IDENTIV RESEARCH

The Security Benefits of Unifying NFC and Blockchain

Blockchain and NFC bring trust and security to real-time processes by distributing large-scale computing efforts and eliminating single points of failure

Although blockchain gained household recognition with the rise of Bitcoin's popularity, blockchain has many uses beyond cryptocurrency. The decentralized, distributed qualities of blockchain processing lends security, transparency, reliability, and authenticity to all kinds of systems. Combined with the power of near-field communication (NFC) devices, systems using both NFC and blockchain promise unprecedented performance for a range of highly secured networks. Early adopters and research teams have found success by bringing both NFC and blockchain technology to a number of applications, from manufacturing and supply chain to financial recordkeeping.

How can NFC and blockchain work together to improve security?

Through blockchain-based solutions, engineers and designers can build an immutable digital ledger and transparent exchange of electronic information. However, blockchain alone operates in a purely digital space — there needs to be an intermediate step to connect physical objects to a blockchain and all the benefits it could provide.

NFC tags translate physical objects, locations, and markers into the digital world. The relatively short range of NFC sensors discourages interference from afar, as close physical proximity is needed to interact with the NFC system. However, NFC tags are susceptible to cloning, modification, and other forms of tampering.

Combining both NFC and blockchain into a single system balances the weaknesses of either technology on its own: NFC provides a medium for blockchain to interact with the physical world, and blockchain verifies NFC tags to detect and prevent tampering. While each of these technologies are well researched individually, new innovation is inspired by the future applications and limitations of hybrid NFC-blockchain systems.

What are some promising applications of NFC and blockchain?

While there are many potential applications that can benefit from the increased security NFC and blockchain can provide, early adopters have already found success in introducing these technologies to their specific use cases. Some research teams have explored applications in supply chain management, paper-based process modernization, sustainable manufacturing, and Internet of Things (IoT) security.

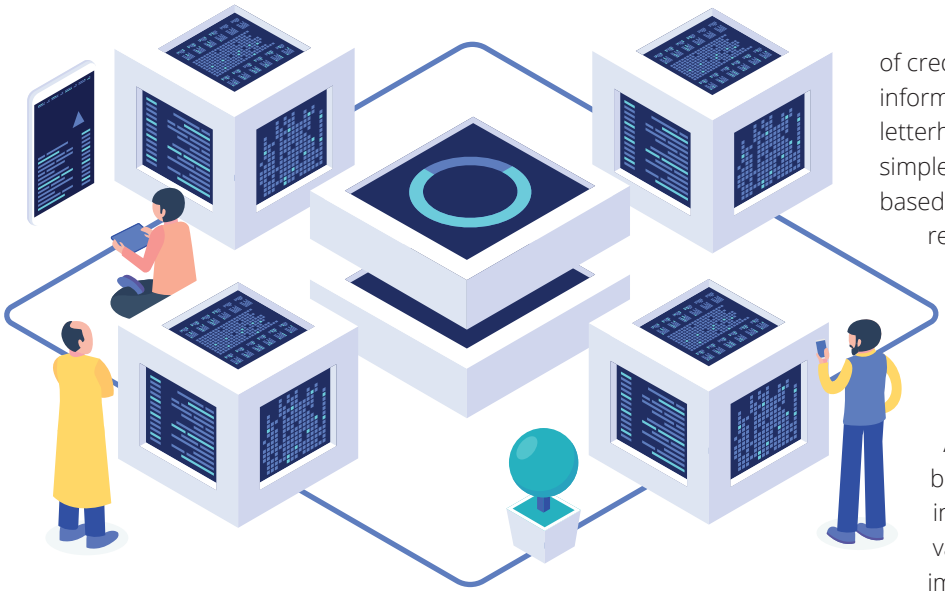
Anti-Counterfeiting Supply Chains

As demonstrated by the recent SolarWinds cyber incident, supply chain vulnerabilities can compromise entire systems. Hackers in this incident were patient and experienced, causing catastrophic damage well beyond the scope of the SolarWinds supply chain system.

Even existing state-of-the-art supply chain protocols rely on centralized processing, including many overlapping weaknesses that were leveraged in the SolarWinds incident. Researchers suggest that a block-supply chain which relies on NFC to detect counterfeiting would bring unprecedented security and efficiency to supply chain management. Centralized supply chains suffer from many problems, including overburdened processing servers, massive digital record storage, and a single point of failure.

This research team focused on preventing three types of counterfeiting that are associated with NFC and RFID tagging:

1. **Modification** of product details, such as expiration date
2. **Cloning** genuine product details onto a counterfeit product's tag
3. **Reapplication** of a tag from a genuine product and attaching it to a counterfeit



Centralized systems suffer from these three attacks due to a lack of transparency, as they only have a single source of information to authenticate a product's data. In a decentralized block-supply chain, each node maintains a blockchain for each genuine product. Each block in the chain is an authentication event. To change any information in the blockchain, the node which currently has the product proposes a new block (or new authentication event), which is validated by a number of other nodes. If the other nodes successfully validate the new block, a copy of this new block is added to all nodes in the supply chain network.

By decentralizing existing protocols with blockchain, researchers efficiently detected over 95% of modification, cloning, and reapplication incidents in large-scale supply chain systems. In certain industries, like pharmaceuticals — where 10-30% of medicine sold in developing countries is counterfeit — this can dramatically improve product quality of essential goods.

Preventing Fraud in Paper-Based Processes

Many financial institutions use letters of credit to confirm that payment will be sent upon the successful delivery of agreed goods and/or services. This is a popular insurance tactic in international sales; however, this is vulnerable to fraud by falsifying documentation for the shipment of inferior goods or unsuccessful delivery of goods. While some banks have already transitioned to electronic letters of credit, paper documentation still dominates international trade due to the complexities of foreign trade transactions.

Novel research has emerged which encourages the use of an NFC-enabled application that uses blockchain to prevent letter of credit fraud. Fraud can occur at any step in the letter of credit process, including fake websites, personal information, account numbers, identification cards, letterheads, and so on. Chance of fraud — or even simple human error — compounds with a paper-based system, as this means manual checking is required for many fields within letters of credit. Further, paper processes take days to weeks to relay information between relevant parties, enlarging windows of opportunity for unauthorized activity.

As modified letters of credit enable fraud, blockchain is a natural choice for financial institutions to employ. Blockchain establishes a validated record of past transactions that is nearly impossible for one party to alter. NFC enables connectivity and electronic verification (via blockchain) of paper-based documents, like letters of credit, that many international banks rely on. As a letter of credit is scanned via NFC in a mobile app, the blockchain is updated in nearly real-time to maximize transparency and ensure genuine authentication from all parties.

Blockchain and NFC eliminate the alteration of letters of credit and related documentation available in paper processes that many previous fraud cases leveraged. Billions of dollars would be saved globally by incorporating NFC and blockchain-fortified authentication procedures for letter of credit transactions and their subsequent wire transfers.

Moderating Sustainable Manufacturing in Industry 4.0

The United Nations identified 17 Sustainable Development Goals to provide economic stability, promote renewable energy sources, and combat climate change. Sustainable manufacturing is critical to both Goal 9 (industry, innovation, and infrastructure) and Goal 12 (responsible consumption and production). A number of innovative manufacturing models – including social manufacturing, peer production, open production, and crowd manufacturing – show promise to bring greener practices to manufacturing. In each model, manufacturers must share protected proprietary information and collaborate in a trustless network, as sustainable manufacturing best practices are often decentralized.

One research team suggests a framework for blockchain-empowered sustainable manufacturing that enables the collaborative, authenticated network that sustainable manufacturing requires. Blockchain enables sensitive data to be shared confidently between various groups without the need for intermediaries. The research team groups the benefits of blockchain to manufacturing in four categories:

1. ***Infrastructure:*** Greater transparency is achieved through improved access, visibility, and traceability of processes and shared ledgers. Easy collaboration and resource sharing increases flexibility across teams to adapt to market changes. Risk management is enhanced through detailed, immutable records that can track the origins of any disruptions to the manufacturing process.
2. ***Offer:*** Profitability improves, as a more sustainable manufacturer will soon gain competitive advantage. Blockchain provides a more secure networking system, increasing resilience in times of uncertainty.
3. ***Customers:*** Intellectual property is protected, but customers gain access to organizational data. Increased availability of information and customer involvement promotes the design and delivery of more customizable products and services.
4. ***Financial Viability:*** After initial deployment, overhead costs are reduced through the use of blockchain's smart contracts. Collaborative optimization reduces redundant data and streamlines order processing.

Manufacturing has much to gain from the use of NFC, and stands to benefit even more from combining NFC in a blockchain-enabled, sustainable manufacturing process. NFC enables easy identification and tracking of components in a manufacturing process, allowing for highly tuned algorithms to further optimize these systems. For a truly sustainable end-to-end approach, Identiv offers eco-friendly NFC tags that have the lowest carbon footprint in the industry.

Securing the Internet of Things

The development of the IoT has exploded with improvements in wireless and RFID technology, including NFC. While the IoT opens opportunities for all kinds of smart devices, there are numerous concerns to secure a low-profile, distributed network. As both the volume and type of IoT-enabled devices increases, security problems for IoT networks have also increased in complexity.

One particular case study focuses on the addition of blockchain to a smart home IoT system to protect personal privacy. Each smart home in this study has a local blockchain that keeps sensitive personal information about the house and its occupants. The private blockchain is locally hosted on a hub within the house, with a low latency, low-resource scheme to maximize performance on IoT devices and home networks with limited computing power. This study aimed to reduce IoT's vulnerability to Distributed Denial of Service (DDoS) attacks, which bring down the network, and linked attacks, which expose personal information. For a holistic evaluation of system security, the team evaluated their blockchain-based IoT system against five requirements:

1. ***Confidentiality:*** Symmetric encryption keeps information only between the intended parties.
2. ***Integrity:*** Hashing maintains data integrity to detect when data has been altered.
3. ***Availability:*** Private blockchain limits the acceptable transactions between IoT devices and the central home hub.
4. ***User control:*** By logging transactions in the private blockchain, users can monitor and manage which devices can access specific information.
5. ***Authorization:*** Blockchain manages shared keys to determine which users and devices can interact on the smart home network

Introducing blockchain added a mere 20 ms to the communication time between IoT devices and a base station. With a nearly unnoticeable impact on performance, IoT systems in smart homes improved security across all five security requirements. Other research teams have generalized this approach to any number of IoT applications to provide similar benefits beyond personal home use.

What are the limitations of NFC and blockchain?

Although NFC and blockchain bring many security benefits, the cybersecurity landscape is constantly changing as new threats emerge. Further, there are many already identified shortcomings of both NFC and blockchain technologies:

- NFC is only relevant for physical devices; it is not applicable for strictly electronic communication. Thus, all the benefits of NFC tagging only apply to systems that have tangible products and services.
- Objects must be no more than four inches away to be picked up by NFC sensors. While this helps discourage remote hacking, a short range relies on precise systems that can consistently bring objects within a specified area.
- Tampering might require expert identification. Modifying, cloning, reapplying NFC tags can be problematic; however, researchers are working hard to prevent these issues.
- While blockchain is extremely secure – and with each additional block, becomes even more challenging to hack – it is still theoretically susceptible to manipulation. If a hacker was somehow able to simultaneously wrest control of at least 51% of the nodes in a blockchain network, the

hacker might be able to make changes without alerting other nodes. However, the computing power necessary for such a feat is so massive that most blockchain experts find a 51% attack extremely improbable.

- Known shortfalls of blockchain are sparse, but several groups have attempted to collect a list of known blockchain weaknesses, including the Common Weakness Enumeration (CWE) under the U.S. Department of Homeland Security.
- Each company and industry will face unique challenges in adopting blockchain. This has been a central focus of research, and techniques that promote smooth incorporation of blockchain across each industry are actively under investigation and early adoption.
- Both blockchain and NFC increase overall cost and overhead. While up-front investment is necessary, blockchain eventually drives cost down for individuals, public entities, and private companies.

In general, as supporting technologies continue to grow, blockchain and NFC will continue to flourish. Research in sensor fidelity, anti-tampering measures, and blockchain implementation will guide the path of NFC and blockchain systems.

How could I introduce NFC and blockchain to my team?

The combined strengths of NFC and blockchain can bring security and validity to a wide range of applications; research has already proven success by applying these technologies to IoT security, sustainable manufacturing, paper-based processes, and supply chain management. These four samples demonstrate refined user control, immutable ledgers, limited user access, and automated authentication that can be translated to any industry.

As blockchain and NFC technology is rapidly developing, partnering with a leader in these technologies will enable secure collaboration for scalable growth — in 2020, Identiv earned global recognition as a finalist for NFC Forum's Award for Most Innovative Use of NFC. We are excited to share our best practices and how our technology can fit your specific needs. Please contact transponder_sales@identiv.com or +1 888.809.8880 to start building a vision of your company's securely connected future.