Proceedings of the ASME 2023
Manufacturing Science and Engineering Conference
MSEC2023
June 12 – 16, 2023, New Brunswick, NJ

DRAFT MSEC2023-105046

CYBER-PHYSICAL TRUST ANCHORS IN ADDITIVE MANUFACTURING: SECURE, LOW-COST, AND EDUCATIONAL

Michele Maasberg[1,*], Brendan Birch[2], Daniel Janes[2], Kirsten Stor[2], Kyungmin Ham[3], Leslie G. Butler[3]

[1]United States Naval Academy, Annapolis, MD
[2]SIMBA Chain, Inc, Plymonth, IN
[3]Louisiana State University, Baton Rouge, LA

ABSTRACT

This abstract reports progress towards development of an educational strategy for cyber-physical trust anchors. The additive manufacturing commercial sector needs cyber-physical trust anchors to establish a secure supply chain, to detect counterfeiting and to ensure part provenance. However, the underlying technology of cyber-physical trust anchors spans several sectors ranging from mathematics, additive manufacturing, materials science, nondestructive evaluation, to cyber science. The fast and effective deployment of cyber-physical trust anchors requires an educational component. The lead author is skilled in the educational value of red team/blue team, an approach particularly well suited for friendly assessment of a secure supply chain procedure. We present a plan for the low-cost and safe instruction of cyber-physical trust anchors for classroom instruction or as a semester project. The anticipated outcome is an educational product suitable for interdisciplinary courses and for developing the workforce needed with cyber-secured physical supply chains.

Keywords: cyber-physical trust anchors, blockchain, education

1. INTRODUCTION

Recent executive level economic reports in the U.S. recognize the fragility of manufacturing supply chains [1]. Additive manufacturing improves manufacturing supply chain resilience due to increased speed and flexibility of production, lowering of barriers to entry for small firms, promotion of OEM/supplier collaboration, and expanding consumer access [2]. With the anticipated growth in additive manufacturing, security of technology and systems must be considered. New attack vectors unique to additive manufacturing have been identified in recent research. The taxonomy includes theft of technical data, illegal part manufacture, and sabotage, which are often conducted for the purpose of counterfeiting [3, 4]

*Corresponding author: maasberg@usna.edu

Counterfeit prevention is a primary defense for fraud related attacks in additive manufacturing systems [3]. A layered approach to anti-counterfeiting is required due to the increased sophistication of counterfeiters. For example, U.S. currency includes a number of features for authentication and tracking. Consider the US $100 currency and its serial number and the other identifying features: special paper, printing, 3D security ribbon, security thread, and more, as shown in Fig. 1 [5]. Furthermore, let us assume that features such as the security thread have orientations and positions that are both random and unique, e.g., each $100 currency has its own fingerprint. The fingerprint uniquely identifies each bill and facilitates counterfeit detection and provenance for $100 currency.

FIGURE 1: TRUST ANCHORS IN US $100 CURRENCY

This concept can be extended to digital fingerprints and additively manufactured parts. Let us consider the serial number of a $100 bill as mapping to a cryptographic hash, and the other features as mapping to a perceptual hash. Furthermore, let us postulate that as the currency passes through the banking system, both the serial number and security features are read and analyzed. Thus, counterfeit currency is detected by non-existent serial numbers or security features that do not correspond to that particular serial number. Is it possible that a counterfeit part could be identified by non-existent or modified hashes?

How do we transfer the security features of currency to additive manufacturing? Moreover, how do we educate the many stakeholders in the supply chain?

The purpose of this research is to develop a low-cost, secure implementation of cyber physical trust anchors for additive manufactured parts with a multidisciplinary approach to integration in university level educational practices. Research in education improves critical thinking, analysis, advances knowledge, and promotes development of employer desired skills. The target audience for this paper are educators. This paper is not a finalized lesson plan, but rather a rough draft or storyboard for educators in disciplines and skills including mathematics, additive manufacturing, X-ray nondestructive evaluation, cyber science, and logistics.

The remainder of the paper is outlined as follows. In sections 2 and 4, we discuss trust anchors and their development in the context of standardization and additive manufacturing. In sections 5-7, we introduce the multidisciplinary technology elements in the cyber-physical trust anchor and their integration into undergraduate projects. In sections 9,9.2 and 10.2, we assess and summarize the technology before integrating blockchain and security testing in sections 9.1, 10.1, and 11. Finally, we conclude the study with limitations and future research, section 12.

2. TRUST ANCHOR AND NIST.IR 8419

A number of empirical studies on anti-counterfeit and provenance techniques have been published. The benefits of counterfeit prevention in additive manufacturing have also been recognized by government and industry in emerging standards. Recent security standards recommend advanced methods for determining component authenticity, identification methods, and audit techniques for accountability [6, 13].

A NIST/MITRE working group released a report in April, 2022 entitled "Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives". The report described the critical features of a cyber-physical trust anchor, i.e., the physical aspect in an additive manufactured part and the data logged in a blockchain. It is apparent that the working group struggled to understand all aspects of the situation. For example, the proposed solution has a "one size fits all" structure, an approach not likely to be adopted across multiple supply chains. Hence, the need for education of the stakeholders through discussions such as this.

The authors have recently received NIST SBIR funding to develop cyber-physical trust anchors. We offer this as evidence of our expertise in the subject.

3. TRUST ANCHOR DEVELOPMENT

The additive manufacturing commercial sector needs cyber-physical trust anchors to establish a secure supply chain, to detect counterfeiting and to ensure part provenance. However, the underlying technology of cyber-physical trust anchors spans several sectors ranging from mathematics, additive manufacturing, materials science, nondestructive evaluation, to cyber science. In addition, a gap between academic research and industry implementation exists. The fast and effective deployment of cyber-physical trust anchors requires an educational component. Research in educational settings can bridge the gap by enhancing student learning and advancing knowledge. In this work, research and development of a trust anchor are integrated with university level educational practices for undergraduates.The following sections describe research and educational components for feature simulation, image processing, statistical analysis for similarity measures, printing hashes into an object, non-destructive evaluation, scanning, data linking, and vulnerability detection.

4. SIMULATIONS

Simulated features are generated starting with a base image, such as pebbles, which can be segmented into a number, on the order of two hundred, components. Multiple similar, but different parts are generated by randomly modifying some components. Fig 2 shows (A) the base image and (B) a modified image with the grayscale intensity values of ten pebbles changed as well as 20% speckle noise, rotation noise, and translation noise added to the base image. Fig 2D shows the normalized difference image. To explore the effect of image noise, Fig 2B is regenerated a total of 25 times, each time with different speckle noise, rotation noise, and translation noise.

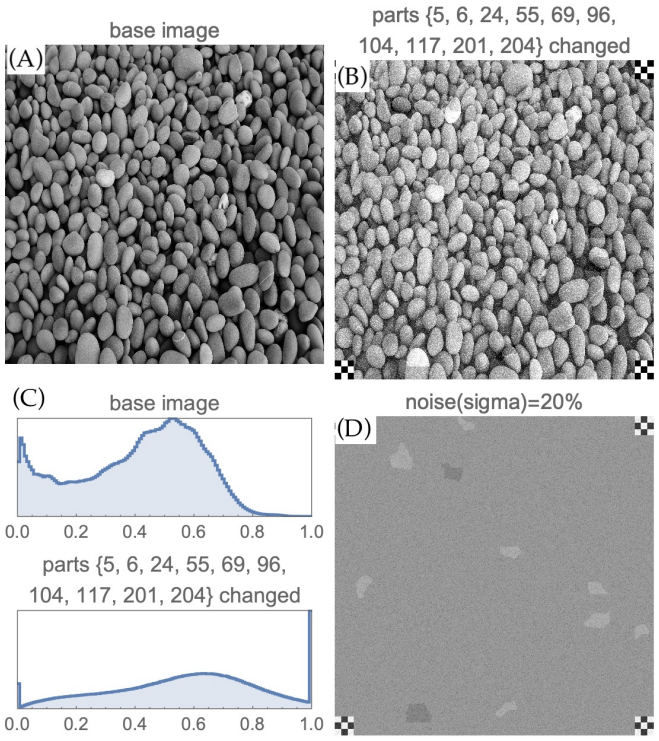

FIGURE 2: PEBBLE: SOURCE OF SIMULATED TEXTURES

Fig 2B is processed by a 2-D Fourier transform and selected coefficients are used to generate a perceptual hash; portions of the hashes for three different modified pebble images, each for the first noise pattern, are shown in Fig. 3. Not shown, due to space

1	-746.19	-993.80	-813.43	-666.20	-634.35	-619.38	-170.14	959.90
2	-589.55	-1217.6	-1075.0	-358.47	-276.39	-723.61	-259.49	864.05
3	-768.12	-1271.1	-850.70	-688.74	-591.26	-381.44	-83.09	1035.29

FIGURE 3: PERCEPTUAL HASHES FOR THREE UNIQUE MODIFICATIONS OF THE BASE PEBBLE IMAGE

limitations, is how the perceptual hashes for each part change with image noise. The effect of image noise will be shown graphically in the next section.

The perceptual hashes have these special features:

- Because of the deletion of some Fourier coefficients, the original image cannot be generated. The deletion is a one-way function.
- Each hash is valuable; each hash is a fingerprint to an item.
- We would like to know the "uniqueness" of the hashes.

5. DISTANCES, STATISTICS, AND FRACTALS

The perceptual hashes listed in Fig. 3 have 32 elements, thus can be treated as vectors in a 32-D space. As noted for Fig. 2B, 25 images are generated with different noise patterns, yielding 25 slightly different perceptual hashes. In 32-D space, these 25 vectors form a cluster. The cluster has a center and a radius. Fig. 4 is a histogram of distance of a hash from its center, measured over all 10 unique pebble configurations. The most probable distance is about 8 units in the 32-D space.

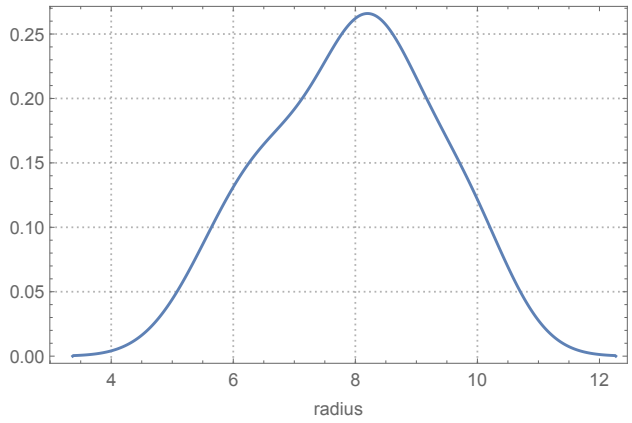

FIGURE 4: CLUSTER RADIUS

The 10 clusters are well separated in 32-D space. All of the pairwise distances are shown in Fig. 5. It is noteworthy that

	1	2	3	4	5	6	7	8	9	10
1	0	1330	1128	1117	1253	1047	1042	1176	1118	991
2	1330	0	936	1104	1183	805	1036	885	1073	1125
3	1128	936	0	956	1263	806	903	718	880	886
4	1117	1104	956	0	908	761	975	935	792	774
5	1253	1183	1263	908	0	1028	1121	1255	999	1141
6	1047	805	806	761	1028	0	619	809	680	843
7	1042	1036	903	975	1121	619	0	939	792	970
8	1176	885	718	935	1255	809	939	0	970	965
9	1118	1073	880	792	999	680	792	970	0	757
10	991	1125	886	774	1141	843	970	965	757	0

FIGURE 5: DISTANCES BETWEEN CLUSTERS

the shortest pairwise distance is many-fold larger than the cluster radius. If we could visualize 32-D space, the large cluster separation would validate the procedure for generating a perceptual hash from what appear to be visually similar pebble configurations.

One strategy for visualizing 32-D clusters is a principal component analysis, a procedure which finds linear combinations of the 32-coordinates which are dominant in 3-D space. A 3-D scatter plot after dimension reduction is shown in Fig. 6.

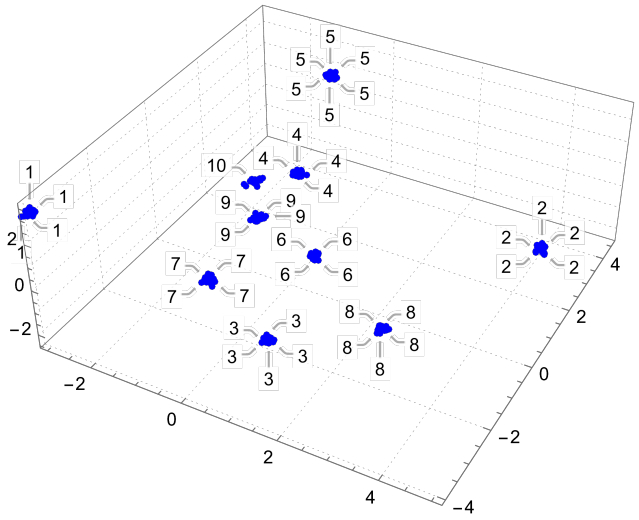

FIGURE 6: CLUSTERS IN N-D SPACE REPRESENTED IN 3-D SPACE

Assessment of additive manufacturing print quality and the ability of nondestructive inspection to measure print defects is conveniently assessed with regions spanning a wide range of sizes. Mathematically, a fractal is a structure easy to code and embed into a 3-D object. Here, we are using a Cantor dust fractal to embed cubic voids into a castle nut. The Cantor dust fractal in three dimensions is constructed, beginning with a cube, by recursively applying a replacement step. In this step, each edge of the cube is divided into three equal segments, resulting in a subdivision of the cube into 27 equal subcubes. All but the eight corner sub-cubes are removed from the original cube. This step is recursively performed on each remaining (smaller) cube, after which the Cantor dust fractal remains. In its interior, the castle nut has a Cantor dust fractal left hollow.

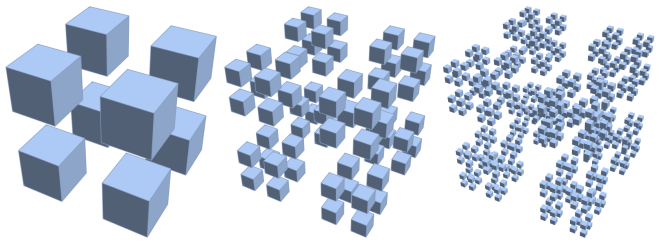

FIGURE 7: CANTOR DUST ORDERS 1, 2, AND 3 IN 3-DIMENSIONS

6. ADDITIVE MANUFACTURING

The embedded Cantor dust fractal has two trust anchor purposes. When the voids are larger than the AM print resolution, the voids demonstrate a method to reliably encode digital information within the part, the start of a cryptographic hash. When the voids are smaller than the AM print resolution, then variations print-to-print create a unique fingerprint for each part. The fingerprint can be converted to a perceptual hash. Also, the internal

surfaces of the large voids may have detectable roughness, giving another fingerprint for converting to a perceptual hash.

For the classroom, ordering polymer additive manufactured test objects from an online print service bureau is very convenient. In this section, we describe two examples of online orders. Note, these orders are given as examples and are not a recommendation of any specific vendor.

The additive manufacturing print files were constructed in a Mathematica notebook with region definition and boolean operations. Fig. 8 shows wireframe drawings of the castle nut regions, including the Cantor dust voids generated by a Boolean negation. The regions were then exported as STL files. The STL files were

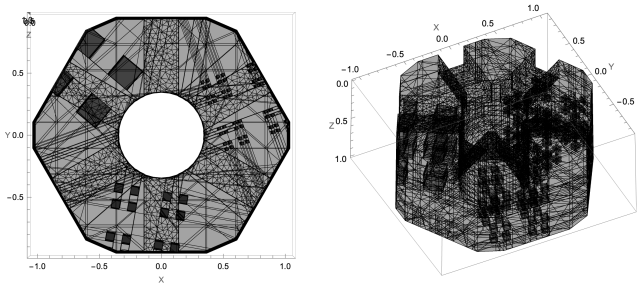

FIGURE 8: CASTLE NUT WITH EMBEDDED CANTOR DUST FRACTALS OF ORDER 1, 2, AND 3

inspected and repaired with MeshLab, an open source software optimized for STL viewing and editing[6]. A MeshLab repair of a Mathematica generated STL is usually simple and often corresponds to closing a hole in the STL triangulation mesh or deleting duplicate mesh structures.

Online orders were placed with Xometry [7] and Sculpteo [8]. The castle nut STL file was uploaded and its scale factor was adjusted to achieve a print size of 3 cm×2.8 cm×1.47 cm.

Xometry offered the stereolithography print technology with a material called *Accura ClearVue*, a polycarbonate-like material. For the X-ray attenuation calculation with NIST XCOM, the material was simulated with an empirical formula of $C_{15}H_{16}O_2$ and a density of 1.2 g/cm^2.

The X-ray data quality can be increased by matching the part size with the capabilities of the X-ray CT scanner. This requires an estimation of the X-ray attenuation based on the chemical composition of the print material and the X-ray energy of the CT scanner, here 70 kVp, corresponding to a peak intensity at 40 keV.[1] The NIST XCOM website is recommended for attenuation calculations.[9] The calculated X-ray transmission is about 50% for 3 cm polycarbonate at 40 keV.

Sculpteo offered a print option with the tradename of *PolyJet* and a material called *VeraClear*, a material with a bulk composition near that of poly(methyl methacrylate) (PMMA) and also containing an unspecified photoinitiator. For X-ray attenuation calculation, the material was simulated as PMMA with an empirical formula of $C_5O_2H_8$ and a density of 1.18 g/cm^2. The calculated X-ray transmission is about 50% for 3 cm PMMA at 40 keV.

[1] kVp = kilovolt peak. keV = kiloelectronvolt

A total of six castle nuts with embedded voids were printed at a cost of $320 with just over one week from STL upload to part delivery. A photo of the castle nuts is shown in Fig. 9.

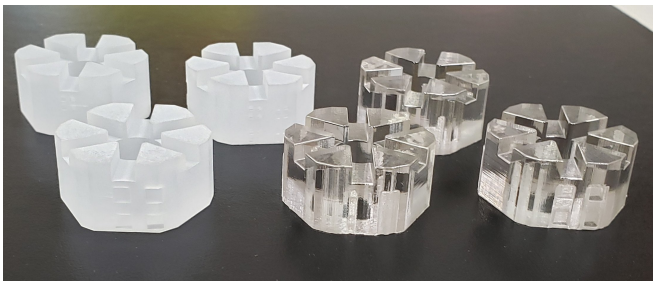

FIGURE 9: CASTLE NUTS PRINTED BY STEREOLITHOGRAPHY (L) AND POLYJET (R)

7. X-RAY NONDESTRUCTIVE EVALUATION

For the classroom, X-ray CT scanning is a rarely encountered, but it is a valuable skill and the instrumentation is often locally available. Here we give an account of using an X-ray CT scanner at a local school of veterinary science.

An introduction to X-ray tomography for materials science applications is available at the University of Texas, High-Resolution X-ray Computed Tomography Facility (UTCT) [10]. UTCT will also perform CT scanning as a service or as a research collaboration. HINT: Scanning costs can be reduced by stacking and taping multiple parts into a single unit.

Two more advanced discussions discuss metrology and the combination of X-ray and neutron tomography. Metrology can reveal density variations and porosity distribution[11]. The combination of X-ray and neutrons allows the examination of hydrogen in the presence of high atomic number elements, such as water flow through concrete[12]. The data volume can be overwhelming, leading to use of machine learning for data analysis; 460 X-ray tomography volumes of bread dough were processed with a U-Net model to extract cell wall thickness, cell shape, void fraction, crumb brightness, and fineness for doughs made with Australian wheat.[13]

Tomography scan was done with SCANO Medical MicroCT 40 with the X-ray tube operated at 70 kVp, 113 μA. The magnification from the cone beam X-ray geometry yielded an effective voxel size of 18 μm. Samples were held in poly-ether-imide tubes with internal diameter of 36 mm, i.e., the largest sample must have an outer diameter less than 36 mm.

Scan time was 2 hrs per castle nut; three castle nuts were placed in the sample tube, separated by styrofoam and scanned sequentially from top castle nut to bottom castle nut, Fig. 10. Then, the stack was scanned again to give duplicate tomography volumes for data analysis. The instrument cost rate is $5-hr without an operator and $20 hr with an operator. For this project, one of the authors operated the CT scanner; the twelve scans of the six castle nuts cost $120.

The SCANO CT scanner outputs data in either 16-bit unsigned integer DICOM or 8-bit unsigned integer TIFF; the 8-bit

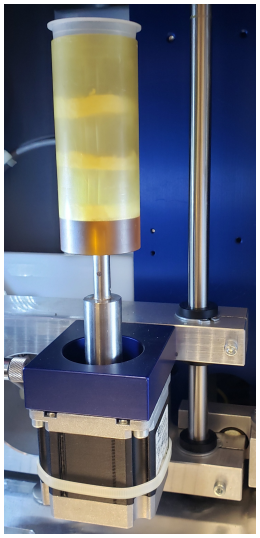

FIGURE 10: THREE CASTLE NUTS MOUNTED FOR TOMOGRAPHY.

resolution format has insufficient intensity resolution for perceptual hash generation. DICOM is an image format optimized for clinical applications. The open source image processing program ImageJ [14] can be enhanced with a plugin to read DICOM format images. The related open source program Fiji [15, 16] includes the DICOM plugin. For compatibility with other program languages such as Matlab, we use Fiji to convert DICOM to 16-bit TIFF.

We have also found that selective laser melting AM printing of the Cantor dust voids in a castle nut can be done with an EOS M290 in stainless steel. The stainless steel castle nut then requires tomography at 450 kVp. Fig 11 shows the stainless steel castle nut in its build direction; traces of overhand can be seen in on the upper surfaces of the voids. The randomness of the overhang make each part unique, and the internal position makes counterfeiting extremely difficult. The conversion of the overhang structure into a perceptual hash starts with a line profile, the yellow line in Fig 11A, to select a line of values proportional to X-ray attenuation. The colormap is adjusted to show zero X-ray attenuation as black and high X-ray attenuation as white. A plot of grayscale intensity values selected with the yellow line is shown in Fig 11B.

The highlighted line plot in Fig. 11B can be converted to a perceptual hash via multiple procedures, where the metrics are minimal sensitivity to imaging noise while retaining sensitive to the detailed structure in the part, in this case the overhang features characteristic of selective laser metaling of stainless steel powders (update for the polymer stereolithography and polyjet). With simple scaling and interpolation, the highlighted line plot in Fig. 11B becomes a 32-element perceptual hash, the black squares in Fig. 12.

8. MID-COURSE ASSESSMENT

It is time for a review session. The essential concepts for the cryptographic and perceptual hashes are:

- Cryptographic hash: The part's serial number, Fig. 1, is encoded. Cryptographic hash comparisons yield true-false.
- Perceptual hash: The part's details, Fig 2B, are encoded, Fig. 3. In multi-dimensional Euclidean space, a distance between hashes can be defined.
- Perceptual hash in multi-dimensional Euclidean space form clusters. With dimension reduction, the clusters are visible in 3-D space, Fig. 6.
- As a guide to the reader, Appendix Table 1 contains terms and definitions used in the cryptography field.
- In multi-dimensional Euclidean space, the clusters have defined radii, Fig. 4, and center-to-center distances, Fig. 5.
- The metric for perceptual hash success depends on the 1:1 matching uniqueness, Fig. 1, not the 1:N matching problem.

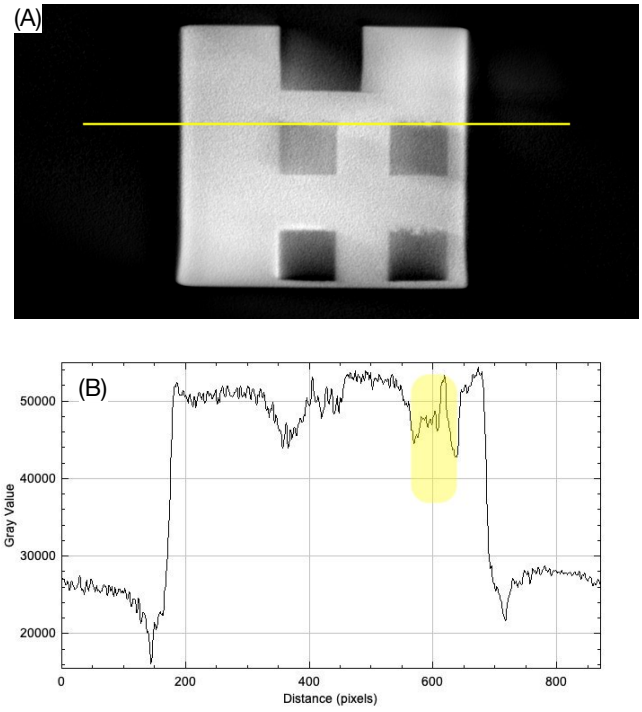

FIGURE 11: STAINLESS STEEL CASTLE NUT TOMOGRAPHY AT 450 KVP

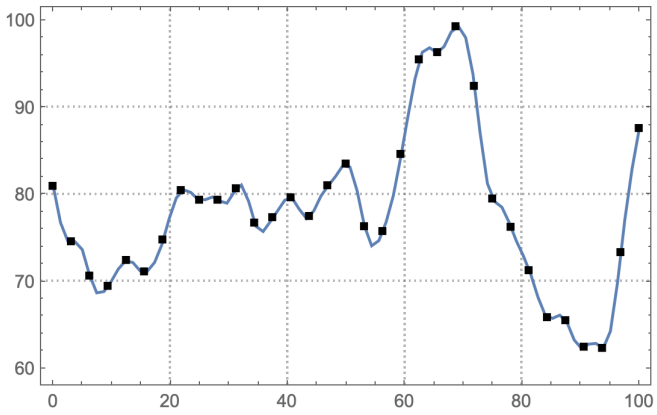

FIGURE 12: PERCEPTUAL HASH DERIVED FROM LINE PLOT

In Fig. 12, we show a perceptual hash obtained from X-ray CT of a real object. The CT shows the interior structure of a castle nut, and we intentionally created internal structure by creating voids in the object. So as to span a range of printer resolutions and X-ray CT resolution, the internal voids were created over a range of sizes derived from a Cantor dust fractal. We are asserting that the internal structure is unique to each part, is stable over time, and is extremely difficult to reproduce. Moreover, we are also asserting that read-out requires special knowledge about part orientation in the X-ray CT scanner and subsequent image processing.

Next, we register the part's serial number and perceptual hash in a secure database. In the next sections, we describe the characteristics of a secure database, and how the database security is enhanced with blockchain.

Safety: The use of commercial databases and blockchain in this class project is to be avoided. In the red team/blue team education strategy, we want the students, and educators, to have a safe environment. For this reason, the deployed database and blockchain will involve simple python code and open source software running on local hosts in isolated environments, compliant with organizational security policies. Thus, if an attack is successful, no harm is done to real systems.

9. BLOCKCHAIN

The part's serial number and perceptual hash identify a part like a unique human fingerprint. X-ray imaging scans the part like biometric systems read human physical characteristics. Fingerprint sensors capture a digital image of a fingerprint pattern as a collection of extracted features and store for matching. Similar to biometrics, a part trust anchor is compared to a database of known hashes to verify the identity of the part. The logging of the part's serial number and perceptual hash is the digital registration process to enable authentication through comparison of credentials. For a part, the comparison of credentials occurs with the similarity matching. If the credentials are similar, the part is presumed to be authentic. Registration of parts requires a secure database with auditing capabilities. The logs must also be resistant to attackers hiding their actions.

Blockchain is an ideal technology for auditing and tracking. Each block contains the cryptographic hash of the previous block, timestamp, and transaction data. Since a cryptographic hash function is used for linking two nodes (i.e., each event is appended to the cryptographic hash of the preceding event), the integrity of events is ensured. The superiority of the technology for auditing and tracking is how the implementation of blockchain with bitcoin solved the double spending problem without a central server.

9.1 Blockchain - Classroom

The ability for students to explore the characteristics of blockchain is limited. The open source versions of blockchain applications, contracts, and wallets for testing security do not yet exist. However, a low-cost class project for building a basic blockchain can be done using Python 3.10 and open source software (i.e., MySQL, Flask, and similar) for an off chain database and web interface. The benefit of programming their own blockchain is enhancing their knowledge of it and identifying basic security issues.

To meet the objectives of a class project with a red team/blue team exercise, an isolated, wholly-owned implementation of blockchain is needed. Fortunately, several python tutorials are published with codes purporting to have blockchain examples. At this writing, we are still in the process of evaluating these codes. Interestingly, many programs are simple and as short as 60 lines of Python (i.e., [17] and [18]). We are seeking an implementation that demonstrates immutability, hashes, proof-of-stake versus proof-of-work, and on-chain data. Other code examples to be considered have been posted by the Free Code Camp, Section, and on GitHub [19, 20].

9.2 Blockchain - Professional

The previous section describing 60-lines of Python code to create a blockchain is just an introduction to the many features and capabilities. SIMBA Chain's chief scientist and CTO, Dr. Ian Taylor, is well published on the varied applications of blockchain.[21–23]. A commercial implementation of blockchain, such as created and deployed by SIMBA Chain, will have these additional features. The following is a high level overview of blockchain along with terms and technologies commonly mentioned in the blockchain/web3 space today.

Blockchain is the name of the technology at a high level[24]. It is more of a catch-all term for different technologies in the space. It is more correct to say that blockchain references a field/specialty rather than a single thing. It's like saying "database" or "API server", which may refer to a single entity but more often is used to refer to categories of things or features that one would expect to be associated with those technologies but don't strictly fall under the definition of the term being used. A basic feature of blockchains is that they are a *Read* and *Write* database. They do not support *Updating* or *Deleting* data. Once something is on "The Blockchain" (or an equivalent would be "in the database"), then no single person or entity can delete it or change it assuming the blockchain network is sufficiently distributed and decentralized enough. It's like writing in ink, so to speak. The immutability of Blockchain is positive factor for its inclusion in the secure supply chain.

Bitcoin is a Crypto Currency on the Bitcoin network. The "Bitcoin Network" is regarded as the first modern Blockchain. The Bitcoin Network was intended only to transfer Bitcoins peer-to-peer, or Wallet-to-Wallet.

Wallets are how identity is handled on Blockchains. A wallet is analogous to a bank account and ID card combined together. If I wanted to send 1 BTC (Bitcoin, the actual Crypto Currency) to Brendan Birch, my co-author, I would need to know his Wallet Address. Essentially, a Wallet Address is the same thing as a bank routing number, but on the respective Blockchain Network and not in the conventional banking system.

There are multiple Blockchain Networks [25] or "Blockchains" in current usage, and none can natively talk or communicate with one another. All Blockchains are their own "Networks," and there is no "internet" to allow these independent "networks" to talk to each other. Some examples of Blockchain Networks are the "Bitcoin Network", "Ethereum Network",

"Polygon Network", "Cardano Network", etc. This independence will be a factor in the use of blockchains in secure supply chains.

Ethereum, or the Ethereum Network [26], was the first, and is the biggest, Blockchain to support Smart Contracts. Smart Contracts are programs that run on the Ethereum Virtual Machine (EVM) which is essentially a basic form of a computer that can execute programs on a distributed Blockchain Network. In this paper, when we refer to "the blockchain" in repects to the project, we are talking about the Ethereum Network or a private version of the Ethereum Network, such as ConsenSys' Quorum Netowrk, which is private and permissioned.

Smart Contracts are applications that run on certain Blockchains. Not all Blockchains support Smart Contracts. Bitcoin, for example, doesn't natively support Smart Contracts. Ethereum, and many other Blockchains, support Smart Contracts to be run on them though the EVM or other execution method. The special thing about Smart Contracts is that thanks to the Read and Write nature of the Blockchain, once a Smart Contract is "Deployed" it can never be changed. There are techniques and development patterns to "upgrade" smart contracts, but that involves deploying a new smart contract rather than completely replacing the previous smart contract.

10. SECURE DATABASE

10.1 Secure Database - Classroom

A secure off-chain database contained within the classroom is needed to allow safe red team attacks. Therefore, a MySQL or similar database, a simple web interface, and Python 3.10 are suggested to develop a simple database to store part serial numbers and corresponding perceptual hashes as well as ancillary data for project development, data such as AM print parameters and X-ray inspection. There are a number of sources for python code for a simple database, such as FreeCodeCamp [27] and RealPython [28].

10.2 Secure Database - Professional

At the professional level, SIMBA Chain recommends *Firebase*, an app development platform from Google that allows users to build and deploy web and mobile apps with relatively little difficulty. The reasoning behind *Firebase* apps for advanced user projects is that, while SIMBA Chain allows for quick and easy deployment to blockchain, it is helpful for users to have a user-configurable interface that they can use to then interact with the blockchain, without those users having knowledge that SIMBA Chain is running in the background. Hence, the *Firebase* app provides a layer that allows users to communicate with our deployed smart contracts, while abstracting away the SIMBA Chain layer. Firebase provides a very valuable added benefit of allowing us to deploy serverless code: code that lives on Google's servers, which we access by calling Google cloud functions that are written in *TypeScript*. Of course, the *Firebase* app and the corresponding *Firestore* database reside on Google servers, and thus are a highly inappropriate subject of red team attacks. In addition, such attacks will be unsuccessful and not yield the educational value of a weaker, in-class database.

11. SECURITY TESTING - RED TEAM/BLUE TEAM

Security testing is performed during cyber-physical trust anchor development to identify and test potential vulnerabilities. A large scale system or organizational level approach (i.e., NIST Risk Management Framework) is not well suited for a small technology prototype with limited resources in an academic atmosphere. However, results from security testing can inform control development and follow-on comprehensive assessments [4, 29]

A technique well suited for a new technology prototype in a low risk setting is the red team/blue team approach. Red team exercises can identify and test vulnerabilities with technology based attacks simulating real world conditions. The results are used to correct the deficiencies. In a classroom setting, the red team simulates a potential adversary and conducts mock attacks on the cyber-physical trust anchor. The blue team objective is to defend against and respond to the simulated attacks.

A classroom project is envisioned around counterfeiting. A controlled environment and review of rules (i.e., organizational security policies) is provided. The topic is then provided. A cyber-physical trust anchor with a 32-D perceptual hash stored on blockchain makes counterfeiting impossible, right? Let's pretend we are on a red team. What are our initial attack vectors?

The red team is given scenarios for simulated attacks, such as the following:

Authentic or counterfeit? During the exercise, the red team presents a series of parts to the blue team to authenticate. Some are counterfeit, and some are authentic. The blue team must identify counterfeits and prevent their entry into the system.

Blacktopping: The red team introduces an end of life part into the system at some point during the exercise. The blue team must prevent the re-entry into system.

Production overrun: The red team presents an extra part that was printed outside of a legitimate order. Can the blue team detect it?

Anchor extraction and sabotage: The, red team dissects a part, physically extracts the trust anchor and inserts into a sabotaged part. Now red teams has two parts with authentic trust anchors and one is sabotaged. Can the blue team detect it?

Lost part: Red team simulates a customer with a lost part and request to make another. The intention is to sell the duplicate parts. The blue team must defend against part duplication.

Packet sniffing: On the path from X-ray image analysis to database, can the red team capture the serial number and perceptual hash?

Injection attacks: Can the red team successfully execute an injection attack?

Denial of service: Can the red team successfully compromise the website or resources related to the blockchain or database?

Unauthorized access: Can the red team gain access to the blockchain or database?

Data modification: Can the red team insert new entries into the database, entries which contain bogus serial numbers and perceptual hashes?

Blue Team: The scenarios are not disclosed to the blue team. The blue team's job is to anticipate attacks and envision mitigation techniques.

Attacks often have unusual access patterns. Based on this observation, a cluster analysis method has been proposed for blockchain attack identification, a contribution developed by the SIMBA Chain chief scientist, Dr. Ian Taylor.[21] It is interesting to note that cluster analysis, introduced in section 5, now comes back to aid the blue team.

12. CONCLUSIONS

A sketch of a class project for exploration of cyber-physical trust anchors is presented. The students can use popular software such as Mathematica and open source software such as MeshLab and ImageJ/Fiji to create and inspect physical objects and generate cryptographic and perceptual hashes. Unfortunately, the student's ability to explore the blockchain features are, at this time, limited. The open source versions of blockchain applications, contracts, and wallets do not yet exist. The 60-line python blockchain code provides a demonstration, but advanced features such as wallets and smart contracts are, at this time, lacking in the open source software.

ACKNOWLEDGMENTS

We gratefully acknowledge the support of the National Institute of Standards and Technology, U.S. Department of Commerce in providing the SBIR support for this project, as well as the U.S. National Science Foundation under grant number OIA-1946231 and the Louisiana Board of Regents for the Louisiana Materials Design Alliance (LAMDA).

REFERENCES

[1] The White House. "Economic Report of the President." Technical report no. Washington, DC. 2022. URL https://www.whitehouse.gov/wp-content/uploads/2022/04/ERP-2022.pdf.

[2] The White House. "Using Additive Manufacturing to Improve Supply Chain Resilience and Bolster Small and Mid-Size Firms." Technical report no. 2022. URL https://www.whitehouse.gov/cea/written-materials/2022/05/09/using-additive-manufacturing-to-improve-supply-chain-\resilience-and-bolster-small-and-mid-size-firms/.

[3] Yampolskiy, Mark, King, Wayne E., Gatlin, Jacob, Belikovetsky, Sofia, Brown, Adam, Skjellum, Anthony and Elovici, Yuval. "Security of Additive Manufacturing: Attack Taxonomy and Survey." *Additive Manufacturing* Vol. 21 (2018): pp. 431–457. DOI https://doi.org/10.1016/j.addma.2018.03.015.

[4] Graves, Lynne M. G., Lubell, Joshua, King, Wayne and Yampolskiy, Mark. "Characteristic Aspects of Additive Manufacturing Security From Security Awareness Perspectives." *IEEE Access* Vol. 7 (2019): pp. 103833–103853. DOI 10.1109/ACCESS.2019.2931738. Accessed 2022-11-01, URL https://ieeexplore.ieee.org/document/8779615/.

[5] Finlay, Richard and Francis, Anny. "A Brief History of Currency Counterfeiting." Reserve Bank of Australia (2022). Accessed 2022-01-20, URL https://www.rba.gov.au/publications/bulletin/2019/sep/pdf/bulletin-2019-09.pdf.

[6] Meshlab. "MeshLab." Accessed 2022-10-31, URL https://www.meshlab.net/.

[7] Xometry. "Where Big Ideas Are Built | Production Parts and Prototypes | Xometry." Accessed 2022-10-31, URL https://www.xometry.com/.

[8] Sculpteo. "Online 3D Printing Service | Instant Quotes - Sculpteo." Accessed 2022-10-31, URL https://www.sculpteo.com/en/.

[9] NIST, XCOM. "NIST XCOM: Element/Compound/Mixture." Accessed 2022-10-31, URL https://physics.nist.gov/PhysRefData/Xcom/html/xcom1.html.

[10] U-Texas, Tomography. "Essentials of Computed Tomography – UTCT – University of Texas." Accessed 2022-10-31, URL https://www.ctlab.geo.utexas.edu/about-ct/essentials-of-computed-tomography/.

[11] Maire, E. and Withers, P. J. "Quantitative X-ray tomography." *International Materials Reviews* Vol. 59 No. 1 (2014): pp. 1–43. DOI 10.1179/1743280413Y.0000000023. Accessed 2022-10-31, URL http://www.tandfonline.com/doi/full/10.1179/1743280413Y.0000000023.

[12] LaManna, J. M., Hussey, D. S., Baltic, E. and Jacobson, D. L. "Neutron and X-ray Tomography (NeXT) system for simultaneous, dual modality tomography." *Review of Scientific Instruments* Vol. 88 No. 11 (2017): p. 113702. DOI 10.1063/1.4989642. Accessed 2022-10-31, URL http://aip.scitation.org/doi/10.1063/1.4989642.

[13] Ali, Salah, Mayo, Sherry, Gostar, Amirali K., Tennakoon, Ruwan, Bab-Hadiashar, Alireza, MCann, Thu, Tuhumury, Helen and Favaro, Jenny. "Automatic segmentation for synchrotron-based imaging of porous bread dough using deep learning approach." *Journal of Synchrotron Radiation* Vol. 28 No. 2 (2021): pp. 566–575. DOI 10.1107/S1600577521001314. Accessed 2022-10-31, URL https://scripts.iucr.org/cgi-bin/paper?S1600577521001314.

[14] ImageJ, NIH. "RSB Home Page." Accessed 2022-10-31, URL https://imagej.nih.gov/.

[15] ImageJ/Fiji. "Fiji." Accessed 2022-10-31, URL https://imagej.net/software/fiji/.

[16] Schindelin, Johannes, Arganda-Carreras, Ignacio, Frise, Erwin, Kaynig, Verena, Longair, Mark, Pietzsch, Tobias, Preibisch, Stephan, Rueden, Curtis, Saalfeld, Stephan, Schmid, Benjamin, Tinevez, Jean-Yves, White, Daniel James, Hartenstein, Volker, Eliceiri, Kevin, Tomancak, Pavel and Cardona, Albert. "Fiji: an open-source platform for biological-image analysis." *Nature Methods* Vol. 9 No. 7 (2012): pp. 676–682. DOI 10.1038/nmeth.2019. Accessed 2022-10-31, URL https://www.nature.com/articles/nmeth.2019. Number: 7 Publisher: Nature Publishing Group.

[17] GeeksforGeeks. "Create Simple Blockchain Using

Python." (2022). URL https://www.geeksforgeeks.org/create-simple-blockchain-using-python/.

[18] Tracey, Anneka. "Building a Blockchain in Python." (2021). URL https://medium.datadriveninvestor.com/building-a-blockchain-in-python-f194a26530fd.

[19] FreeCodeCamp, currency. "How to Create Your Own Cryptocurrency Using Python." Accessed 2022-11-01, URL https://www.freecodecamp.org/news/create-cryptocurrency-using-python/.

[20] Section, Adetu Ridwan. "How to Create a Simple Blockchain using Python | Engineering Education (EngEd) Program | Section." Accessed 2022-11-01, URL https://www.section.io/engineering-education/how-to-create-a-blockchain-in-python/.

[21] Brinckman, Evan, Kuehlkamp, Andrey, Nabrzyski, Jarek and Taylor, Ian J. "Techniques and Applications for Crawling, Ingesting and Analyzing Blockchain Data." *2019 International Conference on Information and Communication Technology Convergence (ICTC)*: pp. 717–722. 2019. DOI 10.1109/ICTC46691.2019.8939746. ISSN: 2162-1233.

[22] Freytsis, Maria, Barclay, Iain, Radha, Swapna Krishnakumar, Czajka, Adam, Siwo, Geoffery H., Taylor, Ian and Bucher, Sherri. "Development of a Mobile, Self-Sovereign Identity Approach for Facility Birth Registration in Kenya." *Frontiers in Blockchain* Vol. 4 (2021): p. 631341. DOI 10.3389/fbloc.2021.631341. Accessed 2022-11-01, URL http://www.webofscience.com/api/gateway?GWVersion=2&SrcAuth=DOISource&SrcApp=WOS&KeyAID=10.3389%2Ffbloc.2021.631341&DestApp=DOI&SrcAppSID=USW2EC0FAE2aKK2X3qaeN4hXLBWKj&SrcJTitle=FRONTIERS+IN+BLOCKCHAIN&DestDOIRegistrantName=Frontiers+Media+SA. Place: Lausanne Publisher: Frontiers Media Sa WOS:000678221000001.

[23] Barclay, Iain, Preece, Alun, Taylor, Ian, Radha, Swapna Krishnakumar and Nabrzyski, Jarek. "Providing assurance and scrutability on shared data and machine learning models with verifiable credentials." *Concurrency and Computation-Practice & Experience* (2022): p. e6997DOI 10.1002/cpe.6997. Accessed 2022-11-01, URL http://www.webofscience.com/api/gateway?GWVersion=2&SrcAuth=DynamicDOIArticle&SrcApp=WOS&KeyAID=10.1002%2Fcpe.6997&DestApp=DOI&SrcAppSID=USW2EC0FAE2aKK2X3qaeN4hXLBWKj&SrcJTitle=CONCURRENCY+AND+COMPUTATION-PRACTICE+%26+EXPERIENCE&DestDOIRegistrantName=Wiley+%28John+Wiley+%26+Sons%29. Place: Hoboken Publisher: Wiley WOS:000778252900001.

[24] Yli-Huumo, Jesse, Ko, Deokyoon, Choi, Sujin, Park, Sooyong and Smolander, Kari. "Where Is Current Research on Blockchain Technology?—A Systematic Review." *PLOS ONE* Vol. 11 No. 10 (2016): p. e0163477. DOI 10.1371/journal.pone.0163477. Accessed 2022-10-31, URL https://dx.plos.org/10.1371/journal.pone.0163477.

[25] Ornes, Stephen. "Blockchain offers applications well beyond Bitcoin but faces its own limitations." *Proceedings of the National Academy of Sciences* Vol. 116 No. 42 (2019): pp. 20800–20803. DOI 10.1073/pnas.1914849116. Accessed 2022-10-31, URL https://pnas.org/doi/full/10.1073/pnas.1914849116.

[26] Wang, Taotao, Zhao, Chonghe, Yang, Qing, Zhang, Shengli and Liew, Soung Chang. "Ethna: Analyzing the Underlying Peer-to-Peer Network of Ethereum Blockchain." *IEEE Transactions on Network Science and Engineering* Vol. 8 No. 3 (2021): pp. 2131–2146. DOI 10.1109/TNSE.2021.3078181. Accessed 2022-10-31, URL https://ieeexplore.ieee.org/document/9426434/.

[27] FreeCodeCamp. "How to Create and Manipulate SQL Databases with Python." Accessed 2022-11-01, URL https://www.freecodecamp.org/news/connect-python-with-sql/.

[28] RealPython. "Python and MySQL Database: A Practical Introduction – Real Python." Accessed 2022-11-01, URL https://realpython.com/python-mysql/.

[29] Joint Task Force. "Security and Privacy Controls for Information Systems and Organizations." Technical Report No. NIST SP 800-53 Rev 5. National Institute of Standards and Technology, Gaithersburg, MD. 2020. DOI 10.6028/NIST.SP.800-53r5. Accessed 2021-03-28, URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Edition: Revision 5.

APPENDIX A. CYBERSECURITY TERMINOLOGY

TABLE 1: TERMS AND DEFINITIONS IN CRYPTOGRAPHY

Term	Definition
Cybersecurity	protection of technology and systems
Cryptography	science of transforming/hiding data; determines methods
Cryptanalysis	science of analysis of cryptographic system (set of transformations/algorithms+key management process in app/context & excludes digital signature, cryptographic hash, key agreement) to break or circumvent
Cryptology	cryptography + cryptanalysis
Encryption	process of converting cleartext (semantic content is intelligible) or plaintext into ciphertext (data that has been transformed & meaning no longer intelligible)
Cipher	cryptographic algorithm for encryption and decryption (i.e., encryption, hash, digital signature, key agreement algorithms)
Key	input parameter/sequence of symbols (usually bits) that varies the transformation performed by the algorithm
Cryptographic Hash (hash function)	algorithm/mathematical function that maps values from a large domain to a fixed length; computationally infeasible to either find a data object that maps to the result or two that map to the same result (collision free)
Perceptual Hash	unique representation of a multimedia file derived from various features from its content. Unlike cryptographic hash functions which rely on the avalanche effect of small changes in input leading to drastic changes in the output, perceptual hashes are "close" to one another if the features are similar
Code	system of symbols used to represent information, which might originally have some other representation (NOT a cipher, hash, ciphertext that refer to applying)
Encode	use system of symbols to represent information (i.e., Morse code, ASCII)
Decode	convert encoded data back to original form of representation
Encrypt	cryptographically transform data to produce ciphertext
Decrypt	cryptographically restore ciphertext to plaintext