Turning on the lights in Africa

Irene Energy embraces confidential computing to safely deliver electricity

IBM Cloud

6-minute read

Irene Energy was aiming high. The tech startup had a breakthrough idea for bringing affordable electricity to remote parts of Africa. Blockchain technologies built on confidential computing were key to that vision, providing robust data security in the cloud.

Access to electricity is so critical to modern society that it might almost be considered a human right, yet nearly one billion people (external link) in sub-Saharan Africa still have no access to any electricity supply. This isn't just because remote areas lack infrastructure; in Tanzania, for example, around 50% of the population lives in close proximity to the grid, but only 16% of homes are connected to it.

The problem is that installing a connection requires significant up-front investment, which puts it beyond the reach of many families. As a result, every time they need to charge their cell phones, they must pay someone who is connected, and the prices are often outrageously high. It's estimated that many people in sub-Saharan Africa spend up to 10% of their income on electricity, which is more than 10 times higher than the average proportion in Europe and North America.

France-based Irene Energy realized that many of these issues could be solved by creating an easier, cheaper and more flexible back-office infrastructure for energy service providers. For example, if payment management and processing costs are low enough, it becomes viable for people to pay small amounts of their weekly income into a community fund until they've saved up enough for a new grid connection to be installed. It also enables electricity roaming; for example, a user could charge their phone at a friend's house but pay for the electricity themselves, ensuring that costs are shared fairly.

"We saw a huge opportunity to change energy markets for the better with a secure, scalable, powerful and affordable back-office infrastructure for energy service providers," explains Guillaume Marchand, founder of Irene Energy. "We just needed to find the right third parties to help us solve the formidable technical challenge."

Irene Energy enlisted 40,000 - 50,000 customers in its

2

years of existence

The company now provides its platform to energy service providers in

5

African countries

Security-rich, affordable transactions at scale

Irene Energy knew that blockchain technologies were the key to building the solution it needed. As members of France's vibrant and close-knit financial technology community, the company's founders were already aware of Talium, a company with a reputation for delivering successful projects built on blockchain technologies. The Irene Energy team reached out to Talium for support with the design and delivery of the new platform.

"Talium helped us evaluate all the blockchain technologies, and Stellar was the best option because of the very low cost per transaction and its

support for simple smart contracts," says Marchand. "However, since we aim to scale up to hundreds of thousands of users, and each user needs a Stellar ID for their digital wallet on our platform, we also needed a very scalable way to manage user credentials that would be highly secure."

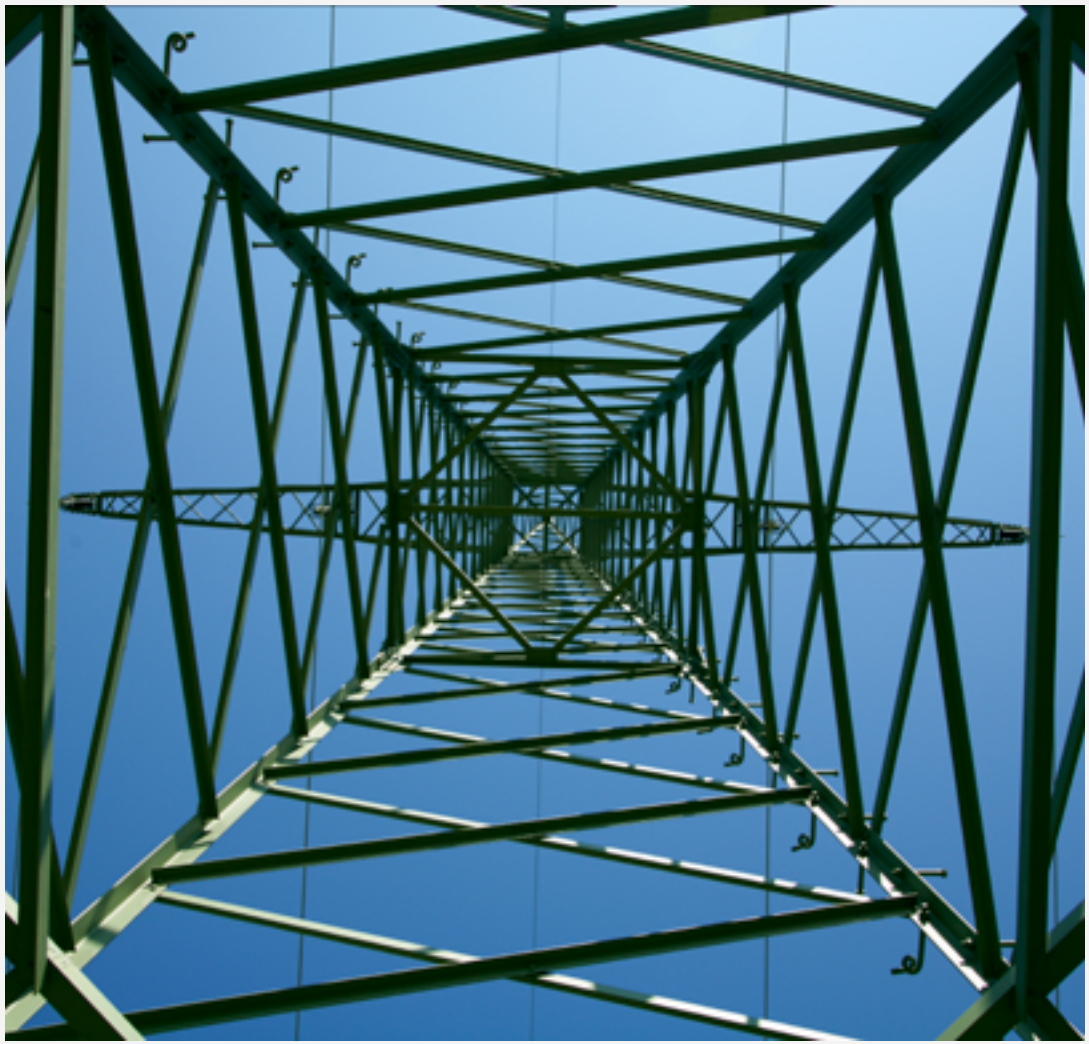
Stellar authenticates users through public key cryptography, so Irene Energy's platform must be able to look up users' private keys whenever they submit a transaction. At the same time, it must ensure that no one—not even its own employees or the customers themselves—can intercept or read the private keys before, during or after the transaction.

"It's relatively easy to encrypt data when it's at rest and even when it's in transit," says Julien Brodier, chief technology officer of Talium. "The

> "IBM Cloud Data Shield has probably accelerated the development of our platform by six months. We can get to market much sooner because we don't have to build SGX-compatible components from scratch."
>
> **Guillaume Marchand**, Founder, Irene Energy

problem we had to solve was how to protect it during the runtime of the transaction itself, when the private key is stored in memory. At that moment, there's a risk that someone who has root access to the server could read the decrypted key." The ability to secure data in use was essential to delivering the confidential computing capabilities the solution required, with complete protection across the data lifecycle.

The traditional approach to solving this type of problem is to invest in specialist hardware with built-in hardware encryption—but these servers are expensive, and Irene Energy knew that its customers would not be able to afford the investment. The company needed a cloud platform that could offer the same level of protection, without the up-front cost.



The team found a solution in IBM Cloud®. Unlike many cloud architectures, IBM Cloud Bare Metal Servers can use an Intel technology called Software Guard Extensions (SGX) (external link). SGX enables confidential computing by creating an encrypted "enclave" within the server's memory that allows applications to process data without other users of the system being able to read it.

"Without SGX, our platform wouldn't have been viable," says Marchand. "SGX gives us access to runtime memory encryption technology on affordable IBM Cloud servers instead of expensive custom hardware."

However, building applications that can take advantage of SGX is complex and time-consuming. To get the platform to market quickly, Irene Energy's developers needed to find a shortcut.

> "IBM Cloud Data Shield abstracts away the complexity of building SGX-enabled apps and lets us focus on building features that add business value, instead of worrying about low-level implementation details."

Julien Brodier, Chief Technology Officer, Talium

"That's when we heard about IBM Cloud Data Shield," explains Brodier. "It was such an exciting proposition for us. It abstracts away the complexity of building SGX-enabled apps and lets us focus on building features that add business value, instead of worrying about low-level implementation details."

IBM Cloud Data Shield is a solution co-developed by IBM and Fortanix Inc., a multicloud security company. It enables Irene Energy to containerize its applications and run them on SGX-enabled bare metal worker nodes within IBM Cloud Kubernetes Service. Instead of requiring companies to design their applications specifically for SGX, IBM Cloud Data Shield automatically converts the code to be compatible with the SGX features.

IBM Cloud Data Shield also provides a catalog of pre-optimized components that developers can easily plug into their applications. For example, Irene Energy was able to integrate its application with an NGINX web server and a MariaDB database from the catalog within just a few hours.

"Cloud Data Shield probably accelerated the development of our platform by six months," says Marchand. "We could get to market much sooner because we didn't have to build SGX-compatible components from scratch."

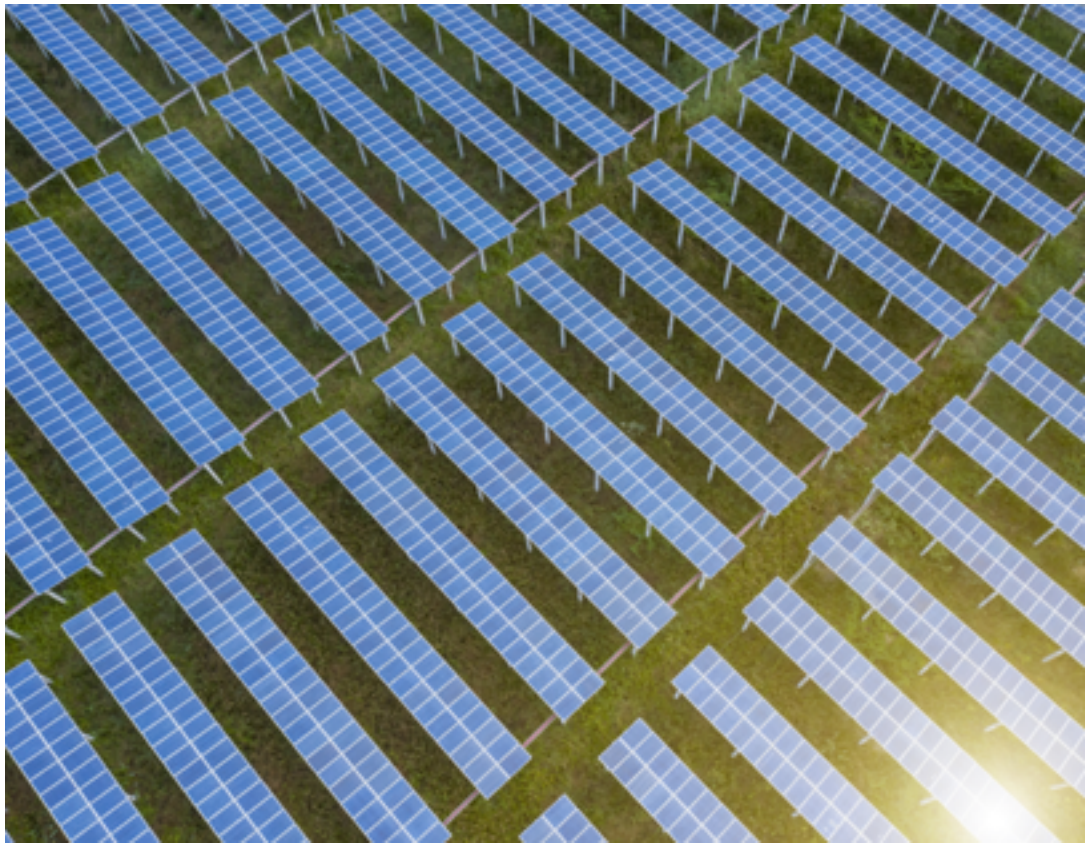
The fact that IBM Cloud Data Shield is built on top of IBM Cloud Kubernetes Service is also an advantage. As Irene Energy scales the platform up to support hundreds of thousands of users, Kubernetes will automatically handle orchestration and cluster management to scale seamlessly and make efficient use of the available bare metal worker nodes.

Finally, the IBM Cloud solutions provide an open architecture that enables Irene Energy to take advantage of a multicloud deployment strategy. As a result, data can flow in a way that is designed to be secure and reliable between the different microservices that make up the application, regardless of which underlying platform they are running on.

Frictionless energy transactions

Since its founding in 2017, Irene Energy has seen its original vision flourish—and grow. “We’ve made very good progress in establishing ourselves. We are presently in five countries in Africa, and we have 40,000 – 50,000 end users on the system,” states Guillaume.

“As the energy industry sees the opportunities that our platform opens up, we’re seeing significant demand,” he continues. “Every time a large electricity company decides to work with us, we can create new Stellar IDs for each of their customers. That could mean adding hundreds of thousands or even millions of new wallets almost overnight. Only IBM Cloud gives us that scalability.”



For the company's customers, the benefits can be significant. The billing and energy trading systems on which traditional utilities rely typically cost hundreds of thousands of dollars to implement, but with Irene Energy's platform, there are no up-front costs. As a result, it's possible for smaller companies—or even individuals—to become active participants in energy markets.

Recent changes in the affordability and availability of electricity are fostering new business opportunities. "We have end users in remote areas in Africa that are buying home systems on a pay-as-you-go model, similar to leasing cars in the US or Europe," says Marchand.

This trend, coupled with price drops in solar panels and improvements in batteries, is rapidly expanding access to electricity. A family that previously had enough electricity to power a few lights and a cell phone charger can now tap into greater amounts of electricity to run more complex devices and appliances.

With that complexity comes increasingly sensitive customer data—data that can provide value to third parties for the purposes of marketing additional products and services. This is where another level of confidential computing comes into play.

Africa falls under the stringent privacy standards of Europe's General Data Protection Regulation (GDPR) regarding the collection and use of personal data. To comply, rather than selling customer data to third parties, Irene Energy is looking into leasing that data while maintaining full ownership of it. Third parties can see the results of the data processing they pay for with no visibility into the data itself. This capability is made possible by the confidential computing capabilities built into Irene Energy's blockchain platform secured by IBM Cloud Data Shield.

"Initially, we were protecting the encryption wallets, transactions and keys," says François de Chezelles, chief executive officer of Talium. "But now, with the same technology, the use case of Irene Energy has evolved, and we're able to process the accumulated sensitive data while preserving its confidentiality.

"Of all the blockchain projects that Talium has engaged in, Irene Energy has perhaps the greatest potential to transform lives around the world," concludes de Chezelles. "From a technical perspective, the use of IBM Cloud Data Shield for secure authentication of a Stellar network is highly innovative, and we're looking forward to applying the same technique with other blockchains too."

About Irene Energy

Irene Energy offers a next-generation back office for the energy industry with an open platform that makes it easy for producers, suppliers, consumers and exchanges to transact without financial or contractual friction. Its support for micropayments and real-time settlement is helping solve some of the most challenging problems in the sector and could help make electricity more affordable and accessible for millions of people in the developing world.

Solution components

- IBM Cloud®
- IBM Cloud Bare Metal Servers
- IBM Cloud Kubernetes Service
- IBM Cloud Data Shield

About Fortanix Inc.

Fortanix provides the Runtime Encryption technology that powers IBM Cloud Data Shield. Runtime Encryption is a new technology that uses Intel SGX to secure the data in use by an application. This technology allows data to be encrypted when in use and uses remote attestation to establish the integrity of the application. To learn more about how Fortanix and IBM are working together to build seamless, zero-trust cloud security solutions for complex distributed applications, visit fortanix.com.

About Talium

Talium is a specialist in digital transformation projects involving blockchain integration and confidential computing. Customers are in the finance, energy, transport, logistics and health industries. The company also edits a fintech SaaS solution, Talium Assets, a comprehensive tokenization platform that simplifies fundraising processes and the creation of efficient investment marketplaces.

© Copyright IBM Corporation 2021. IBM Corporation, Cloud Computing, New Orchard Road, Armonk, NY 10504

Produced in the United States of America, February 2021.

IBM, the IBM logo, ibm.com, and IBM Cloud are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Fortanix, the Fortanix logo, and Runtime Encryption are registered trademarks of Fortanix Inc. in the United States and other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Contact IBM to see what we can do for you.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

RUNTIME ENCRYPTION is not an IBM product or offering. RUNTIME ENCRYPTION is sold or licensed, as the case may be, to users under Fortanix’s terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for RUNTIME ENCRYPTION, is the direct responsibility of, and is provided directly to users by, Fortanix.

SOFTWARE GUARD EXTENSIONS (SGX) is not an IBM product or offering. SGX is sold or licensed, as the case may be, to users under Intel’s terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for SGX, is the direct responsibility of, and is provided directly to users by, Intel.

STELLAR is not an IBM product or offering. STELLAR is sold or licensed, as the case may be, to users under Talium’s terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for STELLAR, is the direct responsibility of, and is provided directly to users by, Talium.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

05037805USEN-00