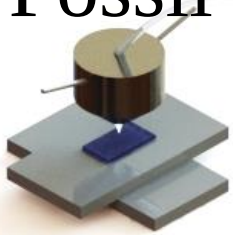
AOI 2: A Novel Access Control Blockchain Paradigm for Cybersecure Sensor Infrastructure in Fossil Power Generation Systems



Rahul Panat[1], Vipul Goyal[2]

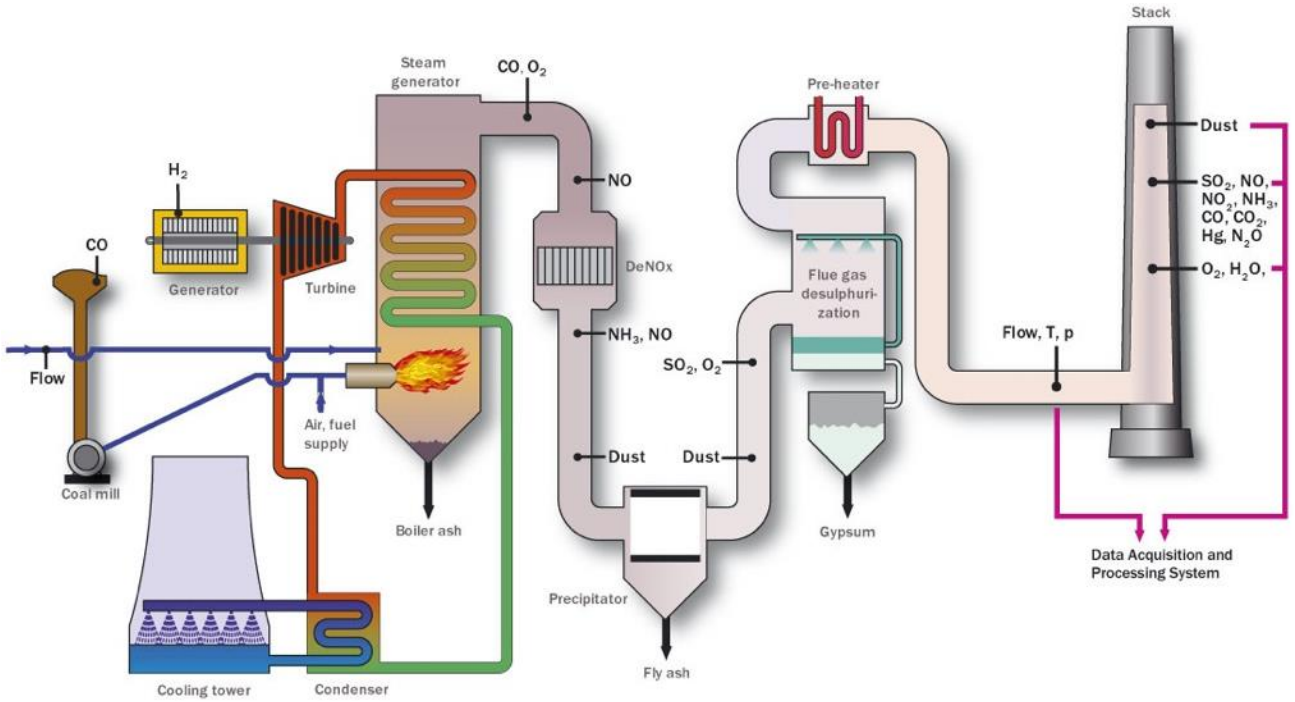
[1]Department of Mechanical Engineering, Carnegie Mellon University, Pittsburgh PA
[2]Computer Science Department, Carnegie Mellon University, Pittsburgh PA

Carnegie Mellon University

Outline

- Background
  - Sensor Systems in Power Plants
- Private Access Controlled Blockchain Concept
- Creating Cybersecure Sensor Networks
- Tasks and Deliverables

Sensing Applications

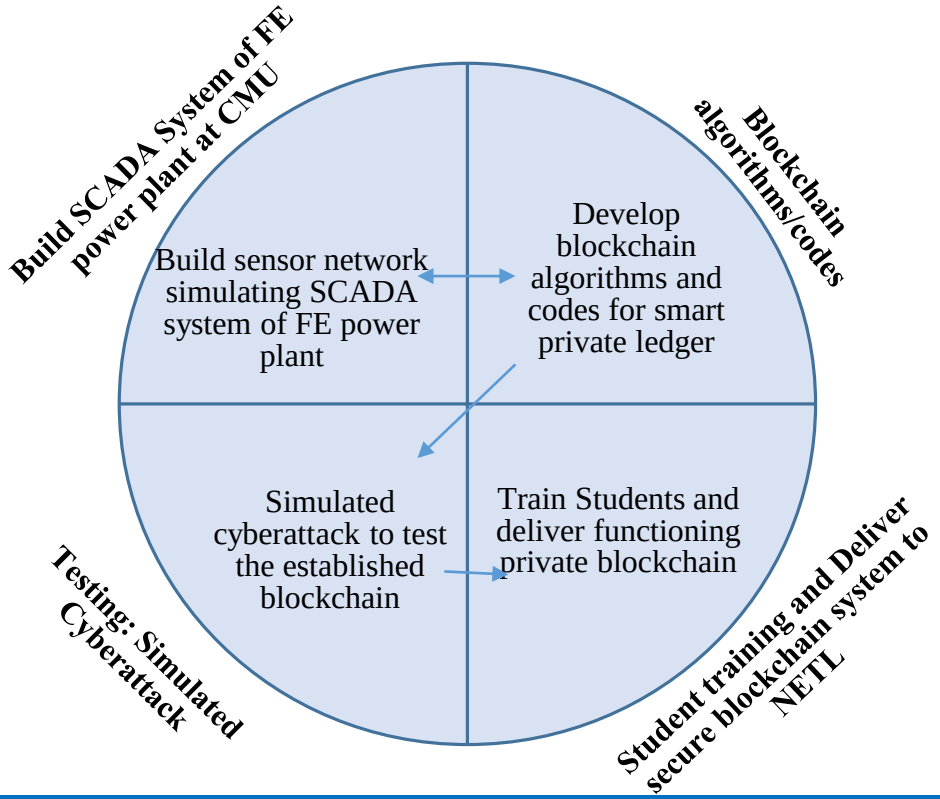


- Power generation and distribution infrastructure can experience both external or internal cyberattacks
- Novel methods are required to secure the data, while also controlling its access

Photo Source: S.R. Thermonix Technologies

Objective of the Project

To design, characterize, and demonstrate a breakthrough secure blockchain protocol, namely smart private ledger with hierarchical access control for fossil power generation systems



Project Timelines and Deliverables

Tasks and Timelines

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

- Project period: 2 years
  - Data acquisition and transmission system
  - Creation of blockchain protocols
  - Simulate cyberattacks and demonstration lab-scale system

Task-1

- Project Management and Planning
  - The PIs will shall manage and direct the project in accordance with a Project Management Plan to meet all technical, schedule and budget objectives and requirements. The PIs will coordinate activities in order to effectively accomplish the work. The PIs will ensure that project plans, results, and decisions are appropriately documented and project reporting and briefing requirements are satisfied.

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

Task-2

- Create a Sensor Network to Generate Data
  - This task will involve the development of sensor networks for the development of the proposed technology. The task will be performed by Panat group

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

Task-3

- Data Transmission to Blockchain Nodes
  - This task will involve the development of wireless transmission of the signal to the blockchain nodes. The task will be performed by Panat group

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

Task-4

- Development of Blockchain with Computers as Simulated Nodes
  - This task will involve the development of the smart private ledger blockchain with hierarchical access control and secret sharing protocols and will be performed by the Goyal group.

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

Task-5

- Create Hierarchical Access Control for Data Retrieval
  - This task will develop algorithms to retrieve the data from the blockchain and will be performed by the Goyal group

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

ONGOING

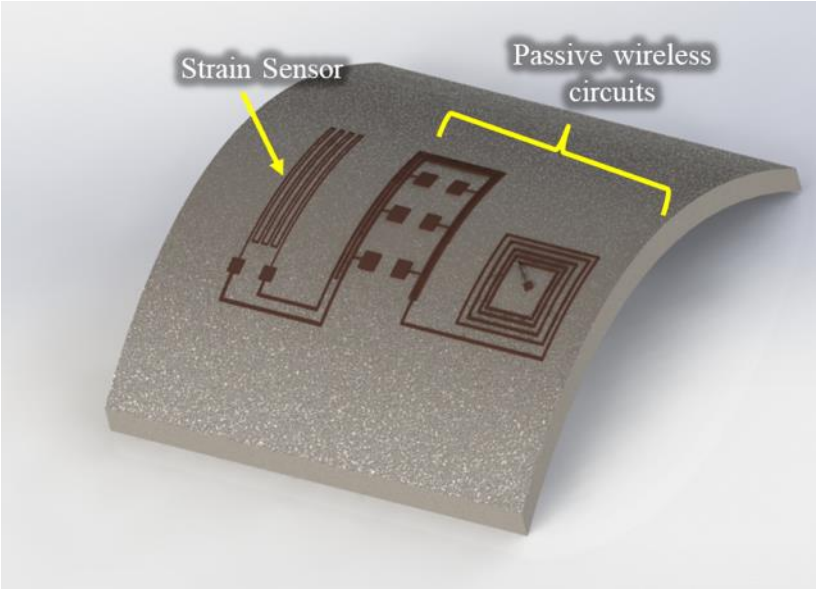
Task-6

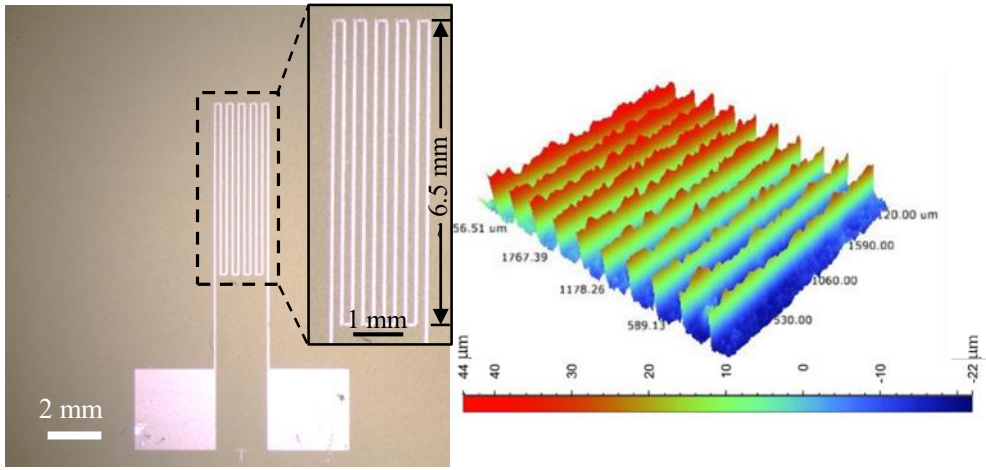
- Simulated Cyberattacks and Demonstration of Robustness of the Blockchain
  - PIs will simulate cyberattacks to harden the blockchain system for real world secure deployment
  - Common strategies such as those used during the Ukranian power grid attack will be studied and the blockchain system will be subjected to similar attacks.
  - Any changes if needed will be made and the entire process will be repeated. We expect our system to provide very high level of security against such attacks by eliminating a single point of failure.

Tasks	Owner	Year-1				Year-2			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Task 1.0: Project Management and Planning	Panat								
Task 2.0: Create a Sensor Network to Generate Data	Panat								
Task 3.0: Data Transmission to Blockchain Nodes	Panat								
Task 4.0: Development of Blockchain with Computers as Simulated Nodes	Goyal								
Task 5.0: Create Hierarchical Access Control for Data Retrieval	Goyal								
Task 6.0: Simulated Cyberattacks and Demonstration of Robustness of the Blockchain	Panat/Goyal								

Building Sensor Network

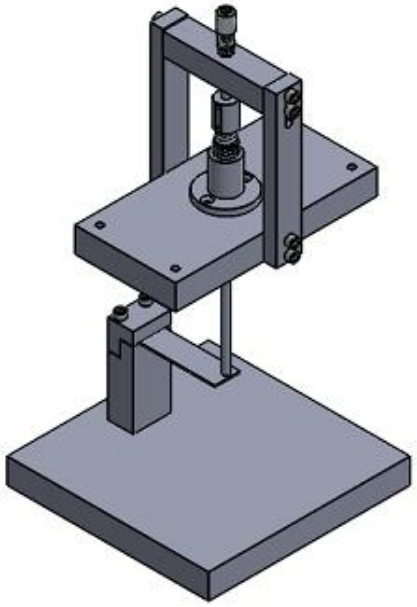
High Temperature Sensor Fabrication

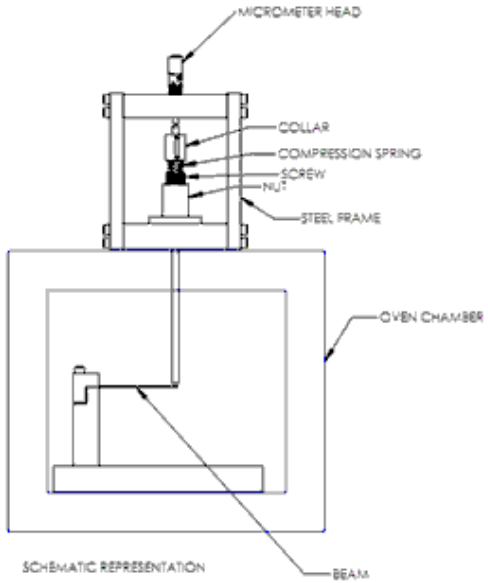




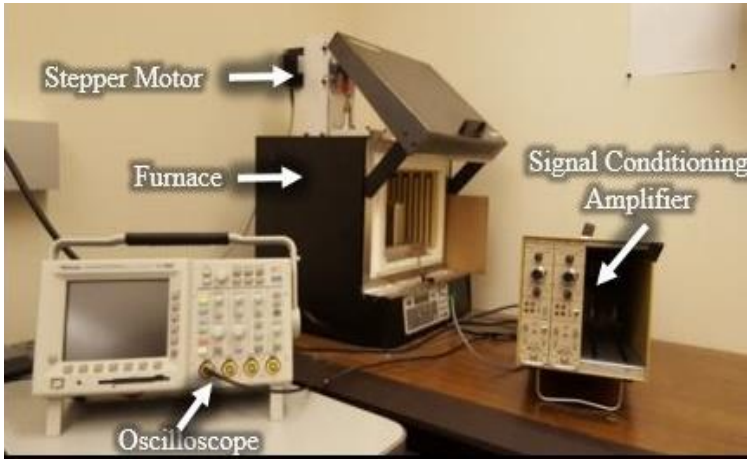
CMU has developed sensor fabrication methods and testing systems for fossil power plants that can work at temperatures up to 500 C

High Temperature Sensor Testing



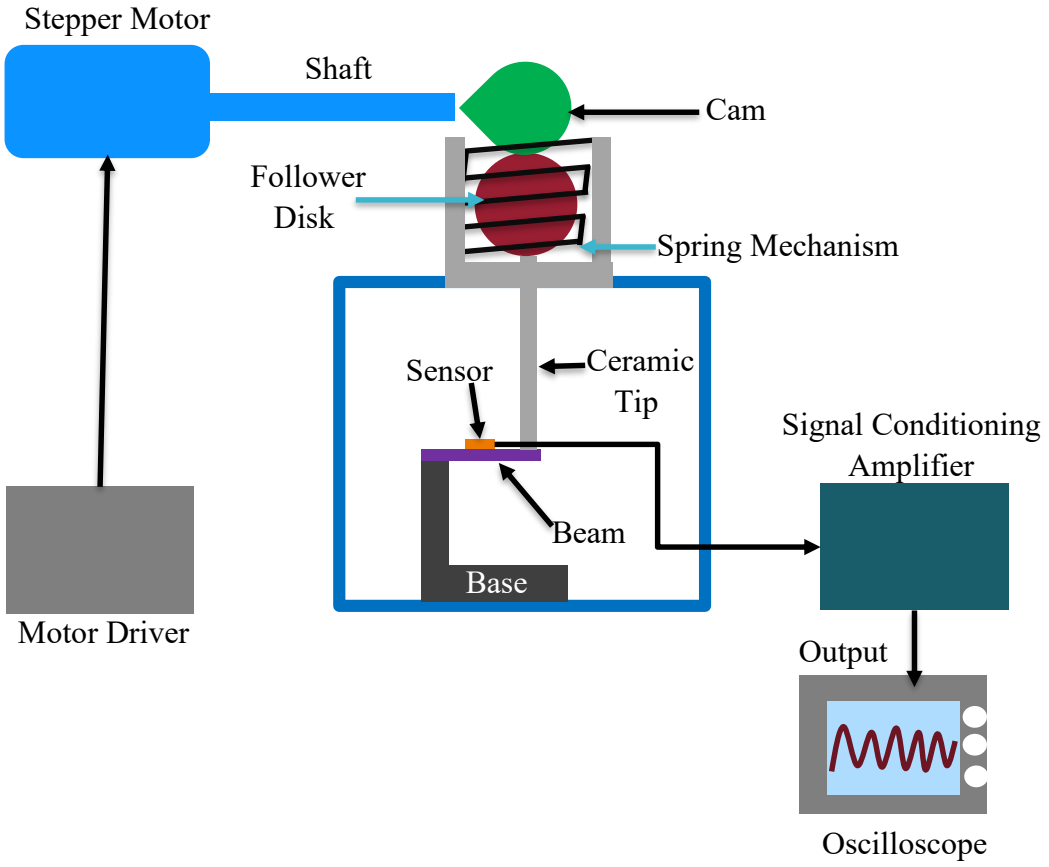


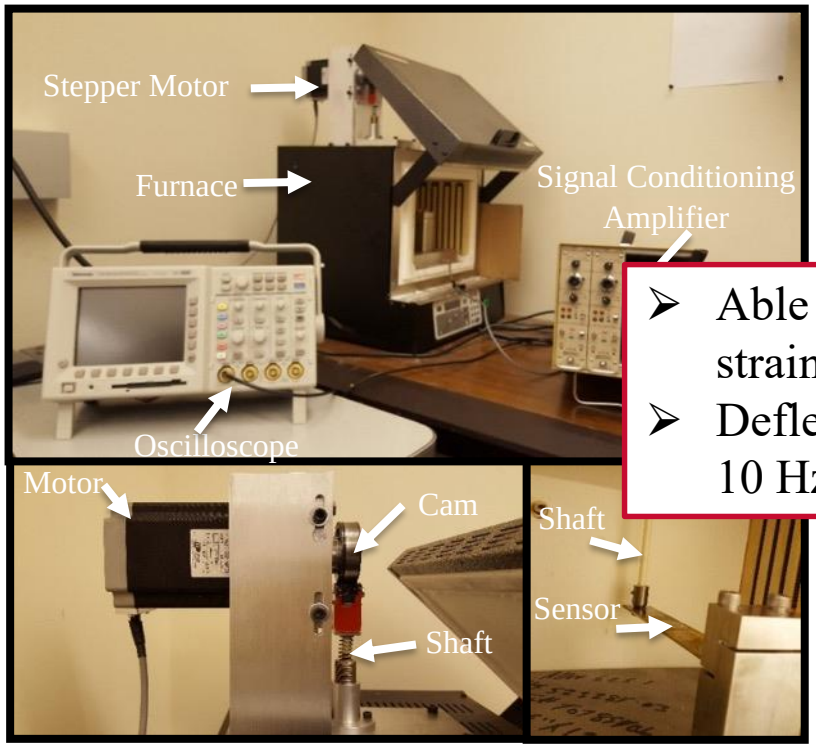
T = 500 °C



CMU has developed sensor fabrication methods and testing systems for fossil power plants that can work at temperatures up to 500 C

High Temperature Data Acquisition System





High Temperature Dynamic Strain Sensor Test Set up

CMU has developed sensor systems for fossil power plants that can work at temperatures up to 500 C

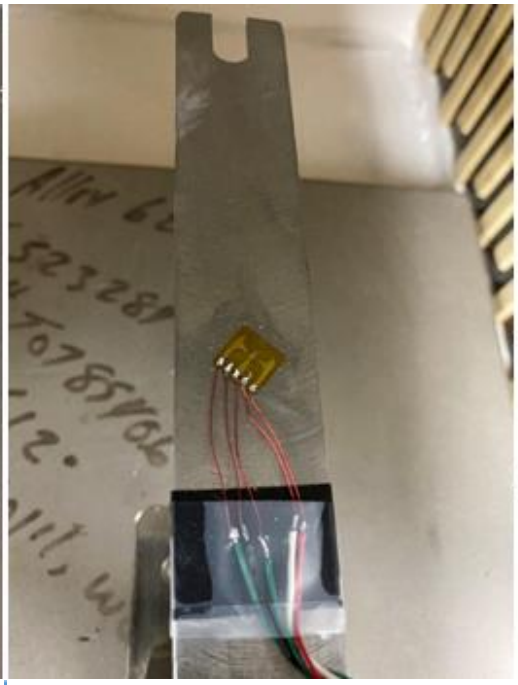
Strain Measurement

Successfully demonstrated strain measurement using Mantracourt T24 telemetry system

1. Installed a commercial strain sensor (VY4 Shear/Torsion full bridge strain gauge) acquired from HBM, USA
2. Integrated the strain sensor with transmitter and base station

Strain Measurement

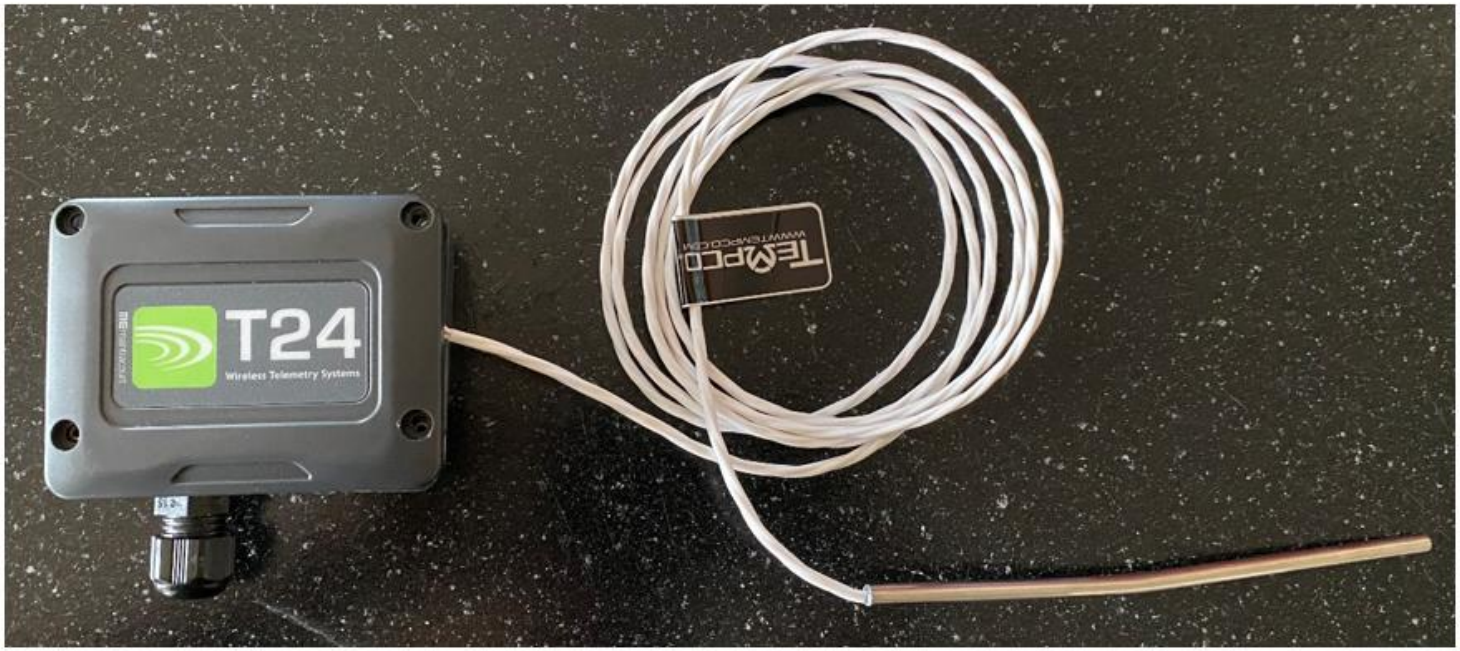
E type beam



Strain sensor showing good adhesion to beam surface

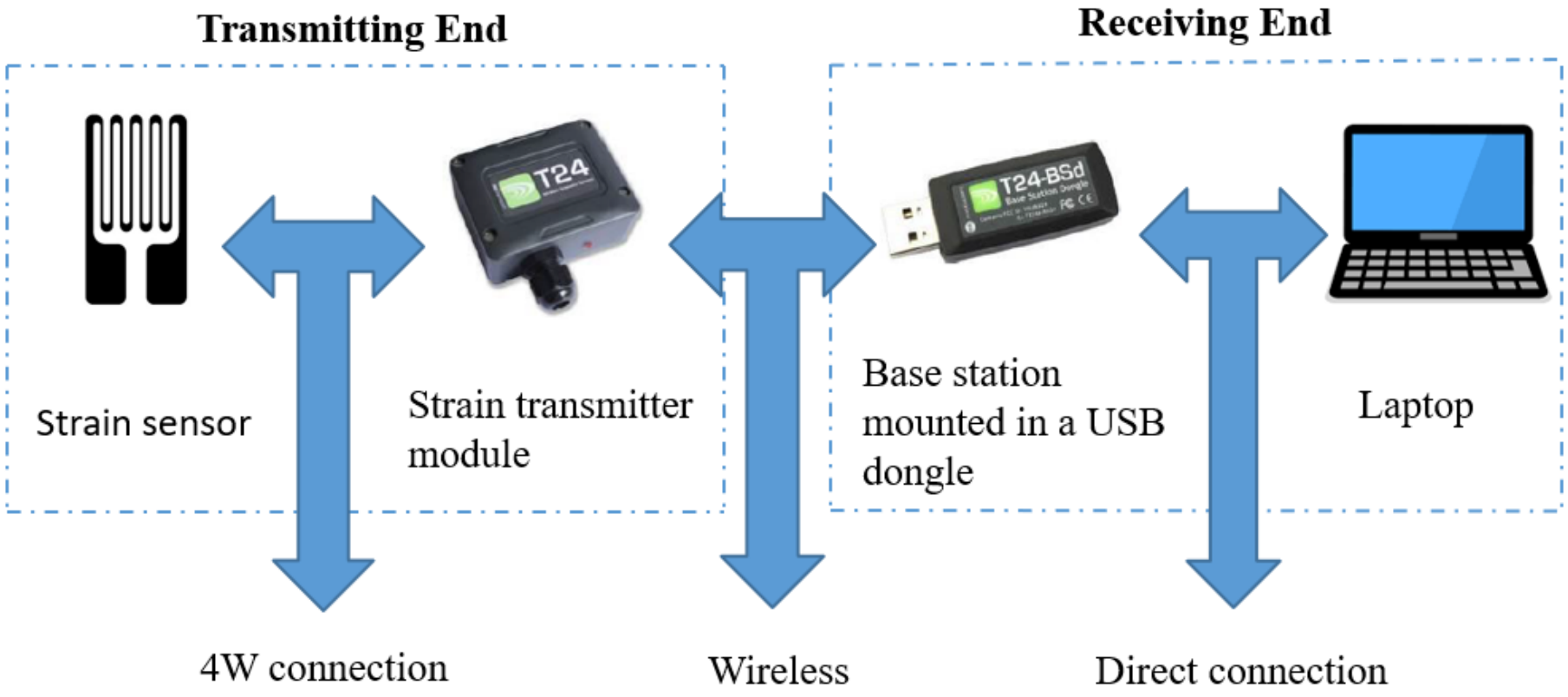
Strain sensor integrated with transmitter module

Temperature Measurement



Temperature sensor integrated with transmitter

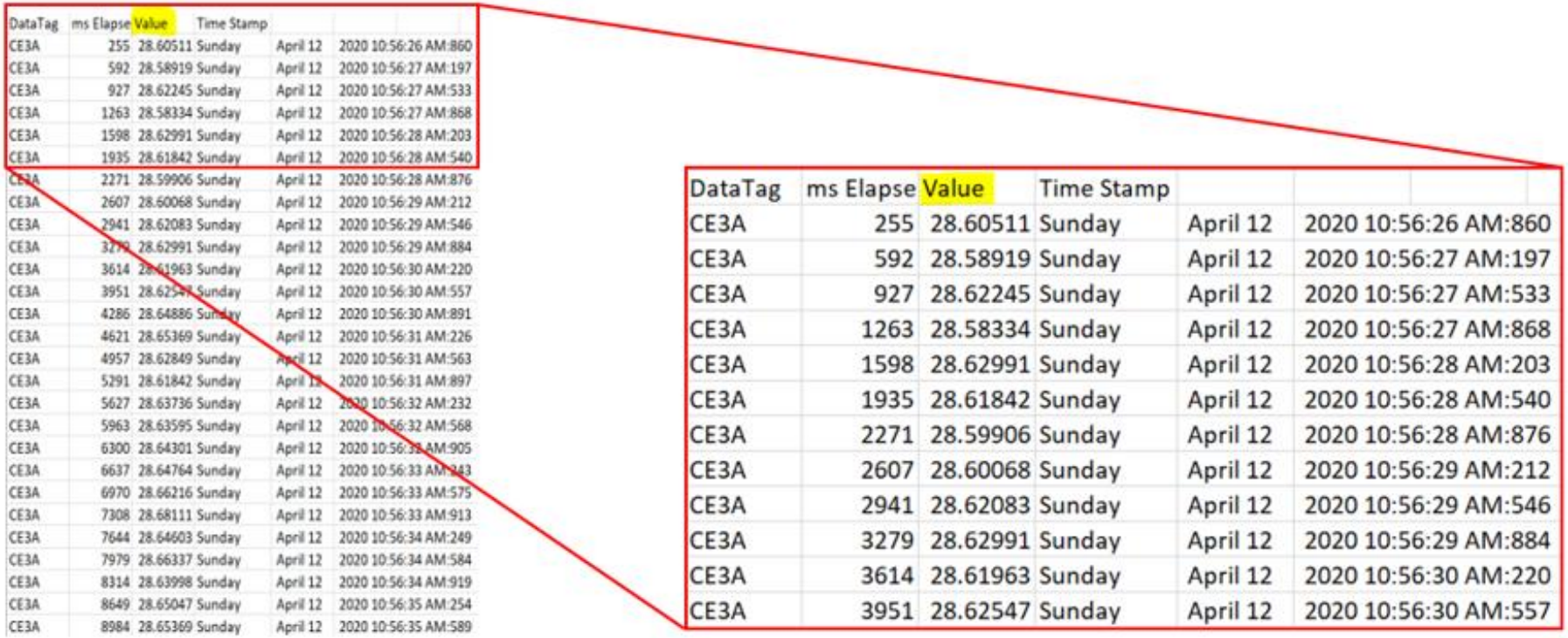
Data Transmission



Data Transmission

- 600 m range in an open field site w/ license free 2.4 GHz direct sequence spread spectrum (DSSS) radio technology
- Data Encryption for complete security (128-bit AES)
- Proprietary protocol based on a 802.15.4 chip allowing T24 range to co-exist with Bluetooth, Zigbee & Wi-Fi devices w/o conflicts!!

Temperature Measurement



DataTag	ms Elapse	Value	Time Stamp		
CE3A	255	28.60511	Sunday	April 12	2020 10:56:26 AM:860
CE3A	592	28.58919	Sunday	April 12	2020 10:56:27 AM:197
CE3A	927	28.62245	Sunday	April 12	2020 10:56:27 AM:533
CE3A	1263	28.58334	Sunday	April 12	2020 10:56:27 AM:868
CE3A	1598	28.62991	Sunday	April 12	2020 10:56:28 AM:203
CE3A	1935	28.61842	Sunday	April 12	2020 10:56:28 AM:540
CE3A	2271	28.59906	Sunday	April 12	2020 10:56:28 AM:876
CE3A	2607	28.60068	Sunday	April 12	2020 10:56:29 AM:212
CE3A	2941	28.62083	Sunday	April 12	2020 10:56:29 AM:546
CE3A	3279	28.62991	Sunday	April 12	2020 10:56:29 AM:884
CE3A	3614	28.61963	Sunday	April 12	2020 10:56:30 AM:220
CE3A	3951	28.62547	Sunday	April 12	2020 10:56:30 AM:557
CE3A	4286	28.64886	Sunday	April 12	2020 10:56:30 AM:891
CE3A	4621	28.65369	Sunday	April 12	2020 10:56:31 AM:226
CE3A	4957	28.62849	Sunday	April 12	2020 10:56:31 AM:563
CE3A	5291	28.61842	Sunday	April 12	2020 10:56:31 AM:897
CE3A	5627	28.63736	Sunday	April 12	2020 10:56:32 AM:232
CE3A	5963	28.63595	Sunday	April 12	2020 10:56:32 AM:568
CE3A	6300	28.64301	Sunday	April 12	2020 10:56:33 AM:905
CE3A	6637	28.64764	Sunday	April 12	2020 10:56:33 AM:243
CE3A	6970	28.66216	Sunday	April 12	2020 10:56:33 AM:575
CE3A	7308	28.68111	Sunday	April 12	2020 10:56:33 AM:913
CE3A	7644	28.64603	Sunday	April 12	2020 10:56:34 AM:249
CE3A	7979	28.66337	Sunday	April 12	2020 10:56:34 AM:584
CE3A	8314	28.63998	Sunday	April 12	2020 10:56:34 AM:919
CE3A	8649	28.65047	Sunday	April 12	2020 10:56:35 AM:254
CE3A	8984	28.65369	Sunday	April 12	2020 10:56:35 AM:589

Snapshot of temperature data collected in a .csv file

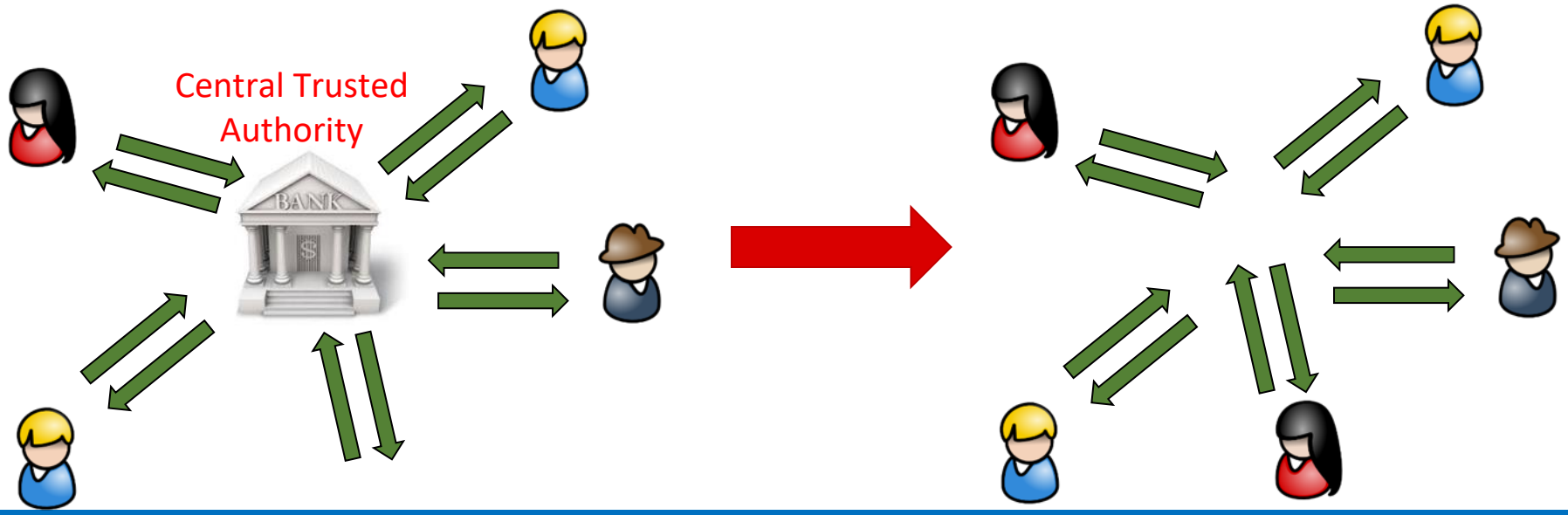
Smart Private Ledger: Blockchains with Private Computation

Bitcoin

- First successful cryptocurrency
- Proposed by “Nakamoto” in 2008, mining started in Jan 2009
- Current market cap > 100B, Price > 8-10k
- First recorded transaction: mid 2010

Bitcoin

- Decentralized, no trusted server
- Miners and users

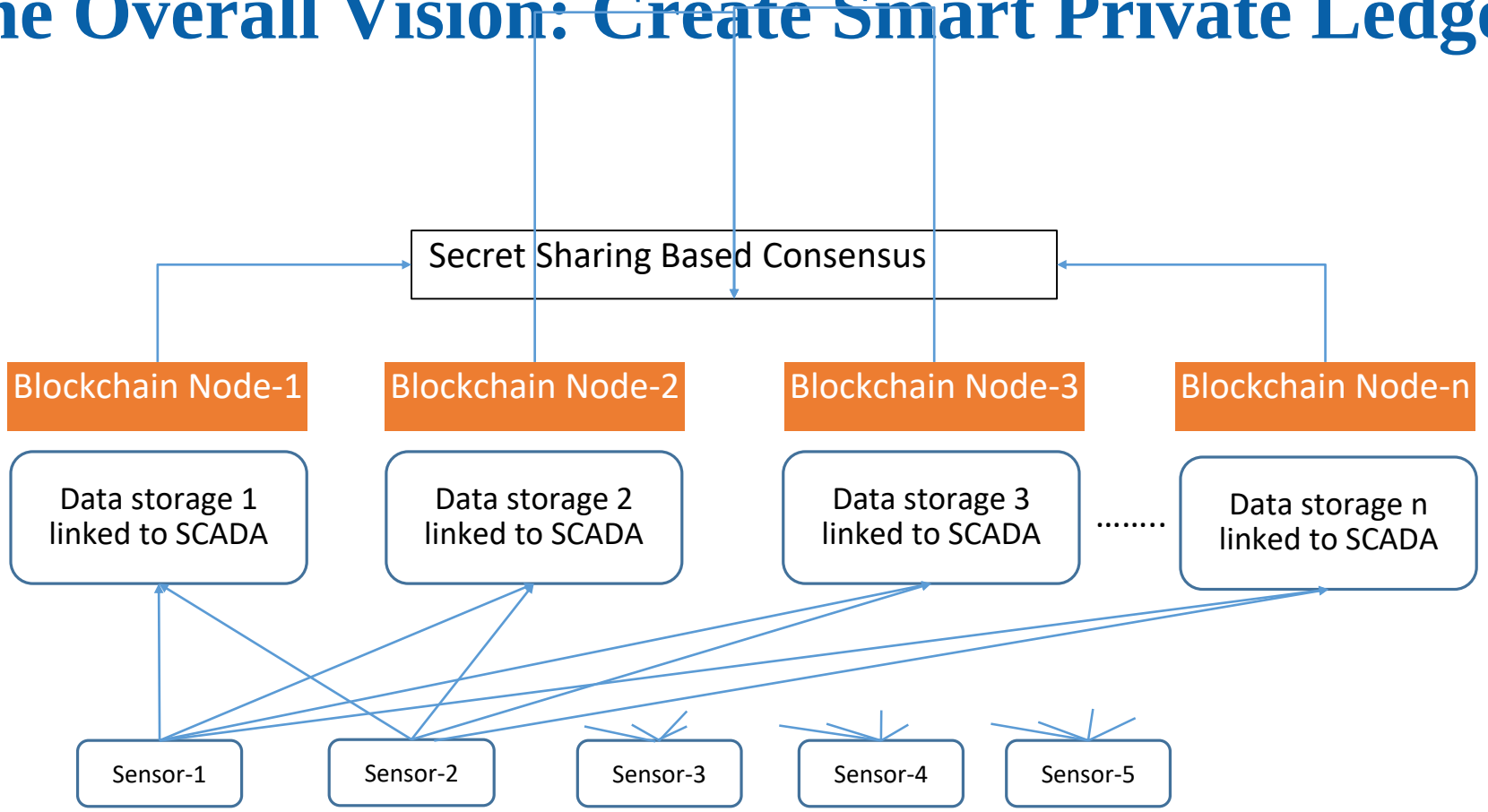


Need for Private Data

- As of today:
  - *All data on public ledger = public*
  - Private, access controlled data?

- Build an intelligent access controlled ledger
  - Different data visible to different parties
  - Even do computation on private data
  - 3rd gen Blockchain tech

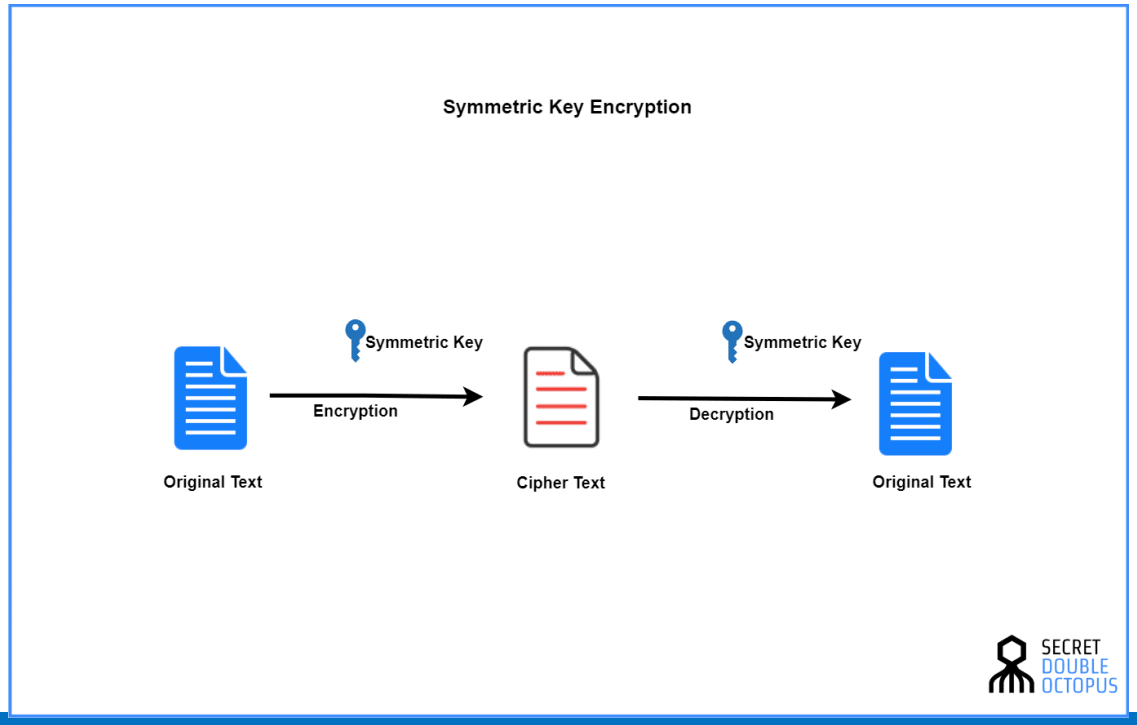
The Overall Vision: Create Smart Private Ledger



Development of Smart Private Ledger

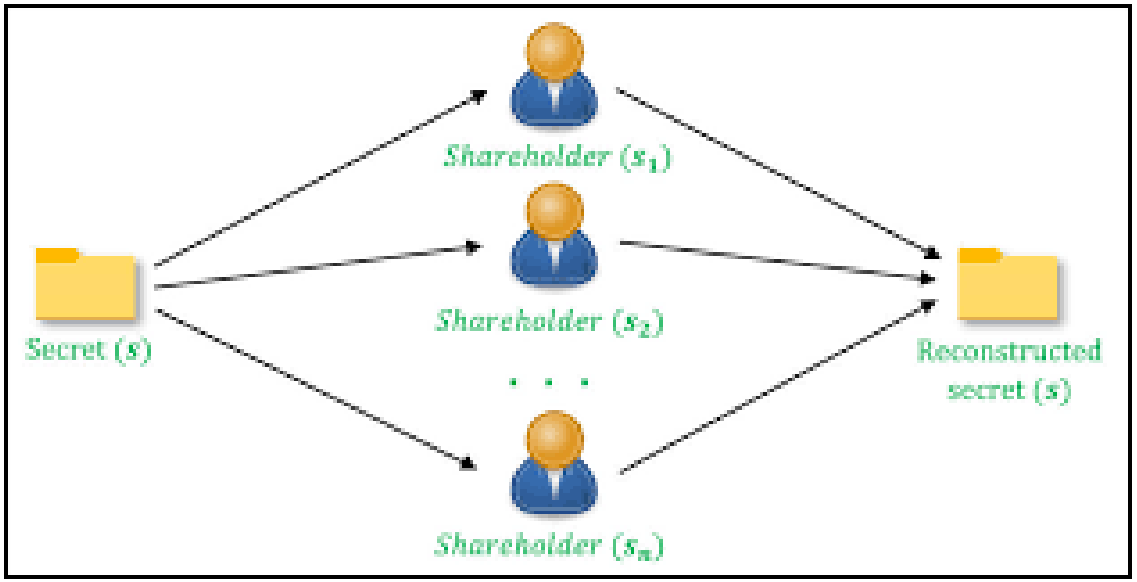
Our system flow is as follows:

- Generating secret key
- Loading and encrypting csv file containing the data from sensor network (using AES secret key encryption scheme)



Development of Smart Private Ledger

- Generating secret key shares
- Encrypting secret key shares (using RSA algorithm)
- Decrypting secret key shares
- Reconstructing secret key
- Decrypting ciphertext to obtain original file containing data
- Smart contract to store/retrieve data from blockchain



System Design

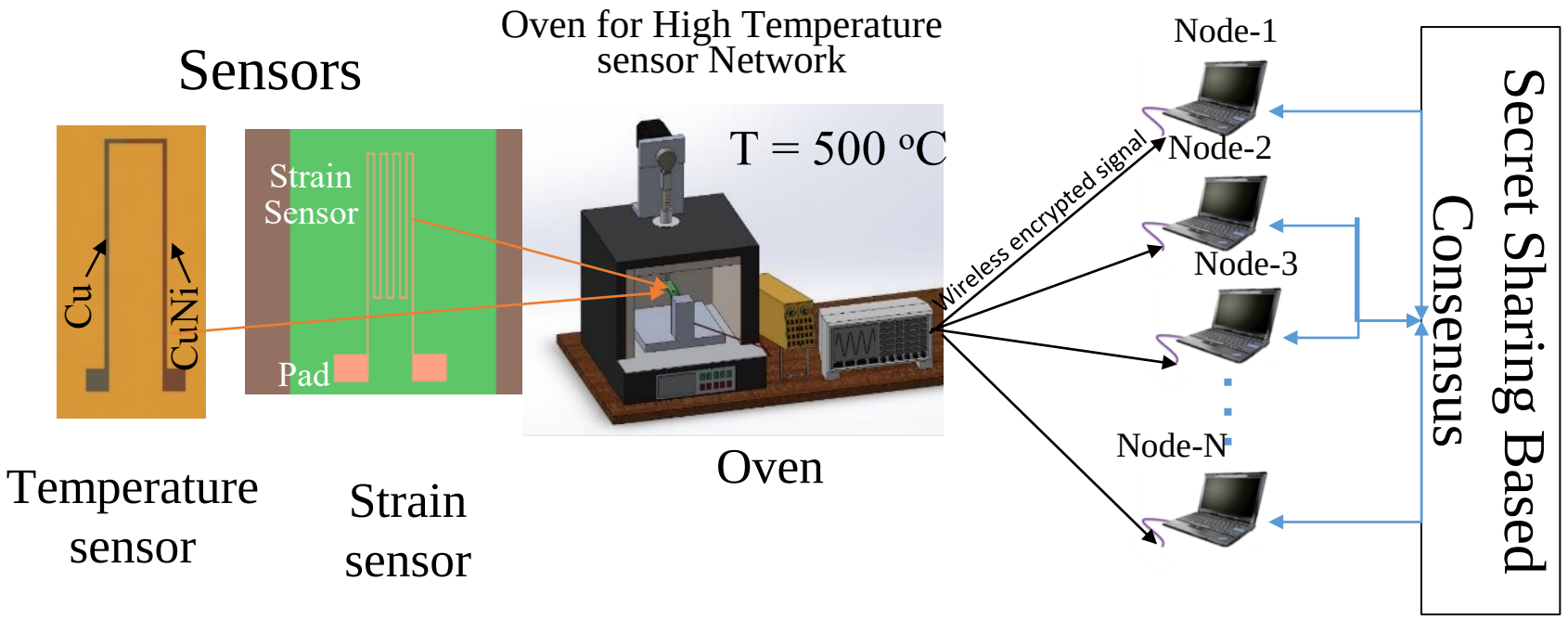
- Secret sharing and file encryption is implemented to be run locally on a given miner's machine. Any file type containing the data can be encrypted with this secret sharing algorithm.
- Once this data is generated, it is stored in the smart contract which is deployed on the blockchain (Ethereum).
- Any miner is then able to access the data from the smart contract and decrypt their respective shares.
- With their keys recovered, they are able to decrypt the data file and have access to the sensor network data.

Smart Contract Storage

We create a smart contract which stores a mapping from miner address to secret key share (of type bytes) with the following functions:

- Add share to the mapping
- Store the encrypted file
- Retrieve the share of a given miner address
- Check if an address is in the map

Integration in Data Acquisition System



Deliverables and Timelines

Task / Subtask Number	Deliverable Title	Due Date
1.0	Project Management Plan	Update due 30 days after award. Revisions to the PMP shall be submitted as requested by the NETL Project Manager.
2.0	Sensor Networks for Fossil Power Generation System	Delivery to NETL 6 months after the start of the project.
3.0	Secure transmission of sensors to blockchain nodes	Delivery to NETL 3 months after Task-2.0, i.e., 9 months after the start of the project.
4.0	Smart Private Ledger Blockchain (codes and algorithms)	Delivery to NETL 12 months after the start of the project.
5.0	Hierarchical Access Control for Data Retrieval (codes and algorithms)	Delivery to NETL 3 months after the Task-4.0, i.e., 15 months after the start of the project
6.0	Robust Blockchain Including Necessary Modifications Ready to be Implemented in the Field	Delivery to NETL 9 months after the Task-5.0, i.e.,24 months after the start of the project

Challenges and Risks

No	Risks	Probability	Impact	Mitigation
i.	Delay in the formation of sensor networks: The PIs propose to create high temperature sensor networks at CMU by leveraging a prior NETL project on sensors and using aerosol jet printing technology. There is a risk for equipment breakdown and the sensor networks not being ready by the end of the third quarter	Low	High	1. Warranties/service agreements with the manufacturers are in place for the equipment. 2. The PIs will use individual commercial temperature sensors in case the sensor network fabrication is delayed.
ii.	Risk for wireless transmission: There is a low probability that the sensor networks cannot send the signal wirelessly to the blockchain nodes.	Low	Moderate	1. The PIs will use commercial wireless sensors (two) as a back-up to demonstrate the concept 2. Multiple suppliers are available in the market with wireless sensors and will be utilized as necessary.
iii.	Risk for formation of Blockchains: there is a small probability that the continuous stream of data coming from sensor readings will cause scalability issues in the blockchain	Low	Moderate	1. The PIs will increase the block size to handle a larger number of transactions per second 2. The number of new blocks per unit time could also be increased to improve the scalability of the system
iv.	Risk for data retrieval: there is a risk that if a number of nodes on the Blockchain go offline, the data stored could become inaccessible	Low	Moderate	1. This risk can be mitigated by increasing the number of nodes. The higher the number of nodes, the better the availability of the system would be. In any case, compared to a centralized data storage, the system will provide much higher level of anonymity.

Acknowledgements

- NETL for supporting this research under grant # DE-FE0031770
- Dr. Robie Lewis, Dr. Vito Cedro, and Dr. Sydni Credle for help on guidance of the project

Questions?