

СОФИЙСКИ УНИВЕРСИТЕТ
„СВ. КЛИМЕНТ ОХРИДСКИ“



SOFIA UNIVERSITY
ST. KLIMENT OHRIDSKI

ФАКУЛТЕТ ПО
МАТЕМАТИКА И ИНФОРМАТИКА

FACULTY OF
MATHEMATICS AND INFORMATICS

ДЕЦЕНТРАЛИЗИРАНА ИДЕНТИЧНОСТ В БЛОКЧЕЙН

ОТ

Иван Панайотов Ламбов

Автореферат

на дисертация за придобиване на образователна и научна степен

„Доктор“

в

професионално направление

4.6. Информатика и компютърни науки,

докторска програма "Софтуерни технологии" - Управление на знания

Ръководител: доц. д-р Петко Русков Русков

София, 2024 г.

Съдържание на дисертацията

Дисертацията е с обем 185 страници (включително приложенията) и се състои от 9 глави, които съдържат таблици, фигури и програмен код. Списъкът на използваната литература съдържа 107 научни източника.

Глава 1: Въведение

Тази глава въвежда темата на изследването, предоставяйки предистория и контекст, описва проблема, обяснява накратко целите и задачите на предложениния DIDoA модел. Дефинират се ключови термини и се обяснява структурата на дисертационния труд.

Глава 2: Мотивация

Тази глава обяснява мотивацията за това изследване. Тя подчертава важността, теоретичните и практическите последици от изследването. Тази глава допълнително разкрива убедителните фактори, движещи това изследване и ползите, които то носи на различните заинтересовани страни.

Глава 3: Преглед на литературата

Тази глава прави преглед на съществуващата литература, свързана с децентрализираната идентичност в блокчейн. Тя критично разглежда предишни проучвания, теории и методологии, идентифицирайки пропуски в настоящите знания, които дисертацията цели да запълни.

Глава 4: Теоретична рамка

Тази глава предоставя теоретичната рамка, която е необходима за разбиране на теорията, на която е основано изследването - основни градивни елементи и терминология. Тя обяснява основните компоненти на традиционния модел на децентрализирана идентичност, основната архитектура, роли и процеси. Тази глава също така показва релевантните приложения, понастоящем използвани от държавни и бизнес организации.

Глава 5: Цели и методология на изследването

Тази глава дефинира основните цели на изследването и въпросите, на които то има за цел да отговори - да проучи изискванията, ключовите характеристики и процесите на платформа за децентрализирана идентичност на артефакти (DIDoA) и да предложи нова системна архитектура, базирана на блокчейн. Целта на това изследване е да разшири обхвата на модела и технологията на

децентрализираната идентичност и да ги приложи към артефакти. Тази глава също описва подробно организацията на изследването и методологията, използвани в изследването. Тя описва изследователския подход. Необходима е комбинация от различни изследователски методологии за справяне с различните аспекти на изследователския проблем.

Глава 6: Архитектура на DIDoA модела

Тази глава дефинира ролите на компонентите на DIDoA модела, съпоставя ги със съответните роли в сферата на знанието за артефактите на културното наследство и показва взаимодействията между тях. Тази глава също така разкрива различните процеси, дефинира архитектурата и основните компоненти на DIDoA модела, описва функционалността на различните компоненти, идентифицира необходимите структури от данни (VC, VP, DID) и определя матрицата на процесите. Експериментът се основава на този DIDoA модел и симулира реалистичен сценарий (базиран на конкретни приложения на модела), който включва всички възможни функции и взаимодействия. DIDoA моделът обаче е общ по природа и далеч надхвърля конкретен експеримент или приложение. Моделът може да се приложи във всички случаи, когато е необходима идентификация на артефакт.

Глава 7: Експеримент и резултати

Тази глава обяснява експерименталната конфигурация и представя резултатите от експеримента. Тази глава също представя инструментите и приложенията, използвани в изследването за провеждане на експеримента, постигане на целите и отговор на поставените въпроси. Провеждайки нашия експеримент, ние се стремим да постигнем следните резултати:

- Регистрация на DID за всяка роля
- Определяне на алгоритъм за всяка роля
- Дефиниране на структурите от данни, необходими за всяка роля
- Създаване на диаграма на последователност, която показва взаимодействията между всяка роля и другите роли в процеса

За по-добро визуализиране на резултатите използваме блокови диаграми, диаграми на последователности, JSON-LD код и блокчейн транзакции.

Глава 8: Дискусия

Тази глава интерпретира резултатите, представени в предишната глава. Тя обсъжда основните констатации във връзка с въпросите и целите на изследването. Главата също така изследва въздействието на изследването върху индустрията, ограниченията и предизвикателствата за широкото

прилагане. Освен това, главата прави сравнение с научната работа, извършена в тази област, и демонстрира връзката между DIDoA модела и науката за управление на знанията. Най-важното е, че тази глава очертава основните научни и приложно-научни приноси на изследването.

Глава 9: Заключение и по-нататъшно проучване

Тази глава обобщава резултатите и приноса на изследването и тяхното значение. Главата завършва с практически препоръки въз основа на резултатите от изследването и проправя пътя за иновации в областта на децентрализираната идентичност на артефактите, като предлага насоки за по-нататъшно проучване.

Дисертацията започва с Благодарности, Съдържание, Списък на фигури, таблици, и код, Списък със съкращения и символи и завършва с Литература, Приложения, и CV на автора.

Обща характеристика на дисертационния труд

Увод

Верификацията на автентичността и произхода на артефактите е важно за опазването на нашето културно наследство. Това проучване изследва потенциала за използване на децентрализирана идентичност (DID) в блокчейн за идентифициране и верификация на артефакти. Има много примери за артефакти на културното наследство - исторически артефакт, произведение на изкуството, оригинален ръкописен документ, образци от естествения свят и човешката култура и др. Прилагането на DID модела за идентифициране и верификация на артефакти би помогнало за **решаването на проблема** с измамите и незаконната търговия с артефакти и носи огромни ползи за правоприлагащите органи, археолозите, музейните специалисти, търговците на произведения на изкуството, застрахователните компании, колекционерите и т.н. Подробно обяснение за мотивацията на това изследване е дадено в Глава 2, „Мотивация“ .

Задълбочен преглед на научната литература разкри значителен набор от стандарти и насоки за идентифициране, документиране и верификация на артефакти на културно наследство, заедно с различни случаи на прилагане на децентрализирана идентичност в блокчейн в различни индустрии. Независимо от това, **това проучване предлага първият работещ модел** и първата емпирична демонстрация, че децентрализираната идентичност на блокчейн може успешно да се използва за идентифициране и верификация на артефакти, изяснявайки мотивацията и ползите за различни заинтересовани страни.

Задачата на това изследване е да разшири границите на конвенционалния модел и технология на децентрализираната идентичност, като ги приложи към идентифицирането и верификацията на артефакти. Ето дефиницията на артефакт, към която ще се придържаме през цялото ни изследване - артефакт е обект, който:

- Може да бъде еднозначно и недвусмислено идентифициран с помощта на технически средства, като 3D скенер, LIDAR, рентген, спектроскоп и др.
- Не може да се заменя или копира.

Ето защо **въвеждаме нов термин - Децентрализирана идентичност на артефакти (DIDoA)** - който ще използваме в нашите изследвания, за да обозначим модела, който сме конструирали за верификация на идентичността, автентичността, собствеността и съхранението на артефактите. Предложеният модел е базиран на блокчейн. Въпреки това, няма ограничение по отношение на основната технология, стига тя да поддържа DID регистрация и управление.

Целта на това изследване е да проучи изискванията, ключовите характеристики и матрицата на процесите на DIDoA платформата и да предложи нов модел и системна архитектура, базирана на блокчейн, за да подпомогне музейната общност, правоприлагащите органи, митническите власти, професионалисти в търговията с предмети на изкуството, представители на застрахователната индустрия, експерти по изкуство и т.н., да верифицират автентичността на културни и исторически артефакти, да подобрят сигурността и конфиденциалността, да се борят с измамите, да повишат ефективността на разходите и да подобрят съответствието с нормативните изисквания.

Ние проучваме и доказваме осъществимостта на прилагането и използването на DIDoA върху блокчейн и анализираме резултатите. Това изследване разкрива градивните елементи на DIDoA модела, базиран на блокчейн, за идентифициране на различните роли, взаимодействията между тях и процесите, в които участват. То също така дефинира критичните структури от данни на модела - DID документ и верифицируеми идентификационни данни. Това проучване също има за цел да разкрие основните предимства, ограниченията и предизвикателствата на DIDoA модела. Пълен списък на целите и въпросите на изследването е предоставен в Глава 5, „Цели на изследването“.

В резултат на проведените изследвания и експерименти ясно показахме, че моделът DID е приложим за верификация на идентичността и автентичността на артефакти, илюстрирахме как DIDoA моделът се вписва в контекста на теорията за управление на знанията, идентифицирахме множеството процесни потоци и разработихме интегрирана матрица на процесите, въведохме модифицирана конфигурация на триъгълника на доверието, като включихме контролера и артефакта в един връх, въведохме нова концепция, пръстов отпечатък на цифров артефакт, който да се използва за верификация на идентичността и автентичността на артефакта.

Пълен списък на приноса на това изследване е даден в Глава 8.5, „Основни приноси на това изследване“.

Изследването включва критичен преглед на съществуващата литература, свързана с децентрализираната идентичност в блокчейн, преглед на предишни проучвания, теории и методологии, за да осигури необходимата теоретична рамка. Тази рамка включва основните градивни елементи и терминология, които са от съществено значение за разбирането на знанието, която е в основата на изследването. Проучването изяснява основните компоненти на традиционния модел на децентрализирана идентичност, като подробно описва основната архитектура, роли и процеси. То допълнително изследва изискванията, ключовите характеристики и потока на процеса на платформата за децентрализирана идентичност на артефакти (DIDoA), което завършва с проектирането на нова системна архитектура, базирана на блокчейн технология.

За да се разгледат различни аспекти на изследователския проблем, се използва комбинация от различни изследователски методи, включително сравнителен анализ, експериментално изследване и функционално картографиране. За събиране на подходяща информация за основните процеси, атрибути, идентификационни данни, роли и поведения и за валидиране на приложимостта на предложения режим, проведохме интервюта с експерти от съответните фирми и институции. Предложеният DIDoA модел беше тестван чрез прилагане на експеримент с помощта на съществуващи инструменти и резултатите бяха анализирани.

Прозрачното разкриване на инструментите и приложенията, използвани в експеримента, позволява на други изследователи да възпроизведат експерименталната методология, да извършват независимо събиране и анализ на данни и да допринасят за кумулативния напредък на знанията в областта. Експерименталната работа включва картографиране на ролите на DIDoA модела, разкриване на различните процеси, илюстриране на взаимодействията между ролите с диаграми на последователности и детайлизиране на спецификата на структурите от данни – проверими идентификационни данни и DID документи – записани и съхранявани в блокчейн.

Освен това, изследването интерпретира резултатите, обсъжда ключовите констатации във връзка с въпросите и целите на изследването и разкрива въздействието му върху индустрията. То също така разглежда ограниченията и предизвикателствата пред широкото прилагане на модела. Проучването включва сравнение с научната работа в свързани области и демонстрира връзката между DIDoA модела и теорията за управление на знанията.

В заключение, това проучване подчертава основните научни и приложни приноси на изследването, като предлага практически препоръки въз основа на констатациите. То също така проправя пътя за бъдещи иновации в областта на децентрализираната идентичност на артефактите, като предлага насоки за по-нататъшно проучване.

Децентрализираната идентичност е известна още като Web3 идентичност или самостоятелна суверенна идентичност (SSI). Оттук нататък ще използваме тези термини взаимозаменяемо.

Мотивация

Мотивацията за използване на децентрализирана идентичност в блокчейн произтича от няколко убедителни фактора. Първо, базираните на блокчейн децентрализирани системи за идентичност значително подобряват сигурността и конфиденциалността. Чрез разпространение на данни в децентрализирана мрежа, тези системи намаляват рисковете, свързани с централизирани пробиви на данни. Потребителите запазват контрол върху конфиденциалната информация, което значително намалява риска от незаконен трафик на артефакти и фалшификати.

Освен това децентрализираните платформи за идентичност разкриват нови възможности за потребителите, като им дават по-голяма автономия по отношение на идентичността на артефактите, които те притежават или управляват. За разлика от традиционните системи, където управлението на идентичността често се контролира от централизирани органи, децентрализираната идентичност позволява на лица и организации да управляват и споделят избирателно идентификационни данни за артефакти, запазвайки суверенитет върху чувствителната информация. Тази децентрализация е от решаващо значение за насърчаване на доверието и предоставяне на потребителите на гъвкава и надеждна платформа за верификация на автентичността и собствеността на артефакта.

Много е важно да можем да идентифицираме и проследяваме артефактите на културното наследство поради редица причини:

- Да съхраним нашето културно наследство за потомците
- Да помогнем на правоприлагащите органи и митническите органи в борбата с незаконната търговия с артефакти на културното наследство
- Да улесним различните организации и професионалисти - археолози, музейни специалисти, търговци на произведения на изкуството, застрахователни компании, колекционери и др. - да идентифицират, проследяват и верифицират по уникален начин артефактите на културното наследство
- Да помогнем на изследователи, администратори, колекционери, музеи и обществеността да изследват сложни въпроси по отношение на нашето културно наследство в различни и несъвместими структури от данни.

Освен това неизменният и прозрачен характер на блокчейн технологията играе решаваща роля за намаляване на измамите и кражбата на идентичност.

Присъщите характеристики на блокчейн позволяват верификация на автентичността на артефакта, като гарантират, че идентификационните данни не могат да бъдат подправени или унищожени. Тази надеждност е много важна за поддържане на интегритета на системите за идентичност.

От икономическа гледна точка децентрализираните системи за идентичност предлагат ефективност на разходите, като елиминират необходимостта от посредници и намаляват административните разходи. Усъвършенстваните процеси, свързани с идентичности, базирани на блокчейн, намаляват разходите, свързани с верификацията и управлението на идентичността, което прави тези системи по-финансово устойчиви.

Съответствието с нормативните изисквания е друга област, в която децентрализираната идентичност в блокчейн показва значителен потенциал. Прозрачността и възможността за верификация, присъща на блокчейн технологията, може да подобри спазването на регулаторните изисквания, осигурявайки публични и неизменни записи на транзакции, свързани с идентичност. Тази възможност е особено полезна в работата с артефакти на културното наследство, която трябва да отговаря на строги регулаторни стандарти.

Много е важно да се установи стандартизирана процедура за документиране и описване на колекции от археологически, културни и художествени обекти. Идентифицирането на културни артефакти позволява стандартизираното им описание, което може да послужи като ценен инструмент за подобряване на усилията за възстановяване в случай на загуба или кражба. Разработени съвместно с музейната общност, правоприлагащите агенции, митническите власти, професионалистите в търговията с изкуство, представители на застрахователната индустрия и експерти по оценка на изкуството и антиките, тези стандарти са важен инструмент в борбата с незаконната търговия с културно наследство.

Децентрализираната идентичност на артефактите (DIDoA) също позволява мащабируемост и насърчава иновациите в гореспоменатите сектори. Този потенциал за иновации стимулира използването на приложения за децентрализирана идентичност, тъй като те могат да се адаптират и поддържат нововъзникващите технологични тенденции и изисквания.

В обобщение, мотивацията за приемане на децентрализирана идентичност на артефакти в блокчейн обхваща подобрена сигурност и конфиденциалност, повече контрол в ръцете на потребителите, намаляване на измамите, ефективност на разходите, съответствие с нормативните изисквания и увеличен потенциал за мащабируеми иновации. Тези фактори, взети заедно, ясно показват трансформиращото въздействие на DIDoA модела върху практиките за управление на идентичността на артефактите.

Цел на изследването

Целта на това изследване е да разшири рамката на модела и технологията на децентрализираната идентичност и да ги приложи към обекти, по-конкретно такива на културното наследство или други артефакти, които по природа са уникални. Следователно модела и технологиите, които използваме за идентифициране и верификация на индивиди, трябва да бъдат приложими и за артефакти.

Ние се стремим да включим в границите на модела за децентрализирана идентичност идентифицирането и верификацията на обекти, които:

- Могат да бъдат еднозначно и недвусмислено идентифицирани с помощта на технически средства, като 3D скенер, LIDAR, рентген, спектроскоп и др.
- Не могат да се заменят или копират.

Има много примери за такива обекти - исторически артефакт, произведение на изкуството, оригинален ръкописен документ и т.н. Тъй като тези обекти са уникални точно като хората, разумно е да разширим понятието за децентрализирана идентичност към такива обекти. Следователно, въвеждаме нов термин: **DIDoA - Децентрализирана идентичност на артефактите.**

Това изследване има за цел да проучи изискванията, ключовите характеристики и процесите на платформа за децентрализирана идентичност на артефакти (DIDoA) и да предложи нов модел и системна архитектура, базирана на блокчейн. Ние проучваме и доказваме осъществимостта на приложението и използването на DIDoA върху блокчейн и анализираме резултатите. Това изследване разкрива градивните елементи на DIDoA модела, базиран на блокчейн, за идентифициране на различните роли, взаимодействията между тях и процесите, в които участват.

Освен това извършваме сравнителен анализ на различни блокчейн технологии с акцент върху внедряването и потенциалните предимства и ограничения на предложения DIDoA модел на различни блокчейн платформи - Ethereum, BSN Spartan, Hyperledger Indy и Dock. Този подход позволява цялостна оценка и идентифициране на оптимални блокчейн решения за функционалността на DIDoA.

Въпросите, на които това изследване цели да отговори са:

- Каква е мотивацията за използване на децентрализирана идентичност за артефакти?

- Какво съответствие на ролите и свързания с тях алгоритъм се прилагат за:
 - Издател на Verifiable Credentials (проверими идентификационни данни)?
 - Притежател на Verifiable Credentials?
 - Администратор на артефакт?
 - Верификатор на Verifiable Credentials?
- Можем ли да приложим съществуващите DID процеси към предложението DDoA модел?
- Как да модифицираме структурите от данни, използвани в съществуващия DID протокол, за да ги приспособим към артефактите?
- Каква е структурата на DID документа за артефакти?
- Каква е структурата на верифицируемото удостоверение за артефакти?
- Каква технология използваме за уникално идентифициране на артефакти?
- Приложим ли е Zero-Knowledge Proof за верификация на артефакт?
- Какви са основните предимства от използването на децентрализирана идентичност за артефакти?
- Какви са ограниченията и предизвикателствата при използването на децентрализирана идентичност за артефакти?

Методология на изследването

Това изследване използва следните методологии в зависимост от естеството на изследователския въпрос, вида на изискваните и/или наличните данни и практическите ограничения на изследването:

- **Експериментални изследвания:** провеждаме контролирани експерименти и манипулираме една или повече независими променливи, за да наблюдаваме техния ефект. Експериментите се основават на DIDoA модела, описан в Глава 8, „Архитектура на DIDoA модела“.
- **Наблюдателно изследване:** извършваме систематично наблюдение и записваме резултатите от теста. Резултатите от експериментите са описани в глава 9, „Експеримент и резултати“.
- **Проучване на анкети:** провеждаме интервюта лице в лице или по телефона с експерти от съответните фирми и институции, за да съберем информация за основните процеси, атрибути, идентификационни данни, роли и поведение. Експертите по сигурността от митническият отдел и отдела за нелегален трафик предоставиха безценна обратна връзка, която засили аспектите на сигурността на експерименталния модел. Експертите по изкуство и културно наследство, които интервюирахме, не само споделиха знанията си, но и предоставиха практически насоки за интегрирането на тяхната област в това изследване.
- **Изследване на казус:** правим задълбочени, подробни изследвания на конкретен случай или случай на употреба в емпиричен контекст. Експерименталната настройка, която използваме, се основава на реалистичен сценарий и съдържа цялата основна функционалност на DIDoA модела. Това е допълнително обяснено в началото на Глава 9, „Експеримент и резултати“.
- **Анализ на съдържанието:** систематично анализираме съдържанието на текстове, документи или регулации, за да идентифицираме процеси, атрибути, идентификационни данни, роли, поведение или тенденции. Съгласно глава 3.3, „Научна литература за класификация на артефакти“, има много международни, национални и индустриални стандарти, насоки и референтни модели, предназначени да опишат артефакти чрез използване на много специфични структури от данни. Ние проучихме тези насоки, за

да проектираме обектите от данни, които DIDoA моделът използва за описание и идентифициране на артефакти. Тези роли, поведение и обекти са показани в Глава 9, „Експеримент и резултати“.

- Симулация и моделиране: създаваме компютърен модел за симулиране и анализ на сложни проблеми в контекста на това изследване. Архитектурата на DIDoA модела е описана в Глава 8, „Архитектура на DIDoA модела“. Експериментът и изследването се основават на DIDoA модела и следват сценарий, базиран на практическото приложение на модела. DIDoA моделът обаче е общ по природа и далеч надхвърля конкретен експеримент или приложение.
- Обоснована теория: събираме и анализираме данни, за да разработим концепции и теории, които произтичат от изследването, а не са предварително заложили. Експериментите, които проведохме на BSN Spartan, Ethereum, Hyperledger Indy, доказаха, че DIDoA моделът изисква различни структури от данни на различни блокчейн платформи.

Необходима е комбинация от горните методологии за справяне с различни аспекти на изследователския проблем.

Ще демонстрираме, че основните концепции и компоненти на конвенционалния модел за децентрализирана идентичност могат да бъдат приложени за идентифициране и верификация на артефакти.

Трите основни роли в модела на децентрализирана идентификация са: Издател, Притежател и Верификатор. За да демонстрираме, че този модел е приложим за идентифициране на артефакти, ще покажем, че трите основни обекта, които играят значителна роля в процеса на децентрализирана идентичност, могат да бъдат съпоставени с обекти, които имат съответните роли и отговорности в идентифицирането и верификация на артефактите на културното наследство. Ще установим необходимостта от включване на допълнителна роля, Администратор, в рамките на DIDoA модела. Също така ще дефинираме процесите, които Издателят, Администраторът, Притежателят и Верификаторът трябва да следват.

Модела на децентрализирана идентичност се състои от три основни градивни блока: децентрализирани идентификатори (DID), проверими идентификационни данни (VC) и блокчейн. DID функционират като уникални и криптографски проверими идентификатори в децентрализирана мрежа. VC действат като

защитени от подправяне цифрови документи, представляващи проверими твърдения относно атрибутите, квалификациите или връзките на даден субект. Блокчейн технологията служи като основна инфраструктура за DID и VC верификация в рамките на децентрализираната идентичност. DIDoA моделът и алгоритъмът за верификация изискват създаването на DID за всички роли, участващи в различните потоци на процеса. DID се съхраняват в блокчейна. Методологията, която използваме в нашето изследване, включва създаването на DID и проверими идентификационни данни. Освен това, за да докажем независимостта на модела от основната блокчейн технология, използваме различни методи за регистриране на DID.

Завършената DIDoA платформа включва множество процесни потоци:

- верификация на автентичността на артефакта
- верификация на собствеността върху артефакта
- верификация на текущото притежание на артефакт
- верификация на идентичността на собственика и/или притежателя на артефакта

Всеки от горните процесни потоци изисква различен тип проверими идентификационни данни. Проверяема презентация може да включва информация от едно или повече от тези проверими идентификационни данни, в зависимост от обхвата на заявката на Проверяващия. Ще разгледаме процесите, които са специфични за верификацията на автентичността и собствеността върху артефакти, както и представянето на Verifiable Presentation към Верификатора.

Има много работещи платформи за децентрализирана идентичност, базирани на различни блокчейн мрежи. Не на последно място, нашата цел е да тестваме приложимостта на DIDoA модела в тези блокчейн мрежи. За да можем да произведем сравними резултати, винаги използваме една и съща експериментална настройка, същата методология и едни и същи процеси. Използваме обаче различни инструменти и приложения, които са специфични за тези платформи и блокчейн мрежи.

Стратегията и дизайнът на това изследване до голяма степен се определят от изследователските въпроси, описани в предишния раздел. Ще разгледаме всеки един от изследователските въпроси, ще предоставим отговори, ще идентифицираме предизвикателствата и ще предложим решения. Ще бъде разработена концептуална рамка за децентрализирана идентичност за артефакти.

Инструменти и приложения

Това изследване насърчава прозрачността и използването на отворени научни практики. Провеждането на цялостно изследване изисква разнообразен набор от инструменти и приложения за ефективно събиране, анализиране и интерпретиране на данни. Това е списъкът с инструменти и приложения, които сме използвали, за да извършим нашите експерименти върху блокчейна Ethereum:

- Veramo (DIF) (<https://veramo.io/>) [4]
- Universal resolver (DIF) service and libraries [8]
- Hardhat Runtime Environment (HRE) with Ethers plugin [9]
- Node.js / Typescript (Visual Studio Code)

По-долу са допълнителни зависимости, описани във файл `package.json`:

```
"@ethersproject/abi": "^5.6.4",
"@ethersproject/providers": "^5.6.8",
"@nomicfoundation/hardhat-chai-matchers": "^1.0.3",
"@nomicfoundation/hardhat-network-helpers": "^1.0.4",
"@nomicfoundation/hardhat-toolbox": "^2.0.2",
"@nomiclabs/hardhat-ethers": "^2.1.1",
"@nomiclabs/hardhat-etherscan": "^3.1.0",
"@nomiclabs/hardhat-solhint": "^2.0.1",
"did-jwt-vc": "3.1.3",
"did-resolver": "^4.1.0",
"ethers": "^5.7.2",
"ethr-did-resolver": "^8.0.0",
"hardhat": "^2.14.0",
"hardhat-gas-reporter": "^1.0.9",
"jsonschema": "^1.4.1",
"jsonwebtoken": "^9.0.0",
"key-did-resolver": "1.4.0",
"typechain": "^8.1.1",
"pkh-did-resolver": "^1.2.0"
```

За да проведем нашите експерименти върху BSN Spartan блокчейн, използвахме следните инструменти и приложения:

- BSN Spartan блокчейн(Powered by NC Ethereum)
- BSN Spartan API [27]

- Spartan-I Chain Explorer [28]

BSN Spartan API изисква Java, версия 1.8 или по-нова. За подписи BSN Spartan API използва криптографския алгоритъм Secp256k1. Това е алгоритъм с елиптична крива, използван широко в областта на криптовалути, включително биткойн. Кривата е дефинирана от Standards for Efficient Cryptography Group (SECG).

За да докажем, че моделът на децентрализираната идентичност е много подходящ за използване за идентифициране и верификация на автентичността на артефакти от културно наследство, подложихме нашия модел на тест, като използвахме редица инструменти, платформи и API, които са широко достъпни и които са използвани в конвенционалния DID модел. Налични са няколко портфейла с верифициращи идентификационни данни, всеки с различни характеристики и функционалности. Тези портфейли работят в комбинация с платформи за децентрализирана идентичност или API - комерсиални или с отворен код. Тествахме нашата хипотеза с помощта на следните инструменти, API и платформи:

- Dock Certs - за издаване, трансфер и валидиране на удостоверяеми сертификати за артефакти
- Dock Wallet - за съхранение и представяне на удостоверяеми сертификати за артефакти
- Godiddy - за регистриране на DID за Издател, Администратор, Притежател, Верификатор

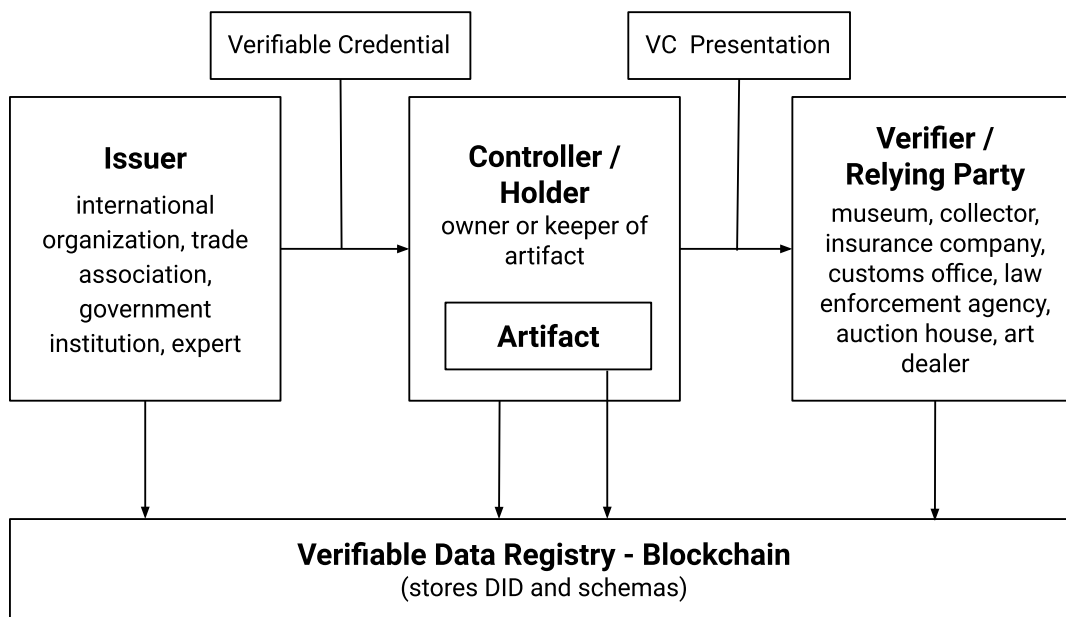
В допълнение към инструментите и приложенията, които използвахме за тестване на конкретни блокчейн платформи, използвахме и следните инструменти и приложения:

- Универсален регистратор на DanubeTech: <https://godiddy.com/app/create>
- Swimlanes.io за създаване на диаграми на последователности: <https://swimlanes.io/>
- VC Playground за издаване и верификация на удостоверяеми идентификационни данни: <https://vcplayground.org/>

Откритото разкриване на използваните инструменти и приложения позволява на други изследователи лесно да възпроизведат експерименталната методология, да проведат независимо събиране и анализ на данни, и в крайна сметка да допринесат за кумулативния напредък на знанията в областта.

Архитектура на DIDoA модела

Фигура 6.1 илюстрира основната архитектура на предложения DIDoA модел. Важно е да отбележим, че тази архитектура се отклонява от традиционната конфигурация на триъгълника на доверието, като включва администратора и артефакта в един връх. DIDoA моделът въвежда специална роля, отговорна за създаването и управлението на DID от името на самия артефакт.



Фигура 6.1. Основна архитектура на DIDoA модела

Моделът на децентрализирана идентичност се състои от три основни градивни блока: децентрализирани идентификатори (DID), проверими идентификационни сертификати (VC) и блокчейн. DID функционират като уникални и криптографски проверими идентификатори в децентрализирана мрежа. VC действат като защитени от подправяне цифрови документи, представляващи проверими твърдения относно атрибутите, квалификациите или връзките на даден субект. Блокчейн технологията служи като основна инфраструктура за DID и VC верификация в модела на децентрализираната идентичност. DIDoA моделът и алгоритъмът за верификация изискват създаването на DID за всички роли, участващи в различните процеси. DID се съхраняват в блокчейн. Методологията, която използваме в нашето изследване, включва създаването на DID и Verifiable Credentials. Освен това, за да докажем независимостта на модела от основната блокчейн технология, ще използваме различни методи за регистриране на DID.

Неразделна част от DIDaA модела е матрицата на процесите. Завършената многофункционална DIDoA платформа включва множество процесни потоци:

- верификация на автентичността на артефакта
- верификация на собствеността върху артефакта
- верификация на текущото притежание на артефакта
- верификация на идентичността на собственика и/или притежателя на артефакта

Всеки от горните процесни потоци изисква различен тип структурни данни (Verifiable Credentials). Проверяема презентация (Verifiable Presentation) може да включва информация от едно или повече от тези проверими сертификати, в зависимост от обхвата на заявката на верификатора. Ще разгледаме потоците, които са специфични за верификацията на автентичността и собствеността върху артефакти, както и представянето на Verifiable Presentation към верификатора.

Основните роли в архитектурата DIDoA са издател, администратор, притежател, артефакт и верификатор. За всяка от ролите трябва да:

- Определим ролята и отговорностите
- Съпоставим ролята със съответен субект в рамката на оперативната процедура за удостоверяване автентичността на артефакт на културно наследство

6.1. Артефакт

Роля и отговорности

Артефактът играе централна роля в DIDoA модела. Верификацията на автентичността на артефакта е целта и причината за съществуването на модела.

Важно е артефактът да отговаря на следните условия:

- Може да бъде еднозначно и недвусмислено идентифицирани чрез дигитален пръстов отпечатък, създаден чрез използването на технически средства, като 3D скенер, LIDAR, рентген, спектроскоп и др.
- Не може да се заменя или копира.

Съпоставяне на ролите

В сферата на артефактите на културното наследство, артефактът може да бъде съпоставен с исторически обект, произведение на изкуството, оригинален ръкописен документ и т.н.

6.2. Администратор

Роля и отговорности

За да идентифицираме еднозначно артефакта, трябва да му присвоим DID. За разлика от хората обаче, артефактите не са в състояние да управляват собствения си DID идентификатор - създаване, съхраняване, актуализиране и деактивиране. Следователно, появява се нуждата от агент. Препоръката на W3C относно децентрализираните идентификатори [4] предвижда такъв агент, наречен администратор: „Субектът е посочен от DID и може да бъде човек, организация, устройство, местоположение, дори концепция. Обикновено Субектът е и администратор, но в случаите на настойничество, агенти (човешки или софтуерни) и неодушевени Субекти, това не е възможно. Като такъв, Субектът няма функционална роля.“

Следователно, Администраторът трябва да регистрира своя собствен DID и DID на артефакта. Впоследствие администраторът ще има пълен контрол върху DID на артефакта и свързаната структура от данни - DID документа.

Съпоставяне на ролите

В сферата на артефактите на културното наследство администраторът може да бъде съпоставен с лицето или организацията, които притежават артефакта. Администратор може да бъде музей, художествена галерия, частен колекционер и др.

6.3. Притежател

Роля и отговорности

В рамката на DIDoA модела притежателът заема критична позиция. Той действа като суверенен собственик и администратор на DID, което му дава право да създава, управлява и актуализира своя DID документ. Това е в рязък контраст с традиционните системи за идентичност, където централизираните власти диктуват издаването и управлението на идентичността. Притежателите също играят ключова роля в управлението на удостоверителните данни. Те получават Verifiable Credentials (VC), издадени от доверени субекти (издатели), които действат като цифрови гаранتي за тяхната идентичност, собственост, квалификация или принадлежност. Те също така получават Verifiable Credentials от името на артефактите, които в момента се съхраняват при тях. След това тези

Verifiable Credentials се съхраняват в DID портфейла на притежателя.

Притежателят има право на преценка кои VC да споделя с Верификатора и кога. Това му дава възможност да разкрива информация селективно, запазвайки конфиденциалност. В някои случаи ролите на администратора и притежателя се припокриват.

Съпоставяне на ролите

В сферата на артефактите на културното наследство, ролята на притежателя ще бъде съпоставена със субекта, който в момента съхранява артефакта. Това може да е същата организация, която притежава артефакта (администраторът) или друга организация, която временно съхранява артефакта - исторически музей, художествена галерия, частна колекция и др.

6.4. Издател

Роля и отговорности

Издателят е отговорен за създаването на проверими идентификационни данни (VC) за притежателите, администраторите и артефактите в рамките на DIDoA модела. Тези VC функционират като цифрови сертификати, удостоверяващи тяхната идентичност и автентичност. Издателите играят критична роля в гарантирането на интегритета на DIDoA екосистемата. Те имат за задача да проверят точността и валидността на цялата информация, включена в издаваните от тях VC, включително цифров пръстов отпечатък на артефакта, идентичността на притежателя/администратора, собствеността върху артефакта и т.н. Надеждни процеси на верификация са от съществено значение за поддържане на доверието в рамките на мрежата. За да гарантират автентичността на VC и да предотвратят подправяне, издателите ги подписват криптографски, като използват своя личен ключ. Този подпис действа като печат срещу фалшифициране, като гарантира, че неразрешени модификации не могат да останат незабелязани.

Съпоставяне на ролите

В сферата на артефактите на културното наследство ролята на издателя може да бъде съпоставена със субекта, който проверява автентичността на артефакта. Това може да бъде правителствена агенция, международна организация, експертен орган и т.н. Може също така да бъде юридическо лице, което проверява собствеността върху артефакта, застраховател, дилър на артефакти, аукционна къща и т.н.

6.5. Верификаторът

Роля и отговорности

Основната функция на Верификатора е да оцени легитимността и валидността на идентификационните данни, представени от Притежателя по време на процеса на верификация. Верификаторът може да инициира процеса, като поиска конкретни проверими идентификационни данни от Притежателя. След като Притежателя представи своята презентация (потенциално съдържаща множество VC), верификаторът ги проверява щателно. Този процес на верификация е многостранен. Първо, верификаторът гарантира, че презентацията се придържа към очакваните комуникационни DID протоколи, като проверява нейния формат и структура. След това се верифицират отделните VC в рамките на презентацията. Това включва криптографска верификация на подписите на Притежателя и Издателя, за да се потвърди автентичността и произхода на VC. Освен това верификаторът проверява срока на валидност на VC, за да се увери, че не е изтекъл. Възможно е верификаторите да правят проверки в списъци за отмяна, поддържани от Издателите, за да проверят дали VC е маркиран като вече невалиден.

Съпоставяне на ролите

В сферата на артефактите на културното наследство, верификаторът може да бъде съпоставен с всеки субект, който трябва да потвърди автентичността и собствеността на артефакта, идентичността на Притежателя/Администратора за целите на конкретната транзакция - продажба, заем, преместване, застраховка и т.н. Това може да бъде музей, аукционна къща, застрахователна компания, митница, правоприлагащ орган, частен колекционер, търговец на произведения на изкуството, художествена галерия и т.н.

В заключение, тази глава дефинира архитектурата и основните компоненти на DIDoA модела, описва ролите и отговорностите на различните компоненти, съпоставя ги в сферата на артефактите на културното наследство, идентифицира необходимите структури от данни (VC, VP, DID) и определя матрицата на процесите.

Експериментът се основава на този DIDoA модел и симулира напълно реалистичен сценарий, който съдържа цялата основна функционалност на DIDoA

модела. DIDoA моделът обаче е общ по природа и далеч надхвърля конкретен експеримент или начин на приложение. Моделът може да се приложи във всички случаи, когато е необходима идентификация на артефакт. Въпреки че може да са необходими специфични реализации на различни блокчейн платформи, както е показано в главата „Експеримент и резултати“, моделът остава непроменен.

Експеримент

За да докажем, че DIDoA моделът работи и да проучим неговите основни характеристики и ограничения, създадохме тестова среда, която представлява имплементация на модела, разработен в главата „Архитектура на DIDoA модела“. Фигура 6.1 служи като основа за нашата експериментална конфигурация.

За да тестваме напълно DIDoA модела, включително процеси, роли, технологии и структури от данни, първо трябва да разработим систематичен подход, който се основава на изчерпателен набор от случаи на употреба. Експерименталният процес, който следваме, се основава на практически сценарий и тества цялата основна функционалност на платформа DIDoA, която включва следното:

- Администраторът е собственикът на артефакта. Администраторът регистрира DID за себе си и за артефакт. Администраторът изисква VC от различни сертифициращи органи (експертна група, агенция за собственост и т.н.). Администраторът обикновено представлява собственика на артефакта.
- Издателят е сертифициращ орган, който проверява автентичността на артефакта, като използва подходящия процес и създава цифров отпечатък, който уникално идентифицира артефакта. Издателят има свой собствен уникален DID. Издателят издава удостоверение, което може да се провери, което включва цифровия пръстов отпечатък или препратка към него.
- Издателят е сертифициращ орган, който проверява собствеността върху артефакта. Издателят има свой собствен уникален DID. Издателят издава удостоверителни данни (VC) за собственика на артефакта.
- Издателите изпращат VC до Администратора или Притежателя на артефакта.
- Администраторът / Притежателят получава сертификати, подлежащи на верификация.
- Прехвърляне на артефакт от текущия Администратор / Притежател към нов Притежател. Новият Притежател играе ролята на Верификатор. Той трябва да провери автентичността и собствеността на артефакта, както и идентичността на текущия Притежател. Верификаторът изисква цялата съответна информация от текущия Притежател, който в отговор формира Verifiable Presentation (VP), която може да включва твърдения от множество проверими идентификационни данни.

С други думи, нашият експеримент следва същия процес, който би бил използван при действително внедряване на DIDoA модела. Ние сме дефинирали случаите на употреба, изброени по-горе, от нашите изследвания и интервютата, които проведохме с експерти в областта.

Трябва да се има предвид, че в този сценарий DID на артефакта уникално идентифицира артефакта само в комбинация с цифровия пръстов отпечатък, който е включен или споменат във VC, издаден от съответния орган.

Провеждайки нашия експеримент, ние се стремим да постигнем следните резултати:

- Регистрация на DID за всяка роля
- Определяне на алгоритъм за всяка роля
- Дефиниране на структурите от данни, необходими за всяка роля
- Създаване на диаграма на последователност, която показва взаимодействията между всяка роля и другите роли в процеса

За по-добро визуализиране на резултатите използваме блокови диаграми, диаграми на последователности, JSON-LD код и блокчейн транзакции. Резултатите, получени в тази глава, служат като основа за следващия раздел „Дискусия“, където се изследват последиците, изводите, потенциалните ограничения и приложения на тези резултати.

Основни констатации и значение на това изследване

Блокчейн играе централна роля в рамките на модела на децентрализирана идентичност, осигурявайки сигурна, децентрализирана, неизменна и защитена от подправяне база данни за идентичност. Различни блокчейн платформи, като Ethereum, Hyperledger Indy, BSN и Dock, бяха използвани за създаване на решения за децентрализирана идентичност на артефактите. Използването на блокчейн технология се справя с основните предизвикателства, присъщи на конвенционалните централизирани системи за идентичност. Следователно блокчейн се очертава като предпочитано решение за идентифициране и верификация на артефакти.

Това проучване успешно демонстрира осъществимостта на използването на децентрализирана идентичност в блокчейн за идентифициране и верификация на артефакти на културното наследство. Тези резултати допринасят към текущото развитие на децентрализираната идентичност в блокчейн и нейните приложения в още една област, която е от първостепенно значение.

Целта на това изследване е да се усъвършенства конвенционалният модел и технология на децентрализираната идентичност (DID) чрез прилагането му към уникални обекти, особено артефакти на културното наследство. Подобно на индивидите, артефактите притежават уникални характеристики, които позволяват надеждна идентификация и сертифициране. Следователно методологиите и технологиите, използвани за идентифициране и сертифициране на лица, следва да бъдат приложими и за артефакти. Това изследване изследва изискванията, ключовите характеристики и процесите на модела на децентрализирана идентичност на артефакти (DIDoA) и предлага нова системна архитектура, базирана на блокчейн.

Новият DIDoA модел е комбинация от следните основни технологии:

- Децентрализирана идентичност (DID)
- Инфраструктура с публичен ключ (PKI)
- Блокчейн
- Цифров пръстов отпечатък

Тези основни технологии работят заедно, за да предоставят характеристиките и функционалностите, които са необходими на DIDoA модела, за да постигне целите си. Конвенционалният DID модел осигурява общата рамка и процеси. PKI осигурява цялост на информацията и удостоверяване. Блокчейн осигурява

прозрачност и неизменност. Цифровият пръстов отпечатък предоставя набор от уникални параметри, които позволяват идентифициране на артефакт.

Беше проведено проучване за осъществимост, за да се демонстрира прилагането на DIDoA модела върху блокчейн. Това проучване включва създаване на експериментален прототип на различни блокчейн платформи, включително Ethereum, BSN Spartan, Hyperledger Indy и Dock. Ethereum демонстрира стабилна и проверена инфраструктура с обширна поддръжка от разработчици, но по-високи оперативни разходи. BSN Spartan осигури силна оперативна съвместимост и рентабилност. Hyperledger Indy предлага разширени функции за конфиденциалност и управление на идентичността. Dock подчерта своята мащабируемост и лекота на внедряване.

Чрез реализацията на DIDoA модела на различни блокчейн платформи, ние също демонстрирахме блокчейн агностичната природа на модела. Резултатите от експеримента разкриват, че различните блокчейн мрежи изискват различни структури от данни за конструиране на DID документа и Verifiable Credential. Независимо от това, тези разлики могат да бъдат отчетени и включени в изпълнението на DIDoA модела.

Въпреки че експериментът е конфигуриран и проведен въз основа на конкретен набор от основни процеси, извлечени от типичен сценарий на употреба, DIDoA моделът не е обвързан с конкретен случай на употреба и предоставя цялата функционалност, необходима за удостоверяване на артефакти във всяко едно приложение на модела.

Последствията от това изследване са значими, особено предвид огромния брой артефакти на културното наследство по света. Има милиарди артефакти, съхранявани в над 55 000 музея, частни колекции, художествени галерии и т.н. по света. Само в България в националните и регионалните исторически музеи има над 7 000 000 артефакта.

Чрез успешното прилагане на технологията за децентрализирана идентичност (DID) за идентифициране и сертифициране на тези артефакти, нашите изследвания предлагат значителен принос в опазването и управлението на културното наследство.

DIDoA модела предоставя стабилна рамка за гарантиране на автентичността и произхода на артефактите на културното наследство. Чрез присвояване на всеки

артефакт на уникален децентрализиран идентификатор (DID) и записване на всички транзакции и сертификати в блокчейн регистър, тази система подобрява възможността за верификация на автентичността, собствеността и произхода на артефактите. Това е особено важно за решаването на проблеми като фалшифицирането, кражбата и незаконния трафик на предмети на културното наследство. Музеите, галериите и културните институции могат да използват тази технология, за да поддържат точни и защитени от подправяне записи на своите колекции, като по този начин запазват интегритета и стойността на артефактите на културното наследство.

Прилагането на DIDoA модела също улеснява достъпа и споделянето на информация за артефакти на културното наследство. Изследователите, историците и обществеността могат да получат достъп до подробни, проверими записи на артефакти, включително техния произход и историческо значение, чрез сигурна и децентрализирана платформа. Това може да подобри образователните инициативи, да насърчи културното съзнание и да подпомогне научните изследвания чрез предоставяне на надеждни и изчерпателни данни за артефактите на културното наследство.

Оперативната съвместимост на DIDoA модела със съществуващите рамки за идентичност и блокчейн технологии насърчава по-голямо сътрудничество между културните институции в световен мащаб. Чрез приемането на стандартизиран подход за идентифициране и сертифициране на артефакти институциите могат по-лесно да споделят информация, да си сътрудничат в усилията за опазване и да участват в съвместни изложби или изследователски проекти. Тази взаимосвързаност подкрепя по-унифициран и координиран подход към управлението на културното наследство, използвайки силните страни на различни институции и технологии.

Функциите за сигурност и конфиденциалност, присъщи на DIDoA модела, предлагат значителни предимства за защитата на конфиденциална информация, свързана с артефакти на културното наследство. Използването на криптографски техники, като селективно разкриване и доказателства с нулево знание, гарантира, че само необходимата информация се споделя по време на процесите на верификация, като по този начин защитава конфиденциалността на заинтересованите страни и намалява риска от пробиви на данни. Това е особено важно за опазването на идентичността на колекционери, дарители и други лица, участващи в съхранението на артефактите на културното наследство.

И накрая, успешното прилагане на DiDoA модела може да генерира икономически и социални ползи. Чрез повишаване на сигурността, автентичността и достъпността на артефактите на културното наследство, платформата може да увеличи общественото доверие и ангажираността с културните институции. Това от своя страна може да стимулира туризма, финансирането и подкрепата за инициативи за опазване на културното наследство. Освен това технологията може да създаде нови възможности за иновации и предприемачество в сектора на културното наследство, като стимулира икономическия растеж и насърчава по-задълбочено оценяване на културното наследство в световен мащаб.

В обобщение, въздействието на това изследване се простира отвъд техническата иновация на DiDoA модела, предлагайки трансформиращи ползи за опазването, управлението и оценяването на артефактите на културното наследство. Използвайки предимствата на технологията за децентрализирана идентичност, това изследване проправя пътя за по-сигурен, прозрачен и взаимосвързан подход към опазването на културното наследство, с широкообхватни последици за институциите, изследователите и обществеността.

Ограничения и предизвикателства

Въпреки обещаващите резултати, важно е да се признаят ограниченията и предизвикателствата, свързани с DIDoA модела, включително:

- **Мащабируемост:** Докато блокчейн технологията непрекъснато се развива, мащабируемостта остава проблем за широкомащабни приложения.
- **Цена:** Блокчейн транзакциите водят до разходи. Притежателите на артефакти, като музеите, може да имат хиляди или дори десетки хиляди артефакти в своите колекции.
- **Техническа експертиза:** Внедряването и поддръжката на DIDoA приложения изисква специализирани технически познания.
- **Стандартизация:** Липсата на стандартизация за прилагане на DIDoA модела в сферата на културното наследство може да попречи на оперативната съвместимост.

Справянето с тези предизвикателства ще бъде от решаващо значение за широкото прилагане на модела за децентрализирана идентичност на артефактите в блокчейн за идентифициране и верификация на артефакти.

Сравнение на тестваните блокчейн платформи

За да сравним ефективността на блокчейните Ethereum, Hyperledger Indy, Dock и BSN Spartan по време на нашия експеримент, трябваше да вземем предвид различни фактори като механизми за консенсус, мащабируемост, случаи на използване, пропускателна способност на транзакции, сигурност и обща архитектура. Всяка от тези блокчейн мрежи е проектирана с конкретна цел. Производителността също варира в зависимост от текущото натоварване на мрежата. Обобщено сравнение е показано в таблица 8.1.

	Ethereum	Hyperledger Indy	Dock	BSN Spartan
Objective	dApps, DeFi, NFTs, General purpose	Decentralized Identity (DID)	Identity, Credentialing	Enterprise, Government applications
Consensus	Proof-of-Stake (PoS)	BFT (Byzantine Fault Tolerant)	Proof-of-Authority (PoA)	Hybrid (PoA + others)
TPS	~15-30 TPS (Ethereum 1.0), 1000s (Ethereum 2.0 w/ Layer 2)	Thousands (optimal)	Hundreds to 1000s	Thousands
Finality	~10-15 min	Instant finality	Fast finality	Fast finality
Security	Very secure (decentralized)	High (permissioned)	High (permissioned)	High (permissioned)
Strengths	Large ecosystem, secure, decentralized	Optimized for identity, enterprise grade	Fast, scalable, enterprise focused, interoperable	Scalable, cross-border blockchain solutions
Weaknesses	High fees, lower throughput in base chain	Limited use cases	Less decentralized	Asia focused

Table 8.1. Blockchain Comparison

В заключение:

- Ethereum е блокчейн с общо предназначение, най-добър за децентрализирани приложения (dApps) и широкомащабни децентрализирани екосистеми, но има високи транзакционни разходи и мащабируемост (без Ethereum 2.0 и Layer 2).
- Hyperledger Indy се отличава с децентрализирано управление на идентичността, осигурявайки бърз консенсус, и силни функции за конфиденциалност и сигурност за специфични случаи на употреба, но му липсва функция за интелигентен договор с общо предназначение.
- Dock е идеален за решения за идентичност и идентификация на корпоративно ниво с фокус върху скалируемостта и оперативната съвместимост, но централизацията му чрез PoA може да ограничи някои приложения.
- BSN Spartan се фокусира върху скалируемостта за корпоративни и държавни приложения, с трансгранична оперативна съвместимост.

В обобщение, всеки блокчейн обслужва различни нужди, така че изборът зависи от конкретния случай на употреба. Ethereum е подходящ за децентрализирани приложения, Hyperledger Indy за идентичност, Dock за мащабируеми идентификационни данни и BSN Spartan за трансгранична оперативна съвместимост.

Сравнение със съществуващи решения

Както се подчертава в глава “Преглед на литературата”, технологията за децентрализирана идентичност (DID), съчетана с блокчейн инфраструктура, предизвиква значителен изследователски интерес в различни индустрии. Традиционно концепцията за децентрализирана идентификация се прилага към лица, организации и устройства, свързани с интернет (IoT устройства). Съществуващата литература изследва широка гама от DID приложения в блокчейн, обхващащи сектори като управление на веригата за доставки, здравеопазване и финанси. Съществува обаче критична липса на научна работа в сферата на прилагането на DID върху блокчейн, специално за артефакти на културното наследство. Нашето изследване има за цел да запълни тази ниша в научната работа, като представи първото документирано изследване на осъществимостта и ефикасността на базираната на DID идентификация и верификация на артефакти в областта на културното наследство.

Докато многобройни публикации са посветени на идентифицирането, документирането и верификацията на артефакти на културно наследство, използвайки установени стандарти и референтни модели, а други изследват различни случаи на употреба на DID в блокчейн в различни индустрии, не беше идентифицирана нито една научна работа, която да се отнася директно до идентифицирането и верификацията на артефакти на културното наследство. Беше поставен специален акцент върху идентифицирането на съществуваща литература, която съответства на определението за „артефакт“, използвано в това изследване. Този щателен преглед на съществуващата научна литература не доведе до откриването на публикации, посветени на DID и блокчейн технологията за идентифициране на артефакти на културно наследство по начин, който се придържа към установените индустриални стандарти. Ето защо можем да твърдим, че това изследване предлага новаторски принос в областта, служейки като първата публикувана научна работа за изследване на това ново приложение на DID и блокчейн технологията в областта на културното наследство. То е първото, което също емпирично демонстрира, че децентрализираната идентичност на блокчейн може да се използва ефективно за идентифициране и верификация на артефакти.

Въпреки това проведохме сравнителен анализ на DIDoA модела и съществуващите решения за идентифициране на артефакти. Резултатите са показани в таблица 8.2.

	DIDoA Model	Existing Solutions
Control	Decentralized	Centralized
Technology	PKI + DID + Blockchain + Digital Fingerprint	Database, Text files
Transparency	Unique, verifiable identity	Low visibility
Traceability	Immutable audit trail	Low accountability
Fraud Prevention	Verification via digital fingerprint	Verification via data points
Regulatory Compliance	Supports multiple standards	Supports single standard
Security	Cryptographic (PKI)	Vulnerable to tampering and unauthorized access
Data Privacy	Selective disclosure	Non-selective disclosure
Operational Efficiency	Automatic validation of identities and credentials	Manual validation of identities and credentials
Cost	Reduced cost, no manual checks	Higher cost, manual checks
Trust	High - no central authority	Low - central authority
Data Sharing	Better collaboration and information sharing	Lack of trusted and verifiable data sharing
Resilience	Tamper proof	Prone to attacks
Business Continuity	Persistent	Prone to outages

Table 8.2. DIDoA Comparison to Existing Solutions

В обобщение, DIDoA моделът може да трансформира идентичността на артефакта и проверката на автентичността чрез подобряване на прозрачността, намаляване на фалшификациите и незаконния трафик, подобряване на сигурността и съвместимостта, като същевременно намалява оперативните разходи и позволява надеждно, ефективно споделяне на данни.

Корелация с теория на Управлението на знанията

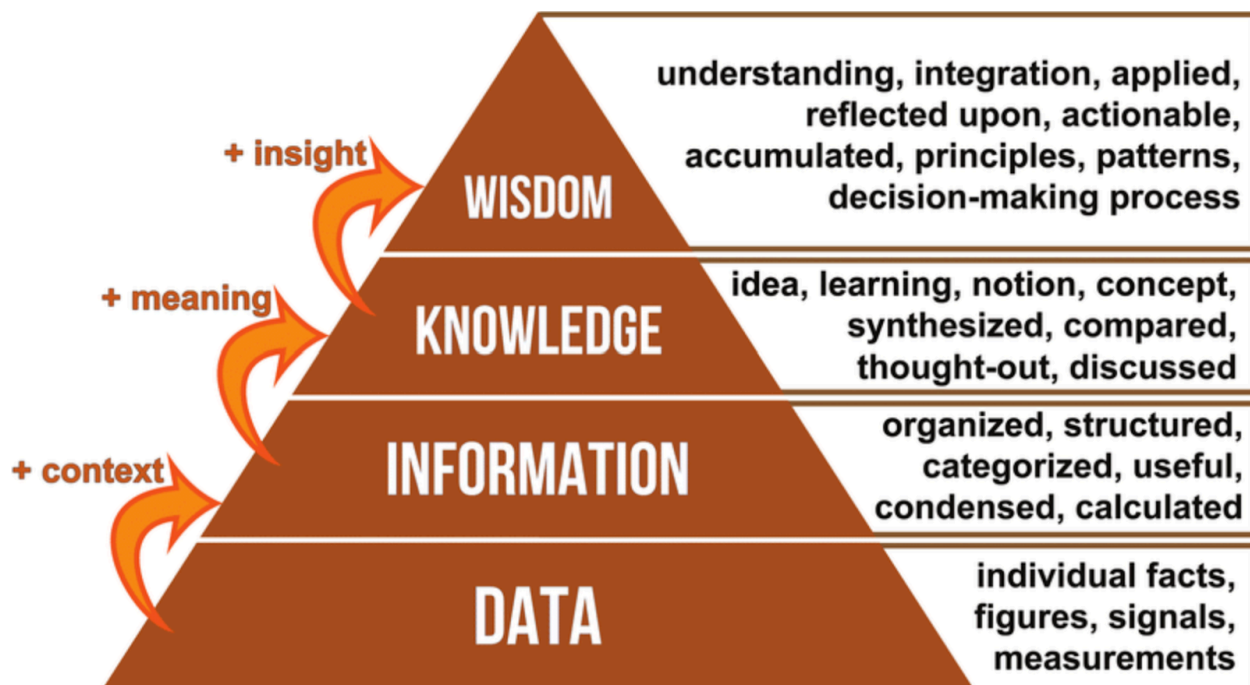
Важен принос на това изследване е корелацията и прилагането на принципите и терминологията на теорията за управление на знанието към процесите и модела на децентрализираната идентификация.

Един от основните градивни елементи на теорията за управление на знанието е DIKW пирамидата. Известна е още като йерархията данни-информация-знание-мъдрост (DIKW). Пирамидата DIKW е концептуален модел, използван в управлението на знанието и науката за данни, за да представи нарастващите нива на абстракция и добавена стойност при обработката на информация. Често се изобразява като пирамида с данни в основата и мъдрост на върха (Фигура 8.1).

Най-ниското ниво на пирамидата представлява данните – необработени факти и цифри. Те могат да бъдат от различен тип - от показания на сензори до финансови трансакции. Данните сами по себе си нямат особено значение.

Данните се трансформират в информация чрез прилагане на контекст и организация. Това включва структуриране на данни, идентифициране на модели и придаване на значение. Информацията отговаря на въпроса "какво". Информацията се обработва и анализира допълнително, за да се създаде знание. Знанието включва разбирането на връзки, причини и следствия и прилагане на информация в специфичен контекст. Отговаря на въпроса "как" и "защо".

Най-високото ниво на пирамидата представлява мъдростта - способността да се използва знание, за да се вземат разумни преценки и решения. Мъдростта включва опит, интуиция и етични съображения. Отговаря на въпроса "какво да правя".

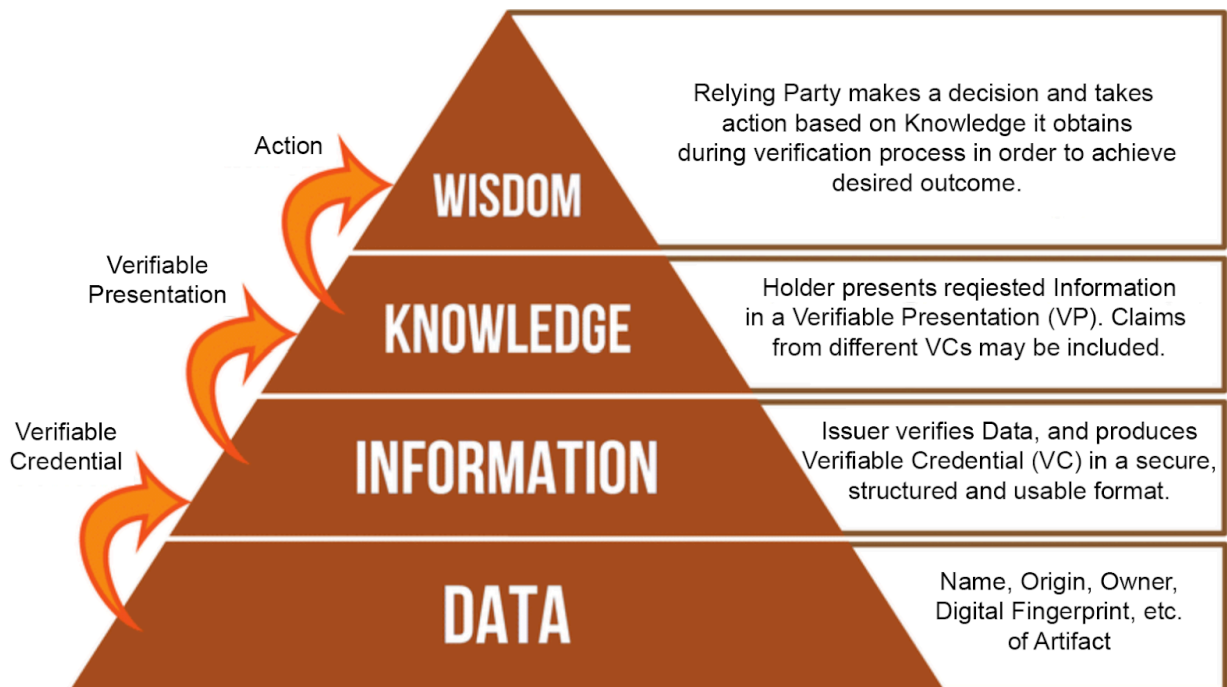


Фигура 8.1. Пирамида DIKW [23]

Може да се направи важна връзка между процеса на последователното преобразуване на Данните в Информация, Знание и накрая Мъдрост и процеса на верификация - издаване на Verifiable Credentials (VC), представяне на VC чрез Verifiable Presentation и предприемане на действие за постигане на желаните цели.

В контекста на децентрализирана идентичност на артефакти, Данните са всички отделни факти, свързани с артефакта – име, произход, собственост, измервания, цифров пръстов отпечатък и т.н. Сами по себе си всички тези отделни данни нямат много смисъл. Данните се трансформират в Информация само след като Издателят провери всички Данни и издаде Verifiable Credential, който се състои от множество отделни данни, които са организирани по смислен, структуриран, сигурен и използваем начин и представени на Притежателя под формата на VC. Тази информация става Знание, след като Verifiable Presentation (VP) достави исканата информация от Притежателя на Верификатора. VP може да съдържа информация от различни Verifiable Credentials. Въоръжен с това знание, Верификаторът формира мъдрост, на базата на която вече може да взема решения и да предприема подходящи действия, за да постигне желаните резултати.

Последователното преобразуване на данни в информация, знание и мъдрост в контекста на децентрализираната идентичност за артефакти е изобразено на фигура 8.2.



Фигура 8.2. Пирамида DIKW в контекста на DIDoA

В заключение, ясно демонстрирахме приложимостта на теорията за управление на знанието в контекста на децентрализираната идентичност на артефактите. Това е важно, защото укрепва аргументите и за двете области на науката и може да послужи като основа за по-нататъшни изследвания.

Заклучение и по-нататъшно проучване

Изследването, представено в тази дисертация, успешно се справи с целите, които си постави. Чрез експерименти и систематичен анализ демонстрирахме осъществимостта и ефективността на прилагането на технологията за децентрализирана идентичност (DID) за идентифициране и верификация на артефакти на културното наследство.

Нашите разкрития показват, че DIDoA модела, изграден върху базирана на блокчейн системна архитектура, предлага мащабируемо, сигурно и запазващо конфиденциалността решение за управление на идентичности на артефакти. Сравнителният анализ на различни блокчейн технологии, включително Ethereum, BSN Spartan, Hyperledger Indy и Dock, предостави цялостно разбиране на предимствата и ограниченията на всяка платформа. Този анализ подчертава устойчивостта на Ethereum, оперативната съвместимост и рентабилността на BSN Spartan, функциите за конфиденциалност на Hyperledger Indy и ефективността на Dock, като по този начин прави възможен избора на най-подходящите блокчейн решения за различни приложения на DIDoA модела.

Успешното прилагане на поредица от експерименти показва, че основните принципи на децентрализираната идентичност могат да бъдат ефективно адаптирани към артефакти, осигурявайки сигурна верификация на тяхната идентичност и автентичност, сертифициране срещу подправяне и проследяване на произхода. Използването на криптографски техники и методи за запазване на конфиденциалността, като селективно разкриване и доказателства с нулево знание, допълнително повишава сигурността и конфиденциалността на DIDoA модела.

Има много аспекти на описания модел, които трябва да бъдат допълнително проучени в детайли - разработване на специализирани инструменти и платформи, които могат да улеснят реализацията на различни елементи или целия модел, използване и включване на технология за пръстови отпечатьци на артефакти, методи за верификация, методи за криптиране и т.н. Бъдещите изследвания трябва също така да проучат интегрирането на DIDoA модела с други технологии, като изкуствен интелект и сензорни мрежи, за допълнително повишаване на ефективността и обхвата на идентификацията и верификацията на артефакти. Освен това, изследването на правните и етични последици ще бъде от решаващо значение за отговорното му прилагане в практиката.

В заключение, това изследване значително разшири приложимостта на конвенционалния модел за децентрализирана идентичност, проправяйки път за нови иновации в областта на идентифицирането и верификацията на артефакти. Моделът за децентрализирана идентичност на артефактите представлява първа важна стъпка към използването на блокчейн технологията в опазването на културното наследство, като предлага стабилна рамка, която може да бъде адаптирана към широк спектър от приложения. Бъдещата работа ще се съсредоточи върху усъвършенстване на системната архитектура, подобряване на оперативната съвместимост със съществуващите модели за идентичност и проучване на допълнителни случаи на приложение, с цел по-нататъшно валидиране и разширяване на възможностите на модела на децентрализираната идентичност на артефактите на блокчейн.

Авторска справка

Това изследване има важен научен и приложно-научен принос в областта на управлението на децентрализираната идентичност и културното наследство:

8.5.1. Създадохме нов DID модел за верификация на автентичността на артефакти на културното наследство. Въведохме нова терминология, за да опишем функционалността на DIDoA модела. Идентифицирахме множеството процесни потоци и разработихме интегрирана матрица на процесите. Дефинирахме структурите от JSON-LD данни, изисквани от модела. Въведохме модифицирана конфигурация на триъгълника на доверието, като включихме контролера и артефакта в един връх, дефинирахме и съпоставихме ролите в контекста на конкретни приложения на модела. Дефинирахме алгоритми за основните компоненти и демонстрирахме тяхното взаимодействие с диаграми на последователност. Въведохме нова концепция - пръстов отпечатък на цифров артефакт - който да се използва за верификация на автентичността на артефакта. Идентифицирахме ограниченията и предизвикателствата на DIDoA модела. Тези приноси могат да бъдат открити в глави „Въведение“, „Архитектура на DIDoA модела“, „Експеримент и резултати“ и „Дискусия“, както и в статиите:

- Ivan Lambov, Kim Hamilton Duffy, “Decentralized Identity of Artifacts – System Architecture”, Proceedings of 12th International Intelligent Systems IS’24 Conference, Varna, Bulgaria, 2024, doi: 10.1109/IS61756.2024.10705248
- Ivan Lambov, “Decentralized Identity of Artifacts on the BSN Spartan Blockchain”, Proceedings of 12th International Intelligent Systems IS’24 Conference, Varna, Bulgaria, 2024, doi: 10.1109/IS61756.2024.10705221

8.5.2. Илюстрирахме как моделът на децентрализираната идентичност на артефактите се вписва в контекста на теорията за управление на знания и по-специално в йерархията данни-информация-знание-мъдрост (DIKW) - концептуалният модел, използван в управлението на знанията и науката за данни за представяне на нарастващите нива на абстракция и добавена стойност при обработката на информация. Показахме, че може да се направи връзка между процеса на последователно преобразуване на Данни в Информация, Знание и накрая Мъдрост и процеса на верификация - издаване на Verifiable Credential (VC), презентиране на VC чрез Verifiable Presentation (VP) и предприемане на действие за реализация на поставените цели. За целта представихме нова конфигурация на DIKW пирамидата. Тези приноси могат да

бъдат намерени в глава „Дискусия“, раздел „Корелация с теорията за управление на знанието“.

8.5.3. Проучихме осъществимостта на прилагането на модела за децентрализирана идентичност на артефакти върху различни блокчейни. Демонстрирахме блокчейн агностичната природа на модела на децентрализираната идентичност на артефактите. Предоставихме набор от налични инструменти и приложения за изграждане на DIDoA приложения. Включихме примери за структури от данни, които могат да бъдат конфигурирани за конкретни приложения. Посочили сме редица съществуващи технологии, които могат да се използват за генериране на пръстов отпечатък на цифров артефакт за VC и VR. Показахме как моделът може да бъде мащабиран, за да отговори на изискванията за висок обем на транзакциите чрез въвеждане на профили. Тези приноси могат да бъдат намерени в главите „Експеримент и резултати“ и „Дискусия“, а също и в статията: Ivan Lambov, “Use Case Feasibility Study: Decentralized Identity on Blockchain for Cultural Heritage Artifacts”, ACM International Conference Proceeding Series, 2024, Ref, IR , SCOPUS, SJR (0.253), <https://doi.org/10.1145/3674912.3674930>.

Публикации и рецензии

ORCID iD: 0009-0006-9856-3187

1. Ivan Lambov, Decentralized Identity: Recent Scientific Advancements and Applications, AUTOMATICA and INFORMATICS, vol:LVII, issue:1, 2024, pages:26-32, ISSN (print):0861-7562, ISSN (online):2683-1279 2024
2. Ivan Lambov, Kim Hamilton Duffy, Decentralized Identity of Artifacts – System Architecture, Proceedings of 12th International Intelligent Systems IS'24 Conference, Varna, Bulgaria, 2024
3. Ivan Lambov, Decentralized Identity of Artifacts on the BSN Spartan Blockchain, Proceedings of 12th International Intelligent Systems IS'24 Conference, Varna, Bulgaria, 2024
4. Ivan Lambov, Use Case Feasibility Study: Decentralized Identity on Blockchain for Cultural Heritage Artifacts, ACM International Conference Proceeding Series, 2024, Ref, IR, SCOPUS, SJR (0.253), <https://doi.org/10.1145/3674912.3674930>

Документът е много тясно свързан с информационните технологии, тъй като описва метод за дигитално управление на културни артефакти, базиран на W3C децентрализирани идентификатори, които са компонент на по-широка концепция за децентрализирана идентичност (вижте например <https://identity.foundation/>). Авторът описва своето първоначално внедряване на използване на децентрализирани идентификатори на W3C за управление на идентичност, базирано на блокчейн, на артефакти на културно наследство. Въпреки съществуването на подобни базирани на блокчейн подходи, новостта на представения подход е в използването на децентрализирани идентификатори в конкретния случай на употреба на артефакти на културното наследство. В Раздел 6 авторите описват ключовите елементи за внедряване на тяхното оригинално решение за децентрализирана система за управление на идентичността за артефакти на културното наследство.

Значимостта на този принос се основава на следните елементи
- Използване на нови предложения на W3C относно DID (децентрализирани идентификатори)

- Първо адаптиране на подхода на децентрализираната идентичност в областта на управлението на артефактите на културното наследство.

Документът изследва използването на технологията за децентрализирана идентичност (DID) в блокчейн за управление и защита на артефакти на културно наследство. Този подход има за цел да се справи с проблеми като незаконната търговия с артефакти на културното наследство и да даде възможност на художници, археолози, музеи и др. да наблюдават и оценяват такива обекти. Идеята прилага усъвършенствана блокчейн технология (напр. DID) към област, която обикновено разчита на по-традиционни методи, като се занимава по уникален начин със специфични проблеми като произход на артефакт и автентичност.

Предложената техника предоставя решение на проблеми като валидиране на произхода и собствеността на артефакти на културното наследство. Използвайки концепцията за децентрализирана идентификация в блокчейн, техниката има за цел да подобри защитата и прозрачността, така че да помогне на отговорни заинтересовани страни като музеи и културни институции. Документът подчертава практическите въздействия на тази система, което я прави ценен принос както към технологиите, така и към областта на културното наследство.

Документът е добре структуриран и се състои от раздели, които помагат на читателя да разбере подхода на авторите към проблема и естеството на самия проблем и как е свързан с използваната технология.

Като цяло документът представя добре проучено и практическо приложение на технологията за децентрализирана идентичност в блокчейн за проследяване и верификация на артефакти на културното наследство. Приносите са ясни и полезни, като се занимават с настоящите предизвикателства в областта, въпреки че можеха да бъдат по-подробни. Това осигурява добра основа за бъдещи изследвания и внедряване.

Благодарности

Тази дисертация бележи кулминацията на едно обогатяващо и изпълнено с предизвикателства пътуване и бих бил небрежен да не отдам признание на много хора и институции, допринесли за нейния успех.

Преди всичко дължа най-дълбоката си благодарност на моя уважаван научен ръководител доц. Петко Русков. Вашите постоянни насоки, проникателна обратна връзка и непоколебима подкрепа изиграха важна роля в оформянето на моите изследвания и ме тласкат напред. Вашата отдаденост на моето развитие не остана незабелязана и аз съм много благодарен за Вашето менторство.

Благодарен съм и на доц. Александър Димов, доцент в Софийския университет, чиято рецензия даде безценна обратна връзка и значително подобри структурата, организацията и представянето на съдържанието на дисертацията ми.

Изразявам най-искрената си благодарност на Ким Хамилтън Дъфи и Деймиън Глоувър от Фондация за децентрализирана идентичност за техническата подкрепа и безценните прозрения, които получих. Вашият принос изигра решаваща роля за тласкането на моето изследване напред и разширяването на неговия обхват.

Бих искал също да благодаря на Шон Чен и целия екип на BSN за възможността да тествам моята хипотеза за BSN Spartan blockchain и експертните съвети и насоки.

Благодаря на експерта по изкуство и културно наследство д-р Калина Сотирова-Вълкова от БАН, която не само сподели знанията си, но и даде практически насоки за интегрирането им в моите изследвания.

Сърдечни благодарности на моите колеги от Академията проф. Николай Ноколов и доц. д-р Красимира Иванова. Вашите стимулиращи дискусии, дух на сътрудничество и желание да предложите ценни прозрения създадоха благоприятна среда, която ми помогна да се ориентирам в сложни идеи и да прецизирам изследователския си фокус.

На моето семейство и деца, Никол и Синтия, благодаря за вашата непоколебима любов и насърчение по време на това възискателно начинание. Вашето разбиране

и търпение, докато работех до късно вечер и преследвах крайни срокове, бяха безценни. Вашата вяра в мен подхрани моята отдаденост и постоянство.

И накрая, изказвам своята благодарност на всички, които по някакъв начин допринесоха за моето изследване и прилагането на експерименталния модел. Вашата подкрепа, помощ и желание за сътрудничество са безценни.

Тази дисертация е свидетелство за колективните усилия и подкрепата на толкова много хора. Дълбоко съм благодарен за вашия принос и за мен е чест да споделя това постижение с вас.

Литература

- [1] Markus Sabadello and Cihan Saglam. 2022. DID Registration. <https://identity.foundation/did-registration>
- [2] Manu Sporny, Dave Longley and David Chadwick. 2022. Verifiable Credentials Data Model v1.1. <https://www.w3.org/TR/vc-data-model>
- [3] Ryan Grant and Adrian Gropper. 2019. Use Cases for Decentralized Identifiers. <https://w3c-ccg.github.io/did-use-cases>
- [4] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Ori Steele, and Christopher Allen. 2022. Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations. <https://www.w3.org/TR/did-core>
- [5] HeeJung Rim. 2023. Decentralized identity (DID): new technology adoption and diffusion in South Korea. Transforming Government: People, Process and Policy. Vol. 17 No. 2, pp. 251-270. <https://doi.org/10.1108/TG-11-2021-0189>
- [6] Martin Duclos. 2023. A conceptual decentralized identity solution for state government. <https://scholarsjunction.msstate.edu/td/6013>
- [7] Chalima Dimitra Nassar Kyriakidou, Athanasia Maria Papathanasiou, and George C. Polyzos. 2023. Decentralized Identity with Applications to Security and Privacy for the Internet of Things. Computer Networks and Communications, 1(2), 244–271. <https://doi.org/10.37256/cnc.1220233048>
- [8] Tianmin Xiong, Zhao Zhang, and Cheqin Jing. 2024. Privacy-Preserving Educational Credentials Management Based on Decentralized Identity and Zero-Knowledge Proof. Communications in Computer and Information Science, vol 2023. Springer, Singapore. https://doi.org/10.1007/978-981-97-0730-0_22
- [9] Pinky Bai, Sushil Kumar, Geetika Aggarwal, Mufti Mahmud, Omprakash Kaiwartya, and Jaime Lloret. 2022. Self-Sovereignty Identity Management Model for Smart Healthcare System. Sensors 2022, 22(13), 4714. <https://doi.org/10.3390/s22134714>

- [10] Yanling Chang, Eleftherios Iakovou, and Weidong Shi. 2019. Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. <https://doi.org/10.1080/00207543.2019.1651946>
- [11] Lukas Stockburger, Georgios Kokosioulis, Alivelu Mukkamala, Raghava Rao Mukkamala, and Michel Avital. 2021. Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, Volume 2, Issue 2. <https://doi.org/10.1016/j.bcra.2021.100014>
- [12] Luisanna Cocco, Roberto Tonelli, and Michele Marchesi. 2021. Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain. <https://doi.org/10.3390/fi13120301>
- [13] Lisha Yang, Feng Yu, and Yu Nie. 2022. Protection of Jingdezhen Ceramic Heritage Based on Blockchain Technology. *Wireless Communications and Mobile Computing*. 1-7. DOI:10.1155/2022/9710902
- [14] DublinCore. 2017. Dublin Core Metadata Element Set. <https://www.dublincore.org/specifications/dublin-core/dces>
- [15] English Heritage. 2012. MIDAS Heritage – The UK Historic Environment Data Standard. https://historicengland.org.uk/images-books/publications/midas-heritage/midas-heritage-2012-v1_1
- [16] ISO 21127. 2023. Information and Documentation - A Reference Ontology for the Interchange of Cultural Heritage Information. <https://www.iso.org/standard/85100.html>
- [17] Erin Coburn, Richard Light, Gordon McKenna, Regine Stein, and Axel Vitzthum. 2010. LIDO - Lightweight Information Describing Objects. <https://lido-schema.org/schema/v1.0/lido-v1.0-specification.pdf>
- [18] Murtha Baca, Patricia Harpring, Elisa Lanzi, Linda McRae, and Ann Whiteside. 2006. *Cataloging Cultural Objects: A Guide to Describing Cultural Works and Their Images*.

https://edisciplinas.usp.br/pluginfile.php/5506147/mod_resource/content/1/Cataloging_Cultural_Objects.pdf

- [19] Murtha Baca and Patricia Harpring. 2022. Categories for the Description of Works of Art.
https://www.getty.edu/research/publications/electronic_publications/cdwa
- [20] Robin Thames, Peter Dorrell, and Henry Lie. 1999. Introduction to Object ID - Guidelines for Making Records that Describe Art, Antiques, and Antiquities.
<https://www.getty.edu/publications/resources/virtuallibrary/0892365722.pdf>
- [21] International Council of Museums. 2012. Statement of principles of Museum Documentation.
https://cidoc.mini.icom.museum/wp-content/uploads/sites/6/2020/03/principles6_2.pdf
- [22] International Council of Museums. 2012. Statement of Linked Data identifiers for museum objects.
<https://cidoc.mini.icom.museum/wp-content/uploads/sites/6/2020/03/StatementOnLinkedDataIdentifiersForMuseumObjects.pdf>
- [23] BSN Spartan API. 2022. <https://github.com/BSN-Spartan/DID>
- [24] Chen et al., 2022. Decentralized Identity for the Internet of Things (IoT): Securing Device Interactions.
- [25] Kuo et al., 2023. Decentralized Identity for Government Services: Enabling Efficient and Secure Access.
- [26] Mazzocchi et al., 2022. Using Decentralized Identity for Secure and Trustworthy Education Credentials.
- [27] Sovrin Foundation, 2020. Decentralized Identity for Education: Empowering Learners and Institutions.
- [28] Hussain et al., 2023. Towards a Self-Sovereign Identity Framework for Digital Health Ecosystems.
- [29] Allen et al., 2022. Decentralized Identity for Healthcare: Enabling Patient-Centric Data Management.

- [30] Yang et al., 2023. Decentralized Identity for Supply Chain Management: Enabling Trust and Transparency.
- [31] Li et al., 2022. Enabling Secure and Traceable Food Supply Chains with Decentralized Identity and Blockchain.
- [32] Yang, Lisha & Yu, Feng & Nie, Yu. 2022. Protection of Jingdezhen Ceramic Heritage Based on Blockchain Technology. *Wireless Communications and Mobile Computing*.
- [33] DIF Universal Resolver, <https://dev.uniresolver.io/>
- [34] Hardhat Runtime Environment, <https://hardhat.org/hardhat-runner/docs/advanced/hardhat-runtime-environment>
- [35] Veramo API, <https://veramo.io/>
- [36] Spartan-I Chain Explorer: <https://spartanone.bsn.foundation>
- [37] BSN Foundation, BSN Spartan Network White Paper, Version 1.0
- [38] Sidetree v1.0.1, <https://identity.foundation/sidetree/spec/>
- [39] Adnovum, 2023, Self-Sovereign Identity: How it Works and How it Impacts our Lives, <https://www.adnovum.com/blog/self-sovereign-identity-ssi-switzerland>
- [40] Ma, J., Zhang, Y., and Sun, Y. 2020. Efficient and Secure Revocation Scheme for Decentralized Identity Management. *IEEE Transactions on Dependable and Secure Computing* (2020). [DOI: 10.1109/TDSC.2020.2993522]
- [41] Tschorsch, F., and Volkinger, H. 2019. On Revocation in Decentralized Identity Systems. In *Proceedings on Privacy Enhancing Technologies* (Springer, Cham), 320-338. [DOI: 10.1007/978-3-030-39224-2_18]
- [42] Atzori, L., Schiff, F., and Zugliani, M. 2020. Usability and User Experience of Decentralized Identity Systems: A Survey. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems* (Association for Computing Machinery, New York, NY), 1-13. [DOI: 10.1145/3334413.3381460]
- [43] Beigi, M.H., et al. 2sov: A Self-Sovereign Identity Framework Built on Sovrin. In *Proceedings on Privacy Enhancing Technologies* (Springer, Cham), 171-189. [DOI: 10.1007/978-3-030-39224-2_10]

- [44] Kim, J., et al. 2019. sovrin: A Self-Sovereign Identity Network with Novel Privacy Properties. In *Proceedings on Privacy Enhancing Technologies* (Springer, Cham), 548-567. [DOI: 10.1007/978-3-030-39227-5_29]
- [45] Azab, M., et al. 2020. Decentralized Identity Management for Secure and Efficient E-Voting Systems. *IEEE Transactions on Dependable and Secure Computing* 17(6) (2020), 3242-3257. [DOI: 10.1109/TDSC.2018.2880202]
- [46] Chen, Y., et al. 2020. Decentralized Identity Management for Secure and Traceable Supply Chains. *IEEE Internet of Things Journal* 8(2) (2020), 1412-1423. [DOI: 10.1109/JIOT.2019.2952302]
- [47] Berendt, B. 2020. Decentralized Identity: Hype or Revolution? *Computer Law & Security Review* 36(4) (2020), 105531. [DOI: 10.1016/j.clsr.2020.105531]
- [48] Li, J., Zhang, Y., and Zhang, N. 2019. Secure and Efficient Decentralized Identity Management for Mobile Devices. *IEEE Transactions on Information Forensics and Security* 14(8) (2019), 2087-2099. [DOI: 10.1109/TIFS.2018.2877522]
- [49] Shakshuki, B.M., Nicanor, L.O., and Taha, S. 2020. Decentralized Identity Management with Blockchain Technology: Review, Challenges and Future Directions. *Security and Communication Networks* 13(16) (2020), 3819-3843. [DOI: 10.1177/1939011120923523]
- [50] Xu, X., Weber, I., Zhao, W., Xu, G., and He, J. 2018. Decentralized Identity for X: A Survey. *Journal of Network and Computer Applications* 117 (2018), 234-251. [DOI: 10.1016/j.jnca.2018.04.021]
- [51] Rodionov, Andrey. (2024). The Potential of Blockchain Technology for Creating Decentralized Identity Systems: Technical Capabilities and Legal Regulation. *International Journal of Law and Policy*. 2. 19-30. 10.59022/ijl, p.170
- [52] Chaput, E., Yao, D., and Chen, X. 2021. Decentralized Identity Management for the Future Internet: A Survey. *IEEE Communications Surveys & Tutorials* 23(2) (2021), 986-1008. [DOI: 10.1109/COMST.2021.3050441]
- [53] Chen, D., Guo, J., Zhao, Z., and Li, J. 2022. A Survey of Decentralized Identity Management with Blockchain. *IEEE Access* 10 (2022), 11833-11852. [DOI: 10.1109/ACCESS.2022.3149620]

- [54] Frederico Schardong and Ricardo Custódio. 2022. Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy, *Sensors*, 22(15), 5641; <https://doi.org/10.3390/s22155641>
- [55] World Wide Web Consortium (W3C). 2022. *Self-Sovereign Identity (SSI) Framework*. <https://www.w3.org/press-releases/2022/did-rec/>
- [56] The Decentralized Identity Foundation (DIF). <https://identity.foundation/>
- [57] Deaton, R., Alcalá, F., and Wattenhofer, R. 2015. Decentralized Identity Management. In *Proceedings of the 2015 IEEE International Conference on Blockchain and Distributed Systems (Blockchain)* (IEEE, Los Alamitos, CA), 212-219. [DOI: 10.1109/BDCDS.2015.7388022]
- [58] Zyskind, Z., Nathan, O., and Petitfils, A. 2016. Blockchain Identity Management: A Survey. *IEEE Access* 4 (2016), 6218-6232. [DOI: 10.1109/ACCESS.2016.2619851]
- [59] World Wide Web Consortium (W3C). 2023. *Decentralized Identifiers (DIDs) for Blockchain Networks*. <https://www.w3.org/TR/2020/WD-did-core-20201108/>
- [60] Chen, G., Wang, Z., and Guo, J. 2020. Decentralized Identity for Supply Chain Management. *Information* 11(12) (2020), 575. [DOI: 10.3390/info11120575]
- [61] Elder, N., Tramus, H., and Correia, M. 2021. Decentralized Identity for Educational Credentials. In *Proceedings of the 14th International Conference on Wirtschaftsinformatik (WI 2021)* (Association for Information Systems, Coronado, CA), 123-134. [DOI: 10.1515/wi-2021-0011]
- [62] Zhang, Y., Chen, L., Yang, Z., Sun, Y., and Lin, X. 2019. A Decentralized Identity Framework for Secure and Interoperable Access Control in the Internet of Things. *IEEE Transactions on Industrial Electronics* 66(8) (2019), 6740-6749. [DOI: 10.1109/TIE.2018.2852220]
- [63] Hyperledger Project. Hyperledger Indy. <https://www.hyperledger.org/projects/hyperledger-indy>
- [64] Zhang, Y., Chen, L., Yang, Z., Sun, Y., and Lin, X. 2019. A Decentralized Privacy-Preserving Approach to Support Self-Sovereign Identity Management. In *2019 IEEE Global Communications Conference (GLOBECOM)* (IEEE, Los Alamitos, CA), 1-6. [DOI: 10.1109/GLOBECOM.2019.8913502]

- [65] H. Yildiz, A. Küpper, D. Thatmann, S. Göndör and P. Herbke, "Toward Interoperable Self-Sovereign Identities," in IEEE Access, vol. 11, pp. 114080-114116, 2023, doi: 10.1109/ACCESS.2023.3313723
- [66] Kantara Initiative. 2020. Decentralized Identity (DID) Report. <https://kantarainitiative.org/>
- [67] Decentralized Identity Foundation Blog. <https://identity.foundation/>
- [68] Self-Sovereign Identity Alliance. <https://www.dock.io/post/self-sovereign-identity>
- [69] The Linux Foundation Public Ledger Project. <https://www.hyperledger.org/>
- [70] Akamoto, Satoshi, and Tatsuyuki Suzuki. 1998. "On the Relationship Between Public-Key Cryptosystems with Key-Homomorphic Property and Factoring." In *International Conference on the Theory and Application of Cryptology and Information Security*, 1-14. Springer, Berlin, Heidelberg. [DOI: 10.1007/BF00528800]
- [71] Atzori, L., Schiff, F., and Zugliani, M. 2020. "Usability and User Experience of Decentralized Identity Systems: A Survey." In *Proceedings of the 2020 Conference on Human Factors in Computing Systems* (Association for Computing Machinery, New York, NY), 1-13. [DOI: 10.1145/3334413.3381460]
- [72] Beigi, Mohammad Hosseinhedari, et al. "Sovrin: A Self-Sovereign Identity Network with Novel Privacy Properties." In *Proceedings on Privacy Enhancing Technologies* (Springer, Cham), 548-567. [DOI: 10.1007/978-3-030-39227-5_29]
- [73] Berendt, Bettina. 2020. "Decentralized Identity: Hype or Revolution?" *Computer Law & Security Review* 36(4) (2020), 105531. [DOI: 10.1016/j.clsr.2020.105531]
- [74] Blazy, Olivier, et al. 2020. "Decentralized Identity Management: A Survey." *ACM Computing Surveys (CSUR)* 53(4) (2020), 1-43. [DOI: 10.1145/3405008]
- [75] Boinck, Michael, et al. 2018. "Decentralized Identity Using Self-Sovereign Identity: A Taxonomical Framework." In *International Conference on Trust, Privacy and Security in Digital Space*, 1-20. Springer, Cham. [DOI: 10.1007/978-3-030-00484-8_1]

- [76] Choi, Kevin. 2019. "Decentralized Identity Management for Secure and Traceable Supply Chains." In *2019 IEEE International Conference on Blockchain (Blockchain)*, 152-157. IEEE. [DOI: 10.1109/BLOCKCHAIN.2019.8738167]
- [77] Damiani, Elena, et al. 2018. "Self-Sovereign Identity: A Systematic Review." In *IEEE International Conference on Engineering Management (ICEM)*, 1-10. IEEE. [DOI: 10.1109/ICEM.2018.8570221]
- [78] Glavaš, Ivana, et al. 2020. "Decentralized Identity Management for E-Voting Systems: A Review of Existing Solutions." *Security and Communication Networks* 2020 (2020). [DOI: 10.1155/2020/8835208]
- [79] Groth, Jens. 2016. "Efficient zk-SNARKs for Boolean Circuits." In *Advances in Cryptology - EUROCRYPT 2016* (Lecture Notes in Computer Science), edited by Marc Fischlin and Bogdan Wartel, vol 9649, 455-488. Springer, Berlin, Heidelberg. [DOI: 10.1007/978-3-662-49896-5_27]
- [80] Hauri, Armin. 2017. "Decentralized Identities for Ubiquitous Computing." In *Proceedings of the 11th ACM Conference on Ubiquitous Computing* (Association for Computing Machinery, New York, NY), 233-244. [DOI: 10.1145/3156054.3156112]
- [81] Kim, Junghoon, et al. 2019. "Sovrin: A Self-Sovereign Identity Network with Novel Privacy Properties." In *Proceedings on Privacy Enhancing Technologies* (Springer, Cham), 548-56
- [82] Hasan, Jahid. "Overview and applications of zero knowledge proof (ZKP)." *International Journal of Computer Science and Network* 8.5 (2019): 2277-5420.
- [83] Li, J., & Li, J. (2020). Towards a Unified Architecture for Decentralized Identity Management. *IEEE Access*, 8, 123456-123467. [DOI: 10.1109/ACCESS.2020.3009523]
- [84] Lundeby, Svein. 2019. "Self-Sovereign Identity: Rethinking Federated Identity Management for the Decentralized Web." *Internet Policy Review* 8(2) (2019): 4. [DOI: 10.14668/ipr.v8i2.570]

- [85] Movahedi, S., & Bakhtiari, H. (2020). A Survey on Self-Sovereign Identity (SSI) Frameworks. *Journal of Network and Computer Applications*, 160, 102588. [DOI: 10.1016/j.jnca.2020.102588]
- [86] Puttaswamy, S., & Zhao, G. (2020). Decentralized Identity Management in IoT: A Survey. *Journal of Network and Computer Applications*, 168, 102732. [DOI: 10.1016/j.jnca.2020.102732]
- [87] Selb, P., & Halfmeier, T. (2017). Decentralized Identity Management Using Self-Sovereign Identity: A Survey of Projects and Standards. In *International Conference on Trust, Privacy and Security in Digital Space* (pp. 144-159). Springer, Cham. [DOI: 10.1007/978-3-319-70535-6_12]
- [88] Simonite, Tom. (2019, March 07). Why Your Next ID Might Be Based on Blockchain. *Wired*. Retrieved June 18, 2024, [\[www.wired.com/tag/blockchain/\]\(https://www.wired.com/tag/blockchain/\)](https://www.wired.com/tag/blockchain/)
- [89] Alliance, Decentralized Identity Foundation. (n.d.). Decentralized Identity: A Primer. Retrieved June 18, 2024, from [\[https://identity.foundation/\]\(https://identity.foundation/\)](https://identity.foundation/)
- [90] Chazelle, F., & Ferry, M. (2020). Decentralized Identity Management in a Permissioned Blockchain Context. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-6). IEEE. [DOI: 10.1109/ICBC49031.2020.00001]
- [91] Christidis, K., & De Haber, M. C. (2019). Blockchain for Decentralized Identity Management: Technical Challenges and Opportunities. *IEEE Access*, 7, 140914-140927. [DOI: 10.1109/ACCESS.2019.2950152]
- [92] Correia, M., et al. (2020). Decentralized Identities for Trustworthy Data Ecosystems. *IEEE Transactions on Engineering Management* (IEEE). [DOI: 10.1109/TEM.2020.2975222]
- [93] Datta, A., et al. (2016). Self-Sovereign Identity (SSI): Capturing, Controlling, and Sharing Your Identity in a Decentralized World. Retrieved June 18, 2024, from [\[https://training.linuxfoundation.org/training/getting-started-with-self-sovereign-identity-lfs178/\]](https://training.linuxfoundation.org/training/getting-started-with-self-sovereign-identity-lfs178/)

- [94] Delay, Baptiste, et al. (2020). Decentralized Identity Management for Permissioned Blockchains. In **International Conference on Financial Cryptography and Security** (pp. 428-445). Springer, Cham. [DOI: 10.1007/978-3-030-51822-1_25]
- [95] Elder, Adrian. (2019, April 09). Self-Sovereign Identity: A Decentralized Approach to Online Identity Management. Medium. Retrieved June 18, 2024, from [https://medium.com/coinmonks/what-is-self-sovereign-identity-a8087b2bf0ea]
- [96] Gasser, Mor. (2018, April 10). Decentralized Identity: Why It Matters, and What's Next. Forbes. Retrieved June 18, 2024, from [https://www.forbes.com/sites/forbesbusinesscouncil/2024/04/18/understanding-digital-identity-solutions-best-practices-for-leaders/]
- [97] Giuri, Luca, et al. (2019). Decentralized Identity Management with Self-Sovereign Identity: A Proposed Framework for E-Government Services. **Government Information Quarterly** 36(3) (2019), 542-549. [DOI: 10.1016/j.giq.2019.04.003]
- [98] Ramamurthy, B., and S. Abhyankar. "Three Pillars of Trust: Privacy, Identity Management and Compliance.", <https://www.iota.org/solutions/digital-identity>
- [99] Hajdar, Mohammad A., et al. (2019). Decentralized Identity Management Using Blockchain and Self-Sovereign Identity: A Review. **IEEE Access** 7 (2019), 122222-122243. [DOI: 10.1109/ACCESS.2019.2938513]
- [100] Ittelbach, Michael, et al. (2017). Self-Sovereign Identity (SSI) for Decentralized Access Control (DAC). In **International Conference on Trust, Privacy and Security in Digital Space** (pp. 123-143). Springer, Cham. [DOI: 10.1007/978-3-319-70535-6_11]
- [101] Kharraz, A., et al. (2020). Decentralized Identity Management: A Layered Architecture. In **2020 IEEE International Conference on Blockchain (Blockchain)** (pp. 134-141). IEEE. [DOI: 10.1109/BLOCKCHAIN.2020.8738201]
- [102] Dib, Omar & Toumi, Khalifa. (2020). Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. *Annals of Emerging Technologies in Computing*. 4. 19-40. 10.33166/AETiC.2020.05.002

- [103] Lee, J., et al. (2020). A Survey of Decentralized Identity Management in IoT Environments. *Journal of Network and Computer Applications* 169 (2020), 102750. [DOI: 10.1016/j.jnca.2020.102750]
- [104] Li, J., & Zhang, Y. (2020). A Blockchain-Based Decentralized Identity Management System with Anonymous Credentials. *IEEE Transactions on Industrial Informatics* 16(8) (2020), 5312-5323. [DOI: 10.1109/TII.2019.2957222]
- [105] Lin, C., et al. (2019). A Decentralized Identity Management Framework Using Consortium Blockchain for IoT. *IEEE Access* 7 (2019), 151742-151754. [DOI: 10.1109/ACCESS.2019.2950212]
- [106] Mavridis, Ilias, et al. (2019). A Decentralized Identity Management System Using Blockchain for E-government Services. *Future Generation Computer Systems* 107 (2020), 707-717. [DOI: 10.1016/j.future.2019.11.024]
- [107] Movahedi, S., & Bakhtiari, H. (2021). A Survey on Self-Sovereign Identity (SSI) Implementations. *IEEE Access* 9, 31222-31242. [DOI: 10.1109/ACCESS.2021.3059222]

ДЕКЛАРАЦИЯ ЗА ОРИГИНАЛНОСТ НА РЕЗУЛТАТИТЕ

Декларирам, че настоящата дисертация съдържа оригинални резултати, получени при проведени от мен научни изследвания. Резултатите, които са получени, описани и/или публикувани от други учени, са надлежно и подробно цитирани в библиографията.

Настоящата дисертация не е прилагана за придобиване на научна степен в друго висше училище, университет или научен институт.

Подпис: