

Multi-Authority Attribute-Based Access Control with Smart Contract

Hao Guo Ehsan Meamari Chien-Chung Shen

Department of Computer and Information Sciences, University of Delaware, U.S.A.

{haoguo,ehsan,cshen}@udel.edu

ABSTRACT

Attribute-based access control makes access control decisions based on the assigned attributes of subjects and the access policies to protect objects by mediating operations from the subjects. Authority, which validates attributes of subjects, is one key component to facilitate attribute-based access control. In an increasingly decentralized society, multiple attributes possessed by subjects may need to be validated by multiple different authorities. This paper proposes a multi-authority attribute-based access control scheme by using Ethereum's smart contracts. In the proposed scheme, Ethereum smart contracts are created to define the interactions between data owner, data user, and multiple attribute authorities. A data user presents its attributes to different attribute authorities, and after successful validation of attributes, obtains attribute tokens from respective attribute authorities. After collecting enough attribute tokens, a smart contract will be executed to issue secret key to the data user to access the requested object. The smart contracts for multi-authority attribute-based access control have been prototyped in Solidity, and their performance has been evaluated on the Rinkeby Ethereum Testnet.

CCS CONCEPTS

• Security and privacy → Access control; Information accountability and usage control.

KEYWORDS

Blockchain, smart contract, multi-authority, attribute-based access control.

ACM Reference Format:

Hao Guo Ehsan Meamari Chien-Chung Shen. 2019. Multi-Authority Attribute-Based Access Control with Smart Contract. In *Proceedings of 2019 International Conference on Blockchain Technology (ICBCT 2019) (ICBCT 2019)*. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3320154.3320164>

1 INTRODUCTION

In computer and information security, the mechanism of access control has been widely used to protect objects from unauthorized operations by subjects. Such operations may include creating,

deleting, discovering, editing, executing, event recording [7], and reading of objects. Formally, access control mechanisms is defined as *the logical component that serves to receive the access request from the subject, to decide, and to enforce the access decision* [9]. With access control, owners of objects have the authority to establish access policies that govern which subjects may perform what operations on the objects. How these access policies are specified depends on the access control models within which the subjects, objects, operations, and rules interact to make and enforce access control decisions. Although each model has its own advantages and limitations, over time, access control models have evolved from identity-based to role-based, and to attribute-based.

In general, attribute-based access control makes access control decisions based on the assigned attributes of subjects and the access policies (complex Boolean rules evaluating attributes) to protect objects by mediating operations from the subjects. Broadly speaking, attribute-based access control has been defined as *an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions* [9].

To facilitate attribute-based access control, one critical component is an *authority* which validates attributes of the subjects to make access control decisions. In theory, one attribute authority (AA) may oversee and validate all the attributes of subjects. However, in an increasingly decentralized society, there may exist multiple authorities which take part in validating different attributes possessed by subjects. For instance, a Delaware resident is a student of the University of Delaware and also interns at the DuPont company. These three attributes must be validated by three different authorities, the University of Delaware, Delaware's Division of Motor Vehicles, and the DuPont company. As another example of a commercial application, two banks, such as JP Morgan Chase and Bank of America, hence two authorities, may both need to validate respective attributes of people who take part in a joint project.

In this paper, we propose a scheme to facilitate multi-authority attribute-based access control by using Ethereum smart contracts. In this scheme, data owner generates a secret key and encrypt the shared data with the AES algorithm, and keeps the secret key with himself. Within Ethereum's smart contracts, a data user presents attributes to respective authorities to obtain attribute tokens after successful validation. Upon collecting enough attribute tokens from multiple attribute authorities, the data user will receive the AES secret key capable of accessing the request data. Our contributions are mainly two parts: First, we propose the multi-authority attribute-based access control mechanism by designing smart contracts and utilizing Ethereum blockchain platform. Second, we implement the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ICBCT 2019, March 15–18, 2019, Honolulu, HI, USA

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6268-9/19/03...\$15.00

<https://doi.org/10.1145/3320154.3320164>

attribute token rules to represent the attribute sets and access policy in traditional attribute-based access control mechanism. With the design of multiple attribute authorities, we achieve the multi-authority functionality for our scheme.

The remainder of this paper is organized as follows. In Section 2, backgrounds of Ethereum smart contract and attribute-based access policy are reviewed. Then, the architecture of smart contract-based multi-authority access control scheme, and the detailed designs of smart contracts are presented in Section 3. In Section 4, we evaluate the costs of executing the smart contracts and analysis the security and privacy issues. Related work is described in Section 5, and Section 6 concludes the paper.

2 PRELIMINARY

In this section, we review the basic concepts of Ethereum with smart contract and attribute-based access policy.

2.1 Ethereum with Smart Contract

Ethereum is a distributed computing platform featuring the smart contract functionality [4],[6]. It is proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer [1]. The Ethereum development was funded by an online crowdsale event which took place between July and August 2014, and the official system went live on 30 July 2015 [1]. In contrast to Bitcoin-like systems where transactions are programmed in a simple non-Turing complete scripting language, and can only specify basic logic relations, which limits their utility to other application domains, Ethereum smart contract provides an event-driven, Turing complete scripting functionality to specify and process complex transactions which can be verified to demonstrate the feasibility of the contract operation. From the perspective of the smart contract, it works like the a event-driven script and will automatically execute the script if the pre-defined logical condition has been satisfied. Before the smart contract is executed, all related logic functions and processes were already established.

Within Ethereum, there are two types of accounts: Externally Owned Accounts (EOA) and Contract Accounts, both of which are uniquely identified by a 20-byte hexadecimal string as their address. An EOA is controlled by its owner’s private key, has an available ether balance, and can send transactions (for instance, send a message to another account for transferring ether or trigger the execution of a smart contract). It has no associated code with EOA account. While a contract account also has an ether balance, but contains the associated code which can be triggered by a transaction or from other smart contract.

Ether is the official cryptocurrency used in Ethereum platform. All the ether balances and values are represented in units of wei: 1 ether is 1e18 wei. The Ethereum platform has a smart contract running environment, which is known as the Ethereum Virtual Machine (EVM) [5]. Each mining node in the Ethereum network (Node receives, broadcast, verifies, and executes the transaction in Ethereum network) runs EVM as part of the validation procedure and later perform the same results and store the data. Every operation in EVM has a specific cost, which is counted by the amount of gas. The sender of the transaction needs to pay for ether for the

Nonce
Receiver Address
Gas Price
Gas Limit
Amount
V
R
S
Data

Figure 1: Data structure of an Ethereum transaction.

operations and the total transaction cost is estimated as Ether = Gas Used * Gas Price.

TxHash:	0xc5ee3ae9cf10fbee05325e3a25c3b19489783612e36cb5b5b054c2cb4f82fc28
Block Height:	290081 (8061724 block confirmations)
TimeStamp:	1088 days 5 hrs ago (Sep-25-2015 09:00:32 PM +UTC)
From:	0x1dcb8d1f0fcc8cbc8c2d76528e877f915e299f8e (Suprnova_1)
To:	0x702bd0d370bbf0b97b66fe95578c82897c583393
Value:	5.00011139 Ether (\$986.92)
Gas Limit:	90000
Gas Used By Txn:	21000
Gas Price:	0.00000005 Ether (50 Gwei)
Actual Tx Cost/Fee:	0.00105 Ether (\$0.21)
Nonce & (Position):	34344 (0)
Input Data:	0x

Figure 2: Ethereum transaction example from etherscan.io.

The Ethereum transaction is a data package which enables user to transfer ether from one account to another account. In addition, it can also trigger the execution of the code in the smart contract through one transaction. Figure 2 and 3 shows the Ethereum transaction data structure and one screenshot from the Etherscan website (etherscan.io). One unique Ethereum transaction consists of the following data field: Nonce, represents for the transaction sequence number from the sender. Receiver address, which contains the receiver account information. Gas price, the price user offer to pay. Gas limit, maximum amount of gas allowed for one transaction. Amount, the total ether balance transferred to the destination address. V, R, and S, together makes up the Elliptic Curve Digital Signature Algorithm (ECDSA) for sender’s signature. Data, optional additional data fields which can be put into any data.

2.2 Attribute-Based Access Policy

Attribute-based access control (ABAC) defines an access control policy, in which the access rights are granted to users through the use of access policies which combine attributes together [3]. The access policies could use any type of attributes. For instance, subject’s attribute, object’s attribute, and environment attributes. Access policy can support the Boolean rule, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action [3]. For example: IF the requester is a University of

Delaware graduate student, THEN allow the access to the data. The critical feature of ABAC is the concept of access policies which can express a complex Boolean rule set that can evaluate many different attributes [9].

In our solution, we adopt the AND-gate access policy AND_m^* , which supports multiple values with wildcards * [14]. An access policy W is a rule which returns either 0 or 1, given an attribute set S . That is, attribute set S satisfies policy W if and only if W evaluates to 1 on S . Note that the wildcard * in an AND-gate policy plays the role of a “don’t care” value. Formally, given an attribute list $S = [S_1, S_2, \dots, S_n]$ and an access policy $W = [W_1, W_2, \dots, W_n] = \bigwedge_{i \in I_W} W_i$, where I_W is a subscript index set and $I_W = \{i | 1 \leq i \leq n, W_i \neq *\}$, and we say that $S \models W$ if $S_i = W_i$ or $W_i = *$ for all $1 \leq i \leq n$ and $S \not\models W$ otherwise [14].

Here we present a concrete example. Suppose an data owner in the Computer and Information Sciences Department at the University of Delaware specifies access policy W to be [UD, PhD Student, Gender*] for accessing encrypted research meeting notes, and we have student Alice’s attribute list $S_{\text{Alice}} = [\text{UD}, \text{PhD Student}, \text{Female}]$, and student Bob’s attribute list $S_{\text{Bob}} = [\text{UD}, \text{Master Student}, \text{Male}]$. As a result, Alice can access the corresponding encrypted research meeting notes, while Bob cannot because he is an Master student. Notice that the Gender* attribute indicates that either gender satisfies the access policy.

3 ARCHITECTURE OF SMART CONTRACT BASED MULTI AUTHORITY ACCESS CONTROL

In this section, we describe the architecture of the proposed multi-authority attribute-based access control scheme based on smart contracts. By referring to Fig. 3, we first enumerate the following entities that take part (either actively or passively) in the architecture.

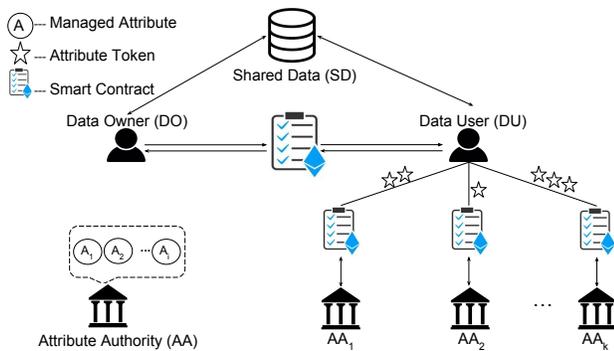


Figure 3: Proposed system scheme.

- Data Owner (DO): A DO is an entity (e.g., person, organization, or process) who owns the data to be shared. A DO actively specifies access policies for the data it shares.
- Data User (DU): A DU is an entity who wants to access data shared by DOs. A DU actively seeks access authorizations from DOs.

- Shared Data (SD): An SD is a piece of data owned by a DO, and can be accessed passively by authorized DUs.
- Attribute Token (AT): An AT is a credential representing an attribute that a DU possesses.
- Attribute Authority (AA): An AA is a pre-verified and authorized node in Ethereum who issues ATs to qualified DUs who possess the corresponding attributes.

In the proposed architecture, after a DU has been validated for possessing a particular set of attributes by an AA, the AA will then issue the corresponding set of ATs to the DU. This validation process is carried out in the context of smart contracts. Consequently, satisfaction of the access policy associated with an SD is now represented by the collection of the corresponding ATs. Once a DU meets the access control policy imposed by the DO of the SD, the smart contract between the DU and the DO is executed for the DU to receive the AES secret key (which is encrypted with DU’s public key) from the DO to access the SD.

Fig. 4 depicts a sample workflow scenario, where a DU, multiple AAs, and a DO communicate via smart contracts, as defined below, to perform multi-authority attribute-based access control.

- (1) AAs, DO, and DU register their respective EOA accounts with Ethereum, so that they may participate in Ethereum blockchain network. (Not shown in Fig. 4.)
- (2) Using a standard symmetric encryption algorithm, such as AES-256, the DO generates a secret key to encrypt the SD, and uploads the encrypted data to a shared database. In addition, the DO defines the access policy for the SD and creates smart contract **DO** to be executed between itself and the DU.
- (3) A DU creates smart contract **RequestAT** with each AA, which contains the function `checkA` that requests validation of its attributes, and returns the corresponding ATs upon successful validation. The DU also creates smart contract **RequestKey** with the DO, which contains function `checkAT` that the DU holds enough ATs to send the AES secret key.
- (4) AA₁ creates a smart contract **AT** between itself and the DU, which contains function `checkAttribute` for validating the DU’s attributes, and the function `sendToken` for granting ATs. Similarly, AA₂ creates another smart contract **AT** between itself and the DU.
- (5) Now, the DU wanting to access the SD executes its smart contract **RequestAT** to request validation of its attributes by invoking function `checkA`. In turns, `checkA` triggers the execution of the smart contract **AT** by invoking the `checkAttribute` function of **AT**. Upon successful validation, the `sendToken` function is invoked to return the associated ATs to be saved in the “balance” of DU’s EOA account.
- (6) After accumulating enough “balance,” the DU will executes smart contract **RequestKey** to invoke its function `checkAT` for validating its ATs so as to obtain the AES secret key (encrypted with DU’s public key) by triggering smart contract **DO** and invoking its `sendKey` function.
- (7) At the end, the DU decrypts the AES secret key (which was encrypted with its public key) with his private key, and uses the AES secret key to access the SD.

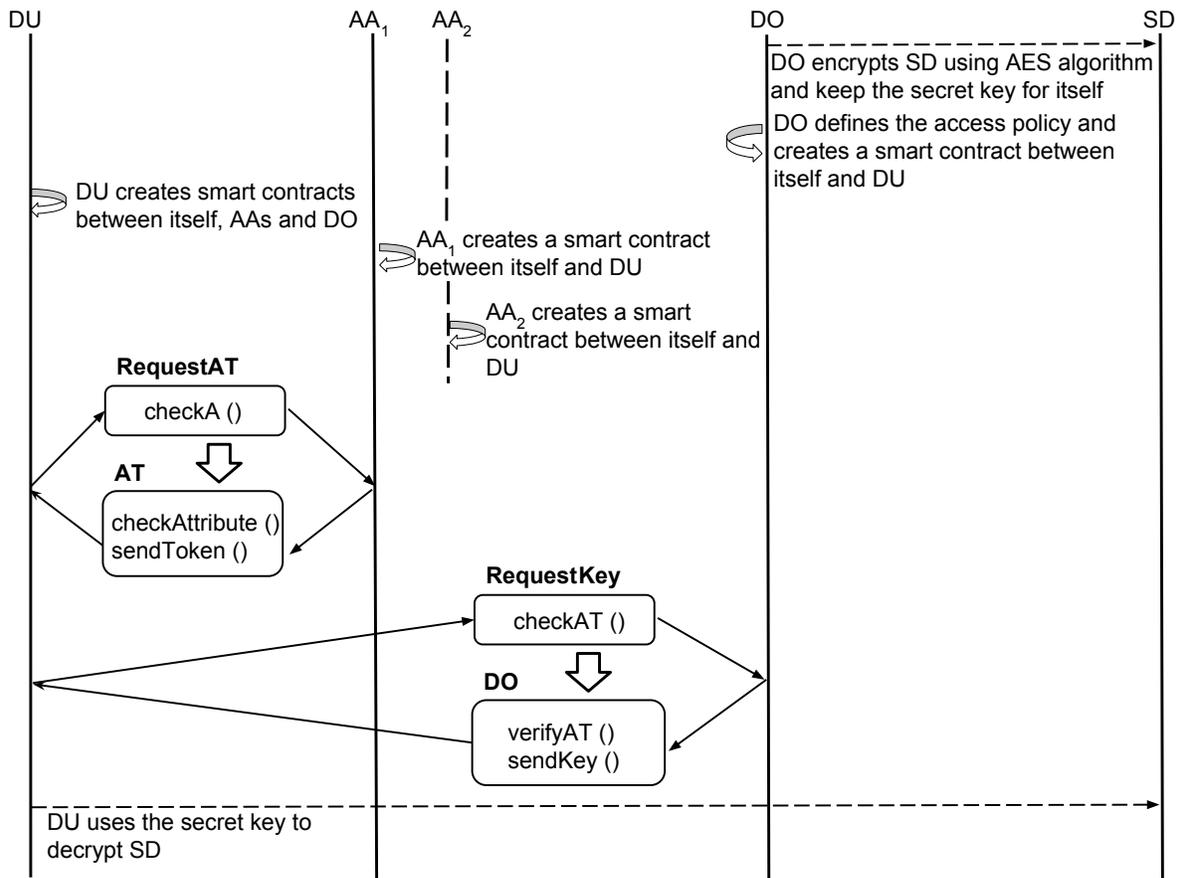


Figure 4: Proposed workflow scenario.

The smart contract created by DU between itself and AA:

```

contract RequestAT {
    function checkA(addressOfAA){
        AT my_at = AT(addressOfAA);
        if (my_at.checkAttribute() == true)
            return my_at.sendToken();
        return FAILURE;
    }
}
    
```

The smart contract created by DU between itself and DO:

```

contract RequestKey {
    function checkAT(addressOfDO){
        DO my_ap = DO(addressOfDO);
        if (my_ap.verifyAT() == true)
            return my_ap.sendKey();
        return FAILURE;
    }
}
    
```

The smart contract created by AA between itself and DU:

```

contract AT is ERC20Interface, Owned{
    string public symbol;
    string public name;
    uint8 public decimals;
    mapping(address => uint) balances;
    mapping(uint256 => Data) CheckAttribute;

    event Sendtoken(address from, address to,
    uint tokens);

    struct Data{
        uint256 AttributeID;
        string attribute;
        string approve;
    }

    function AttributeToken() public{
        symbol = "UD";
        name = "UD Token";
        decimals = 0;
        totalSupply = 100;
        balances [addressOfAA] = totalSupply;
    }
}
    
```

```

    }
    function checkAttribute(uint256
    AttributeID, string attribute, string
    approve) public returns (bool success){
        CheckAttribute[AttributeID] =
        Data(AttributeID, attribute, approve);
        return true;
    }

    function sendToken(address to, uint tokens)
    public returns (bool success){
        require(!frozenAccount[to]);
        emit Sendtoken(msg.sender, to, tokens);
        return true;
    }
}

```

The smart contracts created by DO between itself and DU:

```

contract DO {
    event Sendkey(address from, address to,
    bytes encryptedKey);
    event VerifyAT(address to, uint tokens,
    bytes approve);

    struct AESData{
        bytes encryptedKey;
    }

    function sendKey(address to, bytes
    encryptedKey) public returns (bool
    success){
        emit Sendkey (msg.sender, to,
        encryptedKey);
        return true;
    }

    function verifyAT(address from, address
    to, uint tokens, bytes approve)
    public returns (bool success){
        allowed [to][from] = tokens;
        require(balanceOf(to) >=
        balanceOf(from));
        emit VerifyAT(to, tokens, approve);
        return true;
    }
}

```

Smart contracts provide the benefits of authentication, authorization, and audit as follows. First, when DO or DU executes a transaction, authentication is guaranteed since only the legitimate DO and DU accounts are able to initiate transactions. Second, the authorization is achieved by adopting ATs granted from multiple AAs to the DU if the DU has valid attributes, and later DO could check the ATs provided by the DU to determine if the DU satisfies the access policy or not. Third, by adopting the inherent design of blockchain, every transaction's record has been stored permanently

and it's easy for people to audit the transaction information in future. In the end, each DU and DO has its own public and private keys, any attacker with no prior knowledge of the user's private key cannot decrypt the data send between DO and DU.

Overall, these smart contracts deploy the proposed scenarios as we described before. We implement the proof of concept prototype to illustrate the feasibility of our designed smart contracts and evaluate the experimental result in next section.

4 PERFORMANCE EVALUATION AND SECURITY ANALYSIS

In this section, we evaluate the creation cost of smart contracts and the execution cost of their respective functions that facilitate multi-authority attribute-based access control via experiments on the Rinkeby Ethereum Testnet.

4.1 Experiment Setting

The smart contracts presented in the last section were programmed in Solidity [10] by using the official on-line IDE Remix. In the month of October 2018, 1 ether \approx 205 US\$. In our experiments, 1 gas = 1e9 ether, which is the minimum transaction cost. The lower the gas value, the longer time a transaction will be validated by miners, and vice versa.

4.2 Results

The costs of smart contract creations and their respective function executions are presented in Table 1. As we can observe from the table, the one-time costs of smart contract creation for RequestAT, ResquestKey, and AT are 0.232, 0.208 and 0.359 US\$, respectively, based on the current price of ether. In comparison, the cost of function executions is relatively low. Note that the execution costs of these functions vary based on the different input lengths such as the attribute information and other related data.

Experiment Results			
Contract/Function	Gas Used	Cost(ether)	USD (\$)
RequestAT (C)	1132452	0.001132452	0.232
RequestKey (C)	1022644	0.001022644	0.208
AT (C)	1752958	0.001752958	0.359
checkAttribute (F)	394286	0.000394286	0.080
sendToken (F)	123680	0.000123680	0.025
verifyAT (F)	356070	0.000356070	0.073
sendKey (F)	224520	0.000224520	0.046

Table 1: Cost of smart contracts and functions.

4.3 Security Analysis

In our proposed scheme, we integrate the Ethereum smart contract, multi-authority attribute-based access control policy, and AES mechanism to provide a robust and privacy-preserving system. First, data owners fully control their personal data and there is no third-party authority to collect the information from the data owner. They have the right to distribute AES secret key to qualified data user. Second, in our solution, we utilize the multiple attribute

authorities to avoid possible collusion and single point of failure. Since each attribute authority only responsible for certain number of attribute tokens, the attribute tokens reliability and availability is highly secured. Last, we use the Ethereum’s blockchain platform to perform communications among different participants, which saves all the data records and transaction information. If later people like to trace back certain information, it will be easy to provide the data provenance records due to the character of blockchain technology.

5 RELATED WORK

Several efforts have been done to provide the access control mechanism with the help of blockchain-based technologies. Maesa et al. [8] proposes a solution to publish policies specifying the rights to access resources, and demonstrated a potential implementation based on deploying the eXtensible Access Control Markup Language (XACML) [13] on a Bitcoin blockchain network. Cruz et al. [5] describes a role-based access control scheme using smart contracts, which is composed of two parts, the smart contracts to represent the trust and endorsement relationship and the challenge-response protocol to verify user identity. Al-Bassam et al. [2] proposes the SCPKI (A Smart Contract-based PKI and Identity System), which is an PKI system based on a decentralized design using the web-of-trust model and a smart contract. The web-of-trust model enables an entity or authority in the system can verify attributes of another entity’s identity (such as company name or domain name), as an alternative solution to the centralized authority identity verification model. Uchibeke et al. [11] proposed blockchain-based access control ecosystem which gives asset owners the sovereign right to manage access control for data sets and protect the data integrity. They use the Hyperledger composer tool to implement the smart contracts and other functions deployed on the blockchain network. Westerkamp et al. [12] presents a blockchain-based supply chain traceability system using smart contracts. In their mechanism, each manufacturer defines the composition of products in the form of recipes, and each ingredient of the recipe is a non-fungible token which corresponds to a physical good. Overall, this system preserves the traceability of different product transformations.

In our work, we propose the multi-authority attribute-based access control scheme by using smart contract. Additionally, by utilizing the ERC-20 token standards and other functionalities provided by the solidity language, we map each unique attribute to attribute token to represent the requirement of access policy and other event-driven function to achieve the desired goal.

6 CONCLUSION

Our increasingly decentralized society motivates the need of multiple authorities to take part in attribute-based access control. In this paper, we propose a multi-authority attribute-based access control mechanism. The interactions among data users, data owners, and multiple authorities are programmed into Ethereum smart contracts. We describe the architecture and operational workflow of multi-authority attribute-based access control. As a proof of concept, the scheme is programmed in Solidity and tested on the Rinkeby Ethereum Testnet.

REFERENCES

- [1] 2018. Ethereum — Wikipedia, The Free Encyclopedia. <https://en.wikipedia.org/wiki/Ethereum>. (2018).
- [2] Mustafa Al-Bassam. 2017. SCPKI: A smart contract-based PKI and identity system. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 35–40.
- [3] Attribute based access control. 2018. https://en.wikipedia.org/wiki/Attribute-based_access_control. (2018).
- [4] CoinDesk. 2016. <https://www.coindesk.com/information/what-is-ethereum>. (2016).
- [5] Jason Paul Cruz, Yuichi Kaji, and Naoto Yanai. 2018. RBAC-SC: Role-Based Access Control Using Smart Contract. *IEEE Access* 6 (2018), 12240–12251.
- [6] Ethereum. 2015. Blockchain Application Platform. <https://ethereum.org>. (2015).
- [7] Hao Guo, Ehsan Meamari, and Chien-Chung Shen. 2018. Blockchain-inspired event recording system for autonomous vehicles. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 218–222.
- [8] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. 2017. Blockchain based access control. In *IFIP International Conference on Distributed Applications and Interoperable Systems*. Springer, 206–220.
- [9] NIST. 2014. SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Consideration. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf>. (2014).
- [10] Solidity. 2018. <https://solidity.readthedocs.io/en/v0.4.25/>. (2018).
- [11] Uchi Ugobame Uchibeke, Sara Hosseinzadeh Kassani, Kevin A Schneider, and Ralph Deters. 2018. Blockchain access control Ecosystem for Big Data security. *arXiv preprint arXiv:1810.04607* (2018).
- [12] Martin Westerkamp, Friedhelm Victor, and Axel Küpper. 2018. Blockchain-based Supply Chain Traceability: Token Recipes model Manufacturing Processes. *arXiv preprint arXiv:1810.09843* (2018).
- [13] XACML. 2013. (2013). OASIS: eXtensible Access Control Markup Language (XACML) version 3.0 (January 2013).
- [14] Yinghui Zhang, Dong Zheng, Xiaofeng Chen, Jin Li, and Hui Li. 2014. Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts. In *International Conference on Provable Security*. Springer, 259–273.