An Infrastructure for Service Accountability based on Digital Identity and Blockchain 3.0

A. Furfaro, L. Argento, D. Saccà, F. Angiulli, F. Fassetti

University of Calabria
DIMES – 87036 Rende(CS) - Italy
Email: angelo.furfaro@unical.it

CryBlock 2019 - The 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems
April 29th, 2019, Paris, France

IEEE INFOCOM

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI
INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA
DIMES

Outline

- Accountability issues in the coordination of business processes belonging to different organizations
- Centralized vs. decentralized approaches
- Key technologies
  - Blockchain
  - Digital Identity
- Infrastructure's architecture
- Smart Contracts
- Processes
- Conclusions

Introduction

In the last few years, due to the pervasiveness of ICT-based business processes, the number interactions (e.g. contracts, transactions) established among processes belonging to **different organizations** have significantly increased

Macro process

- Internal business processes: accountability is fully supported
- Inter-organization interactions: the concept of actor's identity is not clearly and globally defined. It is difficult to provide accountability

What is needed

A reliable platform that enables the establishment of the above-mentioned agreements in a fast, secure and *accountable* way.

Centralized approaches

A working solution can be easily devised and deployed by resorting to a centralized coordination/orchestration service under the control of a third-party entity

Trust and security concerns

- The cooperating entities must **strongly trust** a third-party entity
- Such an entity de facto governs and it is responsible for the proper enactment of the interactions
- There is a single point of failure with respect to **security** and **privacy** concerns
- No matter how strong an organization's defense wall is, sensitive data may be improperly/maliciously accessed or compromised by a malware gaining access to the third-party systems.

Decentralized approaches

Goal

Achievement of the above requirements without relying on mutual trust relationships and/or on reputation systems

Issues

1. Reaching a global consensus on the system state among the peers
2. Involved entities must be uniquely and authoritatively identifiable

Key technologies

1. Blockchain technologies can used to address the global consensus
2. (Authoritative) digital identity systems can be exploited for the identification of the involved parties

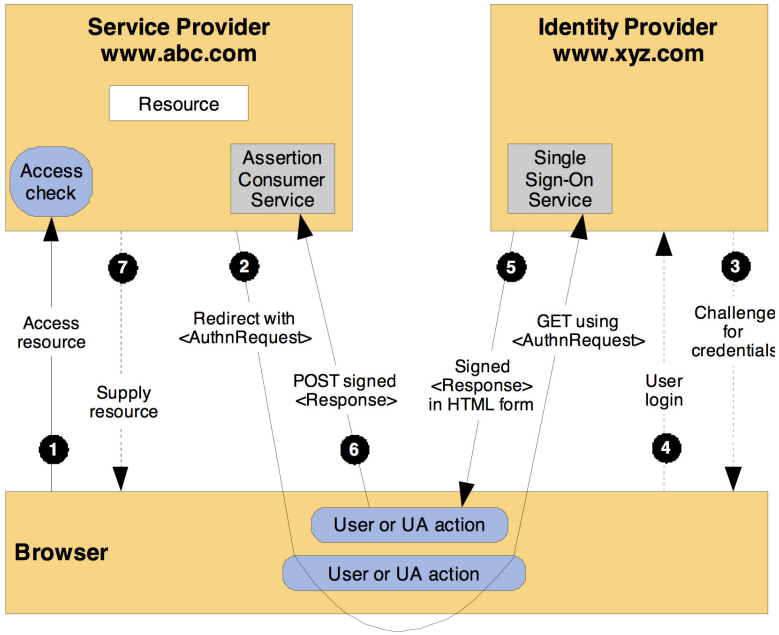
Blockchain

- Blockchain technologies were early developed for supporting the bitcoin cryptocurrency
- A blockchain is a decentralized peer-to-peer system with no central authority which implements a *distributed ledger*
- All participants within a network can have their own identical copy of the ledger and collaborate to obtain an agreed and reliable version of the ledger, where all the transactions are signed by authors and publicly visible, verified and validated
- There is no link between transaction actor in the ledger and his real-world identity
- Blockchain 2.0 introduced the notion of *smart contracts* as tools for creating and customising operations to build new type of blockchain-based applications
- Blockchain 3.0 added a new component, called Master Node (MN), which is a server running on a peer-to-peer network, that provides resource intensive services (e.g. the Dash blockchain)

Digital Identity

- In order to achieve the accountability requirements in cooperative services, the involved parties must be uniquely and authoritatively identifiable
- Digital Identity technologies emerged as key elements in the delivery/fruition of IT based processes in public administrations
- The European Union has recently introduced **eIDAS**: a regulation on a set of standards for electronic identification and trust services for electronic transactions
- The National Institute of Standards and Technology (NIST) also introduced its own digital identity model
- The proposed infrastructure has been devised to be integrated with SPID (The Italian identity provider system compliant with eIDAS)

Italian Public System for Digital Identity (SPID)



SPID identifies the following roles:

- *Identity Provider* (IDP): is in charge of identifying and authenticating a client requiring access to a resource/service and of providing some information (attributes) about the client;
- *Service Provider* (SP): it provides a resource/service to a client after a successful authentication phase through an interaction with an IDP
- *Attribute Authority* (AA): it is an authoritative source of additional attributes (e.g. role, position played in a given organization) about the authenticated client which can be used to define his authorization profile.

Example Scenario

Setting

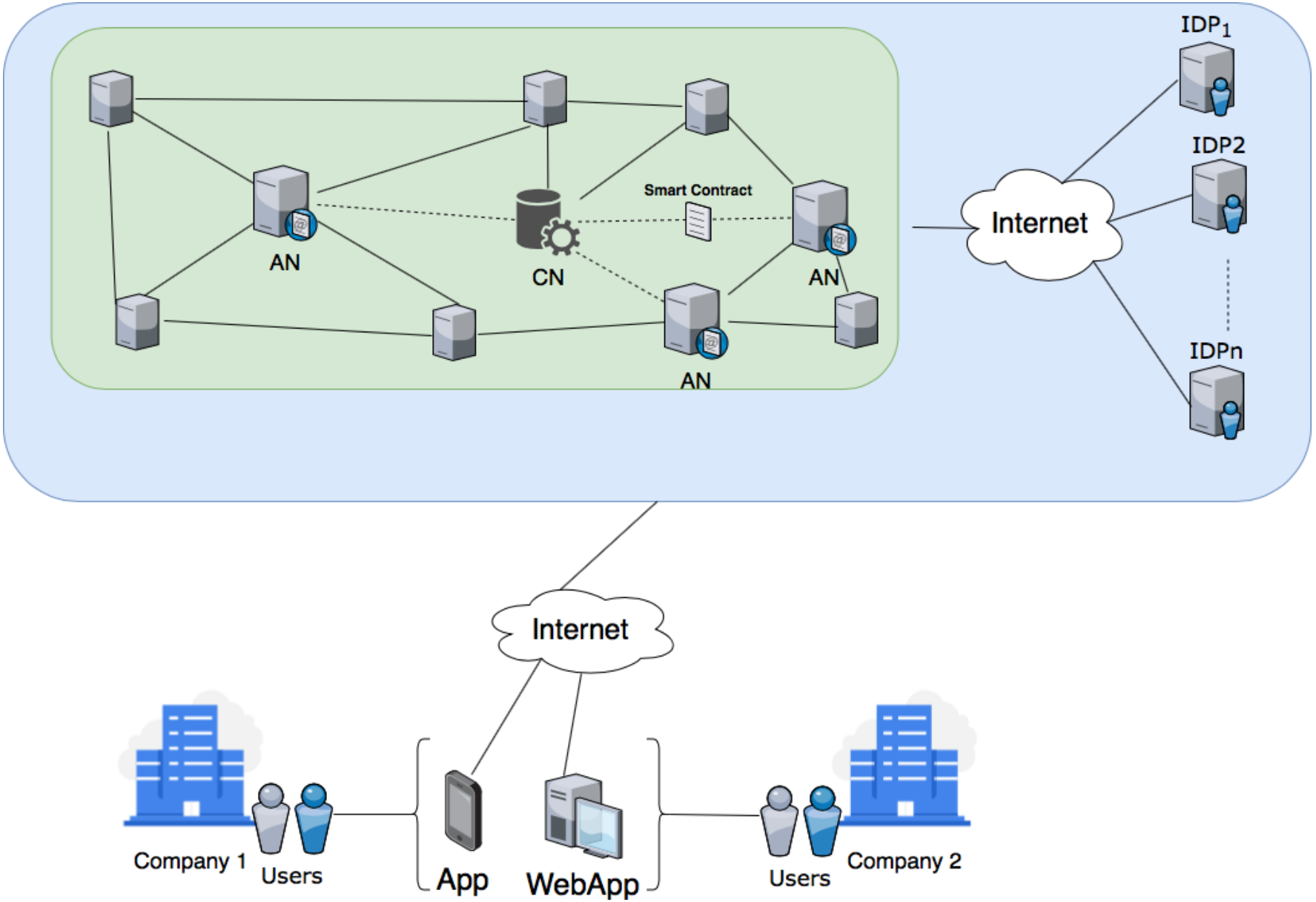
- Company A needs to send Company B a load of product that A has just finished producing.
- Company A contacts a logistics company C to arrange the transfer.
- Behind the scenes, this operation is performed by two or more actors that belong to the two companies.
- Suppose that the transfer is arranged by two actors, i.e. Alice and Bob.
- Alice works for company A, whereas Bob for the logistics company.
- The arrangement is an inter-organisation interaction, hence the actors need to make it accountable.

Example Scenario

Requirements:

- Alice and Bob need a digital identity.
- The digital identities must be certified by a trusted entity.
- Alice and Bob request a service to make the operation accountable.
- The service takes the actors' digital identity and a document describing the operation.
- The service creates a record attesting that Alice and Bob account for the execution of the operation.
- The record stores an association between Alice and Bob's digital identity along with operation-related data.

Accountability Infrastructure – Architecture



Accountability infrastructure

- The infrastructure is made of two macro key components: the **blockchain** and the **digital identity provider** system
- The adopted blockchain is a fork of Ethereum implemented in the form of *permissioned* blockchain
- Two types of blockchain 3.0 nodes have been added:
  - **Accountability node (AN)**:
    - It acts as a delegate for the users with respect to the blockchain, i.e. it executes the transactions
    - It acts as a service provider when it comes to make use of the users' digital identity, for this reason it is federated with one or more identity providers
  - **Central node (CN)**:
    - It is a special AN which is in charge of managing the life-cycle of the ANs and to reward them relative to their contribution to the accountability process

User Roles

End users

They perform operations that need to be accountable in a cooperative process

Managers

They are in charge of establishing what end users can actually do in a cooperative process, through management services

- Both must authenticate themselves through their digital identity provider to access to a service
- Services are implemented by means of smart contracts, which means that when a user consumes a service, he is indirectly requesting the execution of a smart contract, i.e. a blockchain transaction
- These transactions are executed by the AN which acts as a delegate for the users in its user list

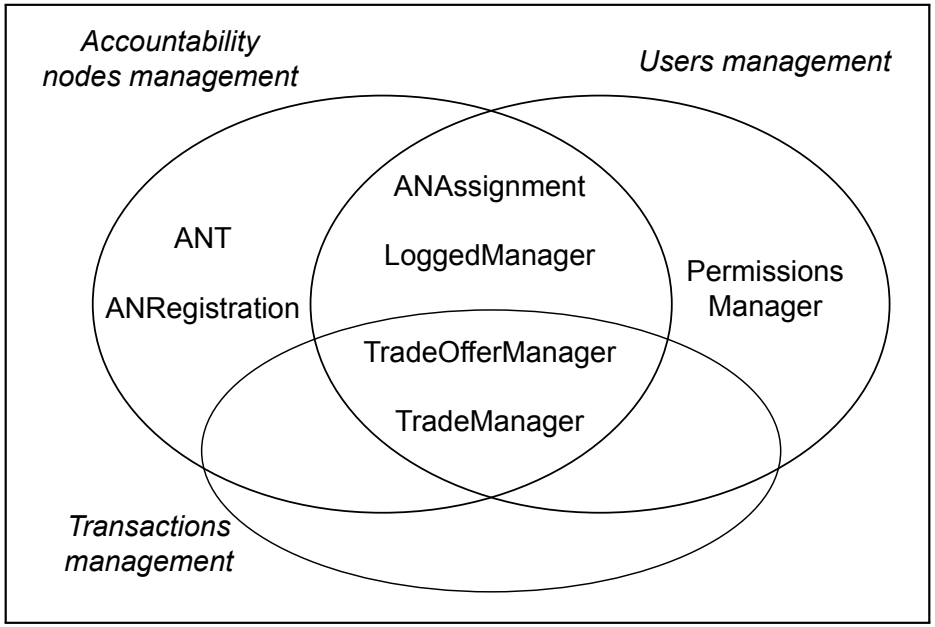
Accountability Node

- An AN can be generated by any miner who has earned enough money to invest as a collateral
- It acts as a SP and constitutes a bridge between the end users and the blockchain
- It is in charge of executing the transactions on behalf of a set of end-users
- ANs implement a service for which the end user has to provide its digital identity, hence the nodes have to be federated to one or more identity providers
- ANs are rewarded by the CN, proportionally to their contribution to the accountability process
- The Ethereum's reward system was modified so that upon the creation of a new block, the block reward is split between the miner and the CN. The CN will then distribute its part to the ANs.
- The transactions executed by an AN are subsequently validated by other ANs and the remaining blockchain nodes.
- Any illicit/illegal action performed by the executor would be detected by the system and punished by taking away all the collateral and disabling the AN.
- The malicious owner would not be able to generate another AN because its digital identity would be added to a blacklist.

Central Node

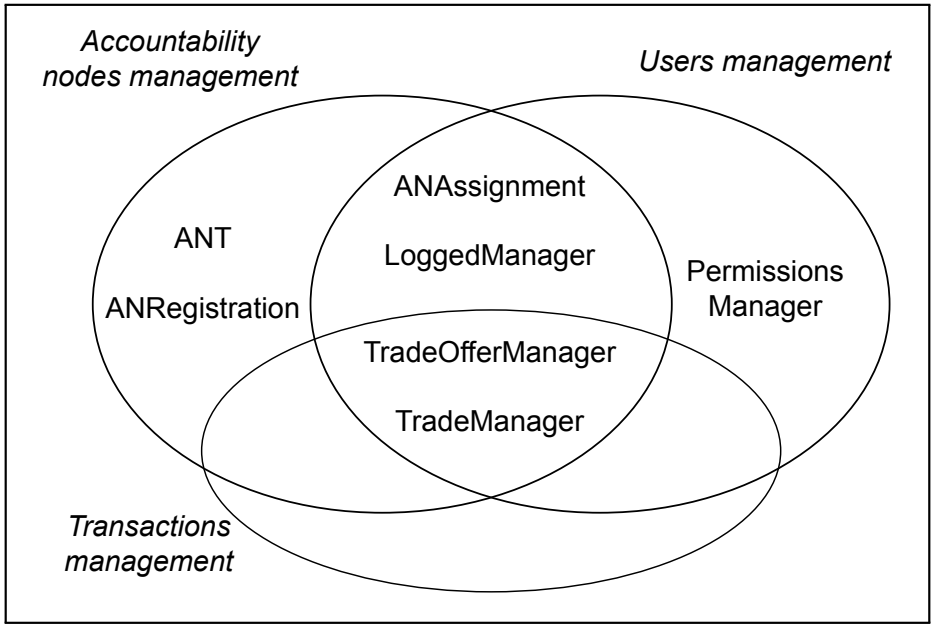
- It manages the life-cycle of the ANs and rewards them relative to their contribution to the accountability process
- Only the ANs and smart contracts that implement processes and services of the infrastructure can communicate with the CN
- The CN acts as an authority for the AN registration. It checks whether the collateral was allocated or not.
- The CN issues a certificate upon the reception of the collateral from an AN, which establishes a trust relationship between the two nodes
- Upon the reception of a request for an accountability service, the CN elects a subset of ANs, called federated ANs, that have to reach a consensus on the service
- It collects and analyses AN-related data, which are used to decide whether an AN should be banned from the blockchain or rewarded
- The CN is periodically elected by the blockchain, by means of a distributed election algorithm

Smart contracts (1)



- TRADEMANAGER and TRADEOFFERMANAGER: are the two smart contracts which supports, synchronously or asynchronously respectively, the accountable exchange of 'goods' between two entities
- ANREGISTRATION handles registration, de-registration and banning of ANs
- ANT (*Accountability Node Tokens*) is in charge of handling tokens used as the collateral required for registering the new AN. It acts as both mint and deposit and it also keeps track of how many tokens are owned by each address

Smart contracts (2)



- ANASSIGNMENT keeps track of the associations between users and ANs
- LOGGEDMANAGER maintains user session-related data. A session is necessary to perform any operation in the infrastructure. Its lifespan is determined in terms of number of blocks
- PERMISSIONSMANAGER is used for permission management purposes

Processes (1)

End-user login

- Is the most critical process in that it ensures the accountability
- It exploits a (public) digital identity system (SPID in our prototype)
- ANs act as Service Providers (SP) with respect to one or more IDPs
- Each registered user u authenticates itself by issuing a request to the accountability node (AN_u) which has been associated to it by the CN during the execution of the ANASSIGNMENT smart contract.
- The CN randomly selects a set of ANs, not including AN_u, that are in charge of verifying that the user successfully authenticated himself through the relevant IDP
- The digital identity token received from the IDP and the SAML request are sent from AN_u to the CN, off-chain
- The CN forwards these data to the federated ANs off-chain so they can independently check their validity.

Processes (2)

Accountability transactions

- They allow the users to exchange a good under the form of a SHA-256 hash which represents a fingerprint of the good and which is permanently stored in the blockchain
- Goods are not directly stored in the blockchain as a byte array because writing huge files is an expensive and slow operation
- These transactions are triggered by the invocation the relevant methods of either TRADEMANAGER or TRADEOFFERMANAGER smart contracts
- A transaction is actually executed on the blockchain by the AN_u assigned to the relevant user u on behalf of which the smart contract is invoked
- The federation of ANs monitors AN_u in order to detect illegal activities

Processes (3)

Permission management

- It requires the interaction of an organisation's manager with the infrastructure in order to manage the permissions that are needed by the end users to execute operations
- This process relies on the PERMISSIONSMANAGER smart contract
- This smart contract implements different functionalities for managing permissions, including grant or revoke operations

Processes (4)

Accountability Node registration

- The requester must have a digital identity and have to pay a collateral (i.e. he needs a wallet with enough money on the blockchain)
- The collateral is used to buy a certain amount of tokens provided by our blockchain by means of the ANT smart contract and cannot be used for any other purpose
- Tokens have been introduced to keep the price of the collateral stable: it is possible to dynamically update their price according to inflationary effects
- Once a user has paid the collateral, he has to confirm to the CN that he is the owner of the wallet which was used for the payment.
- The CN checks if the payment has been recorded in the blockchain and registers the new AN by adding it to the list of active ANs (using ANREGISTRATION) and creates a certificate for the off-chain communications
- A transaction for recording the association between the AN and its owner's digital identity is also executed

Processes (5)

Accountability Node banning

- When an AN is found performing an illegal activity, such as the attempt of executing a transaction for a user that is different from the requester, it will be marked as BANNED
- This operation is performed by the CN, by means of the smart contract ANREGISTRATION
- The digital identity of the AN's owner is added to a blacklist, while the AN is removed from the list of active ANs on the blockchain and its collateral is lost (the owned tokens cannot be reconverted in cryptocoins)

Conclusions and future work

- We developed a novel infrastructure designed to provide accountable decentralized services to certificate operations that are performed by two or more parties in a cooperative process
- The infrastructure uses a blockchain 3.0 implementation achieved as a fork of Ethereum
- We introduced the Accountability Node, a master node which serves the purpose of providing the accountable service and making sure that other ANs are behaving, in order to keep the blockchain healthy

Future work

- Integration with IPFS: end users can store off-chain data through an immutable, permanent IPFS links into a blockchain transaction
- Validation / Formal verification of smart contracts, e.g. by means of model-checking techniques
- Addressing device authentication issues, e.g. by using Physical Unclonable Function (PUF) based IoT authentication mechanisms

Thank you for your attention!
Any questions?