

By Greg Wood

APPLICATIONS OF BLOCKCHAIN TECHNOLOGY ON TRACEABILITY OF PARTS

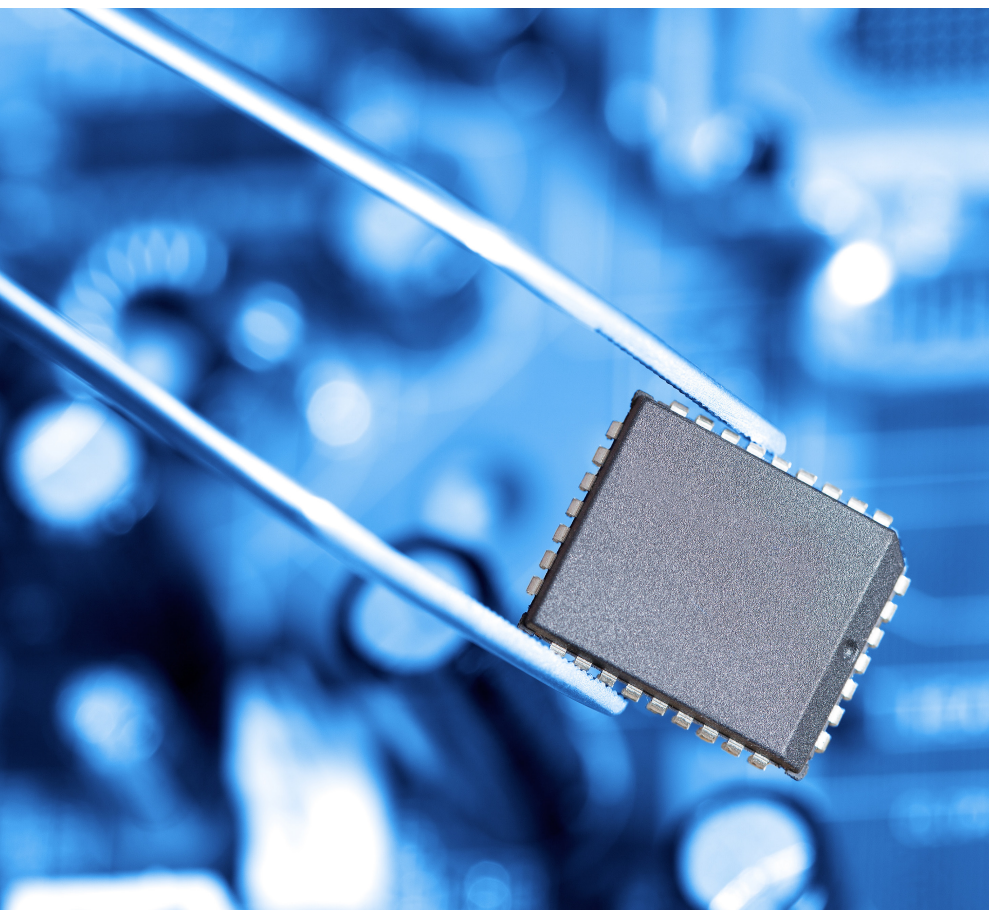
Can Blockchain improve consumer safety of electronic systems?

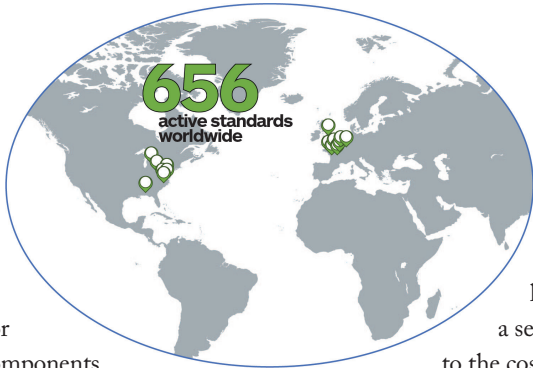
Traceability of electronic components and parts in the supply chain is imperative to medical, transportation, and energy industries; and now has widespread impacts in every industry. Consumer safety

cannot be compromised. Traceability was mandated to U.S. defense and government contractors to reduce counterfeit and substandard electronic components from getting into products and compromising mission success. As a result, starting in 2012 the U.S. government enacted the National Defense Authorization Act. Section 818¹ of this legislation and subsequent revisions require traceability of parts in the supply chain pushing responsibility for tracking components to distributors and component suppliers. Commercial companies now adopt and maintain traceability initiatives to prove their products are environmentally compliant and to ensure accuracy of export control reporting.

THE TRADITIONAL APPROACH TO TRACEABILITY

Traditional approaches to traceability of parts have focused on physical tagging to ensure part authenticity. Counterfeit standards documents developed by SAE, IEC, IPC and JEDEC have enabled companies to implement best practices and educate their employees. More than 600 individual standards have been developed and adopted globally and hundreds of technical books have been published to help address the topic.² Physical traceability included applying





plant DNA aligned in a tiny but tough epoxy dot affixed to electronic or mechanical components.

The DNA could then be analyzed for authenticity by end users via an optical barcode or potentially tracked and traced via a cloud-based digital DNA authentication process.

NEW APPROACHES MISS THE MARK

Another physical traceability technology emerging from DARPA is the SHIELD program or Supply Chain Hardware Integrity for Electronics Defense. The SHIELD program involves implanting an extremely small DIE or “Dielet” which is a self-contained mini circuit within the electronic component. The Dielet can be activated via an external probe which powers the device and receives an encrypted code. The encrypted code is then transmitted to the cloud by the probe, which then communicates with an external server to authenticate the device. An added feature to mitigate counterfeit attempts is that the dielet is easily destroyed should it be tampered with or attempted to be extracted.

These physical modifications to confirm authenticity of components

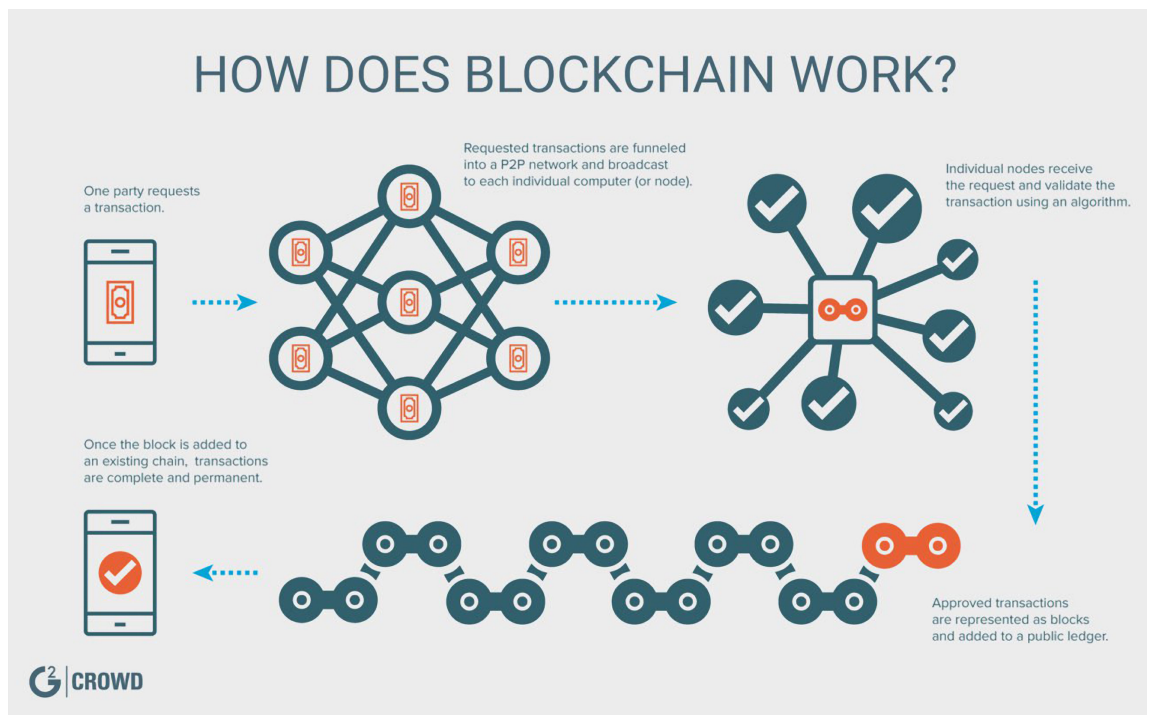
have worked well for the defense industry but have added up to a seven-fold increase to the cost of these

components over their nontraceable counterparts. The added traceability costs of these components make this approach impractical for commercial products where keeping costs down can be a requirement for product success.

COULD BLOCKCHAIN SOLVE THE TRACEABILITY DILEMMA?

What the electronic component industry needs is a reliable, virtual (digital), low-cost and secure solution for traceability, not just satisfying one requirement in isolation. The blockchain could be utilized for such a low-cost solution. The advantages of a virtual approach using cryptocurrencies and the blockchain are:

- › **Global advantages:** Cryptocurrencies are global currencies and not tied to a traditional currency which is only valid for an individual country or region. The electronic component supply chain is global as design, procurement, manufacturing and product sales almost always involve multiple countries.
- › **Authentic traceability tag:** With each electronic component transaction in the supply chain, a very small monetary transaction can act as a traceability element back to the authorized distribution channel and eventually the device manufacturer.
- › **Low cost:** For each production run by the manufacturer, each component would have a traceability identifier included in the cost. Distributors and brokers could recoup the tiny



traceability cost when they sell the component to the next distributor in the supply chain with the end user paying the tiny traceability amount for the parts they need. The advantage to the end user to incur this cost is that parts with traceability could be confirmed as authentic and worth the small extra cost, as low as 9 thousandths of a penny.

› **Counterfeit mitigation:**

Since the transactional information for the blockchain is not stored in a central location, but spread across many computers, the traceability would be less susceptible to hacking and would make counterfeiting of blockchain traceability much more difficult. Counterfeiters would not be incentivized to ship counterfeit parts because of the authentic traceability in place.

be able to understand remaining authentic components in the market and would be able to value their remaining stock appropriately.

VIRTUAL TRACEABILITY SOLUTIONS STILL FACE CHALLENGES.

Some of the challenges of a virtual traceability solution being debated today include:

› **Adoption:**

Perhaps the biggest challenge would be adoption by the various players in the electronic component supply chain. Manufacturers or distributors would need to provide information on parts produced and potentially related environmental compliance and export control/country of origin information.

would need to be modified to ensure adoption.

WHO WILL PIONEER THE CHANGE?

In summary, blockchain technology could be the global mechanism to track authentic parts and provide companies with confidence that their products will operate safely within designed reliability parameters. There are a wealth of tangible, financial and quality benefits from taking a blockchain technology approach while improving the safety of end consumers (businesses and individuals). However, available tools and protocols would need to be modified for the industry to gain adoption of this approach by all companies in the supply chain. Who will step up to pioneer the change? Will it be government that forces change—I doubt it unless there is a catastrophic event? Will it be the

“WHAT THE ELECTRONIC COMPONENT INDUSTRY NEEDS IS A RELIABLE, VIRTUAL (DIGITAL), LOW-COST AND SECURE SOLUTION FOR TRACEABILITY...”

— Greg Wood, IHS Markit expert

› **Access to industry data:**

Environmental compliance information such as component RoHS and REACH could be included in the traceability information and potentially used to prove product compliance. Country of Origin for the final assembly location could assist end users with export compliance reporting.

› **Availability to limited supply:**


For discontinued components, a traceability approach using the blockchain could allow end users to locate remaining inventories of authentic components. Stocking distributors would also

› **Traceability:**

Although complete transactional traceability of components in the supply chain would be beneficial to end users, mid-tier distributors would not be in favor of identifying their source to their customers because their customers could source components higher in the supply chain and damage future business.

› **Tools and protocols:**

Tools and protocols would undoubtedly need to be modified and tailored for the complex information requirements of the electronic component industry while traceability information

OEMs placing mandates on their supply-chain—it’s a tough tight-wire decision of cost, safety and ROI? Will it be the component manufacturers—possibly because this could be a unique way to add value and differentiate? But every stakeholder (participant) in the supply chain (a newly defined blockchain) will have to commit to change. 

REFERENCED SOURCES:

- 1 Government Publishing Office – National Defense Authorization Act for FY 2012, Sec. 818, December 2011
- 2 Research conducted in Engineering Workbench from IHS Markit, April 2018
- 3 Blockchain explained: It builds trust when you need it most; CNET, February 2018