Stamping Out Counterfeit Goods with Blockchain and IoT
Boston Consulting Group (BCG) is a global management consulting firm and the world’s leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

Cisco (NASDAQ: CSCO) powers the world’s Internet experiences. We securely connect people, processes, data, and things to enable innovation that benefits business and society. For more information, visit: http://thenetwork.cisco.com.
Stamping Out Counterfeit Goods with Blockchain and IoT

Akash Bhatia, Zia Yusuf, Usama Gill, Neil Shepherd, Maciej Kranz, and Anoop Nannra

May 2019
With blockchain and IoT, businesses now have an effective way to combat counterfeiting, a global problem that costs companies billions of dollars each year.

**COUNTERFEITING AFFECTS EVERY STAGE OF THE PRODUCT LIFE CYCLE**
Limited visibility across sourcing, manufacturing, and distribution networks makes it hard for manufacturers, partners, and customers to distinguish real goods from fake ones, leading to increased costs, stolen sales, reputational harm, and brand dilution.

**BLOCKCHAIN WITH IOT GIVES STAKEHOLDERS A SINGLE SOURCE OF TRUTH**
Combining IoT’s identification and tracing capabilities with blockchain’s tamper-proof chain of custody information allows manufacturers and stakeholders to verify provenance and differentiate between real and fake products at every point along the value chain.

**BLOCKCHAIN COUNTERFEIT PREVENTION DELIVERS SIGNIFICANT FINANCIAL BENEFITS**
Employing blockchain with IoT can give companies a net incremental benefit of between 2% and 5% of revenue by minimizing lost income from counterfeit sales, lowering service and compliance costs, and reducing reputational risks.
Our research suggests that blockchain with IoT could be a source of significant financial and competitive advantage.

Counterfeiting Exacts a Heavy Toll

Counterfeiting is a massive economic problem that results in billions of dollars in lost business revenues each year, and it exposes individuals and corporations to heightened health, safety, and even cybersecurity risks from fraudulent materials and defective parts. Within the global pharmaceuticals space, between $75 billion and $200 billion in counterfeit drugs are sold each year. In the electronics industry, fake parts cost component manufacturers about $100 billion annually. And in the European luxury goods market, about 10% of all items for sale are counterfeited, representing approximately $28 billion in lost value.¹

What makes the impact of counterfeiting so pernicious is its reach: fraudulent parts and goods affect every stage of the product life cycle—from the manufacturing floor to the point of sale, to the servicing function and beyond—driving up costs, eroding revenues, and damaging company reputations and brands.
Companies invest significant time and money tracking parts, validating provenance, communicating with partners, and filling out copious documentation to ensure the authenticity of their products, protect customers, and satisfy regulatory and compliance demands. The challenges—and the areas in which blockchain and IoT can help—extend across the three major stages of the product life cycle. (See Exhibit 1.)

1. **Procurement and Production**: Large manufacturers often lack the visibility needed to verify the authenticity of parts and raw materials and trace materials back to their source, a problem exacerbated by long, complex global supply chains, varying data and reporting quality across the vendor base, and a growing list of regulatory and compliance requirements. Fake and defective parts add risk and cost because the inadvertent use of counterfeit components during the manufacturing process can compromise product quality, leading to recalls, lawsuits, attrition, and long-term reputational harm. In 2012, US investigators determined that nearly 84,000 fake electronic components had been installed in US military aircraft and missiles by defense contractors. The defense contractor

---

**EXHIBIT 1 | Blockchain with IoT Fights Counterfeiting Across the Product Life Cycle**

<table>
<thead>
<tr>
<th>Procurement and production</th>
<th>Sales</th>
<th>After-sales and support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppliers</td>
<td>Manufacturer</td>
<td>Channel partner</td>
</tr>
<tr>
<td>Counterfeiter</td>
<td>Third-party retailer</td>
<td></td>
</tr>
</tbody>
</table>

**Traditional process**
- Manufacturer’s inability to identify counterfeit parts/raw material leads to product issues
- Lost sales due to counterfeit product sales; retailer/customer unable to identify counterfeits
- Burden of service/support for counterfeits

**With IoT**
- IoT makes identification of genuine products easier, but doesn’t completely eliminate the problem
- IoT sensors can be duplicated/tampered with
- IoT data not trustworthy/immutable
- Lack of common platform; granularity of IoT data not sufficient to establish chain of custody across stakeholders

**With IoT + blockchain**
- Counterfeit materials/parts rejected
- Counterfeit sales prevented
- Service/support for counterfeits denied

**Source**: BCG analysis.
that supplied the parts had purchased them from a US-based company, not realizing that the vendor had procured them from China in violation of US Department of Defense rules.

2. **Sales:** Cleverly manipulated labels and reverse-engineered products can make it difficult for consumers and corporations to spot counterfeit goods and for manufacturers to prove provenance. In consumer goods, the problem is made more challenging by the rapid growth of third-party and online retail channels. These channels make it easier for bad actors to get products to market and harder for legitimate brands and retailers to track illicit activity. Between 2016 and 2018, for instance, more than 385,000 pairs of counterfeit Nike Air Jordan sneakers were shipped to the US from overseas sources, resulting in $70 million in lost revenues for Nike. In durable goods, aerospace, and industrial machinery, uncertain provenance can cause significant downtime if counterfeit products are determined to have entered the service chain and need to be tracked down and replaced. Many counterfeiters also target aftermarket goods, taking advantage of the fact that it’s easier to evade detection in secondary markets. Aside from lost revenues, brands can suffer reputational harm when customers buy what they believe are genuine parts but are disappointed when the inferior substitutes don’t work as expected.

3. **After-Sales and Support:** Counterfeits can lead to spikes in service requests, unnecessary and costly replacements, and skewed customer satisfaction figures. Invalid support requests not only consume time and budget, they make it hard for a company to isolate and address genuine problems in a timely fashion. Brand issues are also at stake. With the knowledge that a product is counterfeit, a company could still entertain the related service requests—in the spirit of providing a superior customer experience—and explain the reason for the service issue to customers in order to safeguard the company’s reputation.

**Blockchain with IoT Tracks Product Genealogy End to End**

IoT provides unique identification and traceability, and blockchain provides a tamperproof chain of custody information. Pairing them can create a shared, distributed ledger capable of recording the origin, location, and ownership of raw materials and products at each stage of the value chain—giving manufacturers, partners, and customers the transparency and authentication they need. Blockchain with IoT, because of its ability to immutably track and share genealogy across multiple stakeholders, can inhibit counterfeiting in ways that traditional technologies cannot.

To thwart counterfeiting, suppliers and manufacturers join a single blockchain platform and use “smart tags” (unique cryptographic identifiers) to track and confirm the provenance and location of each item. The tags can take a variety of forms, including security labels with unique QR codes, RFID, and digital tags that contain an individualized software component. Subtle, deliberate physical imperfections on metallic or ceramic surfaces create distinctive signatures and can serve the same purpose. Smart tags and related marks can be applied to a single item or to a batch. To manage authenticity, only genuine, verified tags and products should be entered onto the blockchain. Entering them early in the manufacturing process allows each
tagged item or batch to be tracked at every stage along the manufacturing, shipping, distribution, and sales journey. Relevant data is logged at each step.

Although no solution can be fully foolproof, smart tags capture the complete genealogy of a product and are hard to replicate. Counterfeit tags won’t show up on the blockchain, for instance, and if a smart tag is somehow duplicated, a quick scan of the blockchain will indicate when and where the genuine item was manufactured and sold, thus revealing the duplicate item as a fake. In addition, when a product comes in for repair, support teams can use the smart tag to confirm legitimacy (and even ownership if that data is recorded). Front-end applications built on top of the platform allow stakeholders, including regulators, to digitally trace the entire chain and confirm the authenticity and origin of each part or good.

**Better Counterfeit Detection Delivers Clear Financial Benefits**

Looking again at the three main stages of the typical product life cycle, we explored how improved tracing and authentication combined with a tamperproof chain of custody could reduce counterfeiting and associated losses. Our analyses determined that blockchain with IoT can improve operational and financial performance in the following ways. (See Exhibit 2.)

- **End-to-end oversight of raw materials reduces product defects.** Because blockchain with IoT serves as a single, immutable source of provenance data, companies can prevent defects due to fake parts and cut down on the labor spent validating materials and satisfying regulatory requirements. When a product shows up at a warehouse and when it leaves are recorded in a verifiable event log that is easily accessible to all stakeholders. Manufacturers and suppli-

---

**EXHIBIT 2 | Blockchain with IoT Can Increase Revenue and Reduce Costs**

<table>
<thead>
<tr>
<th>Lever</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Counterfeit raw materials/parts rejected</td>
<td>Establish single version of truth to track irregularities and detect counterfeit raw materials from suppliers, reducing product defects, lawsuits, and brand damage</td>
</tr>
<tr>
<td>2 Counterfeit product sales prevented</td>
<td>Prevent counterfeiting and the resulting loss of legitimate sales by using IoT sensors to immutably record (in the blockchain) the origin, location, and ownership of goods across the value chain</td>
</tr>
<tr>
<td>3 Service/support for counterfeits denied</td>
<td>Enable access to time-stamped, immutable chain-of-custody information on the blockchain to identify counterfeit products and deny service requests</td>
</tr>
</tbody>
</table>

Source: BCG analysis.
ers can use the blockchain platform to authenticate items, flag deviations from agreed-upon sourcing arrangements, and prevent defective and inferior components from entering the production system. The improved visibility safeguards customers and protects the company from the risk of recalls, lawsuits, and reputational damage, while lowering operating costs.

- **Smart tags coupled with blockchain reduce the likelihood of fraudulent sales.** Smart tags and blockchain allow manufacturers, channel partners, third-party retailers, customers, and regulators to verify a product’s authenticity as goods move through the value chain, making it harder for counterfeit goods with adulterated labels to escape detection. Real-time authentication ensures that the preponderance of sales and revenues goes to legitimate brands and manufacturers. Regulators can digitally trace the provenance and chain of custody for any product being sold.

- **Better tracing helps support centers prevent unnecessary servicing and repair.** Front-end applications linked to the blockchain platform make it easy for support representatives to verify whether a claim is genuine, even without seeing the product. Faster and more accurate authentication allows support personnel to direct more of their time and resources to legitimate, high-value purposes, improving responsiveness, reducing waste, and increasing customer satisfaction.

**Net Financial Benefits Range from 2% to 5% of Revenues**

To study the potential cost and revenue impact of improved counterfeit detection, we looked at the same hypothetical example we studied in our supply chain article: a $1 billion electronics equipment company that manufactures its products in China and sells through channel partners and third-party retailers in the United States. Our modeling assessed two scenarios: an aggressive one in which the company reaped significant returns from blockchain-enabled improvements and a conservative one that delivered a more modest impact. We then averaged the results.

Our analyses determined that preventing fraudulent materials from entering the manufacturing cycle would help the company reduce failure rates and the cost of replacing defective parts and improve support center efficiency. The cost savings would result in an average net benefit of 0.08% of revenue. Far and away the greatest benefit from blockchain-enabled authentication, however, would come from stemming sales losses. Our research found that electronics and technology companies lose between 4% and 7% of revenue annually to counterfeit transactions. By using blockchain with IoT, businesses could reduce the number of fraudulent sales by 60% to 80%, allowing the electronics manufacturer in this case to recoup an average of 3.85% in associated revenues, with the total net benefit ranging from 2% to 5% of revenue. (See Exhibit 3.) The average net impact for our $1 billion electronics company translates to $33 million. The impact could be even greater for businesses whose products face greater counterfeiting exposure, such as pharmaceuticals and luxury goods. Beyond the quantitative benefits, improved counterfeiting detection would also help the company generate significant intangible value through improving regulatory compliance, safeguarding the customer experience, and protecting the brand.
Benefits Will Vary

Not all businesses or industries face the same exposure to counterfeiting; the severity and magnitude of the impact depends on a number of factors. To determine the return on investment from a blockchain-with-IoT counterfeiting solution, companies first need to look at their product characteristics, supply chain composition, and market risk.

High-value products, especially those that can be forged relatively quickly and sold at a premium (for example, designer bags), are most vulnerable to counterfeiting. Stemming that activity would help protect the brand and the top line. But companies also need to consider that some products have a higher likelihood of voluntary counterfeit purchases. Where price and prestige are high, such as with a popular handbag or sneaker, some customers may choose to buy knockoff versions, reducing the value of tools that help establish provenance. To evaluate the overall cost-benefit of a blockchain solution, companies must look across key markets and segments and examine buying behaviors and channel characteristics.

The size and complexity of the supply base is another consideration in weighing the ROI of blockchain with IoT. Companies that have large and diverse supplier networks are more likely to benefit from provenance and chain-of-custody information than are companies whose products and raw materials are tightly controlled internally.

**Sources:** BCG research and analysis; Statista; Warrantyweek.com.
Market risk is a third factor. Some businesses, such as medical-equipment makers, pharmaceutical companies, and food and beverage entities, have a strong fiduciary responsibility to ensure product safety and reliability (consider, for example, Chipotle’s food safety issues, which started in 2015 and wiped out almost 65% of the company value). The ability to rapidly, continuously, and accurately authenticate parts and raw materials across the product life cycle carries profound implications—helping safeguard the public and the brand. Here, a blockchain-with-IoT solution has the potential to generate significant value. However, in situations where counterfeit products and materials are easily identified by their performance, look, or feel, the benefits of a blockchain solution are less clear.

In many cases, knowing that you have the “real deal” in terms of product authenticity will be a real deal in economic terms, but businesses need to run the numbers on the tangible and intangible value that blockchain-enabled counterfeit prevention can deliver and compare that to the cost of implementation.

Blockchains give manufacturers something they have long sought: an effective, scalable means of combatting the risks posed by counterfeit parts and goods. By pairing blockchain with IoT, stakeholders across the value chain can ascertain whether a component or a product is legitimate, where it was sourced, how it was transported and stored, and if it was previously sold. Success requires building a substantial adoption base within a given industry or supply chain, an effort that can benefit from having a large player or industry leader at the helm. Use cases and technologies are evolving as blockchain platforms become more mature and enterprise solutions become more readily available. Our analysis suggests that the potential benefits for most companies will far outweigh the early-stage setup efforts. Manufacturers that embrace blockchain-enabled counterfeit solutions will have a powerful tool to safeguard their customers, protect their revenues, and ensure stronger bottom-line returns for years to come.

Note
About the Authors

Akash Bhatia is a partner and managing director in the Silicon Valley office of Boston Consulting Group and the global lead for BCG’s Internet of Things topic in the Technology, Media & Telecom practice. You may contact him by email at bhatia.akash@bcg.com.

Zia Yusuf is a partner and managing director in the firm’s Silicon Valley office and the global lead for its Internet of Things business. You may contact him by email at yusuf.zia@bcg.com.

Usama Gill is a principal in BCG’s San Francisco office. You may contact him by email at gill.usama@bcg.com.

Neil Shepherd is a principal in the firm’s Silicon Valley office. You may contact him by email at shepherd.neil@bcg.com.

Maciej Kranz is vice president of strategic innovations at Cisco Systems, the author of Building the Internet of Things, and a faculty member at Singularity University. You may contact him by email at mkranz@cisco.com.

Anoop Nannra is a director in the chief technology and architecture office of Cisco Systems, where he heads the company’s blockchain organization. He is also a co-founder and chairperson at the Trusted IoT Alliance. You may contact him by email at anannra@cisco.com.

Acknowledgments

The authors thank their BCG colleagues Vaibhav Malhotra and Sunny Sood, who helped conduct the supporting research for this report. We also thank Marie Glenn for writing assistance, as well as Katherine Andrews, Kim Friedman, Abby Garland, and Ron Welter for their contributions to editing, design, and production.

For Further Contact

If you would like to discuss this report, please contact one of the authors.