Unione europea
Fondo sociale europeo

REGIONE DEL VENETO

Regione del Veneto
Giunta Regionale
Direzione Formazione e Istruzione

RELAZIONE CONSUNTIVA SULL'ATTIVITÀ DI RICERCA (Assegni di ricerca)

DGR n. 1463 del 08/10/2019

Cod. Ente: 2120 Rag. Sociale Università Ca' Foscari Venezia Asse Occupabilità

Cod. progetto 2120-0002-1463-2019 **Titolo** Sviluppo e validazione di sistemi blockchain per l'e-commerce

Cod. Intervento 2120/10258820-001/231/DEC/20 **Titolo dell'Intervento** Sviluppo di una soluzione Blockchain per l'emissione anticipata di credito derivante da fatture **Sede** Verona

Il sottoscritto ***Nicola Fausto Spoto*** *in qualità di* **Referente per la ricerca** *con riferimento all'intervento in oggetto,*

Il sottoscritto ***Fabio Tagliaferro*** *in qualità di* **Destinatario dell'Intervento** *in oggetto,*

DICHIARANO

che l'intervento in oggetto nel **periodo dal 01/07/2020 al 30/06/2021** si è articolato nelle seguenti attività:

Attività

In collaborazione con l'azienda Commerc.io Srl sono state svolte mansioni di sviluppatore usando il linguaggio Go. Principalmente sono stati sviluppati moduli per software relativo a nodi blockchain Cosmos SDK, in particolare per commercionetwork. Collaborando anche con l'azienda Nym Srl è stato sviluppato software relativo a identità digitali Self-Sovereign Identity, in particolare per il progetto Verifiable Credential Authority.

In collaborazione con Università di Venezia sono state svolte mansioni di ricercatore in ambito blockchain. La ricerca si è soffermata su best practice, vulnerabilità e analisi di smart contract scritti in Go per supportare l'obiettivo di ricerca condiviso con gli altri due assegnisti di UniVE. Si sono svolti meeting con l'azienda Alpenite utili per individuare use case blockchain per e-commerce e beni di lusso, come per Lago Srl.

In collaborazione con Università di Verona, sono state svolte mansioni di sviluppatore e ricercatore in ambito blockchain e smart contract, seguendo le direttive del Resp. Scientifico e collaborando con un suo dottorando nel contesto del progetto Hotmoka e durante la fase di scrittura di un progetto europeo.
C'è stata partecipazione attiva da parte dell'assegnista a vari corsi organizzati dal Dipartimento di informatica dell'Università di Verona, in particolare su blockchain, smart contracts e la tutela dei beni immateriali.

In collaborazione con University of Stirling, durante la mobilità (da remoto) sono state svolte mansioni di ricercatore nell'ambito delle identità digitali su blockchain, in particolare su Self-Sovereign Identity. Seguendo le direttive del responsabile Dott. Andrea Bracciali, l'assegnista ha partecipato seminari e conferenze su blockchain e smart contracts e ha collaborato con un suo dottorando nella scrittura di articoli per ricerca, ricevendo feedback sul lavoro svolto.

Metodologie operative

- meeting in presenza presso Università di Verona e Università di Venezia
- smart working utilizzando scambi di email, piattaforme per lavoro in collaborazione (Slack) e sistemi per videoconferenza (Google Meet, Zoom, Skype)
- sviluppo di software nei linguaggi Go e Java, con strumenti per sviluppo software (Eclipse, Goland, Visual Studio), codice sorgente in repository git (GitHub, GitLab)
- scrittura articoli ricerca con linguaggio latex e strumenti di supporto (TeXStudio, Overleaf, Mendeley), registrazione di presentazione per workshop (Microsoft Powerpoint)
- partecipazione a conferenze e workshop da remoto tramite varie piattaforme per videoconferenza

Risultati

- prototipo di applicazione blockchain nel linguaggio Go con Cosmos SDK per rilascio prestiti, utile al progetto "Studio e documentazione del framework di sviluppo Cosmos SDK per la programmazione di reti blockchain" dell'Università di Verona
- nuovo modulo commercionetwork su un meccanismo permissioned di aggiornamento del software
- strategia per documentare la blockchain commercionetwork e aggiunta documentazione
- varie software review per il progetto commercionetwork
- varie componenti del progetto Verifiable Credentials Authority (VCA) che ha superato le varie fasi dell'acceleratore eSSIF Lab di NGI
- presentazioni per meeting con le Università di Verona, Venezia e Stirling su temi legati a blockchain, smart contract e Self-Sovereign Identity
- implementazione di smart contract in Java compatibili con il framework Takamaka del progetto HotMoka
- articolo scientifico su su verifica degli smart contract integrata nel meccanismo di consenso e registrazione di relativa presentazione disponibile online (pubblicato in workshop di una conferenza internazionale)
- articolo scientifico su traduzione di smart contract ERC20 da Solidity al linguaggio Java e compatibile con Takamaka (sottomesso in workshop di una conferenza internazionale)
- articolo scientifico del tipo "Systematization of Knowledge" su Self-Sovereign Identity

Sede di svolgimento dell'attività

Pressana (Smart Working),
Dipartimento di Informatica Università di Verona,
Dipartimento di Informatica Università di Venezia

Luogo e data Verona, 30/06/2021

Firma del Destinatario

Firma del Referente per la Ricerca

Unione europea
Fondo sociale europeo

REGIONE DEL VENETO

Regione del Veneto
Giunta Regionale
Direzione Formazione e Istruzione

ABSTRACT DI RICERCA
(intervento assegni di ricerca)

DGR n. 1463 del 08/10/2019

Cod. Ente: 2120 Rag. Sociale Università Ca' Foscari Venezia Asse Occupabilità

Titolo progetto Sviluppo e validazione di sistemi blockchain per l'e-commerce
cod. 2120-0002-1463-2019 **COD. CUP:** H74I1900182000

Cod. Intervento 2120/10258820-001/231/DEC/20
Titolo dell'intervento: Sviluppo di una soluzione Blockchain per l'emissione anticipata di credito derivante da fatture

Relativamente all'intervento in oggetto che si è svolto nel **periodo dal 01/07/2020 al 30/06/2021** viene riportato un breve abstract sull'attività di ricerca svolta

Inizialmente l'assegnista si è concentrato sulla piattaforma blockchain dell'azienda Commerc.io Srl (partner di progetto) per poter sviluppare nuovi moduli per la blockchain commercionetwork, basata sul framework Cosmos SDK e il meccanismo di consenso Tendermint.
Commerc.io ha seguito l'assegnista (tramite smart working, a causa delle restrizioni legati alla pandemia Covid-19) in una fase di apprendimento del linguaggio di programmazione Go, linguaggio nativo degli smart contract delle applicazioni decentralizzate di Cosmos SDK. Ne è risultato un prototipo di applicazione Cosmos SDK che implementa una sistema di rilascio prestiti (in criptovaluta) decentralizzato e permissionless. Questo lavoro è stato utile per il progetto interno all'Università di Verona "Studio e documentazione del framework di sviluppo Cosmos SDK per la programmazione di reti blockchain" seguito dal Prof. Fausto Spoto. Il prototipo sviluppato è una possibile base per un tool decentralizzato che garantisca l'emissione anticipata di credito derivante da fatture a breve e medio termine da parte dei clienti delle piccole e medie imprese, tramite la tecnologia blockchain e smart contract. Anche un sistema e-commerce potrebbe utilizzare una piattaforma simile, per esempio per accettare pagamenti in criptovaluta.
L'esperienza acquisita ha permesso all'assegnista di sviluppare e testare un nuovo modulo, chiamato "upgrade", per la blockchain commercionetwork. Si tratta di un meccanismo permissioned di aggiornamento del software per i nodi utilizzati per poter partecipare al meccanismo di consenso della blockchain. In breve, un indirizzo con il ruolo di "government" comunica la necessità di aggiornare il nodo entro un certo momento temporale. Chi non si adegua in tempo a questa direttiva perde la possibilità partecipare al consenso e di conseguenza non guadagna criptovaluta con questa attività.
Ne è seguito uno studio su come rendere più efficiente la scrittura della documentazione di REST API per i nodi commercionetwork e la riscrittura di parte della documentazione seguendo la nuova modalità.

Parallelamente, l'assegnista ha approfondito autonomamente le best practice per programmare smart contract scritti in un linguaggio di programmazione Turing-completo come Go. In particolare, l'importanza di garantire esecuzione deterministica degli smart contract e la misurazione del "gas" in fase di esecuzione per evitare computazioni infinite. I risultati della ricerca sono stati comunicati tramite meeting periodici con i Prof. Agostino Cortesi, Pietro Ferrara e Fausto Spoto e successivamente con gli altri due assegnisti dell'Università di Venezia. Un paio di meeting si sono svolti in presenza. Questa modalità ha permesso di allineare le conoscenze acquisite, contribuendo all'obiettivo di ricerca sulla validazione di sistemi blockchain e riguardo a sicurezza e analisi di vulnerabilità negli smart contract scritti con il linguaggio di programmazione Go.

Si sono svolti dei meeting (in smart working) con l'azienda Alpenite Srl (partner di progetto) e il Prof. Pietro Ferrara con oggetto l'utilizzo della tecnologia blockchain in ambito di e-commerce, tracciabilità e marketing per l'industria dei beni di lusso. In futuro, queste discussioni potranno essere utili per l'azienda Lago SpA (partner di progetto).

Con l'Università di Verona e in particolare con il Resp. Scientifico Prof. Fausto Spoto sono stati raggiunti risultati di ricerca riguardo al progetto Hotmoka. in particolare, la pubblicazione di un articolo per il workshop Trusted Smart Contract della conferenza internazionale Financial Cryptography. L'ambito della ricerca riguarda l'area della verifica degli smart contract direttamente on-chain, ovvero effettuare analisi dei contratti come parte integrante delle regole di consenso di una blockchain. Inoltre, l'assegnista ha contribuito al progetto scrivendo smart contract in Java compatibili con il framework per smart contract Takamaka per gestire delle votazioni permissioned in blockchain.
Un altro articolo riguardante il progetto Hotmoka è al momento in fase di revisione. Quest'ultimo lavoro descrive una traduzione efficiente dello smart contract per token fungibili ERC20, sviluppato dal team di OpenZeppelin, dal linguaggio Solidity a Java e compatibile con Takamaka.

La collaborazione con Commerc.io è ulteriormente continuata invididuando come nuovo obiettivo di ricerca l'innovativo l'ambito della Self-Sovereign Identity (SSI) ovvero un modello per identità decentralizzate basate sulla tecnologia blockchain.
Commerc.io assieme all'azienda Nym Srl partecipano all'acceleratore European Self-Sovereign Identity Lab (eSSIF Lab) nel contesto di Next Generation Internet (NGI) e finanziato dall'Unione Europea. Il progetto nel quale l'assegnista è stato coinvolto si chiama Verifiable Credential Authority (VCA) con obiettivo lo sviluppo e implementazione di una soluzione software SSI compatibile con il regolamento europeo Electronic Identification and Trust Services Regulation (EIDAS).
L'assegnista ha svolto il ruolo di software developer utilizzando il linguaggio Go, approfondendo le più importanti componenti di SSI come Decentralized IDentifier (DID), protocolli del framework Hyperledger Aries e Verifiable Credentials compatibili con tecniche crittografiche Zero Knowledge Proof per la rivelazione selettiva dei dati. Il lavoro svolto è stato comunicato tramite meeting coinvolgenti le università del progetto di ricerca e membri di Commerc.io e Nym, risultando in interessanti scambi di punti di vista e l'individuazione di ulteriori spunti per la collaborazione tra mondo accademico e industriale nell'ambito di blockchain e SSI.

La mobilità presso il Department of Computing Science and Mathematics di University of Stirling è stata svolta interamente da remoto a causa delle restrizioni legati alla pandemia Covid-19. Con il responsabile Dott. Andrea Bracciali è stato individuato come argomento di ricerca l'ambito della Self-Sovereign Identity, vista l'esperienza acquisita dall'assegnista nel progetto VCA. La collaborazione ha portato alla redazione di un paper scientifico del tipo Systematization of Knowledge (SoK) che si concentra sull'evoluzione dei modelli per identità, i principi di SSI, la descrizione del framework di riferimento Trust over IP e i principali enti che contribuiscono agli standard legati ad identità decentralizzate.
La supervisione da parte di University of Stirling è stata utile per avere indicazioni su metodologia di ricerca, esposizione in modo formale dei contenuti e utilizzo di inglese accademico. Inoltre, l'assegnista ha seguito da remoto eventi come workshop e conferenze consigliate dal Dott. Andrea Bracciali per approfondire le tematiche di ricerca accademica su blockchain e smart contract.

Verona , 30/06/2021 Firma del Destinatario (assegnista) Cosimo Torchi

Firma del Referente per la ricerca (prof. Spoto) Fausto Spoto