockchain-based smart contracts.

Grid Management: The electricity markets operate multiple processes. The first process comprises pre-market clearing inputs, such as contracts; trade executions; regulations; and logistics.

The second process consists of optimisation (DR is one of the many ways to optimise); unit commitment; economic dispatch; and contingency (all or some of them dependent on the jurisdiction).

The third process includes settlement, billing, and reporting.

[27]https://doi.org/10.3390/en16083606

For all of these processes, grid management applications set 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 requires a flexible, interoperable, cyber-secure, and highly resilient design, with options to upgrade to the best possible solution in the future. Gen 3 blockchain technology can bring additional improvements to the grid management system as it breaks down the centralised architecture and operates on a distributed platform, resulting in no single point of failure and is trustable to drive values in the market. It can allow consensus-based negotiations to procure grid management services using smart contracts. In particular, blockchain technology can assist in the faster tracking of generation, consumption, and network data, along with proper coordination between parties in real-time to stabilise the power grid, which can significantly contribute to avoiding flexibility services required for power grid management. Another advantage of utilising blockchain technology in grid management is that, depending on the type of blockchain used, the blockchain can be accessed and viewed at all times, facilitating authorised personnel to access power grid data whenever necessary to execute grid operations in real time. The security and privacy of such blockchain-assisted power grids can be maintained by using encrypted and public/private key cryptography-enabled features of data, and anonymous signature.

Such use of blockchain-based grid management systems would help in better management of the grid and integrate the DERs in an orderly fashion. This would lower the burden of increasing ancillary market costs, flatten the duck curve, lower the per unit costs of electricity, lower the CAPEX spend, and more. All the grid problems that are highlighted in Chapter 1 can be addressed.

Metering, Billing and Security: Gen3 blockchains can also be used to enhance the metering, billing, and security of such systems. Traditionally, energy metering has been done manually and is often estimated. As the need for more granular, and informative and real-time energy monitoring has risen, smart energy meters have become increasingly common. Now as more complex billing scenarios emerge, where the payments are not just done for energy but also for the type of energy, the preference, its location etc, the billing is becoming overly complicated. And today’s billing systems are bound to fail.

By combining smart energy meter readings with energy attributes and preferences along with the immutable data storage of blockchain, consumers cannot only have increased confidence in the real-time electricity billing, but it also allows them to adjust their usage based on current energy prices, and interact with LEMs transparently and securely.

Image 3 EV charging, Pexels

Blockchain technology allows for integration with electronic billing systems, enabling seamless payments to be processed automatically and without a centralised authority intermediary. Further, these transactions are also easy to track and monitor, and the entire exchange history can be downloaded from the blockchain platform and can be used for periodical bill settlements. The paper, 'Blockchain-based balance settlement ledger for energy communities in open electricity markets[28]' describes one such method.

Electric Vehicles: An emerging example use case for the Gen3 blockchain is Electric Vehicle (EV). EVs, including large battery units, have the potential to smooth out the energy disparity between peaks and troughs of RE supply, for both place and time. Practically, this allows the energy resources (batteries and EVs) 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 demand and prices are high. This can provide the owner of the battery or EV with a faster return on investment. After all, EVs are batteries on wheels and if used properly, we can make them beneficial both to the grid and to the EV owners.

As more EV charging infrastructure is being rolled out, and cheaper models of EVs are introduced, the number of EVs is expected to grow[29]. Blockchain may be used to organise EV charging transactions owned and operated by the energy retailer, as the technology has the capability to store financial and other information permanently, while privacy and security are maintained via advanced algorithms. Besides, blockchain can be used to track and create a digital 'passport' for EVs that includes financial information, the operational parameters (like the number of miles clocked by a given vehicle and its accident-related record) and even the source of the minerals used in the battery. It can also be used for charge management. EVs can be charged and discharged at home or public charging stations either from grid power or guaranteed green sources. Blockchain can manage the process and provide a concrete record of the green supply chain, eliminating any potential 'black-hat' operators. All of these illustrate that the problems

[28] https://doi.org/10.1016/j.energy.2022.124180

[29] https://www.goldmansachs.com/intelligence/pages/electric-vehicles-are-forecast-to-be-half-of-global-car-sales-by-2035.html#:~:text=EV%20sales%20will%20soar%20to,from%202%25%20during%20that%20span.

highlighted in chapter 1 with respect to grid problems, tracking provenance, and avoiding greenwashing claims can be addressed. A few examples[30] of such blockchain-enabled EV-charging platforms are Share & Charge, Chargemap, Aerovironment, Easy Park and Charge.

Additionally, blockchain can be used to tokenize the electricity from the rooftop solar and use the tokens to later charge the EVs. It can also be used to generate rewards and incentivise EV owners. Blockchain-enabled platform can also be used for provenance tracking of green energy for EV charging as well as enabling alternatives of green energy sources for EV Charging Stations through excess rooftop photovoltaic (RTPV). With over 100 million EVs on the planet generating billions of transactions and data points, the use of true Gen 3 blockchains is a vital ingredient for all of the use cases above.

Attribute Certificates: In today's energy system, environment attribute certificates (EACs) are used as part of a worldwide book-and-claim system as a way to reduce one's carbon footprint. They can take the form of Renewable Energy Certificates (RECs), Guarantees of Origin (GOs), and International RECs (I-RECs) when being used to track renewable energy production, or carbon credits when being used to track carbon offset. When offsetting scope 2 emissions, RECs are used to track and verify the production, trade, and consumption of renewable electricity. Each certificate represents proof that one megawatt-hour of electricity has been produced from renewable sources. Carbon credits on the other hand can be used to reduce or "offset" an organisation's scope 1, 2, or 3 emissions, as a net adjustment and are measured in 1 metric tonne of reduced or avoided greenhouse gas (GHG) emissions. Whoever retires (or cancels/redeems) these instruments "owns" the right to claim they are reducing their carbon footprint.

All EACs follow similar creation and ownership pathways. Using RECs as an example, the lifecycle starts at the point of the renewable generation asset registration, during which time a third party verifies the validity of the energy generation device capacity, fuel source and location and that it is not already registered in another tracking system. Once verified and approved, the producer can submit monthly generation data and request the issuance of the corresponding value in RECs for the MWh of renewable energy generated. Prior to doing this, the local REC issuer reviews the generation data against settlement data and then issues the equivalent number of RECs direct to their registry account.

These registries, or tracking systems as they are also known, establish, manage, and oversee the process of generation device registration, REC issuance, ownership transfers and retirement of RECs. Until the REC is retired, it can be traded on the open market by the RE generators or brokers and bought by utilities, energy retailers or large corporate customers to meet state or national regulatory requirements or voluntary environmental (ESG) goals. In locations such as Europe and North America, there are multiple registries that have limited connectivity to each other, which means customers require a separate registry account in any region they wish to purchase and retirement of RECs and RE generators also require separate registry accounts for each tracking region that they have generation facilities. As both regulatory and voluntary targets are set and

[30] https://www.forbes.com/sites/naveenjoshi/2021/12/21/the-role-of-blockchain-in-the-development-of-the-ev-industry/?sh=16c398c93862

measured annually, there is a final annual audit stage for all retired (meaning either redeemed or cancelled) RECs, to check if the voluntary or regulatory targets have been met. All this accounting work traditionally brings with it a host of potential problems which surface from time to time. These include double counting or double selling, mistakes in manual operational processes, system inefficiencies, market inefficiencies, duplicated participation processes and costs, and a lack of transparency. An example is Verra as highlighted in Chapter 2.

RECs are the perfect use case for the application of blockchain technology. As it is decentralised and immutable, a blockchain-based REC registry and marketplace solution is free from all the ills listed above. A blockchain-based REC solution could be used to register generation assets and facilitate the issuance, removing the manual processes followed by traditional registries today when checking that the generation is not already registered with another registry in their market boundary. And in the case of REC trading, deliver instantaneous ownership transfer and settlement, removing counterparty risk. Blockchain also creates an immutable audit trail of ownership from issuance to retirement. This streamlining would allow third parties that support the traditional registry model today, to focus instead on the verification of generation assets and generation data.

Another big advantage of blockchain is the tokenization of RECs. It enables fractional ownership, allowing smaller investors to participate in the renewable energy market. Now when coupled with blockchain's transparency, the traceability and authenticity of RECs are guaranteed. This means the risk of fraud and greenwashing is reduced. Blockchain-based tokenization facilitates seamless and efficient trading of RECs, removing intermediaries and reducing transaction costs.

A blockchain-based REC registry and the marketplace could function as follows:

A. RE generators can apply to have their generation asset registered on the blockchain, and once all details of the device are verified by a third party, a generation asset ID and wallet are created for them. This wallet would act like a ‘bank account’ and be able to receive any RECs issued from the generation assets linked to the wallet and owned by the RE generator within the full market boundary. Any duplicate generation asset would be identified automatically at the point of registration.
B. Smart meters send generation data to the registry. Once the data is verified, the blockchain registry mints a REC token and assigns it to the RE asset owner’s wallet for each MWh of energy, or representing the energy produced on a granular time-scale, post-data verification.
C. Any instances of trading are recorded on the blockchain, providing a strong audit trail that can be verified by third parties.
D. Settlement can occur instantaneously using digital currencies or through traditional bank transfers that can be recorded on the chain.
E. Retirements ‘burn’ REC tokens on the chain, destroying the tokens permanently. When a new REC token is minted on the chain that contains the generative data present on a retired REC, the registry can be alerted to investigate any possible double-issuance.
F. Beneficiaries of retirement can also receive a non-fungible token (NFT) that attests to their consumption of RECs providing added value.

The process above can also be used to significantly enhance all processes within the lifecycle of other EACs like carbon credits and green hydrogen certificates. By leveraging the decentralised and transparent nature of blockchain technology, registries (or similar organisations) can establish a secure and immutable record of every EAC transaction, from issuance to retirement. The metadata about the origin, fuel type, location, time, fractional ownership etc can also be transparently and immutably stored in the chain.

This increased transparency helps prevent fraud and ensures the integrity of the certificates, instilling trust among stakeholders. Moreover, smart contracts on the blockchain can be programmed to enable automated verification of inputs for the issuance and retirement of any EAC. Additionally, a blockchain registry can provide real-time visibility of the ownership and utilisation of certificates, allowing for better tracking and monitoring of the environmental impact of the certificates. Overall, the adoption of a blockchain-based registry and/or marketplace for EACs promotes efficiency, transparency, and accountability, thereby bolstering the effectiveness of environmental initiatives and facilitating the transition to a sustainable future.

A real-world example of blockchain-enabled trading of RECs is Powerledger's TraceX marketplace. TraceX[31] is a digital marketplace that uses blockchain technology to efficiently handle the trading of energy attribute certificates, such as RECs. Being blockchain-enabled, TraceX captures data pertaining to import and export trades, changes in ownership and retirement events of environmental attributes on a proprietary distributed ledger — providing an immutable and verifiable audit trail. Users can link their registry account and import RECs to the marketplace once the link is established. Successful purchases in the marketplace are updated directly through their registry account.

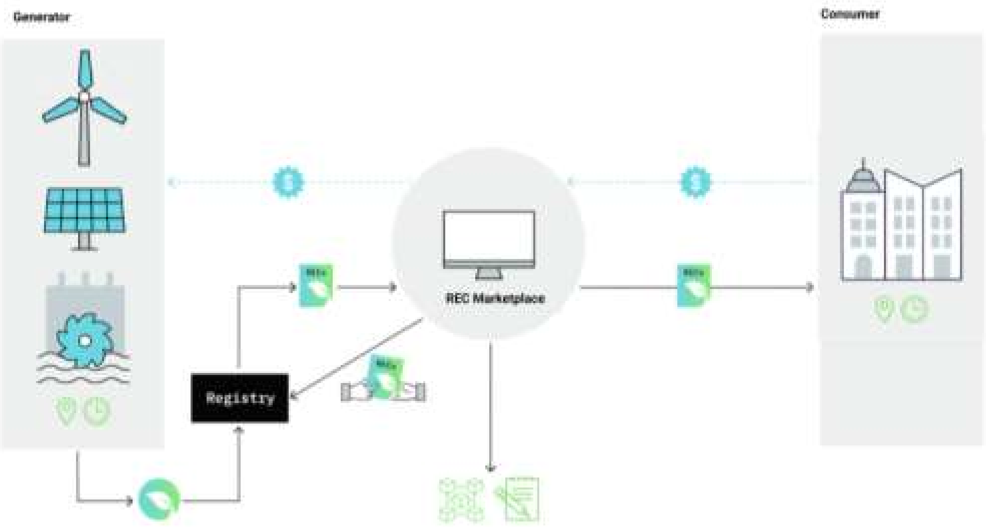


Figure 10: Interaction with generators, EAC registries, marketplace and consumers, authors

[31]https://www.powerledger.io/platform-features/tracex

III. The Agile Grid. What it looks like and why it works better with Gen 3 blockchain

In various sectors, the implementation of a data layer has proven to be a catalyst for unlocking innovation and driving advancements. By establishing a solid foundation of comprehensive and accessible data, organisations can leverage this valuable resource to develop new products, services, and insights. The same concept applies to the energy sector, where a data layer plays a pivotal role in enabling innovation.

Further, energy systems will leapfrog with the application of such blockchain and future-proof itself. Here is why:

Increased Throughput: Gen 3 blockchains often boast improved scalability and higher transaction throughput compared to earlier iterations. This scalability enables the efficient handling of large volumes of energy-related data within the data layer, facilitating faster processing, analytics, and real-time insights. It opens doors for innovative applications and services that require rapid data processing and decision-making.
Tokenisation and Incentive Mechanisms: Gen 3 blockchains commonly incorporate token systems, enabling the creation of native digital assets that can represent energy, credits, or other forms of value. These tokens can be used to incentivise data sharing, participation, and collaboration within the energy ecosystem. By integrating tokenisation into the data layer, innovative market mechanisms can be established, such as energy trading platforms, reward systems for energy-saving practices, or decentralised energy marketplaces.
Smart Contracts and Automation: Gen 3 blockchains often support advanced smart contract functionality. Smart contracts are self-executing agreements with predefined rules encoded within the blockchain. They enable automation, trustless interactions, and streamlined processes. Within the energy sector, smart contracts integrated into the data layer can automate transactions, facilitate peer-to-peer energy trading, enable energy market settlements, or streamline complex energy agreements.

In summary, when coupling energy data with a Generation 3 (Gen 3) blockchain, which offers fast throughput and a token system, the potential for innovation is further amplified. The agile grid can only leapfrog by using such Gen 3 technologies - EACs trading becomes more elegant and transparent, grid management becomes better, chances of fraud and errors are reduced, DERs are orderly integrated and market-based mechanisms like P2P and LEMs can easily be deployed.

6.

Conclusion: Blockchain is not just a nice to have, it is a necessity for the evolving distributed agile energy grid

In conclusion, despite the controversies and debates surrounding blockchain and cryptocurrency, it is essential to take a rational and objective approach to evaluate the true value and opportunities they offer.

In the report, we identified the inherent problems with centralised planning and centralised ways of thinking, like a) increasing renewable curtailment b) increasingly steeper duck curve c) increasing cost burden to the end customers d) increasing ancillary service costs e) issues with greenwashing and f) frauds and errors.

Of course, centralised database systems are working well right now by and large. All the electric utilities run such systems. However, the electrical system is undergoing a massive change that is going to ask for it more than right now. As countries reach their renewables goals or net zero goals, the grid will need to engage traditional consumers to help balance supply and demand.
In order for it to work properly, without spending a fortune on unlimited batteries, we need a very agile energy market that can balance supply and demand and reduce the need to upgrade grid infrastructure, that encourages electricity generation nearer to consumption and that has citizens provide ancillary and network services. In this future you have distributed energy and decentralised markets that reduce the need for centralised energy generation and storage.
While sceptics argue that existing technologies can fulfil the same functions, blockchain represents the culmination of advancements in mathematics that have revolutionised everyday activities like communication and online shopping.

Image 4: Discussions on renewables, Pexels

We argue that the rapidly emerging and more complex energy landscape demands a shift from traditional, centralised databases, to blockchain and the new and decentralised markets they unlock. Realising this is fundamental to reducing the need to invest in battery capacity by using the existing resources better.
Further, the use of True Gen 3 blockchains for the agile grid would help bring down the costs of delivery of these services.

By combining the data layer within a Gen 3 blockchain, the energy sector can unlock new frontiers of innovation. This synergistic approach fosters secure data sharing, incentivises participation, enables faster and scalable processing, and automates processes through smart contracts. It provides a solid foundation for the development of groundbreaking applications, market platforms, and energy management solutions that can reshape the energy landscape toward greater efficiency, sustainability, and consumer empowerment.

Blockchain technology is not just a nice-to-have feature; it is an absolute necessity in building a successful and distributed agile energy grid. Its implementation is vital for effectively managing and coordinating the complexities of a decentralized energy system. By leveraging blockchain, we can ensure the seamless integration of renewable resources, optimize energy transactions, and establish a secure and transparent framework for the future of energy.

7.

Appendices

Appendix I: Definitions and Concepts

Agile grid: Smart electrical grids that are flexible and made for the future, where consumers and prosumers will actively participate in providing grid services.

Ancillary services : Ancillary services[32]are the services necessary to support the transmission of electric power from generators to end users given the obligations of control areas and transmission utilities within those control areas to maintain reliable operations of the interconnected transmission system.

Artificial intelligence: Artificial intelligence (AI) is intelligence demonstrated by computers, as opposed to human or animal intelligence.

Attribute certificates: Also known as Environmental attribute certificates. An Energy Attribute Certificate[33] (EAC) is the official documentation to prove renewable energy consumption. Each EAC represents proof that 1 MWh of renewable energy has been produced and added to the grid. They can take the form of Renewable Energy Certificates (RECs), Guarantees of Origin (GOs), and International RECs (I-RECs) when being used to track renewable energy production, or carbon credits when being used to track carbon offset.

Balancing markets: Balancing markets[34] are generally single-period markets, i.e., a separate session for each trading period. They allow the possibility of trading, in addition to the electric energy ancillary services (e.g., voltage control) needed to maintain the stability of the electric system.

Bitcoin: Bitcoin[35] is an innovative payment network and a new kind of money. It is one of the first iterations of blockchain and hence referred to as Gen 1 (or generation 1) in this paper.

Billing: Billing in the energy systems is generally referred to as a process by which a seller charges the purchaser. The electricity bill is usually made up of two key charges: a 'supply charge' which

---

32 https://www.wiley.com/en-gb/Modern+Electricity+Systems%3A+Engineering%2C+Operations%2C+and+Policy+to+address+Human+and+Environmental+Needs-p-9781119793526

33 https://www.ecohz.com/wiki/what-is-an-energy-attribute-certificate-eac

34 https://www.sciencedirect.com/topics/engineering/balancing-market#:~:text=Balancing%20markets%20are%20generally%20single,stability%20of%20the%20electric%20system.

35 https://bitcoin.org/en/

is a fixed cost per day, and a 'usage charge', which is calculated based on the amount of electricity that you use and, sometimes, what time of day you use electricity.

Blockchain: Blockchain is a shared, immutable ledger for recording transactions, tracking assets, and building trust. The first iteration of blockchains like Bitcoin are Gen 1, the second iteration like Ethereum are Gen 2 and the third iteration like Solana and Powerledger blockchains are True Gen 3 blockchains. The supplementary Blockchain Guide is a less technical analysis of the blockchain in energy. Other resources include "Blockchain Technology for the Energy Sector[36]" by Global Blockchain Business Council and in this article titled "Empowering participation in the energy transition[37]", by IBM.

Battery energy storage system: A battery energy storage system (BESS) is a type of energy storage power device that uses a single or multiple groups of batteries to store electrical energy and use the energy as needed.

Carbon credits: Carbon credits[38] are measurable, verifiable emission reductions from certified climate action projects.

Centralised architecture: It is the current architecture of the electrical grid where the control and monitoring are done by a centralised entity like an independent system operator or a system operator.

Contingency: In an electrical grid, contingency is an unexpected failure of a single principal component (e.g., an electrical generator or a power transmission line) that causes a change in the system state large enough to endanger the security of supply.

Curtailment: Curtailment or renewable curtailment is a technical term for reducing output (at times even shutting it down) from a renewable resource from what it could have otherwise produced.

Demand response: Demand response is an action that results in a change in the power consumption of an electric customer. This is initiated by the grid operator to better match the demand for power with the supply.

Decentralised architecture: It is a grid-of-the-future architecture where the control and monitoring are done by everyday prosumers and consumers, and the current centralised actors (like system operators) might facilitate the process.

Distributed energy resources: Distributed energy resources (DERs) are the renewable energy sources that are typically found on the edge of the grid like rooftop solar photovoltaic.

---

[36] https://gbbcouncil.org/initiatives/open-source-ideas-series/

[37] https://www.ibm.com/downloads/cas/KABXYGAR

[38] https://www.southpole.com/carbon-offsets-explained

Duck curve: The duck curve is a graph of power production over the course of a day that shows the timing imbalance between peak demand and solar power generation.

Economic dispatch: Given a network of power generators, economic dispatch is a solution method that finds how much power each generator should generate for a given demand while minimising the total operational costs.

Electricity markets: These are structures where generators sell electricity and retailers buy electricity. Retailers then typically resell electricity to businesses and households. There are various ways to buy and sell electricity in the electricity markets: through the spot market, and through power purchase agreements (PPAs) or forward contracts.

Electric vehicles: An electric vehicle (EV) is a vehicle that has an electric motor that draws power from a battery and can charge from an external source, such as an electricity grid..

Emissionality: Rather than solely tracking an entity's carbon footprint, emissionality looks at the broader environmental impact of energy consumption and production. Emissionality is a global metric, hence requiring a globally verifiable ledger, linking real-time emissions data with energy metering data. It is a quantitative measurement that compares the impact of renewable energy projects on driving down emissions.

Energy efficiency: Efficient energy is the process of reducing the amount of energy required to provide products and services. For example, insulating a building allows it to use less heating and cooling energy to achieve and maintain thermal comfort. Or a blockchain that consumes less energy than what a normal proof of work blockchain would consume.

Ethereum: Ethereum[39] is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralised applications. It is one of the examples of a second iteration in blockchain evolution. Hence, it is referred to as Gen 2 blockchain in this paper.

Feed-in tariff: If you generate using distributed energy resources, a feed-in tariff (FiT) is generally a credit you can receive for any unused electricity sent back to the grid. Sometimes it is also referred to as a buy-back rate. It is usually a set rate per kilowatt hour paid as a credit on your bills.

Full cost of electricity: Full cost of electricity[40] (FCOE) is an interdisciplinary initiative to identify and quantify the full-system cost of electric power generation and delivery – from the power plant to the wall socket – to inform public policy discourse with comprehensive, rigorous, and impartial analysis.

Grid management: The electricity markets operate multiple processes to manage the security and reliability of the grid. The first process comprises pre-market clearing inputs, such as contracts; trade executions; regulations; and logistics. The second process consists of

[39] https://ethereum.org/en/
[40] https://energy.utexas.edu/policy/fce

optimisation (DR is one of the many ways to optimise); unit commitment; economic dispatch; and contingency (all or some of them dependent on the jurisdiction). The third process includes settlement, billing, and reporting. All of this combined is called Grid management.

Grid operator: Grid operator, independent system operator, or system operator is an entity that maintains grid security and reliability in accordance with the applicable national or international standards.

Guarantee of Origin: A Guarantee of Origin (GO) is an energy certificate defined in Article 15 of the European Directive 2009/28/EC. A GO labels electricity from renewable sources and provides information to electricity customers on the source of their energy.

International renewable energy certificate: An international renewable energy certificate[41] (I-REC) represents transferrable proof that one MWh of electricity was produced from renewable energy sources and added to an electrical grid. Purchasing an I-REC allows the buyer to claim the consumption of one MWh of renewable energy.

Levelised cost of electricity: The levelized cost of electricity (LCOE) is a measure of the average net present cost of electricity generation for a generator over its lifetime. Many times, it is used for investment planning and to compare different methods of electricity generation on a consistent basis.

Local energy market: It is a marketplace that matches many local energy users with many local energy assets like rooftop solar photovoltaic, storage, and controllable loads including EVs. The prosumers and consumers connect directly and do the buying and selling of energy.

Peer to Peer: Peer to Peer (P2P) or Peer to Peer energy trading is a business model based on decentralised grid architecture. In this market, consumers and producers “meet” to trade electricity directly, generally without the need for an intermediary.

Powerledger blockchain: The Powerledger Energy Blockchain is a customised, currently permissioned blockchain based on Solana. The design is both faster and less energy intensive than the existing proof-of-work blockchains and is a fit-for-purpose Gen 3 blockchain for energy use cases.

Provenance tracking: Provenance tracking is keeping track of “where each piece of energy data comes from, the chronology of the ownership, and whether it is still up-to-date”. For example, tracking the source of electricity that is consumed.

Renewable energy certificates: Renewable Energy Certificates (RECs), also known as Green tags, Renewable Energy Credits, Renewable Electricity Certificates, or Tradable Renewable Certificates (TRCs), are tradable, non-tangible energy certificates in the United States that represent proof that 1 megawatt-hour (MWh) of electricity was generated from an eligible

[41] https://3degreesinc.com/services/international-renewable-energy-certificates-irecs/

renewable energy resource (renewable electricity) and was fed into the shared system of power lines that transport energy.

Reserves: In electricity networks, the reserve (or operating reserve) is the generating capacity available to the **system operator** within a short interval of time to meet demand in case a generator goes down or there is another disruption to the supply like a system **contingency**. For balancing the rest of supply and demand and catering for **VRE** sources, reserve for providing frequency support, voltage support, and system inertia is getting more and more popular these days.

Rooftop solar photovoltaic: Rooftop solar photovoltaic or rooftop solar or RTPV is a photovoltaic system that has its electricity-generating solar panels mounted on the rooftop of a residential or commercial building or structure.

Self-sufficiency: Self-sufficiency is relying on one's self and not others (like a grid) for necessary energy supply (as much as possible)

Settlement: It is the process that ensures generators are paid for the energy (and other services that they provide), and customers pay for the energy (and other services) they use, in accordance with the market rules.

Smart grid: Smart grid[42] or smart electrical grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end users.

Solana: Solana[43] is an example of the third iteration of blockchain technology.

24x7 Carbon free energy: 24x7 carbon-free energy (CFE)[44] means that every kilowatt-hour of electricity consumption is met with carbon-free electricity sources, every hour of every day, everywhere.

Unit commitment: Unit commitment (UC) is a popular problem in electric power systems that aims at minimising the total cost of power generation in a specific period, by defining an adequate scheduling of the generating units. The UC solution must respect many operational constraints. Loosely speaking, this is a much more advanced form of economic dispatch.

Variable renewable energy: Variable renewable energy or intermittent renewable energy sources are renewable energy sources that are typically considered as not dispatchable due to their fluctuating nature, such as wind power and solar power.

[42] https://www.iea.org/fuels-and-technologies/smart-grids
[43] https://solana.com/
[44] https://www.un.org/en/energy-compacts/page/compact-247-carbon-free-energy

Appendix II: Blockchain Guide

Blockchain Guide

An introduction for anyone interested in blockchain and how it works

Table of Contents

1. Trust as a vital component of society

I. The need for trust

Blockchain technology 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 them? 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 in various transactions in various societies in the past.

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. You can see trust as a property of individuals, institutions or society as a whole but its importance is incontrovertible.

II. The afterlife and punishment: Church and state tools of trust

Societies have always had ways of ensuring levels of trust. There has always been a mix of religious and cultural prohibitions on acts of untrustworthiness, with variations on the promise of heaven and hell as carrot and stick. And beyond the spiritual, there was physical retribution, trial by fire or water, death or exclusion from the community by being placed in the stocks or being transported to penal colonies.

III. Beyond the social tools of trust

Church and state both have provided ways of ensuring violations of trust are kept under control. But in addition to the sociological route, humans have evolved more technological tools to achieve trust, from tally sticks which allowed proof of agreements and trade, to written language which allowed us to commit agreements to stone, parchment or paper. Government title registries allow us to record the ownership of valuable assets such as land and housing and so permit people other than the king to own things.

The value of trust to society is impossible to estimate - but one study estimates that 35% of all jobs in the US are related to creating and maintaining trust. 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’. So in an era where technology has been used to achieve things that were previously exclusively done by humans, it’s perhaps not surprising that blockchain technology is making its presence felt.

There have been ledgers found in Mesopotamia dating back 7000 years where clay tablets recorded important data. The clay tablets were kept in temples by trusted members of the tribe. Sumerian cuneiform tablet, 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.

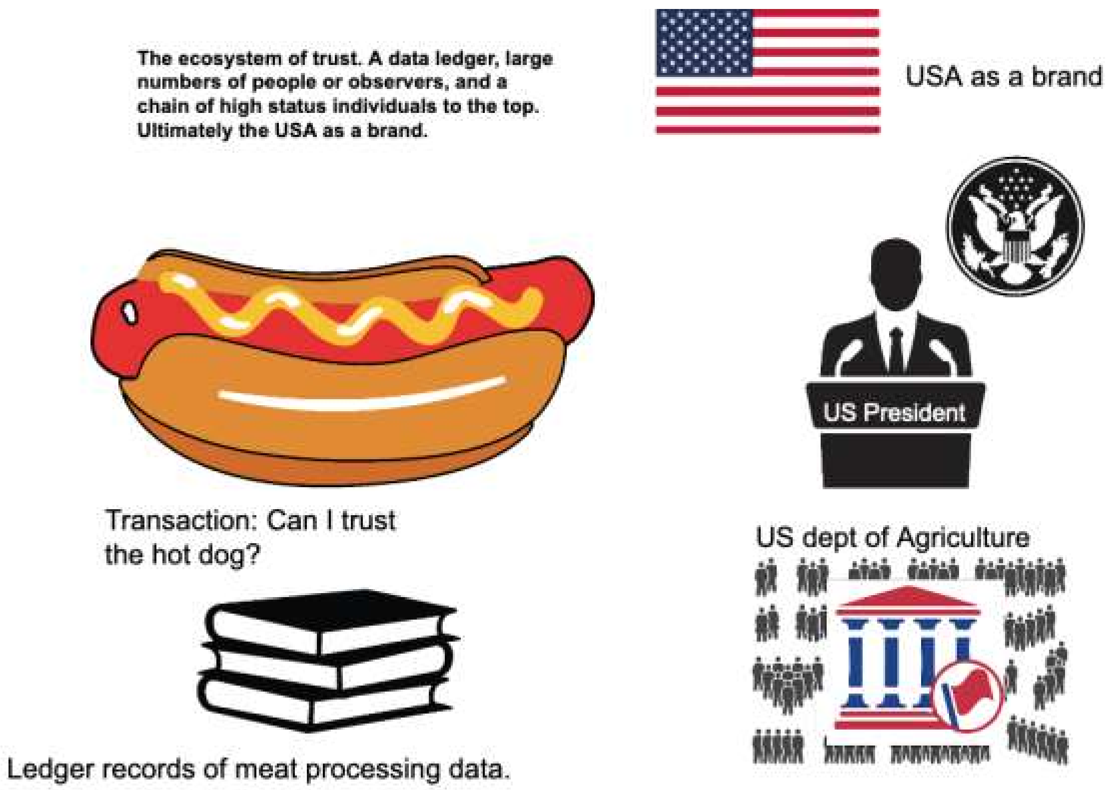
IV. Trust is needed everywhere

For each and every transaction that any person in society executes, there is a certain amount of trust required, and on both sides. When you buy a hot dog at a stall, you trust that the meat in the sausage is fit for human consumption. Equally, the counterparty, the hot dog vendor, trusts that the money you are giving them isn't fake dollar bills. When you pay an insurance premium to your automotive insurance firm, you trust they will pay out if a genuine accident were to occur. It's worth spending a few moments looking at how that trust arises.

V. Trust as a centralised phenomenon

Up until now, it has always been understood that the ultimate upholder of trust was a central authority that regulates the trust agency. The banks regulate the cash you spend on the hot dog ensuring it's not counterfeit. There will be a department that regulates the meat in your hot dog, and other bodies that regulate the insurance companies.

In all these examples, there will be individuals at the top of these companies and institutions whose trustworthiness or probity is essential for us so we can trust the agency they lead and what they are responsible for.



Closely related to the trustworthiness of an item or service is the documentation around it. A classic example of this might be a ledger. In the previous hotdog example, the types of meat and sanitation levels of the equipment used are monitored and dated and entered on a ledger.

Trustworthiness arises because the top of the hierarchy supervises everything beneath it. So you could say that protecting your hot dog transaction is a trio of elements. A set of data in a ledger, a large number of people in an institution and a high-status individual whose probity is beyond question. In the blockchain concept, all of these components look different.

VI. Trust-based to trustless systems

The varied forms of record keeping tools described above could be lost, broken, or tampered with. Eventually, centralised institutions took on the burden of ensuring trust and standardising trust systems. Institutions came to store and validate data records, and in doing so, maintain society's expectations of trust. People chose to trust centralised intermediaries, forming the foundation of a "trust-based" society.

However, institutions are seldom infallible, and every industry has experienced trust problems over time.

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.

VII. Blockchain as a solution to avoiding centralised authority

This brings us to the central concept underpinning blockchain: Instead of using a large number of employees, who are themselves audited by other institutions with large numbers of employees, the system is designed to use large numbers of distributed computers each validating cryptographic proofs provided by the others. This is the promise of what blockchain technology can deliver.

2. The 'trustless' system

For all the areas of centralised authorities with their trustworthy auditors, and ledgers stored under lock and key there will be innovators looking to disrupt them.

Here's an example: If you were to have an accident in a car in the days of old you would begin a process with a trusted authority that deals with your insurance. They would send an independent assessor around, who would take photographs, write a report and begin a process whereby you might receive compensation or maybe a bill for an amount of money from the other side.

All of this, thanks to convergence with blockchain, cryptocurrency, artificial intelligence and smartphones looks like changing.

Now if you have an accident with another car, you take out your mobile phone, make a series of snaps and video sequences of the car's exterior, and also of the car you ran into, and most of the rest of the process is automated.

The phone recognises the car's make and model and starts assessing the damage, the location, the lighting conditions and regulations pertaining at the time and preparing a report. The software then begins chaining in spare parts via the delivery system, estimating costs, and making payments and transfers of cash.

A number of efficiencies are achieved here. The opportunity for fraud is reduced as is the number of days needed to pay for a courtesy car for people who are without transport. The number of employees required to make assessments, checks and audits of the process is drastically reduced and so it's no wonder that systems like this are establishing themselves.

The registry of cars, claims and no claims are all perfect candidates for blockchain and smart contracts, but as you can see the application involves a mix of lots of new technology that goes way beyond blockchain.

Over the coming years, it's widely accepted that we will see a lot of blockchain applications replacing traditional processes where trust is central to the stability of the process.

One area that we will come to is the emergence of blockchain in electrical utilities. Like the accident insurance industry described above it comprises a trio of elements from the new tech cannon. AI, blockchain, and crypto.

I. Smart contracts

The highly automated insurance system described above is one of the scenarios that suggest a use for smart contracts. Smart contracts are lines of self-executing code that can automate many transactions. It works on a 'if this, then that' basis. The promise of automating transactions is part of the reason blockchain is such an exciting proposition.

You can think of smart contracts as something akin to a vending machine. For a limited range of transactions they serve to automate the process completely.

And if the vending machine process can be extended to all our transactions you can see how wide the applications could be. From banks, building societies and insurance companies to payroll and deals of all types.

However, there are two schools of thought on how far the applications can go. Some say the breadth of applications is only limited by the sophistication of computing power. Others suggest that there will always be human creative intelligence required at the edges of where a glorified vending machine cannot go. The reason for this is that there is always a situation that we can't predict in the future and for which the rigid parameters of a vending machine couldn't have anticipated.

The application of blockchain to smart contracts and conducting transactions using cryptocurrency is what is meant by the term web 3.0 technology.

3. Blockchain basics

I. The elements of blockchain

To really understand blockchain as a tool it helps to first appreciate the kinds of tools it is replacing. And the simplest version of the tool blockchain replaces a ledger. A ledger, like a blockchain must be able to fulfil the following:

A. **Accuracy**: The ledger must faithfully record transactions and information, and be error-free.
B. **Consistency**: Similar transactions and events must be recorded in the same way.
C. **Transparency**: Parties to the transactions and events must be able to access and view the ledger.
D. **Security**: The ledger must be secure against unauthorised tampering.
E. **Auditability**: Third parties must be able to observe the ledger and verify that it is accurate, consistent and secure.

It's worth considering in greater depth how classical ledger technology works, starting from when someone writes an entry into a book with pen and paper.

When a pen writes on paper, millions of paper fibres and fibre molecules get coated with ink when an entry is made. To rub that out requires a lot of skill and effort. Indeed, any attempt at rubbing out an entry will almost certainly destroy or blemish the top layer of paper and reveal alteration, which will become obvious to the naked eye and certainly with a microscope.

This will betray the nature of the fraud. If you put the ledger in a safe, you would have to blow the safe open, so you could say the ideal ledger means that any attempt to alter it after the entry creates a catastrophically observable event. Physicists amongst you will recognise the concept of entropy as a theme running through this but it's not essential to understand entropy to understand blockchain.

However, when you delete an electronic record, there is no layer of paper that gets blemished, nor any large number of molecules or fibres that need changing. It's just a few bytes of random access memory that get changed. That means computers aren't naturally good for acting as ledgers. So how do you meet the challenge of creating a digital substitute for the leather-bound ledger guarded in a safe?

4.Stornetta and Haber and the beginning of blockchain

I. Time-stamping a digital document- the one-way function

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" and it was to start a revolution in what was to become known as blockchain technology.

The original problem Stornetta and Haber set out to solve was how do you create a timestamp that's really fraud-proof. A simple example where this might be useful would be the following: A talented screenwriter comes up with a brilliant screenplay idea. Let's say it's something akin to The Maverick concept in Top Gun. Let's assume the screenwriter wants to be able to show they wrote the screen material on or before 1983 and that anyone he sends it to might have been aware of it from then on. In other words, can the writer prove any copycat version 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 a copy of the complete manuscript in an envelope to themselves and leave it closed. That way, anyone could see the script was dated on a certain date. If or when a lawsuit was filed for copyright infringement, the sealed envelope could be opened in front of numerous legal witnesses who were above reproach and could read the script about Maverick, the maverick airforce pilot, determine if it had been copied in subsequent works, and the matter could thus be resolved.

It's not a very digital approach but it does achieve one thing: it leverages a centralised agency (the mail service) and numerous high-status witnesses (intellectual property lawyers) to create a validation of the timing of the material.

In the new Stornetta Haber digital incarnation of this, you would put your entire screenplay, which could be made up of half a million words, into something called a hash function. A hash function takes a series of words and numbers as input and spits out a fixed number of letters and numbers as output. The commonly used SHA-256 hash function returns an output of 64 hexadecimal characters.

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

So let's say you take the Top Gun screenplay and put it through the SHA 256 hash function (or others with similar effects). The result of this is a 64 hexadecimal character string as follows:

c308b46a840689476fd642947b5415197c41add4f2a53c462dc747813352b776

You can now send it to yourself and many others as an email. The others would not be able to decode it or read it.

If anyone doubted that you'd written it, you would show them 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 you could prove you had sent yourself or someone else exactly that hash function two years ago would serve as a timestamp for the original work.

Note also that 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.

II. More witnesses

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

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

Stornetta explains his insight: "I realised 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." Or, put another way, any attempt to change any entry earlier in the document would also now create a catastrophically observable event that many people would notice.

The Haber Stornetta approach to witnessing can best be understood by the way hashing is performed. Instead of hashing just the current entry, this method also hashes every entry before it.

III. An example of storing data where everyone is a witness

Let us imagine Adam, Betty, Charlie, Dan, Eleanor and Freddie representing the community that uses this 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 allows a check of all these entries to be hashed together. This means that changing one entry afterwards would change all of them.

When Adam owes Betty $10 is written into the ledger, it is run through a hash function which comes out as:

7896fe1174a172c47d33270d0216e6eb8bccac04a3ab0a5a60230ded9b1ef5ba

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

7896fe1174a172c47d33270d0216e6eb8bccac04a3ab0a5a60230ded9b1ef5ba Charles owes Dan $17

The new hash of these records is now:

5d9a3d9fbbbef3b5fdb70f78b78b653c31005f8049ce707d99a65bc1d7e97024

Note because a SHA-256 hash only ever returns 64 hexadecimal characters; the result of adding 21 extra characters and hashing this value results in a hash digest that is still only 64 characters long.

When Eleanor and Freddie write their entry in they append theirs to the one above and hash:

5d9a3d9fbbbef3b5fdb70f78b78b653c31005f8049ce707d99a65bc1d7e97024 Elanor owes Freddie $14.

To give yet another new hash:

86f74e2001e0461d06fde364b89f753342eaf81c2593789eedd7661f0f042cf3

And so on. Note that this system brings the entire community in to observe every entry without actually knowing their personal information.

If any one of the communities comprising Adam, Betty, Charlie, Dan, Eleanor or Freddie attempted to change their own entry, this would result in any subsequent hash value also changing, which would be immediately obvious to any observer, as it would alter the blockchain data entries for each and every other participant. In a way, it is analogous to putting a big scratch-out mark or scribbling on a paper ledger in an attempt to rewrite a single entry.

Or, in another analogy, it's also like taking a photocopy of the last page of a leather-bound ledger and sticking it on the current page and doing so for every page, which means all the previous histories are present on every page. In all these scenarios, any attempt to change a single line of a ledger in the past will become apparent to all in the present. This means it's in everybody's interests to pay attention to keeping it free from tampering. This is one of the elements that makes blockchain so secure.

Blockchain also leverages numerous different computers distributed over 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.

IV. Proof of Work blockchains

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.

That unique mathematical problem requires essentially a race between various people who will, in the process of competing to solve the problem, give it a timestamp with lots of 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. Anyone who comes after hasn't competed in the race and will have to solve all the subsequent problems too.

This means that when you make a mistake in a ledger at the start and all the numbers have to be adjusted afterwards. In computing and energy terms, this is eye-watering and prohibitively expensive. It's important to note that not all blockchains use this system, so not all use a large amount of electricity to maintain them.

The Bitcoin blockchain has however adopted this system. 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 specialised hardware to do so.

An attack of this sort is not only practically impossible to achieve but would 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 rules, a game theory concept called a "Nash Equilibrium", and it is a vital component of how the Bitcoin network has remained functional in an adversarial environment.

V. Public and private keys

Users of blockchains also need to have keys to the system. Users will each have both a public key and a private key. The public key is exactly what it sounds like – something that can be known to the whole world. Think of it as being 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 to do so. So your private key should be considered similar to the key to your safety deposit box or your PIN to your bank account. A very important difference, however, is that if your private key is lost, your money is inaccessible forever.

Then we 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.

5. Crypto basics

I. Sending money via the internet

Almost 20 years after Haber and Stornetta's paper, and indeed over 20 years after the early incarnation of the internet, people started to wonder how you could use the internet to send money in a trustworthy, dependable way. After all, you can send film scripts, as we saw earlier, and pictures like selfies and pets doing funny things using the internet, but sending money, if it were possible, would be a much more useful if complex issue. Such a technology, if it could be devised, would be a massive boon.

However, it was very apparent that sending money is different from sending pictures or text. You can't simply photograph your $10 note and send that because the moment you photograph your $10 note, you suddenly have two versions of it which create the possibility of a double spend.

What you need to do is then destroy the $10 note you photographed and just send the picture of it while also stopping others from duplicating your image of a $10 note. All the while making the picture of a $10 note unique and impossible to copy. So making a unique inviolable token while making sure it can't be spent twice becomes the twin problem that technologists of the new money would have to solve.

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

Bitcoin was created in 2009 somewhat mysteriously by a person or group of people using the pseudonym of Satoshi Nakamoto. This, at least, is the name that appeared on the original white paper, which described how blockchain could serve as the backbone of the entire cryptocurrency concept. Because no bank was involved, 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. It also paved the way for smart contracts.

6. Blockchain refined

I. Gen 1, Gen 2 and Gen 3 blockchains

The original blockchain technology, the Bitcoin blockchain, called a **Gen 1** blockchain, developed by Satoshi Nakamoto, suffers from some limitations:

A. **Scalability**: It is not scalable. The original blockchain can only process a limited number of transactions (approximately 5-7 per second) and it is slow to confirm transactions, which can cause issues for many commercial purposes. Additionally, the Bitcoin network is often subject to congestion, which causes increased transaction fees. The Ethereum blockchain has faced scalability issues and the network's capacity has been limited, resulting in congestion during periods of high demand. This congestion leads to increased transaction fees and a slower confirmation time, much like Bitcoin.

B. **Energy intensive**: The original blockchain relies on a mechanism known as 'proof of work' as its consensus (See Appendix 1 that mentions additional consensus mechanisms) mechanism. This technique is very energy intensive.

C. **Not Turing complete**: The original blockchain is not 'Turing complete' i.e. not able to process any complicated functions, the sort that are required to create smart contracts. Since smart contracts allow the automation of all sorts of transactions, Turing complete has become a prerequisite for any higher generation blockchain.

Blockchain technology has evolved over time, with different generations or iterations offering distinct features and capabilities. Let's explore Generation 2 (Gen 2) and Generation 3 (Gen 3) blockchains:

Gen 2 blockchains, also known as second-generation blockchains, introduced advancements compared to the original Bitcoin blockchain. These improvements primarily revolved around the ability to create and execute smart contracts. Smart contracts are self-executing contracts with predefined conditions written into the code. Gen 2 blockchains, such as Ethereum, enabled the development of decentralised applications (DApps) and opened up possibilities for various use cases beyond simple financial transactions. They offered programmable functionality, expanding the scope of blockchain technology. Ethereum also uses a fee mechanism called "gas" to prioritise transactions and prevent network abuse. Gas fees can be volatile and high, especially during peak usage. In summary, Gen 2 blockchains introduced smart contract capabilities (smart contracts can be written using various blockchain programming languages - see

Appendix 2 for more details), enabling the development of decentralised applications.

Gen 3 blockchains build upon the advancements of Gen 2 by addressing scalability, interoperability, and sustainability challenges. These blockchains aim to overcome limitations such as slow transaction speeds, high energy consumption, and limited integration with other blockchain networks. Gen 3 blockchains often utilise innovative consensus mechanisms, like proof-of-stake (PoS) or delegated proof-of-stake (DPoS), or proof-of-history (PoH) to improve scalability and energy efficiency. They focus on creating a robust infrastructure that can support large-scale adoption and seamless interoperability between different blockchain networks. Examples of Gen 3 blockchains include Cardano and Polkadot.

Benchmark/ Coins	Solana	Cardano	Avalanche	Polkadot	Algorand
Transaction Throughput	50,000 - 65,000 tps	250 tps	4,500 tps	1,000 tps	1,100 tps
Transaction Fee	$0.00025	0.4 ADA ~ $0.77	0.001 AVAX ~ $0.63	0.0157 DOT ~ $0.64	$0.002
Consensus Mechanism	Proof of Stake	Ouroboros Proof of Stake	Proof of Stake	Nominated Proof of Stake	Pure Proof of Stake

Significant advancements have been made in the Gen 3 space, particularly in processing multiple blocks concurrently. This innovation has led to substantial improvements in throughput and lower transaction fees compared to earlier iterations. Solana, specifically referred to as a "True Gen 3" blockchain, exemplifies these advancements. It harnesses the power of parallel block processing, enabling higher transaction speeds and more efficient fee structures. Another notable example of a True Gen3 blockchain is Powerledger Blockchain which is an adaptation and enhancement of Solana for energy use cases.

In the following subsection, we will further explain the consensus mechanisms of Gen 1, 2 and 3 blockchains and their applications in the energy industry.

II. Dispelling the energy myth: Unveiling energy-efficient blockchains

In recent years there have been more advanced blockchains that have evolved, which use significantly less electricity. True Gen 3 blockchains are far less energy intensive than the existing proof-of-work blockchains.

Proof of stake reduces this energy requirement (see image on the right that compares energy usage of each Solana transaction with others[45]), because instead of energy intensive mining required to secure the blockchain, it requires all participants to put up blockchain tokens as stakes and allow them to have a share in its maintenance, validation rights, and reward distribution.

[45]Source:https://solanaclimate.com/?ref=solana.ghost.io

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 PoS chain, we do not have 'miners' but rather 'validators'. Validators are required to hold and 'stake' tokens, and if they are discovered to have made an error in the validation of blocks, the validators do not receive any rewards for their efforts, and some blockchains go further and penalised the misheaving validators 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 the proof of stake chain, validators are randomly selected to add the next block and earn transaction fees.

Number of Solana Transaction(s)	Equivalent to
1.25	One Google search
41.67	One hour of using an LED lightbulb
51.71	Fully charging iPhone 13 battery
166.67	One Ethereum transaction (post-merge)
658.33	One hour of working on a computer/monitor
5,096.56	Average US household (per hour)
14,583.33	Central air conditioning (per hour)
140,416.67	One gallon of gasoline
5,791,666.67	One Bitcoin transaction

7. Blockchain use cases in the energy sector

I. Peer-2-Peer (P2P) trading of distributed energy (DE)

When wind and solar started emerging as energy sources capable of producing power for the grid, one of the things that became apparent was that these energy sources would be in all sorts of locations that weren't generally co-located with the major power stations. A wind farm or a solar farm would typically be built where there was no major connector to the grid and therefore, its energy output was essentially stranded.

While states could invest in increasing the transmission capacity and footprint of the electrical grid at that point, doing so could make the project uneconomic. Moreover, the geographical problem was only half of the issue; The intermittent nature of their power required significant amounts of battery storage or BESS and that would be uneconomical too. These twin problems of place and time reflect the very different nature of distributing energy generated by renewable sources and why it demands a different approach.

Into this background came a new notion; That owners of even relatively small-scale power sources could trade power with each other. They could agree on a price between them and transact a certain amount of power at a time and place of their mutual choosing. And, as the market could drive efficiencies, more and more batteries would get included in the system enabling peak demand and curtailment periods to become better managed. This is commonly referred to as Peer to Peer (P2P) power trading.

What was interesting about the P2P concept was that it seemed to be a natural fit with decentralised energy.

While fossil fuels, nuclear and hydro with their very stable power output fit with the classical centralised grid and fixed pricing, renewable energy resources (RE) like solar and wind are almost the opposite. These energy sources produce highly variable power output that is delivered in difficult-to-predict spurts and far flung locations which can play havoc with a centralised system, which needs to maintain a balance between generation and consumption.

But if the paradigm shifts to distributed rather than central distribution, the contributions of renewables can work much better. Localised and agile pricing works well with a distributed approach and the flexibility of pricing helps balance a system where there is the variability of supply and congestion in the network to move energy around.

In this context, blockchain becomes a candidate for acting a ledger to keep track of all energy transfers and relevant financial transactions.

II. The role of blockchain in distributed energy systems

In the new paradigm where lots of players are trading with each other, there are going to be a lot of transactions to keep track of. In this new world of P2P, a central authority like an electrical retailer no longer has control over its customer base, as they are all, as the term suggests peers or equals rather than customers or subordinates. So if an electrical retailer isn't suited to the task, how do you keep count of the transactions? What is the best approach to billing and record keeping in a distributed environment, where transactions are frequent, low margin flat hierarchy and need security?

The answer to this is of course blockchain and is one of the reasons it has become centre stage in the thinking about peer-to-peer energy trading.

Blockchain as described earlier is an immutable, trustless way of managing a database. It also integrates well with smart contracts which suit P2P trading.

Smart contracts use customised deployed code which define the terms, rules, and conditions of bilateral trading agreements. Once P2P trading contracts are written on the blockchain platform, they cannot generally be altered or removed, which facilitates trust in the public using them so that they can be sure the contracts will always be executed as expected. This feature of blockchain is also conducive to storing financial transactions — which are settled among P2P traders keeping the margins of energy retailers and network operators unaffected. Confidentiality and privacy are always guaranteed through symmetric and asymmetric encryption and anonymous signature. At the end of each billing cycle, blockchain-stored P2P transaction data are sent to energy retailers and network operators to finalise the transactions. It may be however that in the future, there will be no such thing as an energy retailer as we know it now and the process will be handled entirely by smart contracts.

Here is an example of a possible transaction: Assume Customer A produces 150 kWh in September and sells 50 kWh to the energy retailer (after P2P trading settlements of 100 kWh) in exchange for crypto-tokens (or Fiat equivalent). Customer A sees on their account that they received x Crypto (or Fiat) for their 50 kWh. They can use the money to spend on charging their vehicle, for example, anywhere in the charging-covered network locations of the energy retailer. The energy retailer can then charge transaction fees and benefit from this process. While both blockchain and crypto can provide significant benefits to P2P trading, their adoption depends on the energy retailer and how forward-thinking and tech-savvy they are.

8. Some future thoughts

One of the interesting questions that open up as we think about decentralised finance is the responsibility of every individual to look after their own housekeeping.

If you lose your credit card and you have a centralised bank, you can go into the bank and ask them to reissue it. If there's some unauthorised activity on your balance, you can discuss it with someone in the bank who has access privileges that you do not. But with decentralised finance or cryptocurrency, it is only down to you. If you can't find your non-fungible token of some great piece of art, you'll just have to resolve that issue yourself, maybe with the help of some kind of specialist you trust. Or lose access to the item represented completely.

So increasingly, it's likely it will be down to the consumer and an app on their phone which means the phone has to become good at de-fi and even more secure, and this creates an interesting predicament for the phone companies.

The architecture of phones was never designed for blockchain and de-fi, so while it's tempting to create fixes and workarounds for this, it's now likely that blockchain companies will try and create their own phone. This means that they will start from scratch on the areas that matter - security and the architecture that prevents hacking into the inner workings of the phone.

Creating a phone based on the needs of the corporation was what Google did very successfully with its Android operating system used by a majority of phones, including Samsung, and this means that much of the complex bespoke software that was previously used by mobile phones could be dispensed with. According to John Bulich of Powerledger, the future could already be here with Solana's newly released Android based Web 3-enabled SAGA mobile device.

It's only relatively recently that phones have become part of our payment rituals, as credit cards and cash are gradually being jettisoned. The notion of building all these physical tools into the phone as virtual cards and certificates are fundamental to the concept of a virtual wallet. 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 and the virtual wallet is now an everyday concept for many people, especially those the under the age of forty.

Many believe this virtualisation trend is set to continue as we become owners of our own data. Medical records, non-fungible tokens, our electrical energy and water data, all these facets of human life, may become decentralised in the coming years.

Such a trend will demand phones with the highest level of security and reliability and in this context, a race to create phones which facilitate Web 3.0 will be an inevitability.

Annexures

Annexure I: Consensus mechanisms in blockchains

Proof of Work (PoW)	PoW is a common form of cryptographic proof developed in 1993 which was revived to be used as a part of the Nakamoto Consensus protocol and demonstrated successfully by Satoshi Nakamoto in 2008 for the Bitcoin network. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. PoW requires high energy consumption and long processing time; but is the most secure method against byzantine failures.
Proof of Stake (PoS)	PoS is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves allocating responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held. This mechanism randomly chooses a maximum coin owner to validate a transaction. It also allows the owner to create a block for the same coin. This mechanism requires comparatively less energy and transaction time. Coins like Ethereum 2.0, Polkadot, Cosmos, Cardano, ThorChain, Nxt and Algorand use PoS. If one person (node) owns 67% or more of a particular coin, then that person can censor transactions on the network, causing an operational risk.
Proof of Authority (PoA)	In this unique mechanism, there are validators with approved accounts which authorise transactions and the creation of new blocks. These validators must disclose their true identity to get the right to validate a transaction. PoA is used for permissioned public and private blockchains. The main requirement for this method is that all participants should be known and highly trusted.
Proof of Activity (PoA)	This mechanism is a combination of both PoW and PoS designed to combine the best features of both. In the beginning, the Proof-of-Activity mechanism functions like PoW. Once a new block is completed, it starts to function like a Proof-of-Stake mechanism. Coins such as DCR (Decred) use this mechanism.
Proof of Elapsed Time (PoET)	Intel Corporation created this mechanism to permit blockchain to decide the person who will create the next block. It uses a lottery system to decide the next block creator. Thus, it gives a fair chance to all traders to create the next block. It is an efficient process involving lesser resources and low energy consumption.
Proof of History (PoH)	PoH was developed by the Solana Project - it is similar to Proof of Elapsed Time (PoET), which encodes the passage of time itself cryptographically to achieve consensus without expending many resources. This is one of the best in class and is discussed in this report when True Gen 3 blockchains are discussed.

Proof of Capacity (PoC)	The PoC mechanism heavily relies on free space available in the hard drive. This is because there are many solutions to a coin's hash problem that a trader needs to store. It is highly efficient as compared to PoW and PoC mechanisms. Coins such as Burst, Storj, SpaceMint and Chia use these mechanisms. Example – Burstcoin and SpaceMint
Proof of Burn (PoB)	PoB aims to improve the quality of blockchain so that it can be used easily and extensively as a tool for faster and more secured transactions. After PoW and PoS, PoB is designed to prevent fraud activities on a blockchain network. Cryptocurrencies such as Bitcoin use this mechanism to offer secure transactions to traders. Example – Slim Coin

Consensus mechanisms are methods used to achieve agreement, trust and security across a decentralised computer network. Consensus mechanisms play an essential part of securing information by providing cryptographic proof that a majority (or supermajority in PoS) agree on the validity of that transaction. All consensus algorithms attempt to be Byzantine Fault Tolerance (BFT) - an approach that solves the Byzantine Generals' problem, where messages and network members cannot be inherently trusted. This means the system should stay intact even if a certain threshold of nodes fail, or try to attack the network.

- Since there is no central authority in a blockchain network to validate the transactions, consensus algorithm is used to arrive at consensus to verify every block of transactions are valid.
- The consensus protocols ensure that every new block added to the blockchain is the one and only version of the truth that is agreed upon by all the nodes in the blockchain.
- Consensus algorithms assume that some processes and nodes will be unavailable at times; algorithms also assume some communications will be lost in transmission – however a response is required from available nodes; algorithms may require at least 51% of nodes to respond to achieve consensus, while other consensus algorithms, such a proof of stake, require over 66% of the nodes to respond to achieve consensus.
- Each block is processed through a hash function to generate a block hash

Annexure 2: Blockchain programming languages[46]

Sl. No	Language	Pros	Cons
1.	**Solidity** Solidity is the most widely used programming language for developing smart contracts on the Ethereum blockchain. It is a statically-typed language specifically designed for writing smart contracts and is similar to JavaScript. Solidity is a statically typed programming language with curly-brace syntax specifically created for developing smart contracts that run on the Ethereum Virtual Machine (EVM). Proposed by Gavin Wood in 2014, Solidity draws influence from programming languages such as Java, C++, and PowerShell. Solidity serves as the primary language for coding smart contracts on the Ethereum platform, enabling developers to create decentralised applications with blockchain functionality.	● Solidity is a statically typed Blockchain Programming Language that provides a more reliable and flexible development paradigm for smart contracts ● Solidity's user-friendliness makes it adaptable ● Solidity provides a secure, dependable, and accurate medium for multiple sources in framing smart contracts between two parties ● The Application Binary Interface (ABI) provides multiple type-safe functions in Solidity	● Once a contract is made in Solidity, it cannot be changed if necessary. The contract cannot be amended to include more features ● Solidity's lack of built-in error handling mechanisms can make it challenging to handle exceptional cases and recover from errors gracefully. ● Solidity's gas optimization can be a complex and time-consuming task for developers. Balancing the need for efficiency with functionality requires careful consideration and can result in code that is difficult to read, understand, and maintain.
2.	**JavaScript** JavaScript is a versatile programming language commonly used for web development. It is also used for developing decentralised applications (dApps) that interface with the	● JavaScript is one of the most popular programming languages, widely adopted and supported by a large developer community. This means	● JavaScript is a highly flexible language that allows for dynamic typing and runtime evaluation,

[46] Sana Afreen, Senior Research Analyst, Simplilearn, 2023 (https://www.simplilearn.com/blockchain-programming-languages-article

	blockchain platforms like Ethereum using libraries like web3.js There are also some blockchains that allow creating smart contracts in JavaScript, although these are not very common.	that there is an abundance of resources, libraries, and frameworks available. ● JavaScript is a versatile language that can be used for both front-end and back-end development. This makes it suitable for building decentralised applications (dApps) where smart contracts are an integral part. ● JavaScript is the native language of the web, and it runs directly in web browsers. This makes it an ideal choice for developing blockchain interfaces or decentralised applications that interact with the blockchain. It enables seamless integration with web-based wallets, browser extensions, and other web technologies.	which can introduce security risks. Smart contracts, in particular, require high levels of security when creating or interfacing with them and requires careful coding practices to mitigate security risks.
3.	**Python** Python, renowned for its versatility, boasts an extensive ecosystem comprising numerous libraries and frameworks. Within the realm of blockchain development, Python plays a significant role in various tasks, including the creation of blockchain applications, interaction with blockchain networks, and data analysis. Leveraging its rich set of tools and resources, Python enables developers to efficiently build robust and scalable solutions for the blockchain ecosystem. By harnessing Python's capabilities, developers can seamlessly integrate blockchain functionality into their applications and leverage its vast library support for streamlined data analysis and manipulation within blockchain environments. Only a small number of blockchains support smart contracts written in python at the moment, these include Solana, NEO, Ontology and Lisk,	● Python evaluates each line one by one, which makes it easier to find and debug mistakes ● Because this language is so simple, users can spend more time comprehending the code instead of framing syntax ● Python's has a extensive native library hence there is less need to rely on external libraries that may have security vulnerabilities ● Its English-like syntax makes it simple to write and comprehend at a glance.	● Because Python is a dynamically typed language, the data type of variables might change at any time, resulting in errors in the output. This needs to be carefully considered to ensure no security risks are introduced. ● Because it requires a large amount of memory, it takes longer to execute, which is not ideal for high performance blockchains.

	either natively or through a translation layer.		
4.	**C++** C++ is appreciated by blockchain programming developers for its richness in run-time polymorphism, function overloading, and multi-threading. The data can be shaped to the developers' specifications using C++. It finds widespread utilisation in the creation of blockchains such as Stellar, Ripple, and Bitcoin. It is also available for use as a smart contract language on blockchains such as EOS, Ontology and Moralis.	• C++ is a structured programming language that offers the convenience of an object-oriented programming language, making it more user-friendly than binary coding languages. • The use of global data and functions in C++ ensures data hiding, enhancing security, which sets it apart from many high-level programming languages. • C++ is developer-friendly, known for its ease of use and intuitive nature. • In terms of speed and power, C++ is comparatively rapid and powerful. Being a multi-paradigm language, it allows for efficient execution.	• Dynamic Memory Allocation is not supported in C++, which means it lacks garbage pickup functionality. • The complexity of C++ code increases as the length of the code increases. • C++ is a platform-specific language commonly used for developing applications specific to particular platforms.
5.	**Rust** Rust provides developers with several advantages. First and foremost, its emphasis on memory safety eliminates common issues such as null pointer dereferences and buffer overflows, which are critical for secure blockchain applications. Rust achieves this through its ownership system and strict borrowing rules, ensuring memory safety without sacrificing performance Rust also offers a rich ecosystem of libraries and frameworks that facilitate blockchain development. The language itself provides robust support for building network applications, which is essential for blockchain protocols and decentralised networks. Additionally, Rust's package manager, Cargo, simplifies dependency management and allows developers to easily integrate existing blockchain libraries into their projects. Rust is used as a smart contract language, and a blockchain development language due to its speed and safety.	• Rust's ownership system and strict borrowing rules eliminate common memory-related vulnerabilities, making it suitable for building secure blockchain applications. • Rust's focus on low-level control and zero-cost abstractions allows developers to write efficient and high-performance code for blockchain applications. • Rust's lightweight concurrency model enables developers to write concurrent and parallel code, making it suitable for scalable and responsive blockchain networks. • Rust has a growing ecosystem of libraries and frameworks specifically tailored for blockchain development,	• Rust has a unique syntax and ownership model that may require developers to invest time in learning and understanding its concepts. • Rust's emphasis on safety and correctness may require more code and effort compared to other languages, potentially impacting development speed. • While Rust's ecosystem is growing, it may not have as many resources, tools, and community

		providing developers with useful tools and resources.	support as more established programming languages.
6.	**Vyper** Vyper is a blockchain programming language built on Python 3. So, even if Vyper does not have all of Python's features, the Vyper syntax is also legitimate Python 3 syntax. It, like Solidity, is commonly used for the Ethereum Virtual Machine (EVM) which is used on many blockchains. Vyper, on the other hand, has distinct control structures than Solidity and tackles security issues differently. Vyper has also removed several of Solidity's OOPS capabilities, as well as other features such as infinite loops, modifiers, recursive calling, and so on. This aids in avoiding the security risks that these features cause.	● Vyper has a strong focus on security and includes built-in features and restrictions that promote secure coding practices. It helps developers avoid common vulnerabilities and reduces the risk of introducing security flaws in smart contracts. ● Vyper's syntax is designed to be similar to Python, making it more accessible and easier to understand for developers who are already familiar with Python programming. The language follows a minimalist design philosophy, emphasising code readability and reducing complexity. ● Vyper's simplicity and restrictions make the code more auditable and verifiable. With fewer language features and limitations on advanced constructs, the code becomes easier to review and analyse for potential issues or vulnerabilities. ● By disallowing certain advanced features and enforcing restrictions, Vyper aims to create more predictable behaviour in smart contracts. This can help developers write reliable and deterministic code.	● Vyper intentionally restricts certain advanced features and low-level operations to prioritise security and simplicity. While this makes the language more secure and auditable, it may limit its flexibility for complex use cases that require more advanced language features. ● It may require a learning curve for developers transitioning from other blockchain programming languages like Solidity. ● As Vyper is a relatively new language, the tooling, documentation, community and ecosystem might not be as extensive or mature compared to other languages. This could pose challenges for developers in terms of finding relevant resources
7.	**Rholang** Rholang is widely recognized as an excellent programming	● Rholang stands out for its reliability and high level of security, providing a	● Being a relatively new entrant in the market,

	language for smart contract development. Its functional approach, as opposed to the object-oriented approach, proves highly advantageous in resolving various blockchain challenges, contributing to its widespread acclaim. In Rholang, applications assess the entire program as a sequence of functions and tackle them in order. This starkly contrasts with languages such as C or Python, which utilise variables to store data and modify their values over time. Rholang is not commonly used for smart contract development outside of the RChain blockchain ecosystem at this time.	dependable environment for blockchain programming. ● It boasts user-friendliness as the flexibility of the Rholang language makes it straightforward and intuitive to work with. ● Rholang is designed to prioritise speed, ensuring efficient and fast execution of blockchain applications.	Rholang is still gaining recognition and familiarity among users. While experienced tech professionals may find it manageable to utilise the language for undeveloped blockchain programming, beginners might encounter challenges due to its relatively limited user base and resources.
8.	**Simplicity** Blockchain programs were developed with a trade-off between expressiveness and reliability. Expressive programs tended to be lengthy and had less reliable smart contracts, while reliable programs were often basic in functionality. However, the introduction of Simplicity, developed by Rachelle O'Connor, aimed to address this issue by reducing the need for low-level understanding of cryptocurrencies. Simplicity was specifically designed to integrate seamlessly with Blockstream's Elements platform. It presents an opportunity to expand the capabilities for users of the Liquid Network, offering trust-reduced escrow, vault, and other advanced smart contracts.	● Simplicity, as a smart contract language, offers a high level of security due to its simplicity-first design philosophy, minimising the potential for bugs, vulnerabilities, and unintended consequences, making it suitable for critical and high-value applications. ● Simplicity's formal verification capabilities enable developers to mathematically prove the correctness and security properties of their smart contracts, enhancing trust and reliability in the execution of critical operations on blockchain networks. ● Simplicity's strong type system and static analysis tools enable developers to catch errors and bugs at compile-time, reducing the likelihood of	● There is still room for further development of code optimizers and other associated tooling and libraries. ● The task of combining functional and formal correctness of cryptographic protocols remains to fully verify smart contracts.

		runtime errors and enhancing code quality and robustness.	
9.	**Go** Hyperledger Fabric smart contracts are called chaincode, and this is primarily written in Go programming language. Hyperledger Fabric is a blockchain framework for developing enterprise-grade applications and is often used in consortium blockchains.	● Go is a statically-typed, compiled language known for its efficiency and performance. It offers low memory footprint and fast execution, which is crucial for enterprise-level blockchain applications handling large volumes of transactions. ● Go has a robust ecosystem with extensive libraries and frameworks that can facilitate smart contract development on Hyperledger Fabric. The Hyperledger Fabric project itself provides a Software Development Kit (SDK) in Go, offering a comprehensive set of tools and utilities to simplify the development, testing, and deployment of Go-based smart contracts. ● Hyperledger Fabric is primarily designed to support Go-based chaincode (smart contracts). As a result, using Go for smart contract development on Hyperledger Fabric ensures native compatibility and seamless integration with the platform's architecture.	● While Go is considered a relatively simple language to learn, developers who are unfamiliar with Go may require some time to become proficient. Transitioning from other languages to Go may involve a learning curve, especially if developers are more accustomed to dynamic languages. ● Go is intentionally designed to be minimalistic, focusing on simplicity and readability. This approach enhances code maintainability, but it also means that Go lacks some advanced language features found in other languages. This can be seen as a limitation when developing complex or sophisticated smart contracts. ● Go does not have as extensive or diverse community, toolset or support around it compared to more widely

			used languages like JavaScript or Solidity.
10.	**Michelson** Michelson is a stack-based programming language designed specifically for the Tezos blockchain. It is known for its emphasis on safety, security, and formal verification. Michelson allows developers to write smart contracts that are highly secure, efficient in terms of gas usage, and compatible with the Tezos blockchain's unique architecture.	● Michelson is designed with a strong emphasis on formal verification, which is a rigorous method of mathematically proving the correctness of smart contracts.By using Michelson, developers can leverage formal verification tools to detect and eliminate potential vulnerabilities or bugs in their smart contracts, enhancing the security and reliability of their smart contracts. ● Michelson's architecture is built around the principle of safety and security. It is a stack-based language that enforces strong type-checking and explicit stack manipulation. These features help prevent common programming errors, such as type mismatches and stack overflows, leading to more reliable and secure smart contracts. ● Michelson is optimised for gas efficiency, aiming to minimise the computational resources required for executing smart contracts on the Tezos blockchain. The language enables developers to write compact and optimised code, resulting in lower gas fees for executing transactions and smart contracts. This efficiency is particularly important for decentralised applications (dApps)	● Michelson has a unique syntax and paradigm that may present a learning curve for developers accustomed to more mainstream programming languages. ● Compared to more mature smart contract languages like Solidity or JavaScript, Michelson has a smaller ecosystem and a more limited set of development tools and libraries. This can pose challenges when seeking community-driven resources, code snippets, or reusable components for Michelson-based smart contract development. ● Due to its niche nature and relatively smaller developer community, finding experienced Michelson developers may be more challenging compared to more widely adopted smart contract languages.

		running on Tezos, resulting in a better user experience and lower user cost.	
11.	**DAML** DAML (Digital Asset Modeling Language) is a high-level, domain-specific language designed for writing smart contracts and modelling business processes on various blockchain platforms. It prioritises simplicity and safety by abstracting away low-level blockchain details and focusing on expressing contract logic and workflows. With its interoperability features and emphasis on correctness, DAML offers developers a streamlined approach to building secure and scalable blockchain applications, ultimately reducing development complexity and accelerating time to market. DAML is available for use as a smart contract on blockchains such as Hyperledger Fabric, Corda, Amazon Aurora and VMware blockchain.	● DAML is designed to simplify smart contract development by focusing on modelling the workflow and logic of contracts. It offers a higher-level abstraction that allows developers to express complex business processes and agreements more easily. This simplification can lead to faster development cycles, reduced code complexity, and improved productivity. ● DAML is built with interoperability in mind. It allows for seamless integration and interaction with multiple blockchain platforms, making it easier to migrate or extend applications across different blockchains. This allows developers to write smart contracts that can be deployed on various blockchain networks. ● DAML incorporates strong static typing and strict contract validation, minimising common programming errors and ensuring the correctness of smart contracts. It provides built-in safeguards against common vulnerabilities like data inconsistencies, unauthorised actions, and invalid states. These safety features enhance the security and reliability of smart contracts.	● Compared to more established smart contract languages like Solidity or JavaScript, DAML has a smaller ecosystem and a more limited range of libraries, frameworks, and community support. This may result in a narrower set of available resources, tooling, and development community expertise. ● While DAML aims to simplify smart contract development, it has its own syntax and concepts. The initial learning curve may be steep for developers who are not familiar with functional programming or the specific features of DAML. ● Platform Compatibility: Although DAML supports interoperability, not all blockchain platforms have native support for DAML-based smart contracts. Integration with specific blockchains may require additional layers or

			adapters, depending on the platform's capabilities.

List of Figures

List of Images

Key Authors and Contributors

Anand Menon
Director Digital Grid
Power Ledger

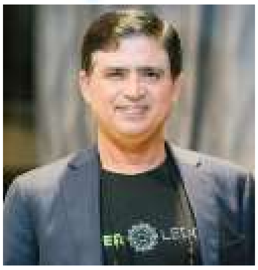
Dr. Jemma Green
Co-Founder & Executive Chairman
Power Ledger

Parul Shribatham
Assistant Manager
(Technical Services)
India Smart Grid Forum

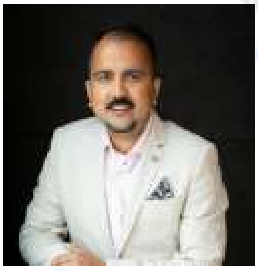
Reena Suri
Executive Director
India Smart Grid Forum

Reji Kumar Pillai
President- India Smart Grid Forum
Chairman- Global Smart Energy Federation

Shashi Bala
Business Analyst
India Smart Grid Forum (ISGF)



Vinod Tiwari
Global Head of Business Development & Partnerships- Power Ledger



Dr Vivek Bhandari
Chief Technology Officer

Copyrights and Disclaimers