OVHcloud | intel.

WHITE PAPER

How Integritee is re-inventing Blockchain Security & Confidentiality using Intel® SGX technology and OVHcloud

Discover how Integritee uses Intel® Software Guard Extensions (Intel® SGX) and OVHcloud to help to secure blockchain applications. The future of blockchain security is here, so get ready to experience a game-changing technology poised to reshape blockchain's future! Let's dive in!

Tablet content

Executive Summary

In today's digital era, Blockchain technology has emerged as a reliable and security-focused way to manage and store data. However, one of the biggest challenges for blockchain projects is ensuring the privacy and security of their data, especially when it is being stored on the cloud.

To tackle this challenge, Intel, Integritee, and OVHcloud have teamed up to offer an innovative solution that leverages Intel® SGX technology. This technology provides a confidential computing layer which helps protect data in use via an application isolation technology, so that the data is not viewable by third parties.

It will be expedient to know that Integritee, a blockchain solution provider, has emerged as a key player in the race to develop security-oriented and scalable blockchain solutions. Its innovative SDK allows developers to build decentralized applications that are private while offering high security standards.

In collaboration with Intel and OVHcloud, Integritee is providing innovative and efficient blockchain solutions that benefit from speed, confidentiality and scalability. Thus, the collaboration offers a distinctive solution to the biggest challenge that blockchain projects are currently facing. The high privacy and security standards enable application developers to focus on developing innovative applications that transform industries, and disrupt traditional business models.

This whitepaper explores the collaboration between Intel® SGX, Integritee and OVHcloud, and how it provides a solution for the privacy and security of blockchain data stored on the cloud. We also examine the benefits of confidential computing for blockchain development, presenting compelling statistics demonstrating its importance. Ultimately, this whitepaper aims to provide insights into how this collaboration is shaping the future of the blockchain industry and how businesses can leverage it to help to protect their data and develop innovative applications with confidence.

Market Overview

The blockchain market has been growing rapidly over the years and this burgeoning tech is expected to continue growing in the coming years. According to market insight data[1], the global blockchain market is projected to reach $60 billion after 2023, growing at a compound annual growth rate (CAGR) of 85.0%, especially in all regions where OVHcloud is operating. This growth can be attributed to the increasing demand for blockchain technology across various industries, such as healthcare, finance, supply chain management, etc.

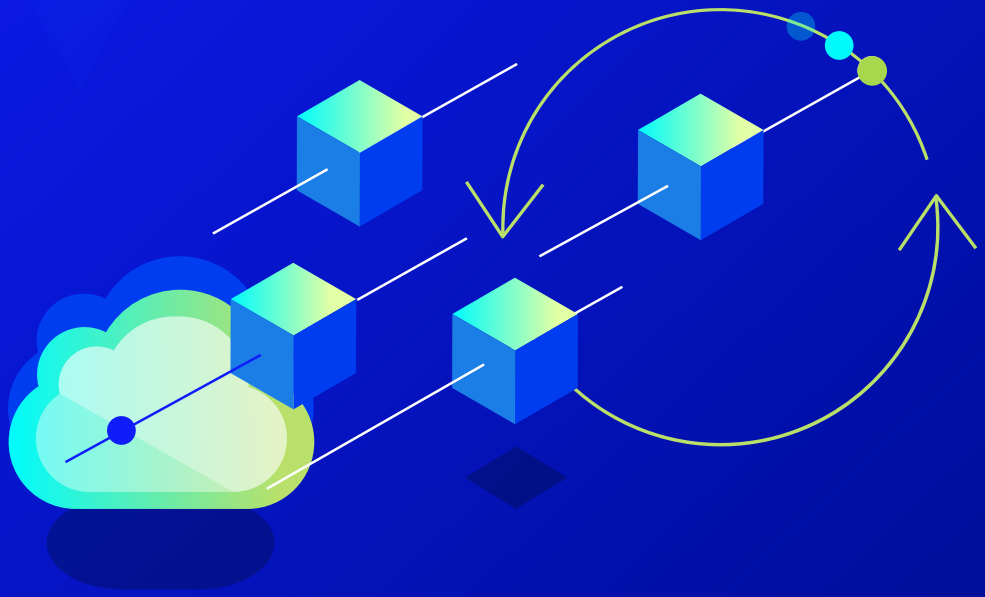
Research analyst forecasts expect the global cloud market to reach 1,500 billion by 2030. The role of cloud infrastructure in blockchain development cannot be overlooked anymore, especially with our innovation.

Cloud computing and blockchain have several similarities but have major significant differences. One major difference is that traditional cloud computing uses centralized architecture, while blockchain cloud architecture massively relies on decentralization. With OVHcloud's storage plus Intel® SGX, data is encrypted, making it difficult for hackers to tamper with it.

OVHcloud has provided reliable and security-focused cloud infrastructure services to businesses of all sizes for over 20 years. Our innovative approach to cloud infrastructure has made us a preferred choice for businesses that require high-performance cloud services.

Overall, the blockchain and cloud infrastructure market is expected to continue growing in the coming years. OVHcloud is well-positioned to take advantage of this growth with our cloud infrastructure services.

[1] Source OVHcloud 2023



Challenges in Blockchain Development

The blockchain sector has been experiencing an accelerated expansion over time, and this burgeoning technology shows promising signs of continued growth in the forthcoming years. The driving force behind this growth is the rising demand for blockchain technology in a myriad of industries, such as healthcare, finance, supply chain management, and beyond. And as the blockchain sector is expanding, blockchain companies have to cope with the following business challenges:

Scalability

Scalability is one of the most significant challenges facing blockchain networks today. As more users and transactions are added to the network, it can become slow and congested, leading to slower transaction processing times and increased transaction fees, ultimately discouraging users from using the blockchain.

OVHcloud offers large cloud capacities that enable easy scaling. Moreover, efficient consensus mechanisms and Layer 2 (L2) approaches are often leveraged to overcome the issue of network congestion. Integritee addresses this scalability challenge through L2 sidechains, which have a greatly simplified consensus protocol with confidential validator nodes that leverage Intel® SGX technology. These validator nodes are remotely attested, proving their trustworthiness and ensuring that blockchain applications can handle increasing numbers of users and transactions without sacrificing performance. With OVHcloud's infrastructure and Integritee's solution, developers can build scalable blockchain applications that compete with traditional systems in terms of performance and user experience.

Cost-effectiveness

Another challenge faced in blockchain development is cost-effectiveness. Blockchain transactions can be expensive due to the high computational power required to validate transactions. This can make it difficult for smaller companies or individual developers to enter the market.

To tackle this challenge, the solution that Integritee, OVHcloud, and Intel provide offers a cost-effective solution that can help lower the barriers to entry for blockchain developers. By using OVHcloud's powerful and cost-effective infrastructure, developers can reduce operational costs and focus on creating innovative blockchain applications accessible to a wider audience.

Security & Data Privacy

Security is another significant challenge in blockchain development. As blockchain technology becomes more widely adopted, it becomes more vulnerable to cyber-attacks. Hackers can target the endpoints of the blockchain network, steal private keys, and manipulate transactions.

To address this challenge, OVHcloud offers bare metal servers with integrated Intel® SGX technology: A huge advantage compared to the other providers. As bare metal ensures independent key management offering best-in-class data sovereignty and integrity, Intel® SGX provides hardware security. High data protection and security standards, as well as data sovereignty at every infrastructure level guaranteed by OVHcloud.

With datacentre locations in the EU - OVHcloud, as the largest European cloud provider, operates according to European values and highest data protection standards while leveraging our advanced security features. Developers can build blockchain applications with confidence, knowing that their data and assets are safe and secure.

OVHcloud understands the unique challenges of blockchain development and is committed to providing innovative solutions that can help developers build scalable, cost-effective, and most secure blockchain applications. By leveraging our infrastructure and services, developers can focus on creating innovative blockchain applications that can drive the growth of the blockchain industry.

Innovative Blockchain Solution Based on Integritee Network, Intel® SGX and OVHcloud Infrastructure

OVHcloud has joined forces with Intel to offer privacy-enhancing infrastructure solutions to their clients. With Intel® SGX, embedded into Intel® Xeon® Scalable processors, Confidential Computing is enabled across the cloud. OVHcloud can now provide an additional security layer for Blockchain and Web3 developers that will help to enhance the privacy and security of their data and business logic.

Essential Functions

Isolation
Separation of the TEE from underlying software, admins, and other cloud tenants

Encryption and Control
Workload owner holds key to decrypt data, retaining control and preventing access by cloud provider or other entities

Verification
Cryptographic confirmation that TEE is genuine, correctly configured, and software is exactly as expected

Application Isolation with Intel® SGX Technology

Intel® SGX is a hardware-based security technology that provides a protected enclave for sensitive data and computations. It enables the creation of trusted execution environments (TEEs), protected enclaves within the computer's processor that helps to protect data and computations from unauthorized access.

With the rise of blockchain technology, Intel® SGX has emerged as a crucial component of blockchain security. Intel® SGX provides an isolated environment for blockchain applications to run in. It helps to ensure that sensitive data, such as private keys and personal information, are kept confidential and encrypted and computations are executed with integrity. This is especially important for decentralized applications (dApps) that rely on smart contracts to execute transactions.

One of the key benefits of on OVHcloud is its ability to provide confidential computing on the blo Intel®ckchain. This means thatSGX computations can be executed securely within the TEE, so that malicious actors do not intercept or manipulate them. It also ensures that the execution of smart contracts can be performed in a trusted environment, helping to assure users that the transactions are protected and tamper proof.

Remote Attestation,
Of course, there's still one issue. How can a third party trust that their data is handled securely? After all, a process could be written that dumps private data outside of a protected enclave, removing the point of this protected environment. The way to strengthen enclave trust is with remote attestation.
Attestation provides crucial information - the identity of the software being attested, details of an unmeasured state (such as the execution mode), plus an assessment of possible software tampering. After an enclave successfully attests to a relying party, an encrypted communication channel can be established between the two. Secrets, such as credentials or other sensitive data, can be provisioned directly to the enclave.

With Intel technology providing this aspect of trust, Intel® SGX provides protection by design for processing data while maintaining privacy. Through protected enclaves, data can be pulled in for processing via existing APIs and processed in a confidential way that generates necessary digital proofs.

Integritee Network
Integritee network is a blockchain protocol that enables scalable, fast and privacy-preserving Web3 applications. The key to success is an infrastructure layer based on Confidential Computing and developer tools to easily build next-gen applications.

Integritee offers a Software Development Kit (SDK) and infrastructure solution that enables developers to create second-layer sidechains that offer advanced transaction speeds and volumes while enabling privacy by design and superior interoperability.

The Collaboration between OVHcloud, Intel and Integritee

In a world where data privacy and security are of utmost importance, Intel and Integritee have come together to provide an innovative solution for the blockchain industry with integrated confidential computing technology. By leveraging Intel® Software Guard Extensions (Intel® SGX) technology, Integritee offers highly secure and private computing on the blockchain, enabling developers to create powerful blockchain-based applications that benefit from speed, confidentiality, and scalability.

These highly secure and privacy-preserving blockchain applications are shardable second-layer (L2) sidechains, which can be built with Integritee's Software Development Kit (SDK). The Integritee SDK simplifies building these L2 sidechains, allowing developers to create sidechains with additional security and privacy features. The validator nodes for these L2 sidechains can be run on OVHcloud's bare-metal servers with integrated Intel® SGX technology, providing additional security and optional data privacy through computations inside hardware-encrypted Intel® SGX enclaves.

The 'confidential' validator nodes that run sidechains are remotely attested on Integritee's L1 blockchain, which carries out remote attestation with Intel on behalf of validator operators. This process provides evidence that validator nodes powering sidechains have integrity and are not compromised. The remote attestation result is published and stored on the Integritee network, making it transparent to anyone who would like to validate the integrity of the business logic run by the application.

Thus, applications built with Integritee's SDK benefit from enhanced security and data privacy through Intel® SGX technology and proven and transparent integrity of the business logic via remote attestation via Intel and stored on the Integritee network. Due to the extra layer of security and proven integrity, validator nodes carrying out computations for the same sidechain can trust each other. This greatly facilitates consensus and ensures efficiency and speed of the applications, resulting in sub-second block production times – another significant benefit alongside security and data privacy. The efficiency guarantees the sustainability of the solution, as consensus is established with low computational efforts.

The unique combination of Intel® SGX technology, Integritee's blockchain solutions, and OVHcloud's reliable and scalable infrastructure provides developers with the requirements to effectively build next gen blockchain applications that offer advanced transaction speeds and volumes while offering security and privacy by design. The collaboration between OVHcloud, Intel and Integritee is a great example of how blockchain technology's benefits can be leveraged, without compromising on security, data privacy, scalability, and sustainability of your infrastructure.

OVHcloud's Solution to the Problem

OVHcloud is a leading cloud infrastructure provider offering a wide range of services, including cloud computing, storage, and network solutions, with 34+ data centers worldwide. OVHcloud provides a stable network with a backbone capability of 70 Tbps.

Many blockchain-based companies utilize its services, including some of the most popular blockchains networks that are currently staking on OVHcloud.

OVHcloud offers a multilocality advantage to its customers, which means they can choose from a range of data centers across the world, depending on their specific needs. As a result, OVHcloud is an ideal solution for blockchain-based projects that require a reliable and stable network infrastructure.

Regarding pricing, OVHcloud offers a pay-as-you-go and transparent pricing approach, which means customers can benefit from the flexibility to scale up or down as required without being locked into a fixed contract. This feature is valuable in the volatile blockchain space, where demand can vary greatly.

OVHcloud offers several solutions for its customers, including dedicated servers with root access, public cloud instances with pre-prepared automation, open-stack-based infrastructures, managed Kubernetes, managed databases, and hosted private clouds with VMware or Nutanix.

OVHcloud Bare Metal servers delivered the high-performance and confidential computing capabilities it needed, while OVHcloud Public Cloud provided a scalable, secure, and reliable cloud. Managed Kubernetes added further value, helping to drive efficiency by removing the burden of container management.

Overall, OVHcloud's services offer a reliable and flexible cloud infrastructure well-suited for blockchain-based projects.

With its multilocality advantage, pay-as-you-go approach, and a range of solutions, OVHcloud can help businesses build and scale their blockchain-based solutions efficiently and cost-effectively.

What OVHcloud is supporting

OVHcloud, the cloud infrastructure provider, has put its foot down on PoW (Proof-of-Work). OVHcloud understands the unsustainability of the energy requirements for PoW and the potential harm it could cause to the environment. This is why OVHcloud has forbidden the use of PoW on its infrastructure. PoS (Proof-of-Stake), on the other hand, is welcomed on OVHcloud infrastructure, as it aligns with OVHcloud's values and goals for sustainability.

Client Testimonials

We believe in delivering the best-in-class cloud infrastructure solutions that help our clients achieve their goals. Here are some testimonials from satisfied clients who have leveraged our combined solution of OVHcloud, Intel and Integritee for blockchain development.

A brief case study of Ajuna (a decentralized gaming provider)

Ajuna is leveraging Integritee's technology to run high-end gaming engines in TEEs to create fast, secure, and scalable decentralized gaming ecosystems. Using Integritee's SDK and Confidential Computing platform, Ajuna can leverage Intel® SGX technology to develop a new generation of Web3 games and OVHcloud's bare-metal infrastructure for deployment seamlessly.

Ajuna's CEO, Cédric Decoster, expressed his satisfaction with the partnership with Integritee, stating, "Being able to leverage the power of TEEs with minimal effort on our end and not having to worry about a reliable and secure infrastructure was our reason to choose Integritee as a partner." He also mentioned that Integritee's technology enables Ajuna to provide game developers with the opportunity to create competitive Web3 games through the usage of TEEs, which provide the basis for fast interactions with sub-second block times, and scalability.

Integrating Intel® SGX technology, TEEs, and OVHcloud's infrastructure has enabled Ajuna to create a decentralized ecosystem for games and virtual goods. The collaboration between Intel and Integritee has allowed Ajuna to focus purely on developing its own tech and decentralized gaming ecosystem while leveraging the power of TEEs with minimal effort. This will result in the creation of a new generation of Web3 games that can compete with traditional non-blockchain-based games.

Conclusion:
The Future of Blockchain Security and Scalability

Integritee is at the forefront of providing the foundation for next gen Web3 applications that combine security and data privacy with speed and scalability by leveraging Intel® SGX technology and OVHcloud's advanced infrastructure.

Their approach of integrating Intel® SGX technology into L2 solutions is powerful for Web development. By utilizing Integritee's SDK, Web3 developers can create a Trusted Execution Environment (TEE) and benefit from confidential computing, in order to enhance data privacy and reduce the risk of security breaches.

Integritee's partnership with OVHcloud is also a testament to high quality standards made in Europe. With OVHcloud's multi-location scalability, sustainability, and pricing transparency, Integritee can provide reliable, performant, and scalable infrastructure for its blockchain solutions that meet the demands of its clients.

Integritee is more than just a solution provider. They are visionaries committed to advancing the blockchain space by providing innovative solutions that unlock the true potential of this game-changing technology.

Whether you are a blockchain startup or an established enterprise, Integritee has the tools, expertise, and infrastructure you need to succeed. Start innovating today and discover the possibilities that await with Integritee, Intel® SGX technology, and OVHcloud.

Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

OVHcloud

Contact us:

ovhcloud.com/en-ie/contact-sales/