Decentralized and Traceable IoT Network Based on Ethereum

Presenter: Guo ZiNan
Advisor: Prof. Cheng-Fu Chou

Outline

- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Outline

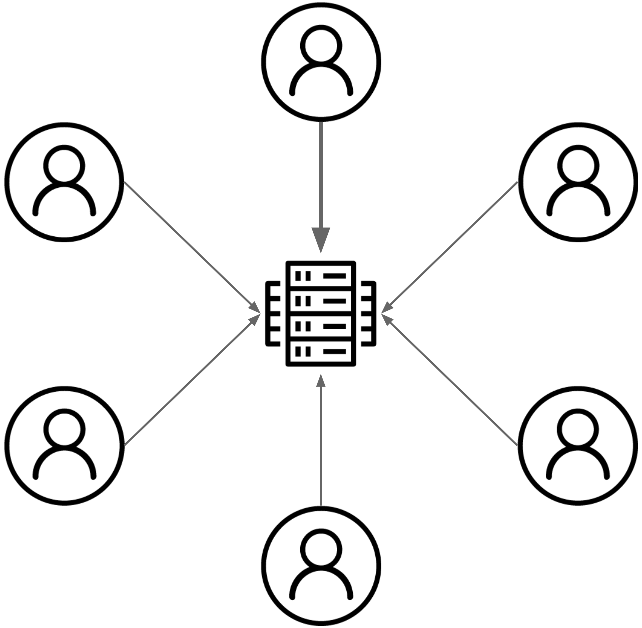
- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Ubiquitos IoT Devices

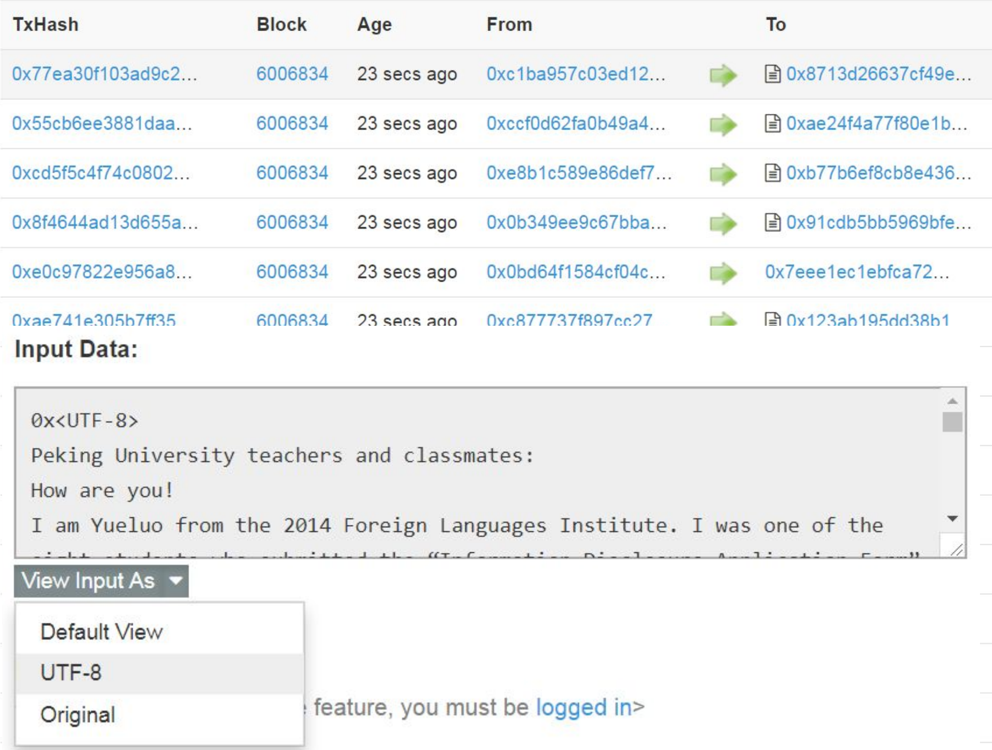
Call for Responsible Sensory Data

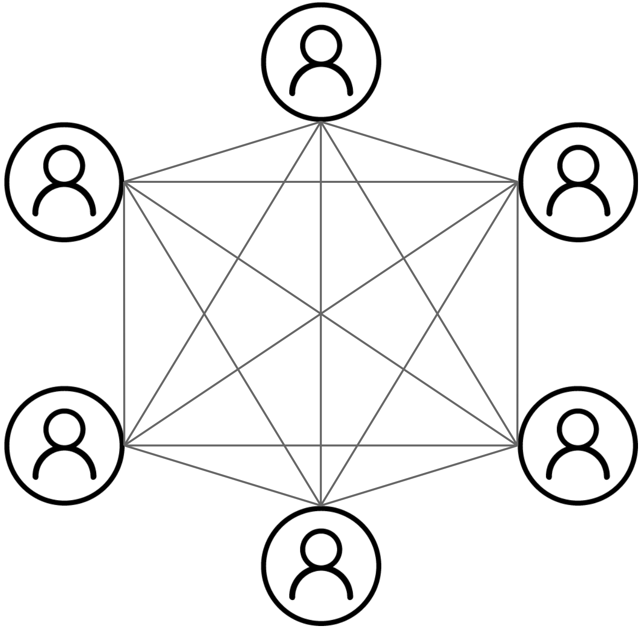
- Effective
- Traceable
- Verifiable

Centralized Sensory Data



Decentralized Sensory Data with Blockchain





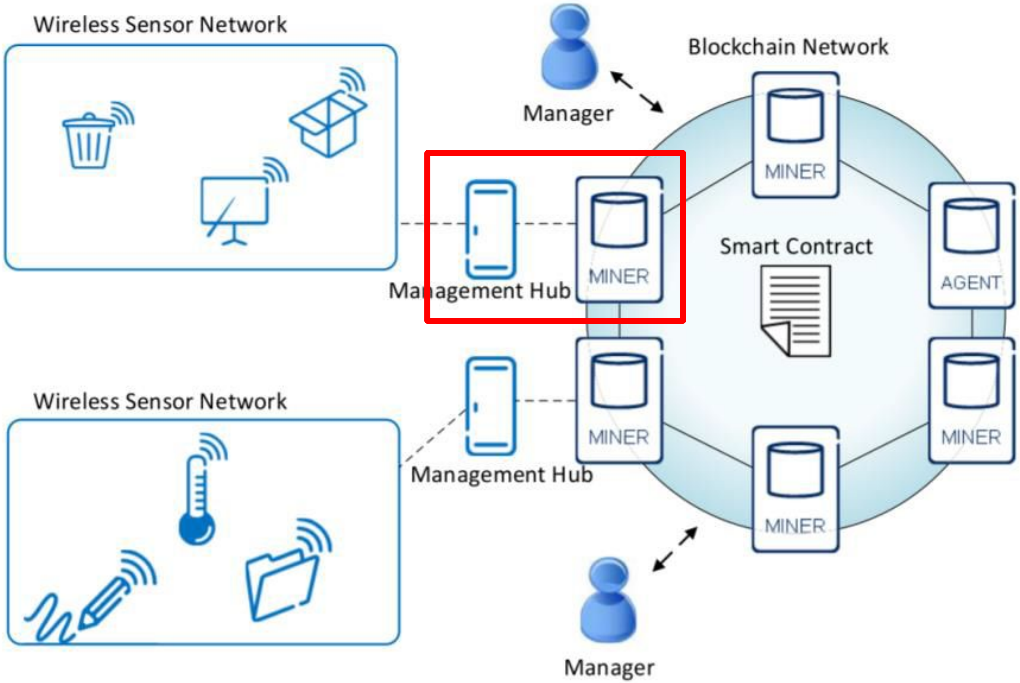
Contradiction between IoT and Blockchain

Traditional IoT Device	**Blockchain Enabled**
Wake Up on Demand	Continuous Network Connection
No Storage	ChainData Storage
Low Power Device	Performance for Verification

Outline

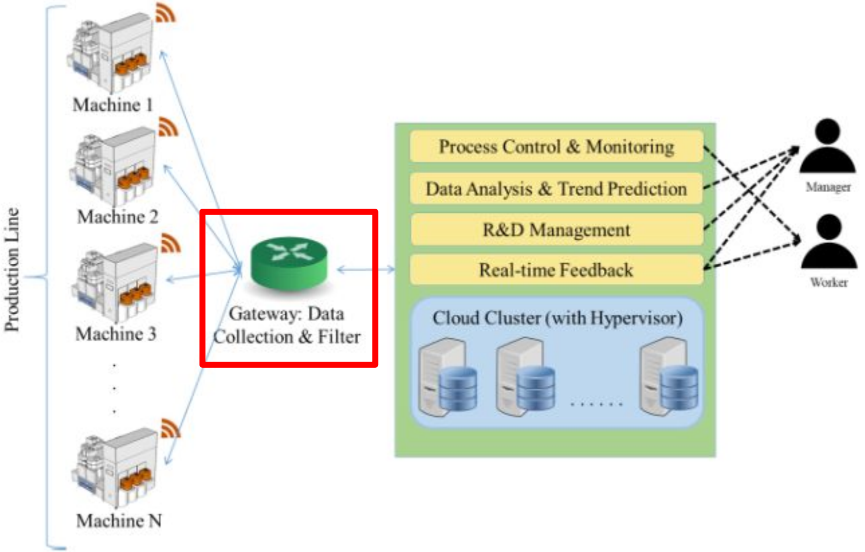
- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Gateway Based Solution

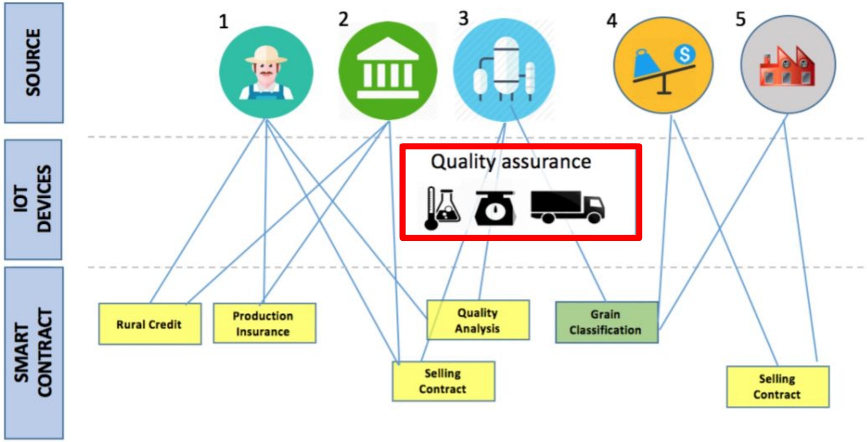


Novo, O. (2018). Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal.

More Examples



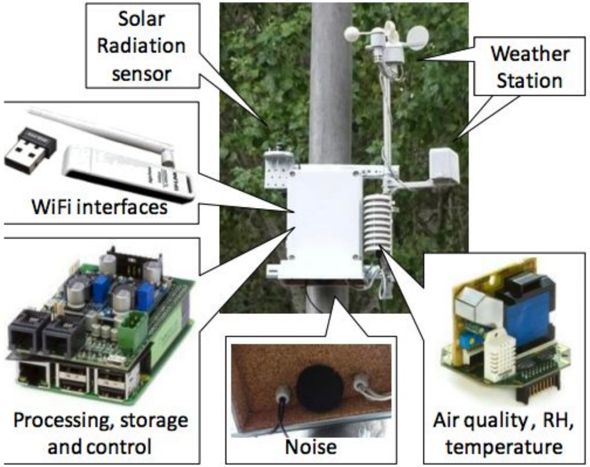
Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2018). Challenges of securing Internet of Things devices: A survey. Security and Privacy, 1(2), e20.



Lucena, P., Binotto, A. P., Momo, F. D. S., & Kim, H. (2018). A Case Study for Grain Quality Assurance Tracking based on a Blockchain Business Network. arXiv preprint arXiv:1803.07877.

Standalone Solution

Upgrade to More Powerful Devices



Halunen, K., Kreku, J., Vallivaara, V., & Suomalainen, J. (2017). Evaluating the Efficiency of Blockchains in IoT with Simulations. Iotbds.

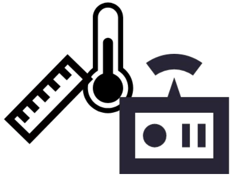
Outline

- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Shortcomings of Standalone Solution

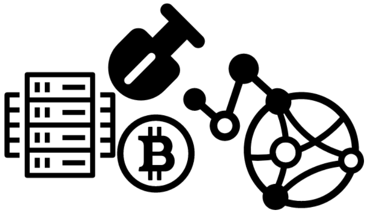
- High Performance Requirement
- High Power Consumption
- High Price

Shortcomings of Gateway Based Solution



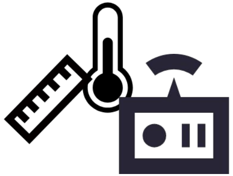
IoT Device Operator

Sensory Data Subscriber



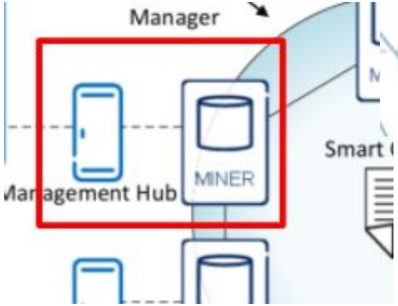
Blockchain Node

For IoT Device Operator



- Self-owned Network
  - Sensor
  - Gateway
  - Protocol

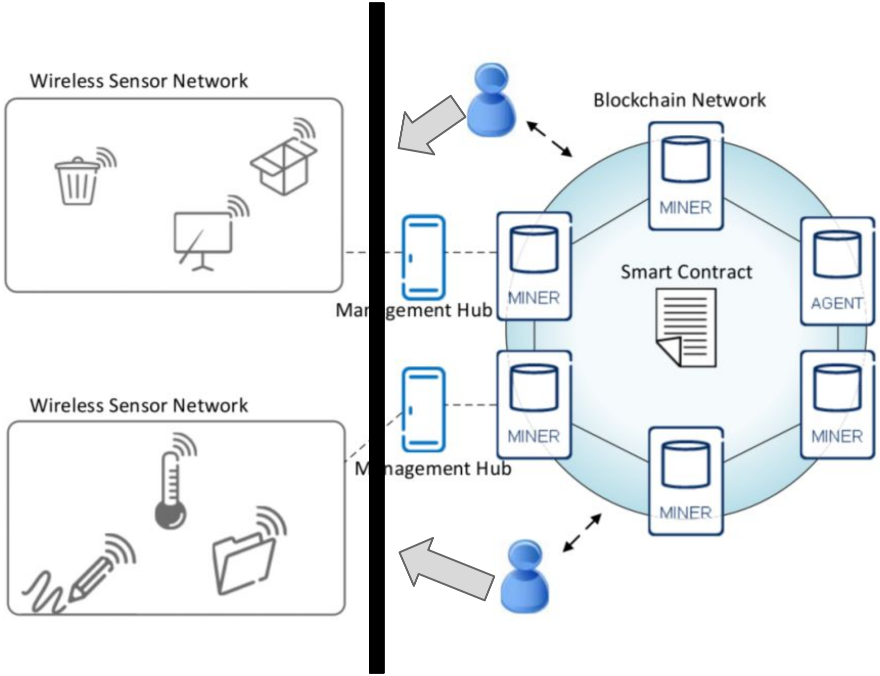
- Maintenance Cost
  - Bandwidth
  - Performance



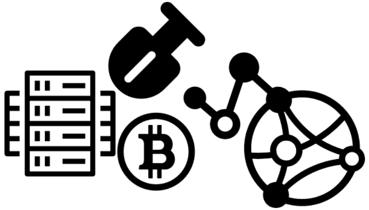
16

For Sensory Data Subscriber

- Black Box
    - Data Generation
    - Transmission
- Centralized Server



For Blockchain Node

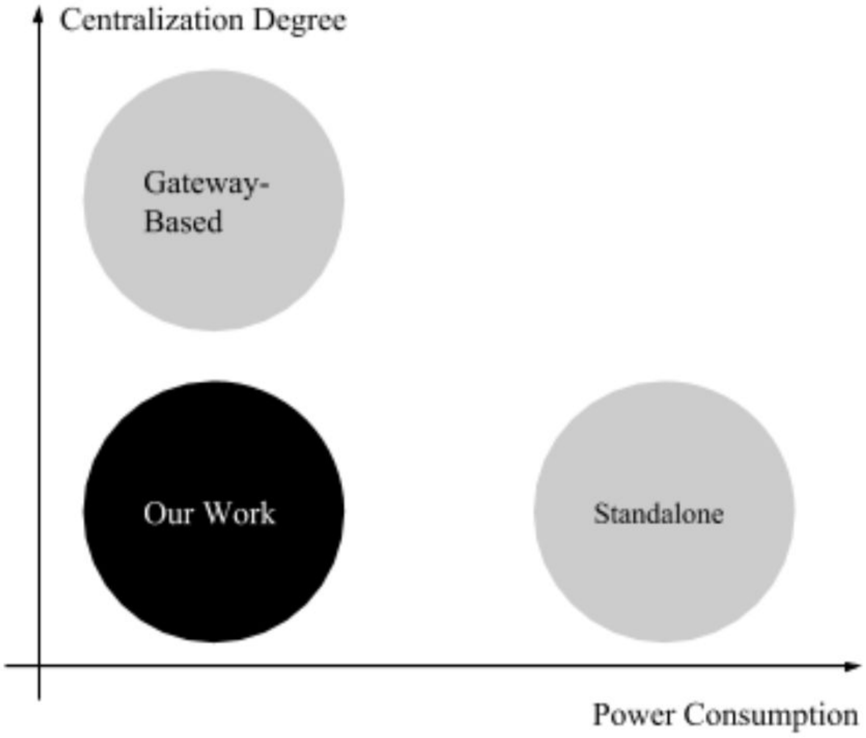


- No Optimization For IoT
  - No Lightweight Protocol
  - No Mobile Node
- No Connection with IoT Devices

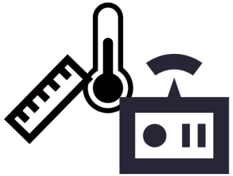
Outline

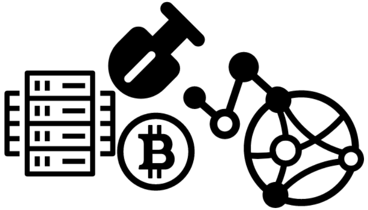
- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Centralization Degree v.s. Power Consumption



Our Target





IoT Device Operator

- Public Network
  - No Gateway
  - Standarlized Protocol

Sensory Data Subscriber

- Open Box
  - Data Generation
  - Transmission

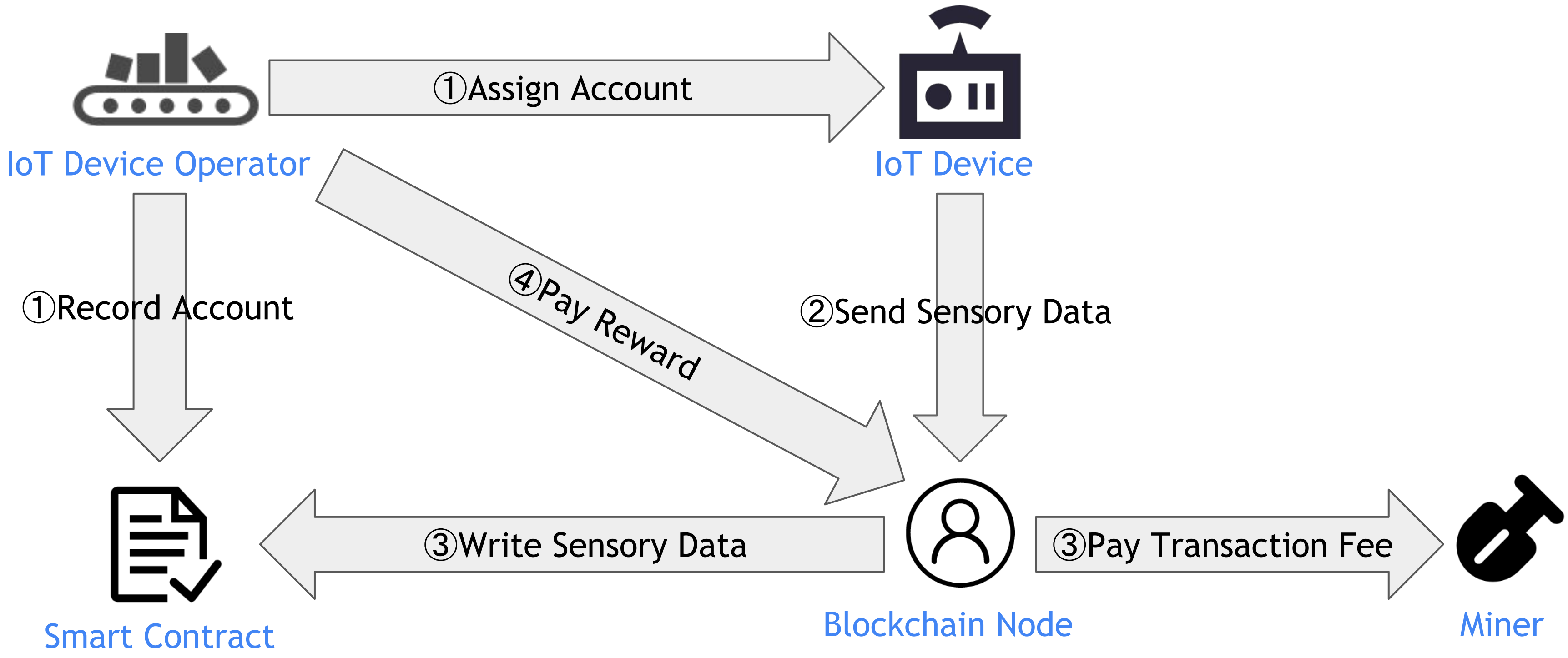
Blockchain Node

- Optimization For IoT
  - Lightweight Protocol
  - Mobile Node

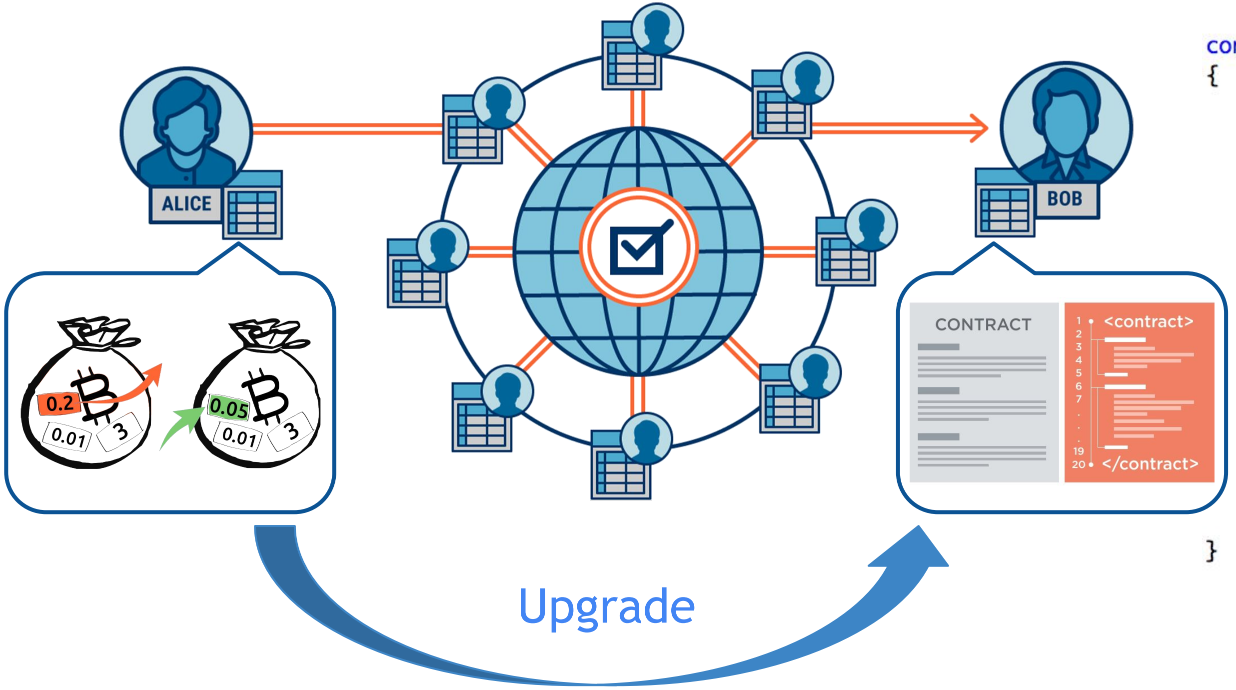
Outline

- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Flow Chart


IoT Device Operator
①Assign Account
IoT Device
①Record Account
④Pay Reward
②Send Sensory Data
③Write Sensory Data
③Pay Transaction Fee
Smart Contract
Blockchain Node
Miner

About Smart Contract

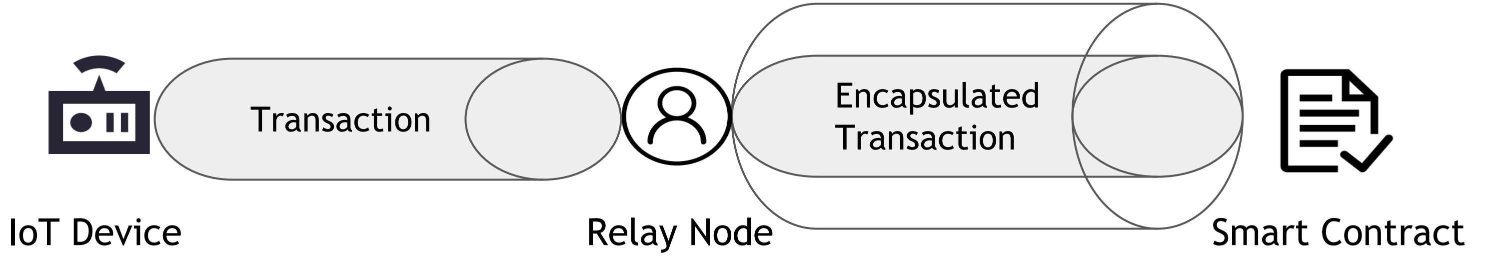



```
contract Storage
{
    bytes public data;
    address public owner;
    modifier isOwner()
    {
        require(msg.sender == owner);
        _;
    }
    constructor() public
    {
        owner = msg.sender;
    }
    function writeData(bytes _data) public isOwner
    {
        data = _data;
    }
}
```

Account Generation

Transplanted		Original
Same Curve	**Public / Private Key Pair**	ECC with secp256k1
Same Hash Function	**Address**	keccak256(Pubkey)

Transaction Issuance

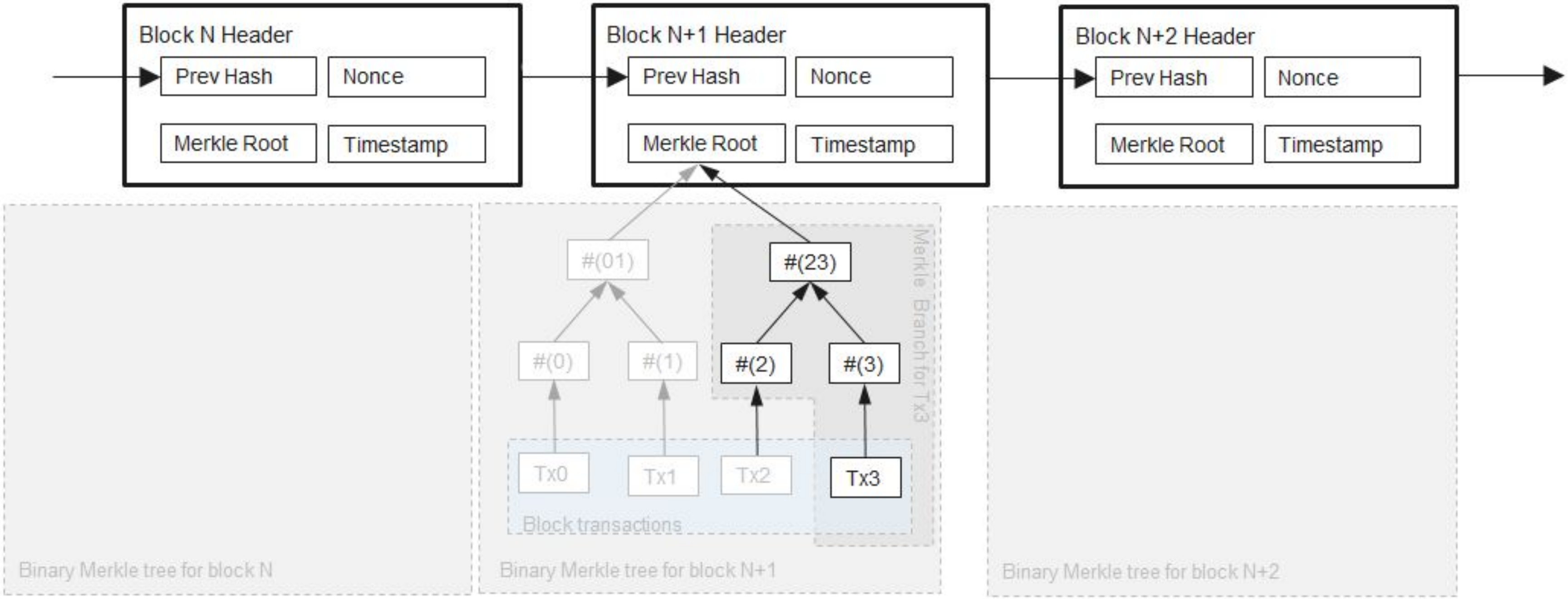


Transplanted		**Original**
IoT Device	**From**	Transaction Sender
- (Sent to Relay Node)	**To**	Transaction Receiver
Data Timestamp	**Nonce**	Transaction Order
Sensory Data	**Input Data**	None or Function Call
Transaction Signature	**Signature**	Transaction Signature

Smart Contract

Transplanted		Original
Standard Contract	**Contract Verification**	- (Decided by Sender)
IoT Device White List	**Device Verification**	Modifier
• *nonce* • *ecrecover(hash, sig) returns (address)*	**Data Verification**	Done by Miner
Decided by Operator	**Gas Price**	Decided by Sender
Decided by Operator	**Gas Limit**	Auto Calculated

Mobile Node: Lightweight Protocol



Outline

- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

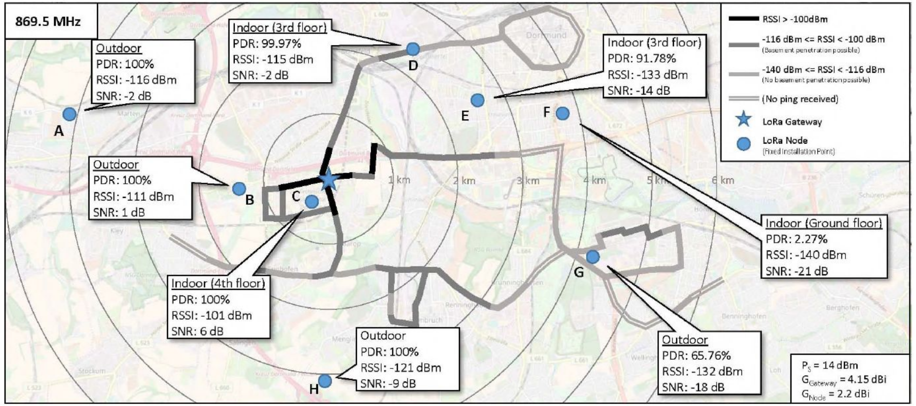
Urban IoT Scenario

- Deployed in Crowded Areas
- Short-range Communication with Pedestrian
    - NFC

Santos, P. M., Rodrigues, J. G., Cruz, S. B., Lourenço, T., d'Orey, P. M., Luis, Y., ... & Sargento, S. (2018). PortoLivingLab: An IoT-Based Sensing Platform for Smart Cities. IEEE Internet of Things Journal, 5(2), 523-532.

Factory IoT Scenario

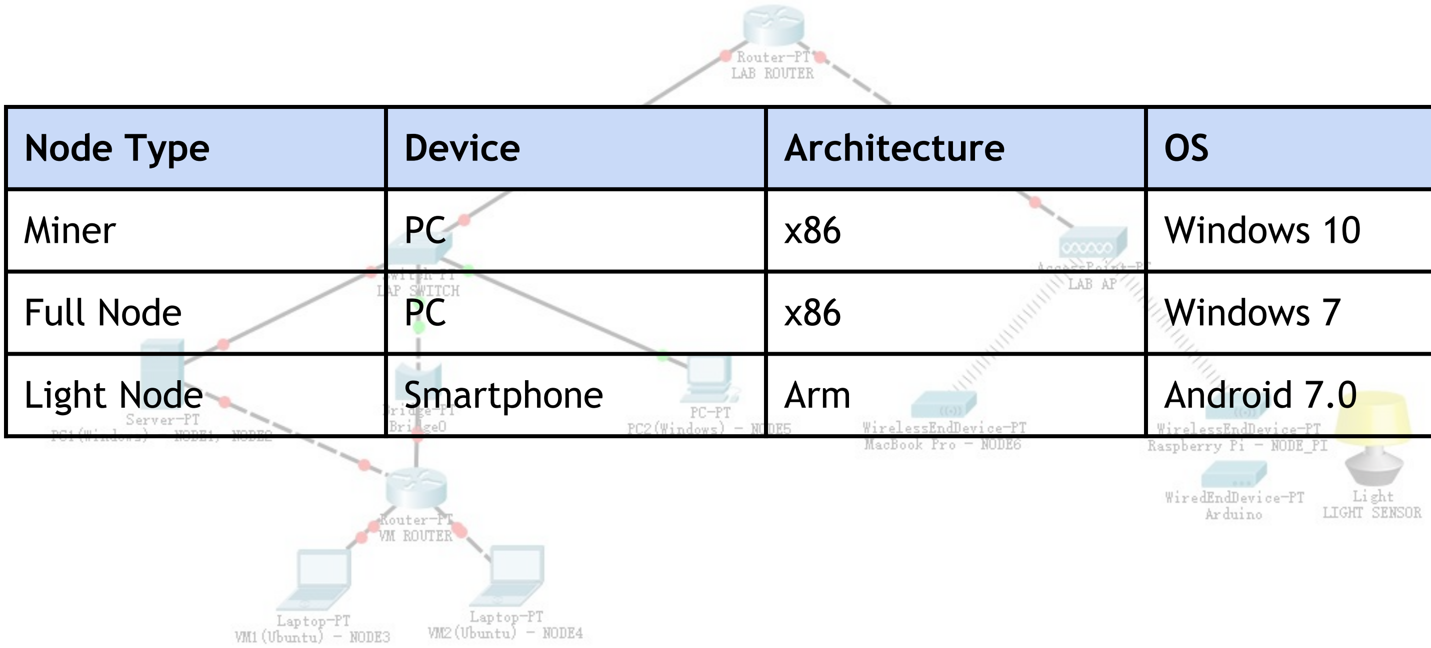
- Deployed in Broad Areas
- Long-range Communication with Pedestrian
  - LoRa

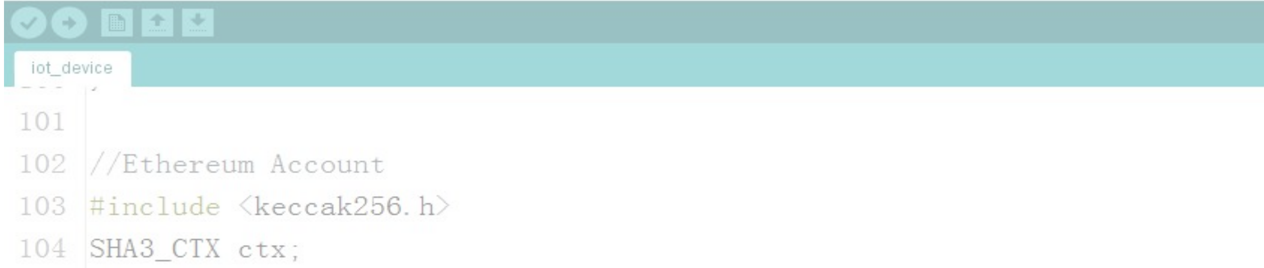


Jörke, P., Böcker, S., Liedmann, F., & Wietfeld, C. (2017, October). Urban channel models for smart city IoT-networks based on empirical measurements of LoRa-links at 433 and 868 MHz. In Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on (pp. 1-6). IEEE.

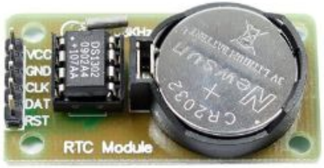
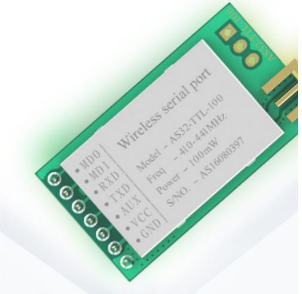
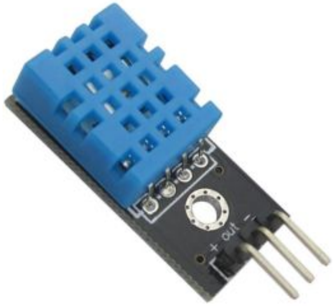
Ethereum Private Chain

Node Type	Device	Architecture	OS
Miner	PC	x86	Windows 10
Full Node	PC	x86	Windows 7
Light Node	Smartphone	Arm	Android 7.0





IoT Device

MCU	Timestamp	Data		Sample Sensor
Arduino Pro Mini 	DS1302 	NFC (MFRC522) 	LoRa (SX1278) 	DHT11 

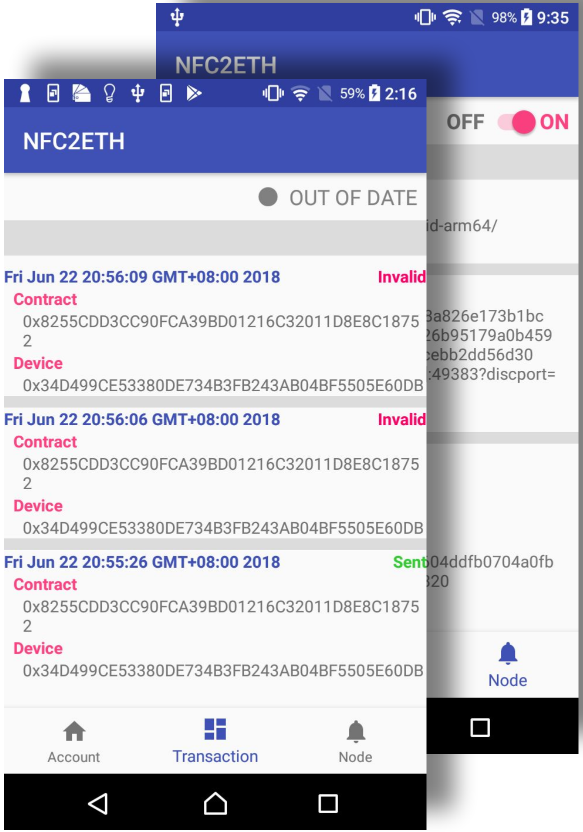
Data in NFC Card

<table>
<tr><th></th><th>Block 0</th><th>Block 1</th><th>Block 2</th><th>Block 3 (Trailer)
KeyA’s View</th></tr>
<tr><td>Sector 0</td><td>UID</td><td colspan="2">Contract Address
(20 Bytes, Right Padding)</td><td rowspan="5">Read Only</td></tr>
<tr><td>Sector 1</td><td>Magic Header
“bonborubonboru93”</td><td colspan="2">Device Address
(20 Bytes, Right Padding)</td></tr>
<tr><td>Sector 2</td><td colspan="2">Signature_R</td><td>Nonce
(4 Bytes,
Right Padding)</td></tr>
<tr><td>Sector 3</td><td colspan="2">Signature_S</td><td>Length</td></tr>
<tr><td>Sector 4
~
Sector 15</td><td colspan="3">Data (Up to 576 Bytes)</td></tr>
<tr><td>Sector 16</td><td colspan="2">Private Key</td><td>Reserved</td><td>Access Denied</td></tr>
</table>

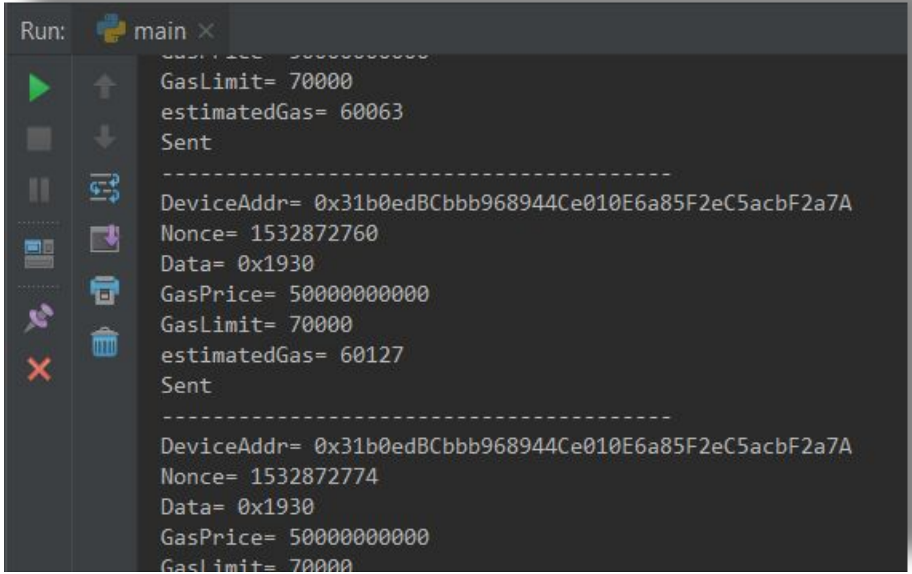
Data in LoRa Packet

Packet Header	Contract Address	Device Address	Signature	Nonce	Data	Packet Trailer
“*bonboru93*”	20 Bytes	20 Bytes	64 Bytes	4 Bytes	Up to Maximum LoRa Payload Size	“*39urobnob*”

Relay Node



98% 9:35
NFC2ETH
OFF ON
id-arm64/
3a826e173b1bc
26b95179a0b459
cebb2dd56d30
:49383?discport=
04ddfb0704a0fb
320
Node
59% 2:16
NFC2ETH
OUT OF DATE
Fri Jun 22 20:56:09 GMT+08:00 2018
Invalid
Contract
0x8255CDD3CC90FCA39BD01216C32011D8E8C1875
2
Device
0x34D499CE53380DE734B3FB243AB04BF5505E60DB
Fri Jun 22 20:56:06 GMT+08:00 2018
Invalid
Contract
0x8255CDD3CC90FCA39BD01216C32011D8E8C1875
2
Device
0x34D499CE53380DE734B3FB243AB04BF5505E60DB
Fri Jun 22 20:55:26 GMT+08:00 2018
Sent
Contract
0x8255CDD3CC90FCA39BD01216C32011D8E8C1875
2
Device
0x34D499CE53380DE734B3FB243AB04BF5505E60DB
Account
Transaction
Node



Run:
main
GasLimit= 70000
estimatedGas= 60063
Sent

DeviceAddr= 0x31b0edBCbbb968944Ce010E6a85F2eC5acbF2a7A
Nonce= 1532872760
Data= 0x1930
GasPrice= 50000000000
GasLimit= 70000
estimatedGas= 60127
Sent

DeviceAddr= 0x31b0edBCbbb968944Ce010E6a85F2eC5acbF2a7A
Nonce= 1532872774
Data= 0x1930
GasPrice= 50000000000

Demo

Outline

- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Target Review

Entity	Target	Status
IoT Device Operator	No Gateway	Yes, Gateway Elimited
	Standarlized Protocol	Yes, by Standard Contract
Sensory Data Subscriber	Data Generation	Yes, by Direct Connection
	Transmission	Yes, by Relay Node
Blockchain Node	Lightweight Protocol	Yes, by Ethereum LES Protocol
	Mobile Node	Yes, by Android App

Responsible Sensory Data

Requirement	Status
Effective	Yes, Exactly from IoT Device
Traceable	Yes, by Blockchain and Smart Contract
Verifiable	Yes, by Data Consistency Check among Device, Environment and Contract

Power Consumption of IoT Device

- Average Current

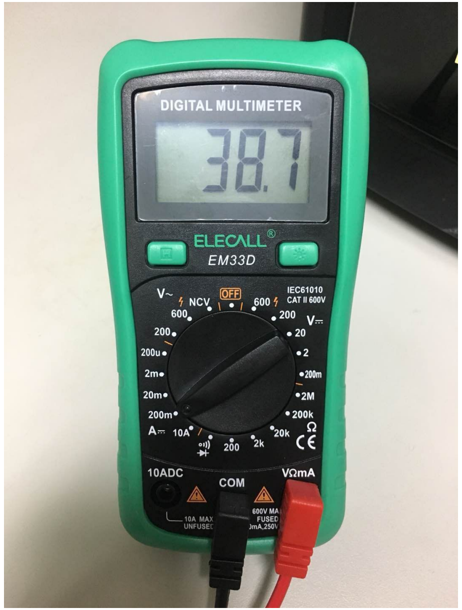
$$\text{Average Current} = \frac{t_a * c_a + t_s * c_s}{T}$$

$$= \frac{5\text{s} * 40\text{mA} + 3595\text{s} * 0.06\text{ mA}}{3600\text{s}}$$

$$= 0.11\text{ mA}$$

- Driven by 10000mAh Power Bank
- Battery Life

$$Battery\ Life = \frac{10000mAh}{0.11\ mA} = 10.38\ Year$$



Active Mode: < 40 mA

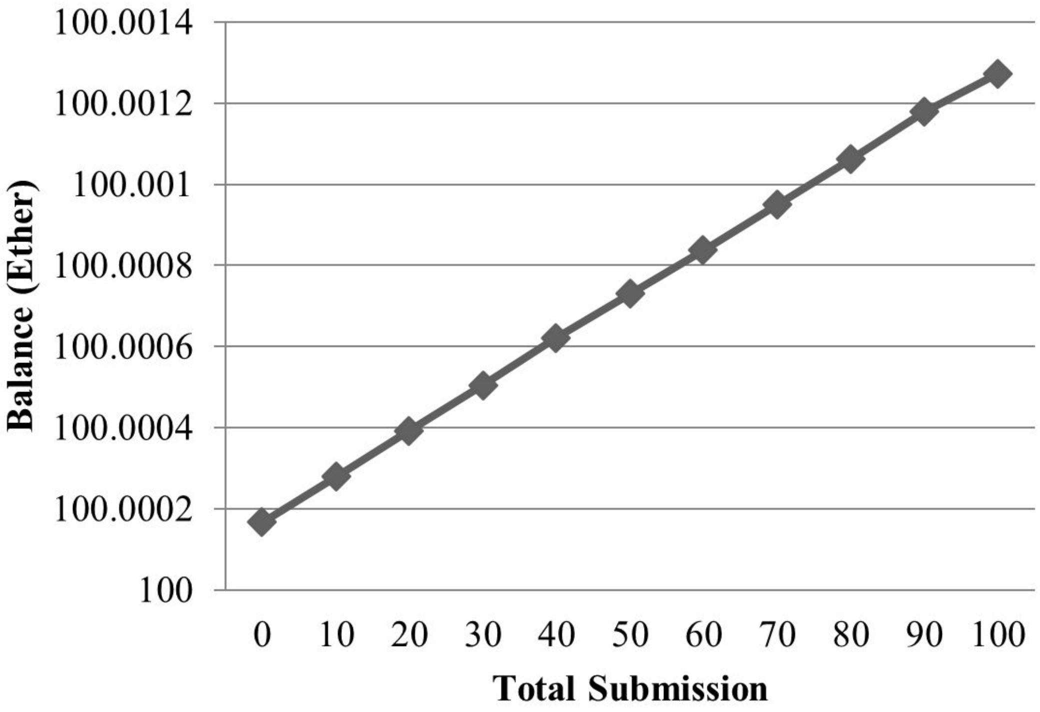
< 5s

Sleep Mode: < 60 uA

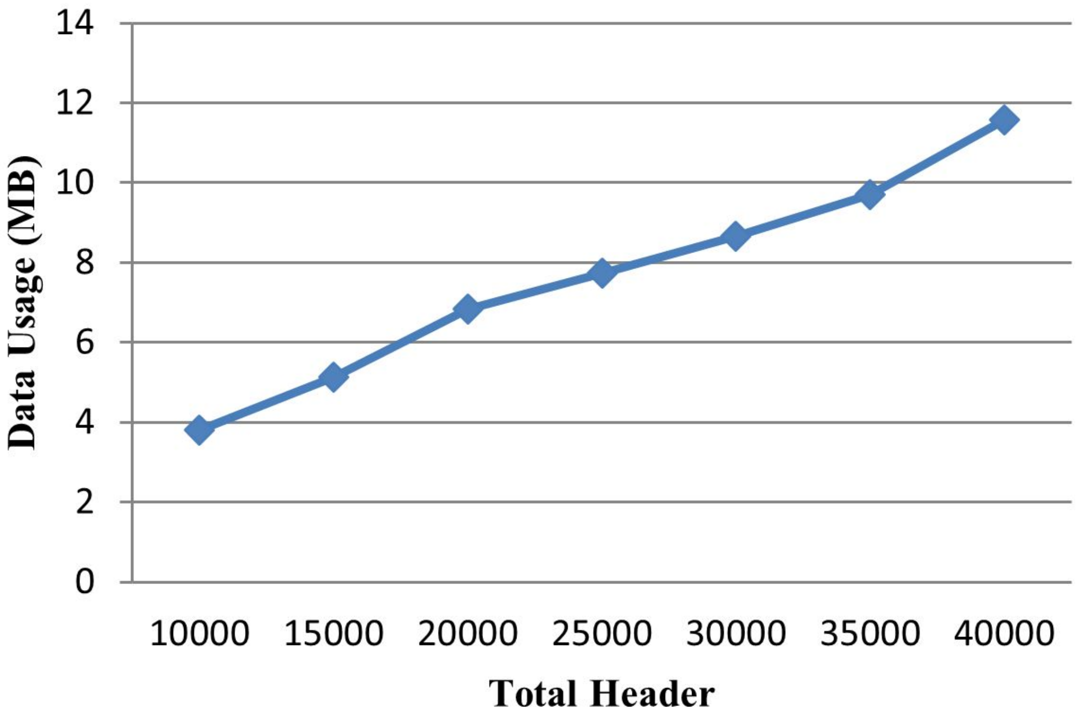
~

Reward of Relay Node

Gas Price	1 gWei
Gas Limit	70000
Real Gas Cost	~60000



Data Usage of Relay Node



Outline

- Introduction
- Related Work
- Shortcomings of Existing Solutions
- Our Target
- Methodology
- Implementation
- Evaluation
- Conclusion and Future Work

Our Contribution

Integrate IoT Devices into Blockchain

with Low Centralization Degree and Low Power Consumption

for Responsible Sensory Data

https://github.com/bonboru93/master_final

Future Work

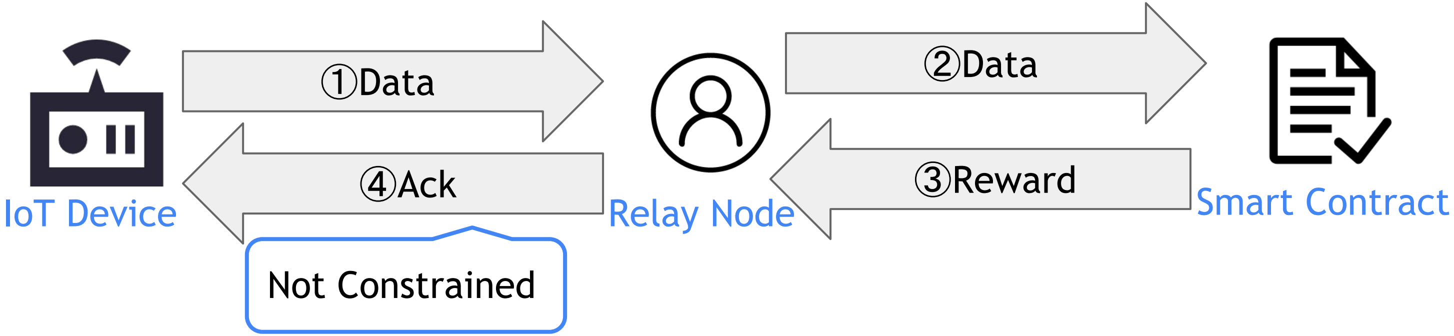
- Extend to Other Communication Method, like QR Code, NB-IoT
- Extend to Other Blockchain Network, like HyperLedger
- Cooperate with Smart City and Product Traceability Programs

Q & A

Why NFC and LoRa

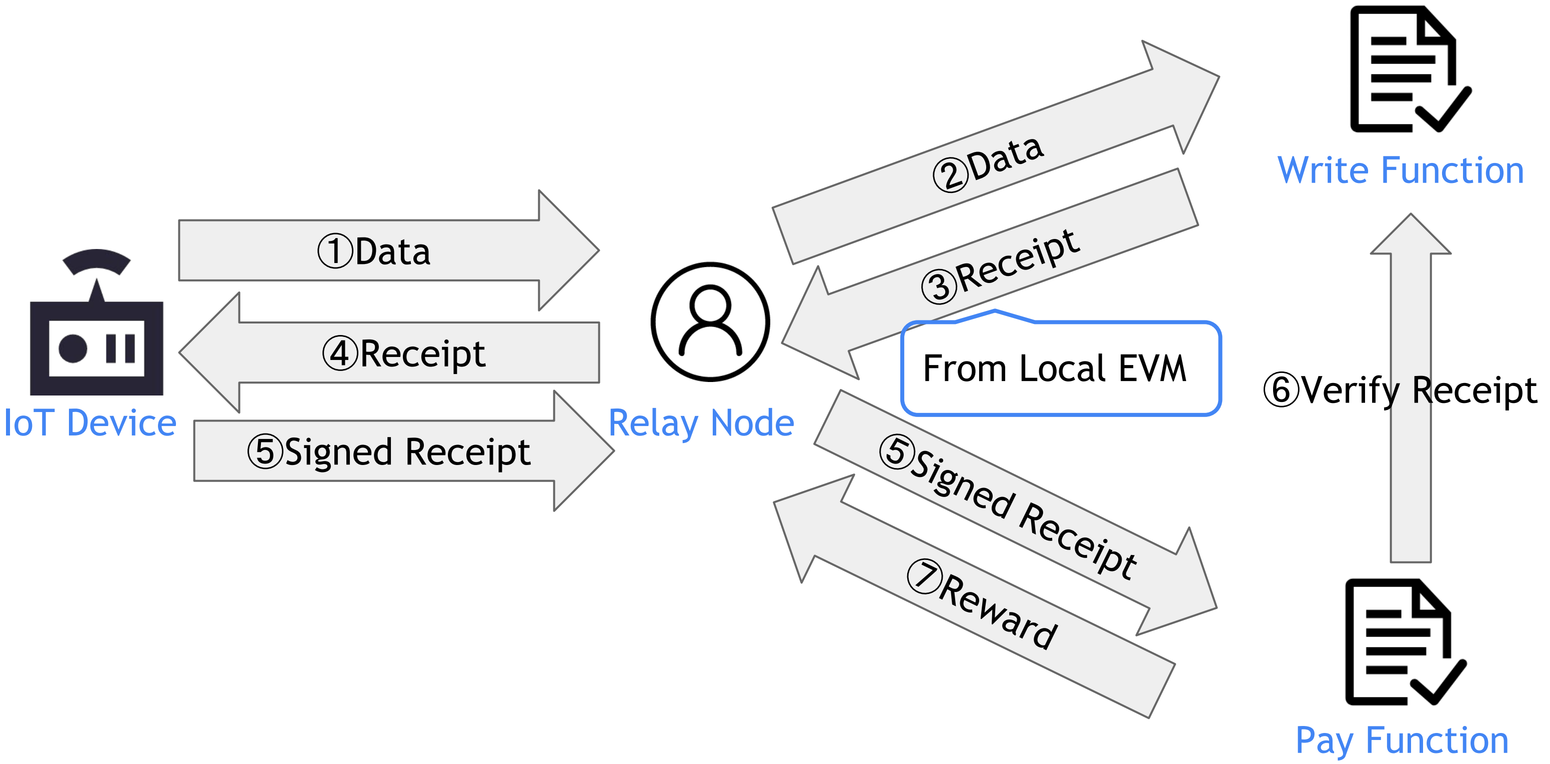
Property	NFC	LoRa
Distance	Short (< 4 cm)	Long (> 10 km)
Broadcast Mode	Passive	Active
Supplement	Active Method	Own Relay
Feature	Sleep Mode	Non-IP Based
Backup	E Ink Screen with QR Code	NB-IoT

Why No Ack



IoT Device
①Data
④Ack
Not Constrained
Relay Node
②Data
③Reward
Smart Contract

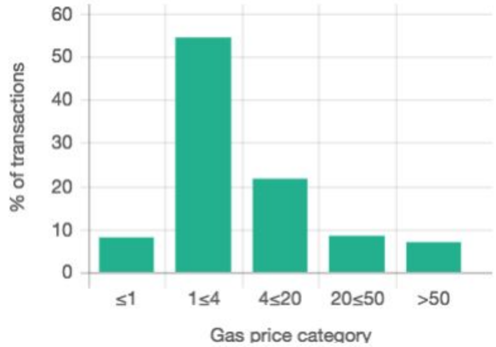
How about 2-Way Ack



Gas Price Detail

Std Cost for Transfer	Gas Price Std (Gwei)	SafeLow Cost for Transfer	Gas Price SafeLow (Gwei)	Median Wait (s)	Median Wait (blocks)
$0.014	1.4	$0.011	1.1	45	3

Transaction Count by Gas Price



Recommended Gas Prices

(based on current network conditions)

Speed	Gas Price (gwei)
SafeLow (<30m)	1.1
Standard (<5m)	1.4
Fast (<2m)	3

Note: Estimates not valid when multiple transactions are batched from the same address or for transactions sent to addresses with many (e.g. > 100) pending transactions

https://ethgasstation.info/

Gas Cost of Hash and Signature Verification

Keccak256	30 + 6 * (size of input in words)
ecrecover	~ 3000 in Our Implementation
Transfer	21000

Power Consumption of Raspberry Pi

Table 2: Use cases and their estimated execution time for mining 400 blocks.

Platform	Nodes		Execution time	Average power		Energy
	Total (n)	Mining (k)		k nodes	(n-k) nodes	
Raspberry Pi 2	1	1	3082 s	1724 mW	0 mW	5.3 kJ
	2	1	3082 s	1724 mW	1144 mW	8.8 kJ
	2	2	1710 s	1704 mW	0 mW	5.8 kJ
	4	1	3082 s	1724 mW	1143 mW	15.9 kJ
	4	2	1710 s	1704 mW	1144 mW	9.7 kJ
	4	4	954 s	1667 mW	0 mW	7.5 kJ
	8	1	3082 s	1724 mW	1143 mW	30.0 kJ
	8	2	1710 s	1704 mW	1144 mW	17.6 kJ
	8	4	954 s	1667 mW	1145 mW	10.7 kJ
	8	8	575 s	1612 mW	0 mW	7.4 kJ
	16	1	3082 s	1724 mW	1143 mW	58.1 kJ
	16	2	1710 s	1704 mW	1144 mW	33.2 kJ
	16	4	954 s	1667 mW	1145 mW	19.5 kJ
	16	8	575 s	1612 mW	1146 mW	12.7 kJ
	16	16	386 s	1544 mW	0 mW	10.0 kJ
Nvidia Jetson TK1	1	1	702 s	6517 mW	0 mW	4.6 kJ
	2	1	702 s	6517 mW	1990 mW	6.0 kJ
	2	2	393 s	6308 mW	0 mW	5.0 kJ
	4	1	702 s	6517 mW	1973 mW	8.7 kJ
	4	2	393 s	6308 mW	2006 mW	6.5 kJ
	4	4	223 s	5948 mW	0 mW	5.3 kJ
	8	1	702 s	6517 mW	1968 mW	14.2 kJ
	8	2	589 s	6308 mW	1990 mW	9.7 kJ
	8	4	223 s	5948 mW	2032 mW	7.1 kJ
	8	8	138 s	5435 mW	2184 mW	6.3 kJ
	16	1	702 s	6517 mW	1966 mW	25.3 kJ
	16	2	393 s	6308 mW	1985 mW	15.9 kJ
	16	4	223 s	5948 mW	2018 mW	10.7 kJ
	16	8	138 s	5435 mW	2071 mW	8.3 kJ
	16	16	96 s	4838 mW	0 mW	7.6 kJ

Halunen, K., Kreku, J., Vallivaara, V., & Suomalainen, J. (2017). Evaluating the Efficiency of Blockchains in IoT with Simulations. Iotbds.

Reward of Relay Node

(80000 - 70000) * 10^9 * 10 / 10^18 ≈ 0.0001 Ether

Gas Price	1 gWei
Gas Limit	80000
Real Gas Cost	~70000