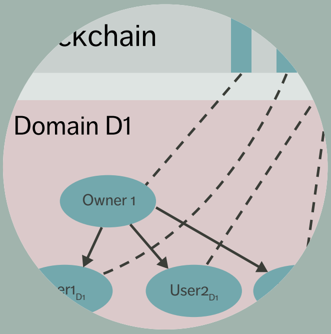
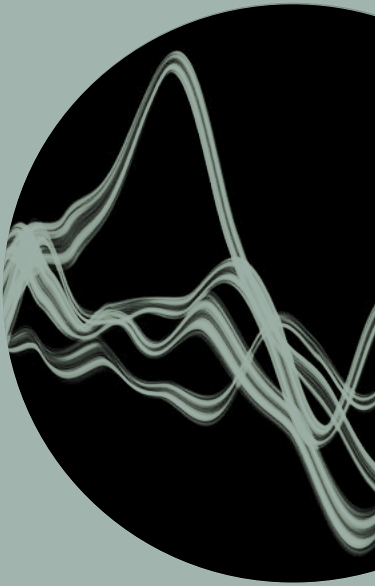
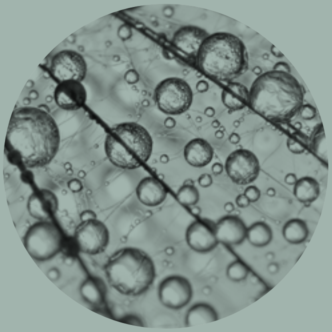
CHARTING THE FUTURE OF INNOVATION | #03·2019

ERICSSON TECHNOLOGY Review





BLOCKCHAINS AND ONLINE TRUST



ERICSSON

FACILITATING ONLINE TRUST WITH blockchains

A decade after its launch, blockchain is still the only internet-age technology that is able to facilitate online trust using mathematics and collective protocolling exclusively.

DANIEL BERGSTRÖM,
BEN SMEETS,
MIKAEL JAATINEN,
JAMES KEMPF,
JONAS LUNDBERG,
NICKLAS SANDGREN,
GASPAR WOSA

One of the fundamental challenges in the online, digital world is that implicit, fundamental concepts in the off-line, physical world need to be formalized and made explicit. Trust is a prime example.

■ In the physical world, trust is intangible but it is nonetheless central to our interactions with other people and to our consumption of services. Creating an online environment in which people feel secure when interacting and consuming in a similar way requires the development of technologies and protocols that formalize and digitalize trust.

The current solution to the challenge of facilitating trust online is to rely on trusted third parties such as banks and major internet companies to act as trust anchors, creating and attesting certificates for people or web-based services. Each device, browser and operating system comes preconfigured with a list of these trusted third parties and their certificates – their digital fingerprints. By instructing our devices to trust the root certificate of the trusted third party, they are able to computationally infer trust in all underlying entities.

The primary weakness of this hierarchical approach to establishing trust stems from the underlying structure of centralized power. The root keys of each certificate authority are a core asset of today’s internet, but they are privately managed and sensitive to exposure. Blockchain was originally designed to uproot this hierarchy and create a new kind of trust system for electronic transactions. In essence, the blockchain itself becomes its own trust anchor based on a distributed, transparent and community-driven infrastructure.

A blockchain removes the need for trusted third parties, distributes the centralized power of the certificate authorities, and allows anonymous members to join and contribute to the infrastructure at their own discretion – although at a very high cost in terms of throughput. While digital currencies are strongly associated with blockchains – the "coins" are generated by contributing resources to the networks and spent by making transactions that are processed by the networks – the value of blockchains goes beyond digital currencies.

Public versus private blockchains

Bitcoin and Ethereum are both classified as public, permissionless blockchains. These systems have three properties that form the basis of trust. Firstly, anyone can become a participant by contributing computing resources – there is no need to have a prior relation to any other node in the system. Secondly, generating a new block on the blockchain is computationally expensive, as the consensus mechanism is designed to require a certain amount of wall-clock time to complete regardless of the size of the network. And lastly, it is impossible to predict which contributor will be the first to complete the next block.

If more than half of the computational resources in the system are technically well-behaved, their results will dominate any malicious or malfunctioning nodes that may try to alter the history of the system in an erroneous direction. In the consensus method used in these systems, known as proof of work (PoW), there are no shortcuts to generating new blocks; it can only be done through a computationally intensive hashing process. Other schemes for consensus are being developed and discussed, but these have yet to see widespread use.

> “ [PRIVATE BLOCKCHAINS] EMPLOY STRONG IDENTITIES, USER MANAGEMENT AND A PROTECTED DATA STRUCTURE ”

The difference between public blockchains and private, permissioned ones is that the latter employ strong identities, user management and a protected data structure. Private blockchains target use cases somewhere between a public blockchain in an untrusted public environment and a distributed database hosted in a fully trusted internal deployment. This segment includes bank consortia, for example, that have a mutual reliance and at least some level of preestablished trust, but where a privately managed backend for transaction management is not a feasible alternative. Due to the difference in network constitution and the presence of at least partial trust, the computationally expensive PoW scheme is not required in private blockchains. Instead, they can use the same consensus algorithms that are used in other distributed systems, designed to compensate for both malicious and malfunctioning nodes.

The differences in scope between public and private blockchains have a large impact on technology choices. From a technical standpoint, there is virtually no overlap between the two different types of blockchains. It is also significant to note that public blockchains are by design very difficult for companies to monetize, which is why most firms have chosen to focus on private blockchains instead.

Terms and abbreviations

ABI – Application Binary Interface | **IoT** – Internet of Things | **JSON** – JavaScript Object Notation | **PoW** – Proof of Work | **REST**– Representational State Transfer | **SOFIE** – Secure Open Federation for Internet Everywhere | **TEE** – Trusted Execution Environment

The most commonly used software technology to realize private blockchain installations is Hyperledger Fabric.

Key technical properties of suitable use cases

We have identified four key technical properties of the partial-trust use cases that we expect to be suitable for blockchains: (1) a shared trusted history, (2) structure built on multiple stakeholders of equal standing, (3) largely independent nodes, and (4) access to data history.

Shared trusted history

The key benefit of the blockchain is trust between stakeholders, and to establish a history of transactions that is very hard to tamper with.

Multiple, equal stakeholders

The main niche of blockchains lies in the area of partial trust between roughly equal stakeholders.

Largely independent nodes

Use cases where each node operates independently and uses the blockchain for support are desirable due to the relatively high cost and/or delay of running transactions on the blockchain.

Access to data history

Because the historical data is normally retained indefinitely, it is highly beneficial if there is a value to the use case in having access to historical transactions.

> “THE SMART CONTRACT WILL MONITOR, VERIFY AND ENFORCE AGREED CONDITIONS AUTOMATICALLY”

Related technologies

The technical development and broadening of blockchains is constantly ongoing. By altering or extending the core functionality, we can both widen the scope and applicability of blockchains as a technology and mitigate the limitations of existing offerings.

Smart contracts

With traditional databases, it is straightforward to create software that monitors a database, determines whether or not a certain condition has been fulfilled, and updates the database accordingly. This is exactly what smart contracts do as well, but in the trusted environment of blockchains. A smart contract is neither smart nor a legal contract; rather, it is an agreement between two or more parties that is formulated and enforced with immutable cryptographic code. This code is executed on every node within the blockchain network and determines how data in the distributed ledger is modified. If a smart contract depends on external information, an oracle must be used to feed this information into the ledger to make it accessible to the smart contracts.

Smart contracts remove reliance on trusted intermediaries when making business agreements. Typically, a smart contract includes terms and conditions, performance metrics and possibly penalties. During execution, the smart contract will monitor, verify and enforce agreed conditions automatically, which can potentially save time and money for the parties involved.

The technology behind smart contracts is promising, but there are some caveats; smart contracts need to be very carefully designed and implemented to ensure that the resulting contract acts exactly as intended given any input or event. Misconfigured smart contracts are virtually impossible to cancel (unless they have been designed for renegotiation from the start), which considerably increases the demands of deploying a smart contract.

Hashgraphs

The drawbacks of the PoW consensus algorithm used by public blockchains (in terms of delay, throughput, energy efficiency and transaction costs) have inspired the development of other technologies targeting the challenge of distributed trust. Hashgraphs are one such example. Hashgraphs reorganize the transaction blocks from a chain of blocks to a directed acyclic graph of blocks, which enables new blocks to be added to the system without waiting for all previous blocks to be organized.

The organization of blocks enables multiple lines of transactions to be run in parallel, and in theory allows for a system that has considerably lower delays and higher throughput compared with a conventional blockchain. Hashgraphs also try to replace the computationally expensive PoW consensus algorithms with other approaches to increase the throughput and energy efficiency of the system. Smart contracts can run on hashgraphs in a way that is similar to how they run on blockchains.

Hashgraphs represent a bold technological leap that strives to overcome all the drawbacks of public blockchains. However, current hashgraph technologies are not open and available in the same way as public blockchain technologies are, which arguably makes them better suited to solve different use cases that are closer to those of private blockchains. Some hashgraph technologies are also designed around patented algorithms and built-in claims to parts of the revenue, which goes against the original intention of blockchain to create a decentralized and democratic infrastructure.

Trusted Execution Environments

A Trusted Execution Environment (TEE) is established within an individual device by using an enclave – a hardware-protected part of the CPU chipset that operates on encrypted memory and storage for security purposes. This approach enables the execution of selected software in isolation from the underlying operating system layers, effectively in isolation from any attacks originating from hacking or exploiting operating system software. The technology was initially launched for some chipsets in the early 2000s but has only recently reached wide-scale deployment in device, desktop and server hardware.

> “TEEs MAY OFFER A BREAKTHROUGH IN TERMS OF CONSENSUS ALGORITHMS”

From a public blockchain perspective, TEEs may offer a breakthrough in terms of consensus algorithms. A key feature of modern TEEs is the ability to attest the code running inside the enclave through a hardware-supported asymmetric key exchange. The ability to execute trusted and verifiable code on otherwise compromised systems lays the foundation for a new generation of consensus algorithms, anchoring the trust in the signature of the code being executed rather than in the work being carried out or the identity of the node owner. Early results of this development in public blockchains show considerably increased transaction speeds and reduced energy consumption. The implications are yet to be fully determined for private blockchains that rely on classical distributed system algorithms for consensus.

Use cases and applications

At Ericsson, we believe that a robust blockchain foundation can increase ecosystem involvement and enable new business models for revenue generation. In light of this, we have been testing the application of blockchain technology in the realm of telecommunication for some time, and we have identified three use cases that are particularly promising in terms of services with monetization potential. One is called the smart contract platform, the second is known as ID brokering, and the third is a Nubo-based virtual services marketplace.

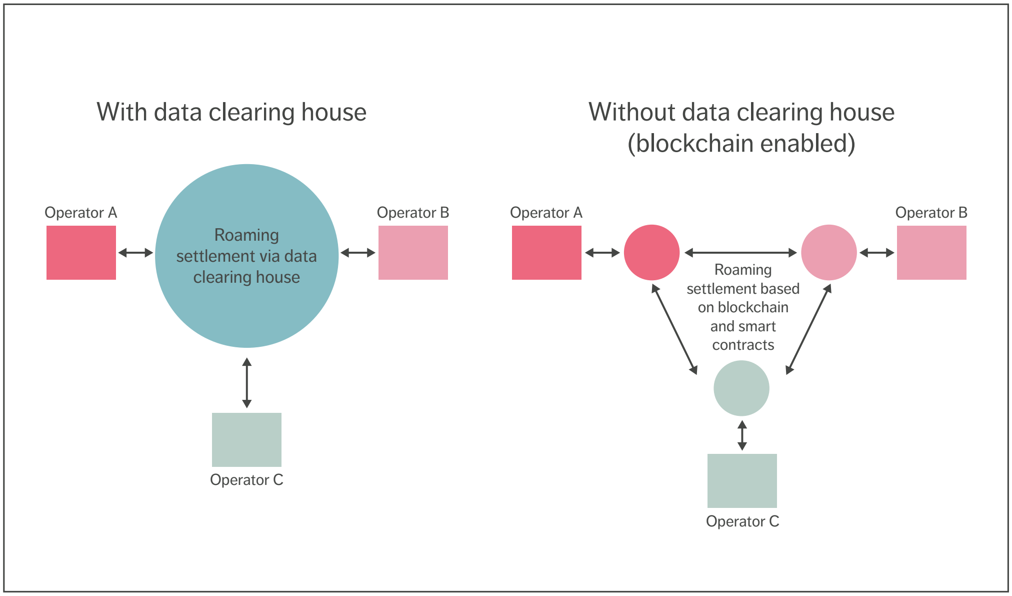

With data clearing house
Operator A
Roaming settlement via data clearing house
Operator B
Operator C
Without data clearing house (blockchain enabled)
Operator A
Operator B
Roaming settlement based on blockchain and smart contracts
Operator C

Figure 1 Roaming clearance and settlement, with and without third-party support

Smart contract platform for services providers

The smart contract platform is an innovation platform driven by Ericsson that allows operators who are innovating with us to explore blockchain and smart-contract technology to offer new services, evaluate platform business opportunities and address internal efficiencies to reduce the cost of doing business. One interesting use case for the platform is its application to roaming clearance and settlement services [1] as depicted in *Figure 1*.

The handling of roaming subscribers today relies on trusted third parties (data clearing companies, for example) to manage the clearing processes and settlement related to billing. The smart contract platform roaming settlement application replaces these (often expensive) third parties with a trusted, distributed and decentralized blockchain solution that includes smart contracts (for example, Hyperledger Fabric chain code).

The smart contract platform can take advantage of core attributes of blockchain's shared ledger approach to provide trust, security and transparency across the participating ecosystem. Smart contracts can be used to support the following three main groups of services:

- roaming management, including agreement definition and archiving
- data clearing, such as billing record creation, conversion services and fraud management
- financial clearing and settlement services for voice, SMS, MMS and data transactions.

The insights from smart contract platform experiments will validate the key technical properties where trust can be distributed and govern in a decentralized manner and through data integrity and transparency supported between the counterparties.

ID brokering

We have designed and implemented a decentralized system for ID brokering based on a concept that creates trust relations between digital identities and the systems that handle them. The system capitalizes on the strength of blockchains to express and manage trust relations in industry-wide solutions and creates a unified mechanism for ID management across underlying heterogeneous ID technologies.

ID brokering makes it easy to establish encrypted and trusted connectivity for IoT devices that are on the move, or for personal devices that are carried across different administrative network domains. For example, by allowing device IDs to act as digital passports and registering the (non-sensitive) passport IDs of devices when booking a trip, the networks the devices pa ss through (including airports, hotels and conference facilities) can use their own trusted IDs to grant secure internet access without manual authentication.

The ID brokering concept is based on three key aspects:

1. the self-sovereignty of ID domains, where devices are provisioned with any secure ID technology deemed appropriate, and where the ID secret is securely stored in a TEE
2. authentication utilizes the trust relation expressed in a blockchain-based backend, where instantaneous access rights for specific devices in specific networks are managed
3. the blockchain backend enables the system to reach a shared consensus on a global scale, as no single party is the main controller or beneficiary of the system.

Ericsson demonstrated an ID brokering implementation – in this case a custom layer on top of Hyperledger Fabric using blockchains and TEEs – at Mobile World Congress in 2017. In it, each IoT device is represented by a node, belongs to a domain, and has relations with owners expressed by links, as illustrated in *Figure 2*. With this approach, we emphasize the decentralized nature of applications enabled by the blockchain. Each domain owner

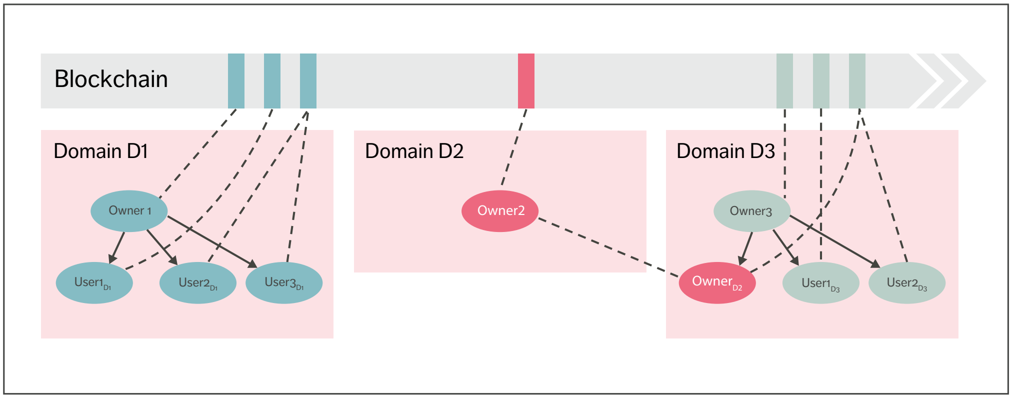


Figure 2 ID domain creation and ID crosslinking with the support of blockchain

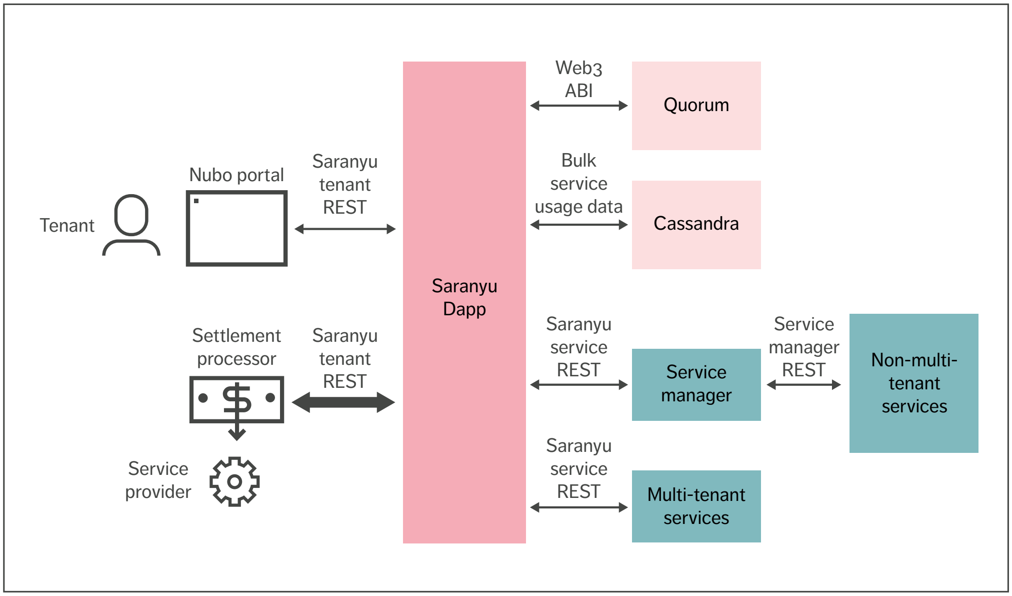


Figure 3 Nubo virtual services marketplace architecture

has full sovereignty of their domain, and shared context of the blockchain enables a domain to interact and to grant and revoke access dynamically.

The ID brokering solution shares the concept of self-sovereignty with the Sovrin system [2], and is oblivious to the specific ID technologies used for authentication and ID provisioning. Since 2017, we have been working on ID brokering and its coexistence with public key infrastructure solutions.

Nubo virtual services marketplace

New 5G features enable operator networks to be virtually segmented into different logical networks (slices) similarly to how network resources in cloud infrastructure can provide different virtual networks for different tenants. The rise of virtual network functions – that is, virtualized and software-based routers or firewalls – has created the foundation for a market of network services where the set of components can be composed specifically for each tenant. With slicing and virtualization of network components in 5G, we envision that future 5G operator services are likely to have similar characteristics, with a tailored composition of services for each network slice.

We designed the Nubo virtual services marketplace to meet the specific requirements of virtualization use cases. Its architecture is illustrated in *Figure 3*. The Nubo marketplace is made up of buyers of virtualized services, referred to as "tenants", and the sellers of those services, referred to as "service providers". The tenants can be individual users, enterprise customers or even operators. A blockchain with smart contracts provides the tenants with the basic trust platform for price discovery on the services. Nubo's tenant and service management microservice (known as Saranyu) utilizes the J.P. Morgan Quorum blockchain, which supports smart contracts written in Solidity.

Tenants and services have contract accounts on the blockchain, which govern their interaction with the marketplace and each other. Services list their resource offerings on the blockchain through Saranyu in the form of a JSON (JavaScript Object Notation) document describing the attributes of the resources. Attributes can be quota limited or have charges associated with them. Tenants request the delegation of resources and must cryptographically sign the JSON document, indicating that they commit to abide by the charging and quota advertised in the resource offerings.

Services record tenant usage and send usage records to Saranyu, which Saranyu stores in the Cassandra distributed database, depositing a signed hash of the record into the blockchain to ensure the records are not changed. Periodically, Saranyu runs a billing cycle in which tenant charges for services are totaled up and submitted to a settlement processor, which can be a credit card processor or a cryptocurrency account.

Nubo can also support cloud compute/networking/storage services as well as serverless functions or distributed operating system types of services. A prototype of Nubo was developed at Ericsson in 2018, featuring an experimental cryptocurrency charging system that charged for services using a private Ethereum account deployed in the Ericsson Research Data Center in Lund, Sweden. Services listed included the Nefele Cloud 3.0 distributed operating system, the Ethereum serverless function system, and the University of California, Berkeley, RISELab artificial intelligence execution environment Ray.

Standardization and external collaboration

The mass adoption of blockchains will require both technical and business-model interoperability between organizations, permissioned blockchain consortia, and even permissionless blockchains. Consequently, blockchain standardization is underway and several industry consortia have formed to strive for interoperability and harmonized processes. Ericsson is contributing to the standardization process through our active involvement in the GSMA and all major telecom and ICT standardization bodies, as well as by becoming a founding member in an ETSI (European Telecommunications Standards Institute) working group on permission distributed ledgers.

With respect to collaboration, the EU and several national governments are currently sponsoring academic and industrial collaboration for blockchain research and business acceleration. Ericsson has chosen to participate in the EU H2020-IoT SOFIE (Secure Open Federation for Internet Everywhere) project 2018-2020 together with several industry-leading companies and academic institutions to research blockchain interoperability across siloed IoT applications, including the demonstration of results through several live pilots. We are also collaborating directly with global technology companies in the areas of trusted computing and blockchains.

> “THE MASS ADOPTION OF BLOCKCHAINS WILL REQUIRE BOTH TECHNICAL AND BUSINESS-MODEL INTEROPERABILITY”

Conclusion

Ericsson sees significant value in blockchains as a trust enabler and potential disruptor that can enable completely new business models in the digital asset market. The use cases we have evaluated for private blockchains so far, both in-house and together with

> OUR NEXT STEPS WILL INCLUDE FURTHER EXPLORATION OF THE POTENTIAL OF PUBLIC BLOCKCHAINS AND HASHGRAPHS

global telco and enterprise customers, have achieved promising results. To date, we have demonstrated the value of blockchain for roaming settlement and other use cases such as IoT data monetization, supply chain management, handling of privacy-sensitive data, license management and ID management.

Our next steps will include further exploration of the potential of public blockchains and hashgraphs.

While we are keen to accelerate our blockchain efforts from exploration to commodification and mass adoption, we recognize that a number of fundamental issues must be resolved before we get there. Appropriate governance models around blockchain consortia must be established, for example, along with technology and business model interoperability. The questions of how to create a viable platform business and how to ensure that contracts act on trustworthy data must also be answered. We will continue to work on these aspects in close collaboration with our customers and other industry stakeholders through standardization and joint innovation.

References

1. **Monitor Deloitte, Blockchain @ Telco: How blockchain can impact the telecommunications industry and its relevance to the C-Suite, 2016, available at:** *https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf*
2. **White paper, Evernym in cooperation with the Sovrin Foundation, What Goes on the Ledger?, September 2018, available at:** *https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf*

Further reading

- **Ericsson, blog, Secure brokering of digital identities, available at:** *https://www.ericsson.com/en/blog/2017/7/secure-brokering-of-digital-identities*
- **Ericsson, blog, Smart contracts for identities, available at:** *https://www.ericsson.com/en/blog/2017/10/smart-contracts-for-identities*
- **Ericsson, blog, Secure IoT identities, available at:** *https://www.ericsson.com/en/blog/2017/3/secure-iot-identities*

THE AUTHORS

Daniel Bergström
◆ is a senior researcher in distributed computing at Ericsson Research. He joined Ericsson in 2014 and works with all things distributed. His current focus is on secure infrastructures for artificial intelligence workloads. He holds a Ph.D. in computing science from Umeå University, Sweden.

Ben Smeets
◆ is a senior expert in trusted computing at Ericsson Research. He holds a Ph.D. in information theory from Lund University, Sweden, where he also serves as a professor. He joined Ericsson in 1998, working on security solutions for mobile phone platforms. Smeets is currently working on trusted computing technologies in connection with containers and secure enclaves.

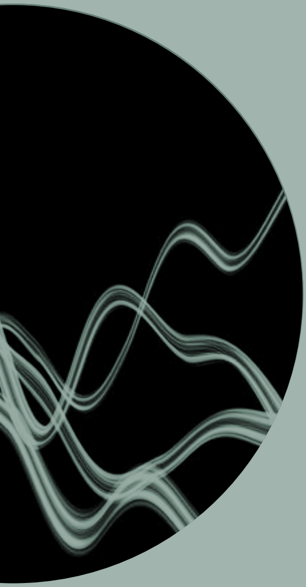
Mikael Jaatinen
◆ is a security specialist at Business Area Technologies and New Businesses. He joined Ericsson in 1996 and has been working with blockchains since 2014. He holds an M.Sc. in computer science from Åbo Akademi University in Turku, Finland. Jaatinen is currently responsible for work packages in the blockchain project SOFIE and with artificial intelligence/ machine learning-based security analytics.

James Kempf
◆ worked for Ericsson Research in Silicon Valley as a principal researcher from 2008 to 2018. He earned a Ph.D. in systems engineering from the University of Arizona in Tucson, the US, in 1984, holds 21 patents and is the author of three books and many papers. He currently works as a senior principal architect for Equinix in Sunnyvale, California.

Jonas Lundberg
◆ joined Ericsson in 1997 and currently serves as a senior researcher at Ericsson Research. His research interests include distributed computing and blockchain technology, and his current focus is blockchain platforms for rapid prototyping. Lundberg holds an M.Sc. in computer science from Luleå University of Technology, Sweden.

Nicklas Sandgren
◆ is a senior researcher in the field of distributed computing at Ericsson Research. He joined Ericsson in 1998 and has worked in many different areas, including speech and channel coding, VoIP prototyping, WebRTC and DevOps. He holds an M.Sc. in computer science from Luleå University of Technology.

Gaspar Wosa
◆ currently serves as innovation manager at Ericsson ONE in Business Area Technologies and New Businesses. He joined Ericsson in 1997 and his primary interest at present is the business model impact of blockchain and smart contracts. He holds a B.Sc. in telecommunication engineering from Polytechnic University of Indonesia and an MBA from IPMI International Business School in Kalibata, Indonesia.



ISSN 0014-0171
284 23-3327 | Uen

Ericsson
SE-164 83 Stockholm, Sweden
Phone: +46 10 719 0000