Università degli Studi di Napoli "Parthenope"

DIPARTIMENTO DI SCIENZE E TECNOLOGIE
Corso di Laurea in Informatica

Analisi ed Implementazione di un Discount Token su Consortium Blockchain

Relatore
Alessio Ferone

Candidato
Antonio Della Porta
Matricola 0124001252

Anno Accademico 2018-2019

Obiettivi

- Progetto sperimentale Napoli Blockchain, gruppo “Pagamenti e Token”

- Implementazione e sperimentazione di servizi **basati su blockchain** per i cittadini dell’area metropolitana di Napoli

- Analisi di sistemi blockchain esistenti e applicabilità al caso di studi del Comune di Napoli

- Analisi ed implementazione di un Discount Token per l’area metropolitana di Napoli

La Blockchain

- Introdotta nel 2009 da Satoshi Nakamoto con Bitcoin

- Registro **aperto** e **distribuito** (DLT) che può registrare transazioni tra due parti in modo verificabile e permanente senza bisogno di una terza parte fidata

- Il ruolo della terza parte fidata viene **distribuito** tra i partecipanti alla rete che devono trovare un accordo sullo stato della blockchain

- Il meccanismo che permette la consistenza del registro distribuito è chiamato **consenso distribuito**

Il consenso distribuito

- Un gruppo di N processi indipendenti deve convergere su una **decisione comune** (valore di una variabile, azione da intraprendere)

- Necessità di gestire eventuali **crash** o **processi malevoli**
  - **Fail-stop faults**
  - **Byzantine faults (Consenso Bizantino)**

- Gli algoritmi di risoluzione del problema del consenso distribuito presentano problemi di scalabilità in caso di reti **decentralizzate** e ad **accesso pubblico**

Il consenso di Nakamoto

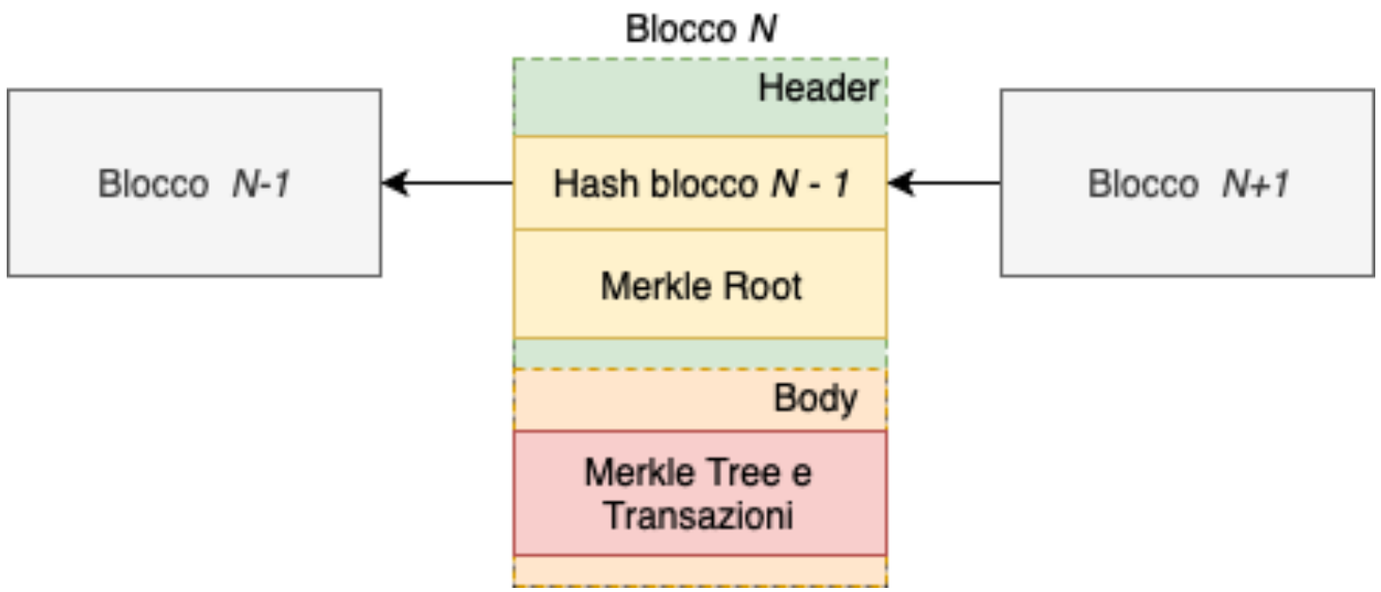
- Consenso basato sulla **competizione** tra i processi e su **incentivi economici**

- Ogni peer della rete impegna risorse computazionali partecipando alla competizione per la **decisione** di un blocco in cambio di una ricompensa

- Risoluzione di **fail-stop faults** tramite la creazione di una rete peer-to-peer ridondante

- Risoluzione di **byzantine faults** tramite la disincentivazione di comportamenti malevoli

Struttura di una Blockchain



- Ogni blocco è legato al precedente (parent block) tramite il suo **hash**, in modo che la modifica di un determinato blocco richieda la modifica di tutta la catena

- Le transazioni vengono identificate dal loro valore di hash e memorizzate in una struttura dati chiamata **Merkle Tree**

- Gli utenti operano sulla blockchain grazie a una coppia di chiavi che li identifica adoperando primitive di crittografia asimmetrica (ECC)

Classificazione dei sistemi blockchain

- **Blockchain Pubbliche:** partecipazione pubblica al consenso, bassa probabilità di mutabilità, basso throughput, nessuna centralizzazione

- **Blockchain Consortium:** partecipazione al consenso riservata ad un **gruppo mutabile di autorità**, alto throughput, centralizzazione parziale

- **Blockchain Private:** partecipazione al consenso riservata ad un solo nodo o organizzazione, possibilità di restrizione di permessi di lettura/scrittura, alto throughput, centralizzazione totale

Ethereum

- Progetto nato nel 2013 e proposto da Vitalik Buterin, lanciato nel 2015

- L'idea principale è quella di fornire agli sviluppatori gli strumenti per costruire **applicazioni distribuite** e **on-chain**

- Introduzione di **smart contracts** ed **EVM** (Ethereum Virtual Machine) che consentono l'esecuzione di **transazioni condizionali**

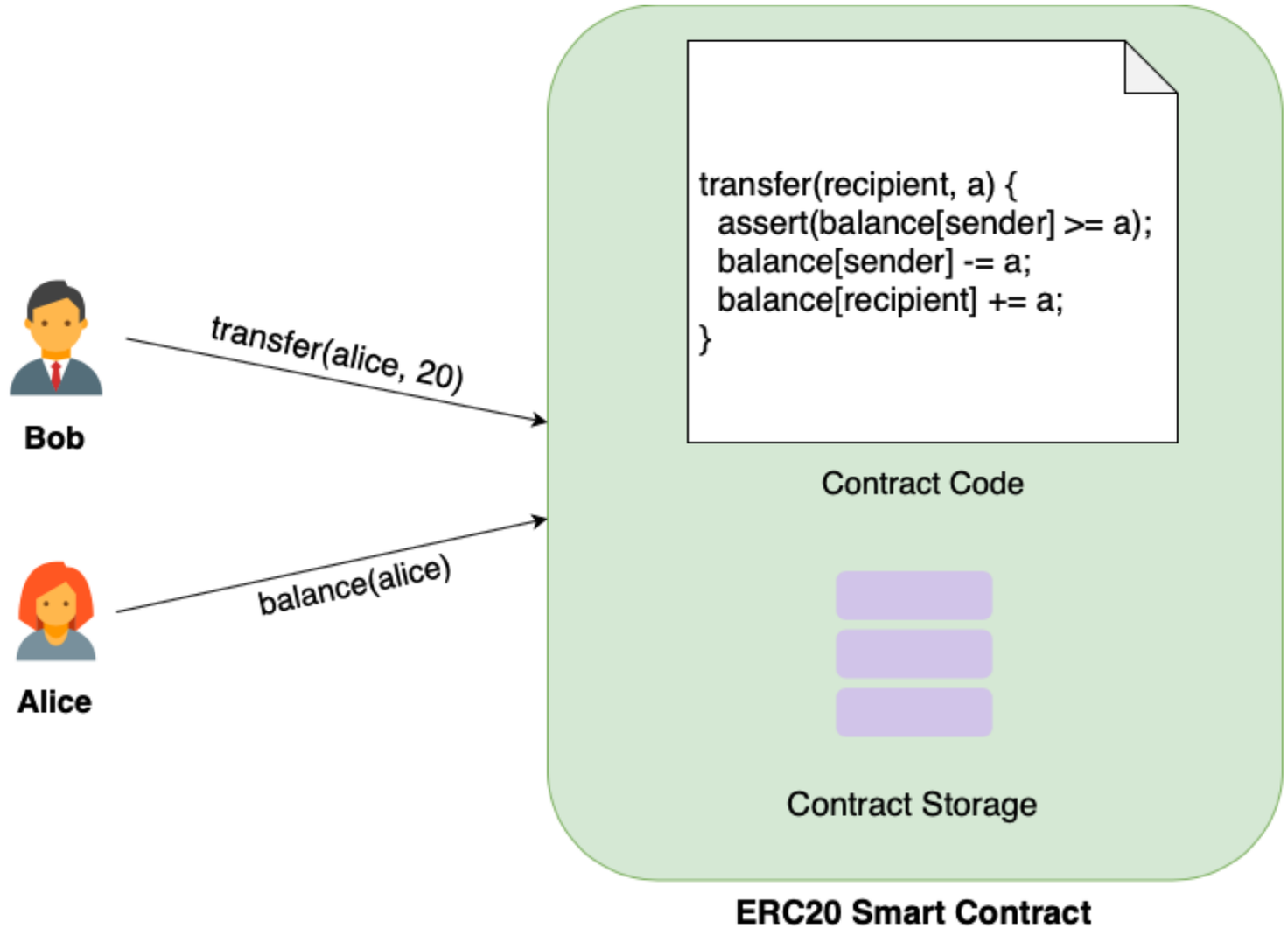
- Consente la creazione di **reti private** o **consortium** con algoritmi di consenso basati su premesse off-chain

ethereum

Smart contracts ed EVM

- Gli **smart contracts** definiscono le logiche operative e gestiscono i dati relativi a protocolli e applicazioni definiti al di sopra della rete Ethereum
    - L'esecuzione avviene **globalmente** rispetto alla rete
    - Sono disponibili HLLs traducibili in EVM bytecode
- La **EVM** è una macchina virtuale Turing-Completa il cui stato trasla a seguito di chiamate agli smart contracts
    - Ogni operazione ha un costo definito in moneta nativa (ETH)
    - Rende possibile l'interoperabilità tra gli **smart contracts**

Smart contracts: un esempio



- L’interazione tra utenti e smart contract avviene tramite applicazioni chiamate **wallet** (Metamask, Coinbase Wallet, etc)

Il sistema proposto

- **Consortium Blockchain** manutenuta da un consorzio di autorità riconosciute e autorizzate

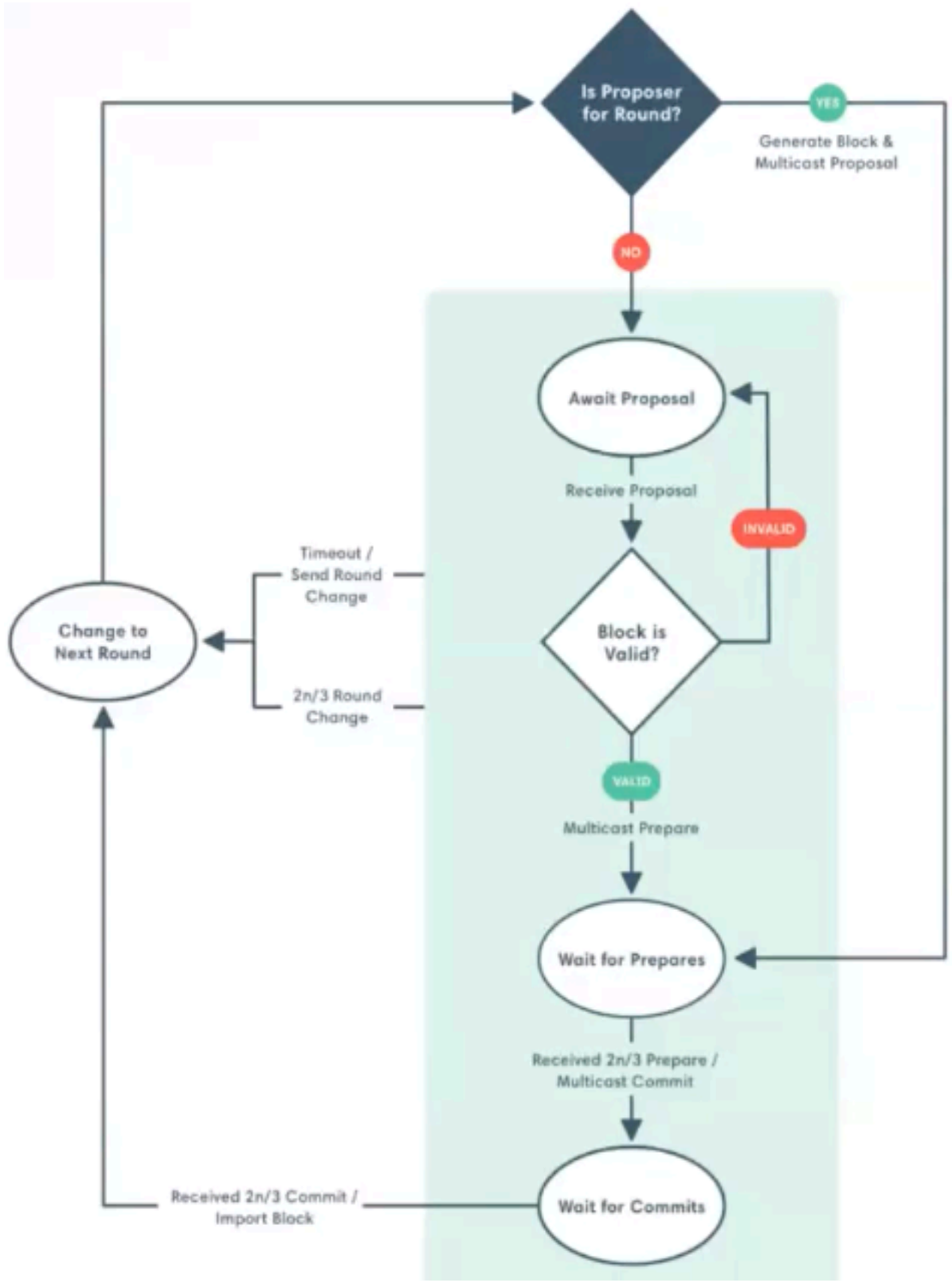
- Token **ERC20** grazie al quale è possibile usufruire di servizi legati ad esso

- **Sistema di scontistica** basato sul token

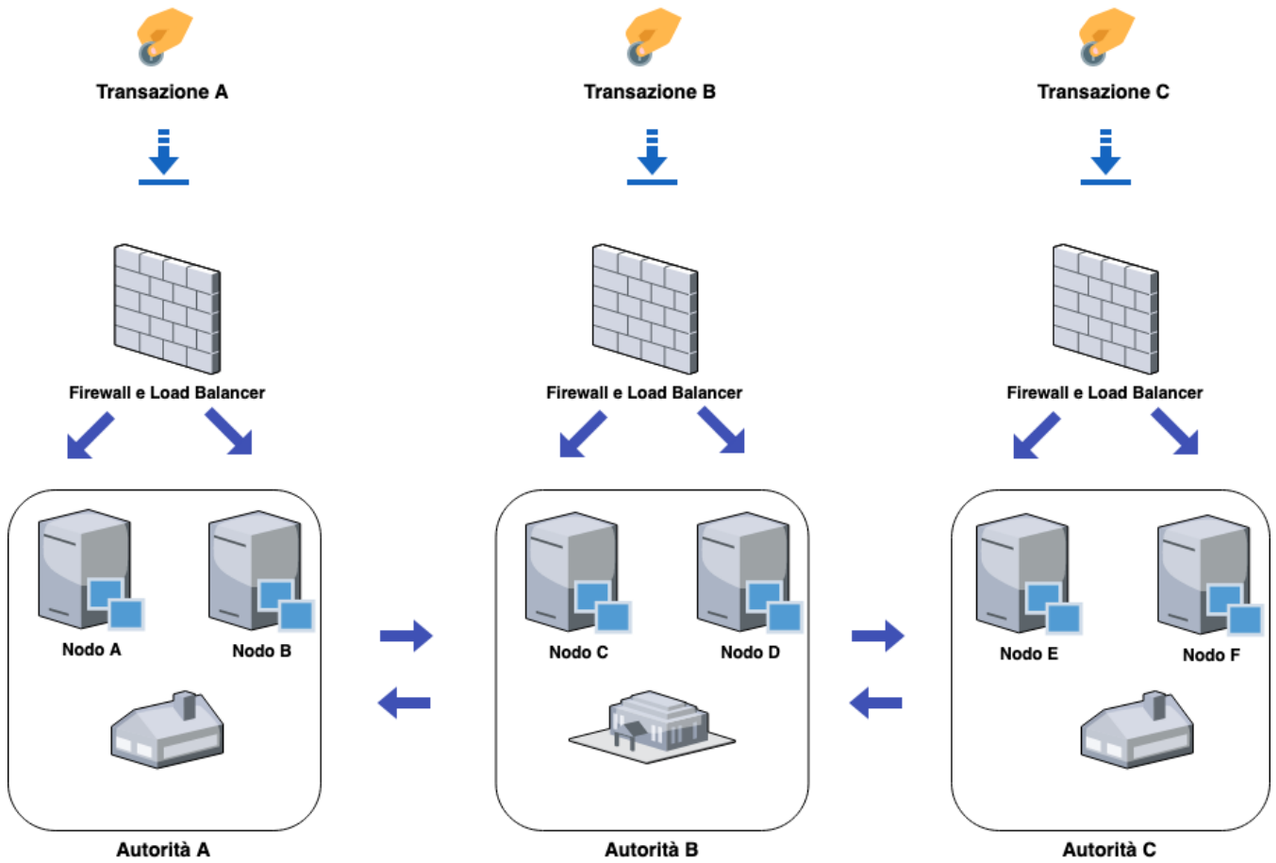
- **Applicazione distribuita** per l'interazione tra utenti e blockchain

Il consenso

- **IBFT 2.0** è un algoritmo di consenso della classe di algoritmi nota come **Proof of Authority**
- Basato su una finite-state machine
- Formalmente corretto, offre **safety**, **liveness**, **t-Byzantine-Fault-Tolerance**, **finality immediata**
- Alte prestazioni a discapito della scalabilità
- Implementato in **Besu**, progetto di Hyperledger



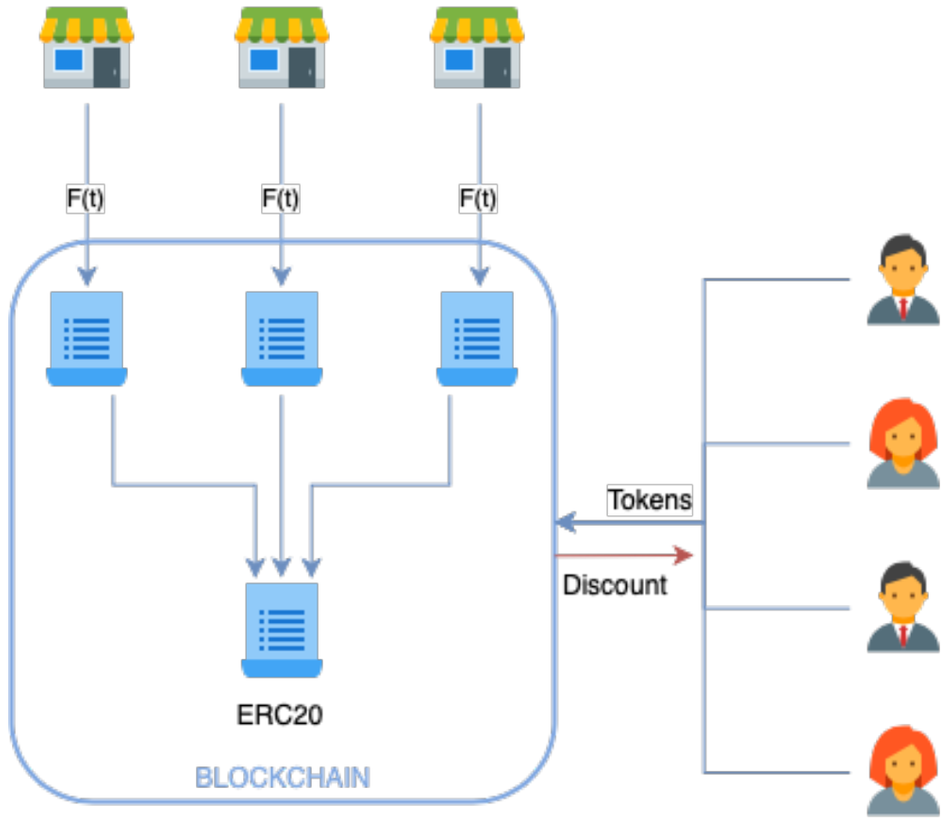
Struttura della rete e consenso



- Algoritmo di consenso IBFT 2.0

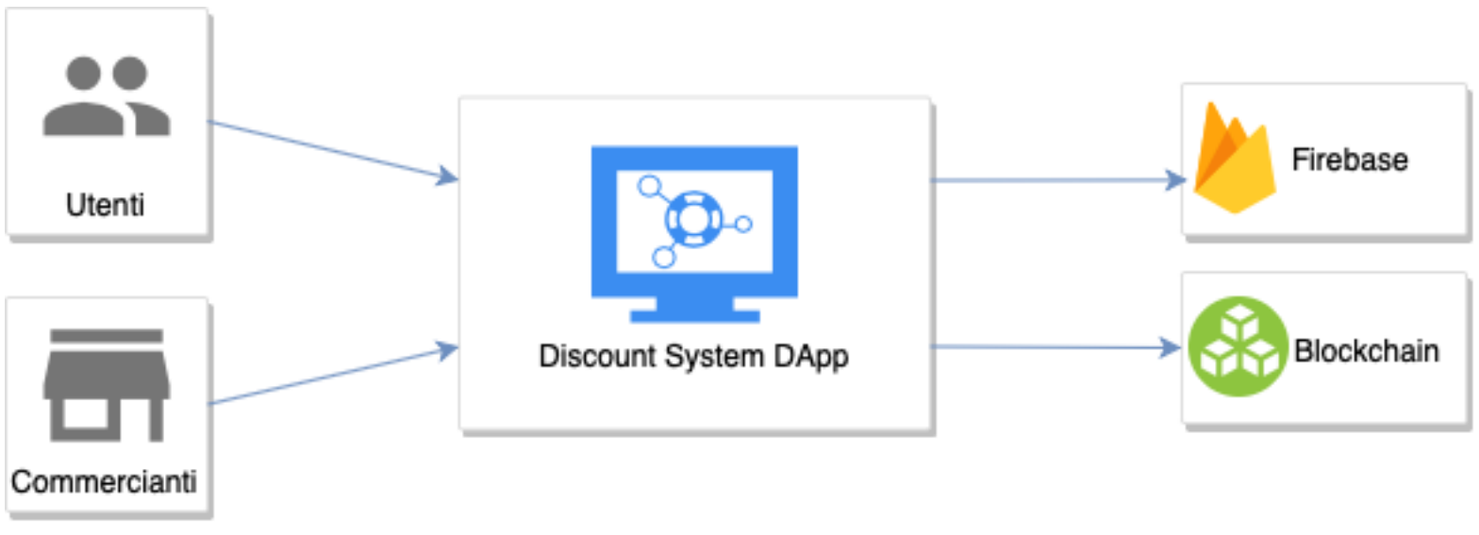
- Ogni **autorità** possiede uno o più nodi Ethereum che includono le transazioni in nuovi blocchi

Il sistema di scontistica



- Prezzo dei prodotti variabile in base alla funzione $C(t, X) = c \cdot (1 - f(t, X))$
- Ogni commerciante pubblica sulla blockchain la propria funzione di sconto $f(t, X)$
- I cittadini ricevono uno sconto in funzione dello stato della rete X e del numero di token t spesi

Discount System DApp



- Applicazione web che consente di interagire con gli smart contracts e mantenere un insieme di prodotti
- Database Firestore in cui vengono mantenuti i prodotti e il rapporto tra un prodotto e il proprio contratto di sconto
- Query verso i contratti per ottenere percentuali di sconto e indirizzo di pagamento dei commercianti

Dimostrazione Live

MarketplaceApp

localhost:4200/dashboard

Come iniziare | Machine Learning - ...

Dashboard | Deploy Contract | Products | Logout

Market Address 0x39Fd...9A05

Locked NT 0

Unlock funds

Address	Discount Factor	Max discount
0x2Aa3460286545832623666B7B83f29334E3036D3	2	40

Conclusioni

- Contratti rilasciati su rete di test Ropsten e su una blockchain di test su macchine di proprietà di ANM (Azienda Napoletana Mobilità)

- Ricerca di commercianti per la fase di beta testing

- Codice disponibile su Github

    - Discount Token: https://github.com/antodp/DiscountToken

    - Discount System Dapp: https://github.com/antodp/Discount-Dapp

Sviluppi Futuri

- Risoluzione questioni legate alla **distribuzione di Ether** (ETH)
- Creazione di un **token multilivello** e di un mercato di token basato su **bonding curves**
- Binding tra **identità digitale** e identità off-chain
- Sviluppo di un vero e proprio **modello economico**