YourD Research

Klaytn Dev Ambassador Research

***Disclaimer**

본 아티클은 클레이튼의 데브 엠베서더 리서치 프로그램의 활동 결과물로, 데브 엠베서더가 작성했습니다.

아티클 내 소개되는 프로젝트들과 아티클의 저작권 및 소유는 저자로 참여한 엠버서더와, 참조한 프로젝트 또는 기관들에게 있습니다. 본 아티클의은 블록체인 프로젝트의 기술 지식을 공유하는 데 기여하는 데 그 목적이 있으며, 특정 프로젝트에 대한 투자 추천이나 조언이 아님을 알려드립니다. 본문에 대한 수정 제안은 아래의 저자 /검토자 연락처로 의견 주시면, 검토후 반영 하도록 하겠습니다.

***저자**

- 염재경 (email : yeomjaegyeong@gmail.com) | klaytn Dev ambassador
- 차영훈 (email : yhc125g@gmail.com) | Klaytn Dev ambassador
- 김지황 (email 4uphwang@gmail.com:) | Klaytn Dev ambassador

***검토 및 수정**

- iron.cho (iron.cho@klaytn.foundation) | Klaytn Foundation

들어가며

최근 블록체인에서의 Web3.0의 ID라는 연구 주제가 하나의 트렌드로 제시 되고 있습니다. 과거 DID의 연구가 현재의 Web 3.0의 ID에서의 하나의 식별 ID체계로 사용이 되며 퍼블릭 블록체인에서 사용자들의 데이터의 소유권을 지키며 이를 활용하는 여러 관련 서비스들이 제시되고 있습니다. 이러한 Web3.0의 ID의 연구주제를 가지고, 데브엠버서들이 YourD라는 프로젝트를 연구 개발하였습니다. YourD 프로젝트는 Web3.0 ID를 실현 하기 위해서 DID기반의 데이터 소유권 서비스을 목표로한 오프소스 기반으로 연구 개발한 프로젝트이며, 이번 하반기에 클레이튼 위에서 서비스 오픈을 위해 준비중에 있습니다. YourD는 Web3.0에서 DID를 통해 사용자가 스스로 데이터의 소유권을 가지며, 이러한 데이터들을 활용 할 수 있도록 하는 zkp기반의 광고 프로토콜을 개발했습니다. 또한 기존의 web3.0의 지갑의 편의성을 제공하기 위하여 DID기반의 간편 로그인과 Digital Data Wallet을 개발했습니다. 본 아티클에서는 YourD의 프로젝트에서 연구개발한 내용들을 소개하고 지식들을 공유하고자 합니다. 이를 위해 아티클의 1장에서는 YourD를 이해하기 위한 배경지식인 DID에 대해서 설명을 하고, 2 장에서는 YourD에 대한 소개, 3장에서는 YourD의 주요 기능들을 소개, 4장 결론에서는 향후 로드맵을 기술하고, 5장 부록에서는 W3C 표준에 등록된 YourD에 대해서 설명합니다.

목차

1. YourD 프로젝트 배경 지식 : DID
    1.1. DID는 무엇인가?
    1.2. DID의 주요 기술 구성
2. YourD 프로젝트 소개
    2.1. YourD 프로젝트
    2.2. YourD의 컴포넌트
3. YourD는 어떻게 동작하는가 ?
    3.1. YourD : DID
    3.2. YourD 간편 QR 로그인
    3.3. Digital Data Wallet
    3.4. YourD Login Saas
    3.5. Web3.0 광고 서비스 : D-Ad
4. 결론
    4.1. YourD 기대효과 : 클레이튼 에코시스템 측면
    4.2. YourD 로드맵
5. 부록 - YourD W3C 표준 내용
6. 저자 소개

1. YourD 프로젝트 배경 지식 : DID

1.1 DID는 무엇인가 ?

우리는 일상에서 개인이나 제품을 식별하기 위해 아이덴티티(ID)를 사용합니다. 예를 들어, 사람은 여권이나 운전 면허증으로, 제품은 일련번호 또는 바코드로, 웹페이지는 URL로 식별됩니다. 온라인 환경에서도 이메일 주소나 소셜 미디어 ID 등으로 사용자를 식별하고 통신합니다. 이러한 ID를 통해 우리는 온라인 소유권을 주장할수 있습니다. 예를 들어 게임에서는 ID 인증 후 해당 ID의 자산을 이용할 수 있습니다. 하지만, 이런 ID는 외부 기관에 의해 발급, 관리되므로 완전한 소유권을 주장하기 어렵습니다. 사용자의 ID가 사라질 수도 있고, 개인 정보가 노출될 수도 있으며, ID의 자원이 기관에 의해 활용될 수 있기 때문입니다. 결국, 현재의 시스템에서는 개인이 ID에 대한 완전한 소유권을 가진다고 볼 수 없습니다.

이렇듯 ID에 대한 소유권을 플랫폼 기업들이 갖고 이를 관리하면서 사용자들을 유입하고 편리한 서비스 제공을 통해 성장했습니다. 그러나 이러한 플랫폼의 거대화로 인해 생기는 문제들이 존재하는 것도 사실입니다. 그 예로, 페이스북은 2016년 미국 대선을 앞두고 영국 정치 컨설팅업체 케임브리지 애널리티카가 정치 광고 목적으로 페이스북 이용자 8천여만명의 데이터를 불법 수집[1]한 것으로 드러나 논란이 되었고, 2019년에는 페이스북 이용자 4억1900만여명의 개인정보가 유출[2]된 것으로 알려졌다. 구글은 2019년 비밀리에 수백만명의 미국 환자 정보를 수집하고 유튜브 또한 아동 개인정보 불법 수집 협의로 미국 연방거래위원회(FTC)에 벌금을 내기도 하였습니다.[3] 그리고 가장 최근인 2023년 테슬라 내부고발자의 폭로로 고객 개인 정보 및 전현직 직원의 은행계좌와 같은 민감한 정보까지 유출하는 사건[4]이 있습니다.

더욱이 이 중앙화된 플랫폼에서 사용자들이 자신의 데이터에 대한 권한을 잃고 프라이버시가 침해되는 문제는 빅데이터 기반으로 학습한 AI의 등장으로 점점 더 심각해지고 있습니다. 대표적으로 ChatGPT가 학습에 사용되는 자료에는 문자메시지, SNS 게시물, 이메일 등 개인정보가 포함될 수 있기에 학습

[1] Inside the Facebook Cambridge Analytica Data Scandal : Link
[2] Unsecured Facebook Databases Leak Data Of 419 Million Users : Link
[3] Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law : Link
[4] CLEAN TRANSPORTTesla 100 GB Data Bomb Turned Over To Handelsblatt : Link

과정에서 개인정보 침해가 발생할 수 있습니다. 실제로 JP모건체이스, 골드만삭스 등 일부 해외 기업들은 ChatGPT 사용을 제한하는 사내 규정을 발표하면서 AI와 관련한 개인정보 보호 규제의 필요성이 높아지고 있습니다.[5] 이러한 배경 속에서 SSI(Self-Sovereign Identity, 자기주권 신원증명)의 실현은 선택이 아닌 필수가 되어가고 있습니다. 그리고 DID(Decentralized Identifier, 탈중앙화 신원증명)는 이러한 문제에 대한 대안으로 떠오르고 있습니다. 아래의 그림1은 기존의 인증 체계인 SSO(Single Sign-On)와 DID를 활용한 SSI 모델을 비교한 그림입니다. SSO는 기존 Naver, Google,Kakao와 같이 플랫폼 계정으로 다른 여러 사이트 로그인을 진행하는 방식으로 플랫폼 서비스에 개인정보를 관리하는 것이 특징입니다. 이는 지금까지 새로운 서비스를 이용할 사용자에게 회원가입 정보를 따로 기입하지 않아도 간편하게 이용할 수 있게 만들었지만 개인 정보 이용과 유출 문제의 위험성이 있습니다.

<그림 1> 자기주권 신원 모델 개요, 이미지 출처 : URACLE https://uracle.blog/2020/09/11/did/

DID는 탈중앙화된 형태의 신원 인증에 대한 새로운 방식으로 개인 스스로 타 기관없이 스스로 신원 인증을 가능하게 한다는 점에서 주목 받기 시작했습니다. 즉, 중앙 집중화된 공급자 중심의 인증 시장을 사용자 중심으로 바꾸는 새로운 패러다임입니다. 데이터 소유권에 대한 인식을 드러내고자 하는 Web 3.0

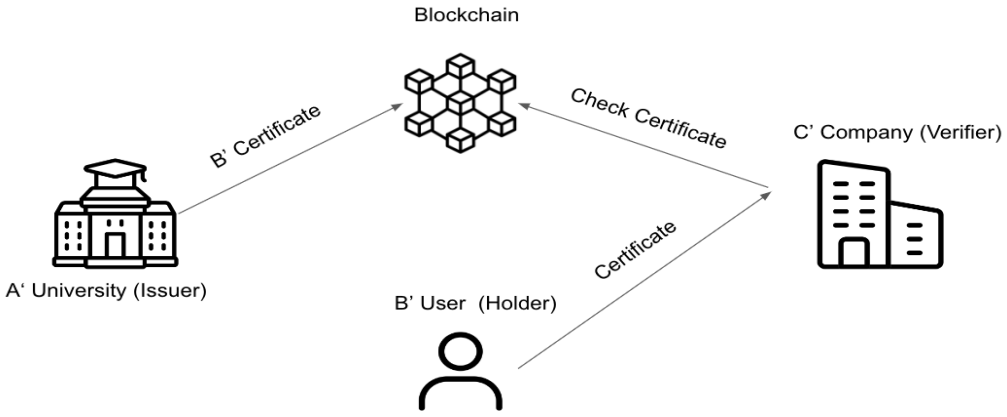
[5]Don't tell anything to a chatbot you want to keep private : Link

시대에는 사용자 중심의 데이터 경제가 확대될 것이며, 사용자가 특정 플랫폼이나 서비스에 종속되지않고 정보를 자유롭게 교환하면 개인 정보를 스스로 관리할 수 있습니다.

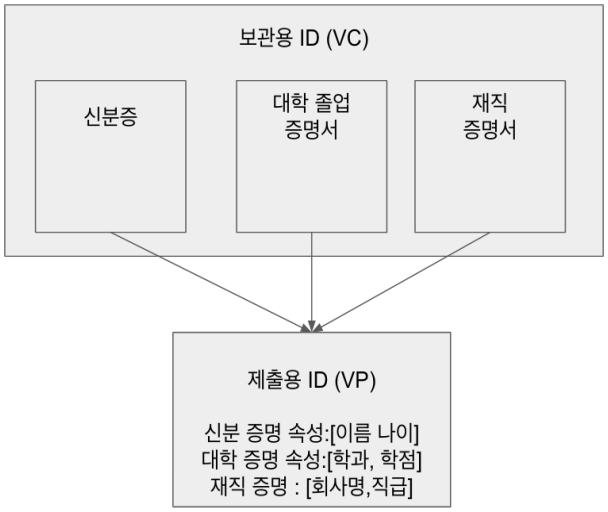
DID를 활용한 SSI는 사용자의 모바일 기기에서 사용자 자신의 개인 정보를 관리하면서 여러 서비스를 이용할 때, 특정 플랫폼 계정이 아닌 자신의 고유한 계정으로 로그인하는 방식입니다. 이는 개인 정보의 통제권을 다시 되찾아옴으로써 데이터 주권을 확보할 수 있습니다.

1.2 DID의 주요 기술 구성

DID를 활용해서 어떻게 SSI를 실현할 수 있는지 졸업증명서를 회사에 제출하는 예시 시나리오를 통해 알아보겠습니다. B라는 사용자는 A대학에서 졸업을 하였고, C라는 회사에게 자신의 A대학의 졸업 증명을 제출을 하는경우를 살펴보겠습니다. 기존 졸업 증명 시스템의 경우 A 대학에서 B 유저에게 졸업증명서를 발급을 하는 형태 (실제로는 다른 신뢰된 발급기관이 있으나, 이해를 위해 A대학에서 발급하는것으로 설명을 합니다) 입니다. 그럼 B 유저는 이를 들고 C 회사에 제출을 하고 난 뒤, C 회사는 받은 졸업 증명서에 대한 진위 여부 확인을 합니다. 이 과정에서 A, C의 국적이 다르다면 공증 기관을 거쳐야하고 같더라도 진위 여부 확인을 위한 절차는 많은 비용과 시간을 요구합니다. 아래의 그림2와 같이 블록체인을 활용한 DID 증명 시스템의 경우 A 대학에서 마찬가지로 B 유저에게 졸업증명서를 발행하지만 이후에 A 대학은 졸업 증명에 필요한 데이터를 블록체인에 등록합니다. B 유저는 졸업 증명서를 C 회사에 제출하고 난 뒤, C 회사는 블록체인에 등록되어 있는 데이터를 조회하여 졸업 증명 여부 확인을 합니다. 이때, A 대학에서 발행한 졸업 증명서는 Verifiable Credential(VC)로, A 대학이라는 Issuer가 발행한 자격증명 문서 입니다. 그리고 B 유저가 제출하는 졸업 증명서는 Verifiable Presentation(VP)로, Holder인 B 유저가 Verifier인 C 회사에게 제출하는 문서입니다.



<그림2> DID를 이용한 발급 시스템 예시



<그림3 VC와 VP와의 관계 예시>

VC는 신분증, 졸업증명서, 재직증명서와 같은 각 기관에서 발급하는 전자증명서라고 라고 생각하면 됩니다. 그리고 VP는 위의 그림3과 같이 사용자가 VC의 속성 중 필요한 부분만 추출하여 VP를 생성한 뒤 제출할 수 있습니다.

DID 증명 시스템에서는 위와 같은 개체들을 식별 하기 위해서 DID라는 식별자를 사용합니다. 즉 A대학, B 사용자, C회사를 식별하기 위한 고유한 DID가 있습니다. 그리고 우리가 기존의 ID/PW를 사용하여 ID에 대한 소유권을 증명하듯이, DID에 대한 소유권을 증명하기 위한 DID Document가 있고, 이 Document에는 해당 DID를 소유하고 있는 인증 수단이 포함되어있습니다. 기존의 증명 시스템의 경우,

A 대학, B 유저, C 회사 라는 이름으로 식별하였다면 DID 증명 시스템에서는 DID라는 식별자를 이용합니다. 그리고 이 DID의 소유권을 증명하기 위해 DID document가 필요합니다. 즉, DID document에는 해당 DID를 소유하고 있다는 인증 수단이 포함되어있습니다.이처럼 DID는 제3자 기관이나 서비스 제공자가 중앙에서 개인의 정보를 통제하는 기존의 신원 증명 방식과는 다르게, 개인이 자신의 정보를 완전히 통제할 수 있게 하는 기술입니다. 중앙화된 ID 시스템에서는 ID, 비밀번호, 개인정보 등이 ID 제공자나 서비스 제공자의 서버에 저장되지만, DID를 통한 탈중앙화된 ID 시스템에서는 개인의 모바일 기기에 저장하여 개인이 정보를 관리 및 제공합니다.

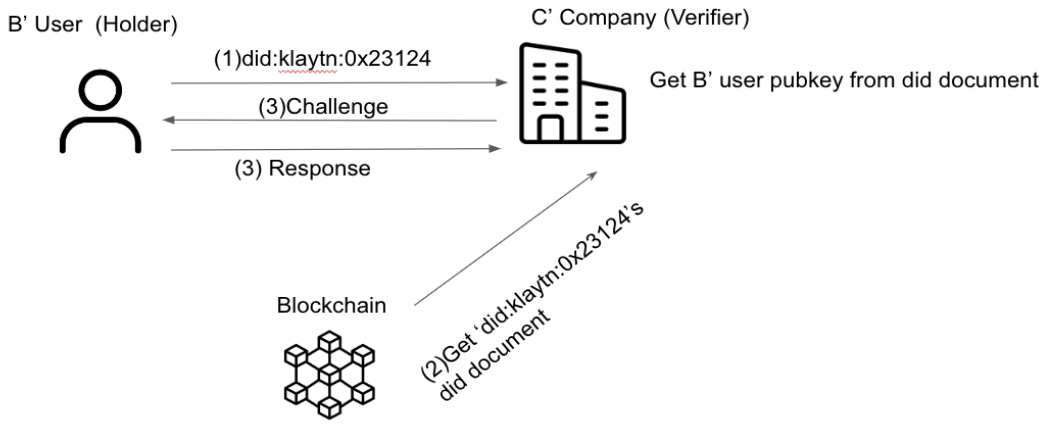
1) DID

<그림4> DID 식별 체계 , 이미지 출처 : W3C DID-CORE https://www.w3.org/TR/did-core

위의 그림 4와 같이, DID는 DID Scheme / DID Method / DID Method-Specific Identifier 3가지 파트로 이루어져 있습니다. DID Scheme는 항상 “did” 라는 문자열로 정의됩니다. DID Method는 DID의 생성, 해석, 관리, 인증 등과 관련된 프로토콜, 알고리즘, 네트워크 등을 나타냅니다. DID Method-Specific Identifier는 DID Method 내에서 사용되는 식별자로 DID 체계와 해당 Method에 따라 고유한 형식과 규칙을 갖습니다. 예시로, did:klaytn:0x1234567890abcdef의 경우, klaytn 블록체인에서 0x1234567890abcdef의 계정 주소를 고유한 식별자로 이용한다는 의미입니다.

2) DID document

C 회사는 B 유저의 확인을 위해 B 유저의 신원을 조회하여 아래의 그림 5와 같이 검증을 하는 과정이 필요합니다. 이 과정은 1) B 유저는 자신의 did를 C회사에게 제출하고 2) C회사는 블록체인에 기록된 B유저의 DID document의 정보를 가지고 가지고 옵니다. 3) 아래 그리고 C회사와 B사용자와 시도-응답 인증(Challenge/Response)를 통해 B유저의 해당 did의 소유권을 증명할수 있게 됩니다.



<그림5> DID 인증 예시

DID document는 해당 DID를 소유하고 있는 사람임을 증명하기 위한 문서입니다. 따라서 Verifier가 DID document를 조회하여 사용자의 DID의 소유권을 확인하는 것입니다. 이를 위해 DID document에는 사용자의 디지털 신원에 대한 정보, 인증 수단인 공개키, 인증 방법, Service Endpoint 등의 속성을 포함하고 있습니다.

EXAMPLE 1: A simple DID document

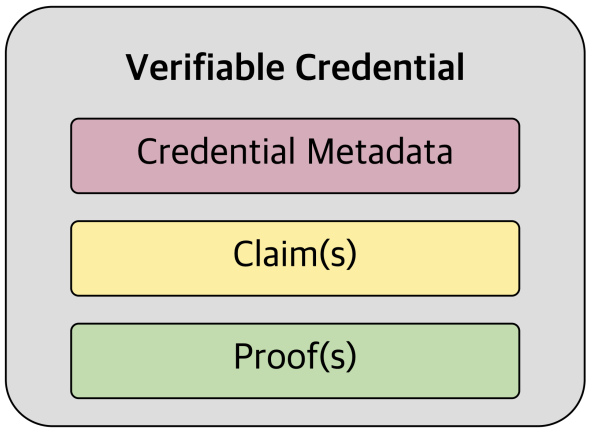
```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

<그림6> DID Document 예시 , 이미지 출처 : W3C https://www.w3.org/TR/did-core/#a-simple-example>

위 <그림6>은 W3C core (표준)문서에 있는 간단한 DID document의 예시입니다. JSON-LD 형식으로 구성되어 있으며 @context, id, authentication 속성을 갖고 있습니다. @contexts는 key-value 구조의 key 값에 대한 데이터를 정의하는 역할을 합니다. 쉽게 말해, 문서를 읽는 방법을 정의하는 것입니다. id는 id를 통해 식별되는 객체의 DID가 들어갑니다. A 대학을 식별하기 위한 document라면 A 대학의 DID가 들어갈 것이고, B 유저를 식별하기 위한 document라면 B 유저의 DID가 들어갑니다. authentication는 해당 did를 인증하기위한 정보들인 id, type, controller, publicKeyMultibase 들의 속성으로 이루어져 있습니다. id 속성에는 did:example:123456789abcdefghi#keys-1라는 값이 들어가있는데 # 뒤에 keys-1은 fragment라는 부분입니다. fragments는 DID document 내에서 특정 섹션 또는 요소를 가리키는데 사용됩니다. 따라서 목적에 맞게 여러 공개키를 관리할 수 있게 됩니다. type 속성에는 공개키의 알고리즘을 명시하여 Verifier가 해당 공개키를 어떤 알고리즘으로 복호화해야하는지 알려줍니다. controller 항목에는 해당 공개키와 쌍을 이루는 비밀키를 가지고 있는 DID가 입력되어있습니다. 위 예시의 경우 DID document의 소유자가 곧 비밀키 소유자임을 명시하고 있습니다. 마지막으로 publicKeyMultibase 항목에는 type 속성에 제시된 알고리즘으로 만들어진 공개키를 명시합니다.

3) Verifiable Credential

A 대학에서 B 유저에게 졸업증명서를 발행해주는데 이러한 신원 증명을 Verifiable Credential(VC)라 부릅니다. 주민등록증과 같은 신분증부터 각종 증명서, 자격증, 대인 관계까지 자신을 표현할 수 있는 모든 종류 의 속성이 VC에 포함될 수 있습니다. VC는 아래의 그림7과 같이 1)Credential Metadata, 2) Claim(s), 3) Proof(s) 속성으로 이루어져 있습니다.



<그림7> VC 속성, 이미지 출처 W3C https://www.w3.org/TR/vc-data-model/#credentials

먼저, 1) Credential Metadata는 VC 발행 주체(Issuer), VC가 명시하고 있는 객체 (Credential subject, Holder), VC 만료 기간 등이 정의되어있습니다. 2) Claim(s)에는 Credential subject의 속성에 대한 정보가 Subject-Property-Value 방식으로 저장됩니다. 예를 들어, B 유저라는 Subject의 대학명이라는 Property와 A 대학이라는 Value로 이루어져있습니다.

마지막으로 3) Proof(s)는 VC에 대한 진위 여부 검증에 필요한 값이 포함되는데 p256, secp256k1, eddsa 등의 다양한 알고리즘을 활용한 암호 기법이 사용될 수 있습니다. Verifier는 Issuer의 Proof를 검증함으로써 해당 VC가 VC에 명시된 Issuer로부터 발행된 것인지 검증할 수 있습니다.

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": [
    "VerifiableCredential",
    "UniversityDegreeCredential"
  ],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:42Z",
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3FXQjecWufY46yg5abdVZsXqLhxhueuSoZgNSARiKBk9czhSePTFehP
8c3PGfb6a22gkfUKods5D2UAUL5n2Brbx"
  }
}
```


<그림8> DID 인증 Documet 예시 체계 VC 속성, 이미지 출처

:https://www.w3.org/TR/vc-data-model/#example-usage-of-the-id-property

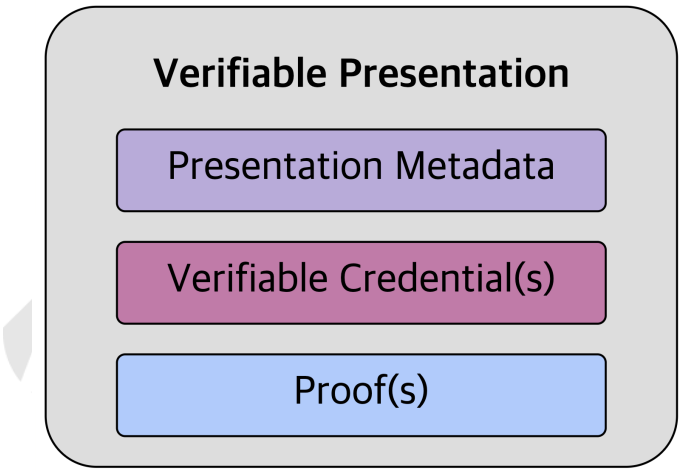
위 <그림8>은 대학 졸업증명서 VC 예시입니다.

id 속성에는 “http://example.edu/credentials/3732”으로 해당 데이터가 VC임을 나타내고 있습니다. issuer 속성에는 발행자를 나타내고 있고 issuanceDate 속성으로 VC 발행 일자를 넣었습니다. id 속성은 누군가를 식별하기 위한 목적이기에 위 예시에서는 issuer 속성에 DID가 아닌 URI 형식으로 담아서 발행 주체가 누구인지를 나타내고 있습니다. Credential Subject 항목의 id 속성에는 VC를 받는 객체 (B사용자) DID인 "did:example:ebfeb1f712ebc6f1c276e12ec21"를 넣고 degree라는 Subject에

type과 name이라는 Property로 구성되어있고 이에 각각 Value가 담겨져 있습니다. 마지막으로 proof 속성에는 “Ed25519Signature2020”의 디지털 서명을 하였다고 명시하면서 proofValue에 디지털 서명값을 나타내고 있습니다.

4) Verifiable Presentation

A 대학에서 받은 졸업증명서 VC를 B 유저는 C 회사에 제출하려고 합니다. 이 때 VC를 직접 제출하지 않고 가공하여 Verifiable Presentation(VP)으로 제출합니다. VP는 아래의 그림9와 같이 1) Presentation Metadata, 2) Verifiable Credential(s), 3) Proof(s) 속성으로 이루어져 있습니다



<그림9> VP 속성 , 이미지 출처 : W3C https://www.w3.org/TR/vc-data-model#presentations

먼저, 1) Presentation Metadata에는 해당 데이터가 VP임을 명시한 type, Terms of Use 등 VP 검증에 참고할 수 있는 데이터가 포함될 수 있습니다. 2) Verifiable Credential(s)에는 이름에 알 수 있듯이 VC가 포함되어 있습니다. VC 내에 존재하는 Claim 중 Verifier가 요구하는 속성을 가진 Claim만 선택합니다. 이를 통해 사용자(Holder)가 자신의 개인정보를 스스로 통제하고 관리할 수 있게 됩니다. VP를 수신한 Verifier는 VC 내에 포함된 3) proof(s) 항목을 통해 VC의 진위 여부를 검증할 수 있습니다. Proof(s)에는 사용자의 서명이 들어갑니다. Verifier는 이 속성을 통해 VP가 현재 통신하고 있는 사용자로부터 제출된 것인지 검증할 수 있습니다. VC와 마찬가지로 다양한 암호 기법이 사용될 수 있습니다.

EXAMPLE 14: Basic structure of a presentation

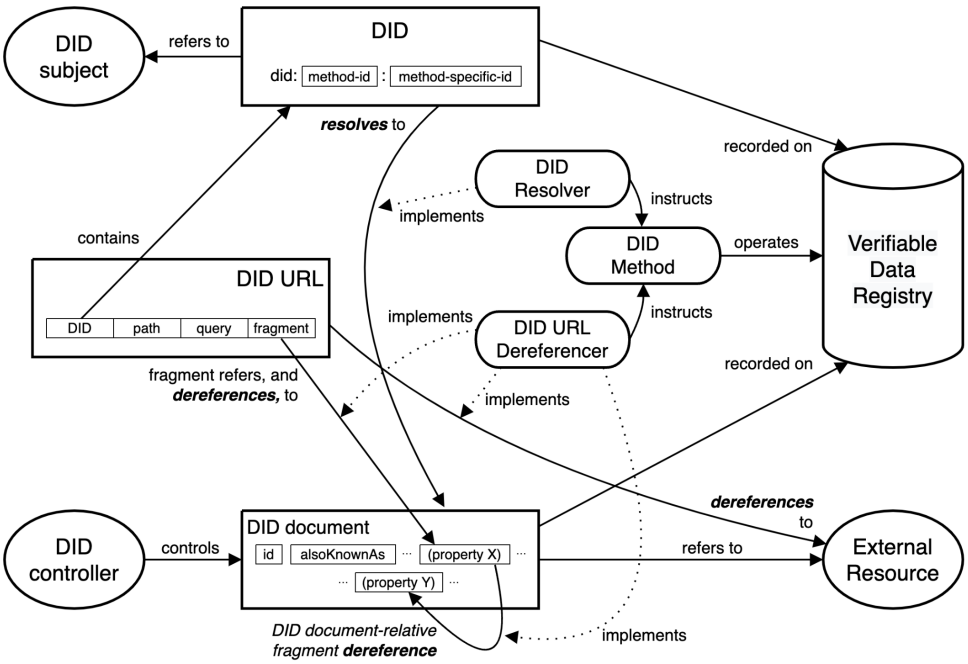
```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5",
  "type": ["VerifiablePresentation", "CredentialManagerPresentation"],
  "verifiableCredential": [{ ... }],
  "proof": [{ ... }]
}
```

<그림10> VP 구조예시, 이미지 출처 W3C https://www.w3.org/TR/vc-data-model/#presentations-0

위 그림은 VP의 기본적인 구조 예시입니다. 대부분의 속성들이 VC와 매우 유사한 구조를 띄고 있습니다. 몇 가지 차이점은 id 속성값에 사용자의 DID가 들어가고, verifiableCredential 속성값에 사용자가 갖고 있는 VC를 취한 데이터를 넣는다는 점입니다.

5) DID Architecture Diagram

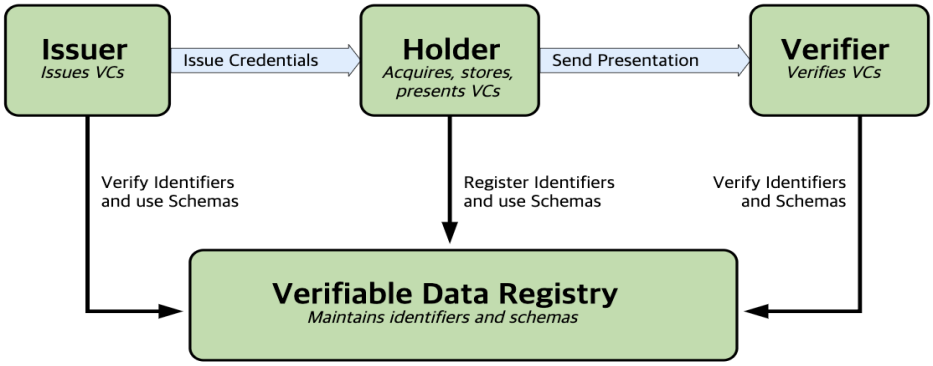
아래 다이어그램을 통해 DID의 Workflow를 세분화해서 추가적인 항목들을 알아보겠습니다.



<그림11> DID 아키텍처 다이어그램, 이미지 출처 : W3C https://www.w3.org/TR/did-core/#bib-did-spec-registries

- DID subject : DID에 의해 식별되고 DID document에 의해 묘사되는 객체입니다. A 대학, B 유저, C 회사처럼 조직, 사람, 그룹이 될 수도 있고 IoT 기기와 같은 물리적인 것이 될 수도 있습니다.
- DID URL : DID 뒤에 추가적으로 path, query, fragment 속성이 포함될 수 있습니다. 이는 DID document에서 특정 속성값을 찾기 위한 경로를 나타냅니다. 이전 document 예시에서 #keys-1이 붙어있는 것을 확인할 수 있었습니다.
- DID controller : DID document를 변경할 수 있는 권한을 가진 객체입니다. 이전 document 예시에서는 B 유저의 did document의 소유주가 B 유저 자신이기에 id속성과 controller 속성에 들어간 did가 동일했습니다. 하지만 여러가지 시나리오를 그려볼 수 있습니다. 부모와 자식의 관계에서는 자식의 document를 부모가 관리하게 할 수 있습니다. 그렇다면 id 속성에는 자식의 did가 들어가지만 controller에는 부모의 did가 들어갈 수 있습니다. W3C core 문서에는 이를 DID delegate라 칭하고 있습니다.
- DID Resolver : DID를 입력으로 받아 DID document를 출력하는 함수입니다. C 회사에서 B 유저의 did를 통해 DID document를 조회한다고 했을 때, DID Resolver를 이용해서 조회하게 됩니다.
- DID URL Dereferencer : DID Resolver가 DID document를 반환한다면 DID URL Dereferencersms DID document의 특정 속성값을 반환하는 함수입니다. 그래서 입력값으로 DID URL을 받아 마치 검색해오는 것입니다.
- Verifiable Data Registry : 이름에서 알 수 있듯이 검증 가능한 데이터 저장소로 블록체인, 분산 저장소 등이 될 수 있습니다. 그 중에 하나인 블록체인은 데이터의 무결성을 보장해줄 수 있다는 점에서 DID 도입에 적합하다고 볼 수 있습니다. 일반적으로 DID, DID document를 블록체인에 저장하여 관리하게 됩니다.

6) DID 전체 흐름 요약



<그림11> DID 전체 흐름 , 이미지 출처 : W3C https://www.w3.org/TR/vc-data-model/

블록체인 기반의 DID증명시스템을, 졸업 증명 시나리오로 흐름을 정리하면 다음과 같습니다.

1. A 대학(Issuer), B 유저(Holder), C 회사(Verifier)의 DID와 DID document를 각각 생성한 후, 이를 블록체인에 기록합니다.
2. B 유저는 A 대학에게 자신의 DID를 제출하면서 졸업증명서를 요청합니다.
3. A 대학은 DID resolver를 활용하여 B 유저의 DID document를 획득합니다.
4. B 유저의 DID document의 authentication 항목을 통해 B 유저의 publicKey를 통해 유저 검증 후, Verifiable Credential 형식의 졸업증명서를 발급합니다.
5. B 유저는 졸업증명서 VC를 포함하여 C 회사에서 요구한 VC 속성들을 조합하여 Verifiable Presentation를 제출합니다. 이 또한 VC를 포함한 디지털 서명을 통해 이루어집니다.
6. C 회사는 B 유저의 DID를 이용해 유저 검증과 졸업증명서 VC의 issuer인 A 대학 또한 동일한 방식으로 검증을 진행합니다.
7. 디지털 서명 검증이 모두 완료되면 C 회사는 받은 VP가 올바른 발행 기관에서 발급된 문서를 올바른 유저가 제출했음을 확인할 수 있습니다.

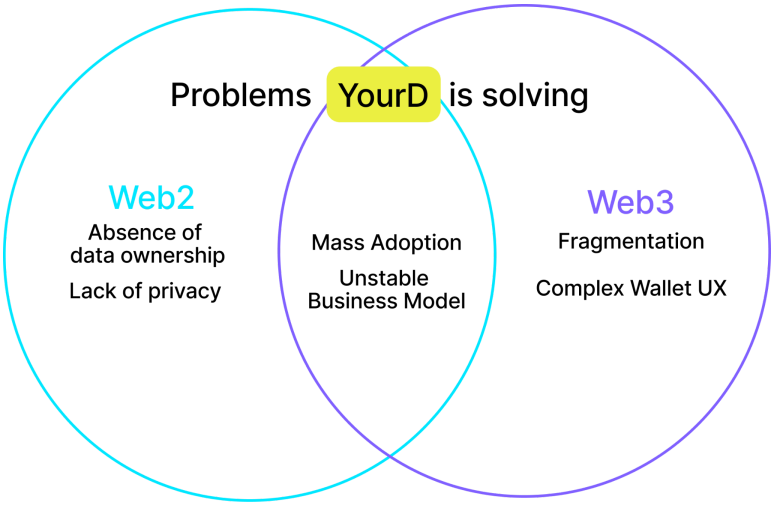
2. YourD 프로젝트 소개

2.1 YourD 프로젝트

‘DID 기반의 데이터 소유권 가치를 실현하기 위한 프로토콜’

Web 3.0의 가치중 하나인 개인 데이터 소유권 문제를 해결하는데, 탈 중앙화된 블록체인 네트워크가 필수적입니다. 하지만 현재의 블록체인 네트워크 구조에서는 사용자가 Web3.0 데이터 소유권을 실현하기에는 어려운 부분이 있습니다. 블록체인 네트워크의 프라이버시 문제와, 디지털 자산들(FT/NFT등)의 한정된 데이터표준과 프로토콜로 인해, 개인의 데이터 소유권을 실현하기에 어려움이 있습니다. 개인의 신원과, 다양한 데이터의 소유권 증명을 위해서는 프라이버시와 데이터들을 표현하는 데이터의 구조와 프로토콜들의 설계가 필요합니다. 또한 현재의 Web3.0의 지갑(Wallet)을 통한 사용자의 증명은 기존 ID체계에 익숙한 Web2.0 사용자들에게 어려움이 있습니다. Web3.0의 데이터 소유권을 실현하기 위해서 블록체인 네트워크 환경에서 데이터 표준과 프로토콜이 필요로 하며, 사용자에게 편의성을 제공할수 있어야 합니다. 이러한 문제를 해결 하였을때, Web3.0과 블록체인은 사용자에게 실질적인 서비스와 가치를 제공할 수 있습니다.

이러한 배경으로 YourD는 web3.0의 개인의 데이터 소유권 가치를 실현 시키기 위한 새로운 ID 서비스 입니다. YourD의 서비스 목표는 블록체인의 탈중앙화된 네트워크에서, 1) 데이터 주권이 사용자에게 주어지며, 2) 이 데이터들이 가치있게 활용 될 수 있도록 하게 하며, 3) Web3.0 Identity 사용을 사용자 중심의 편의성을 제공하는것 입니다.



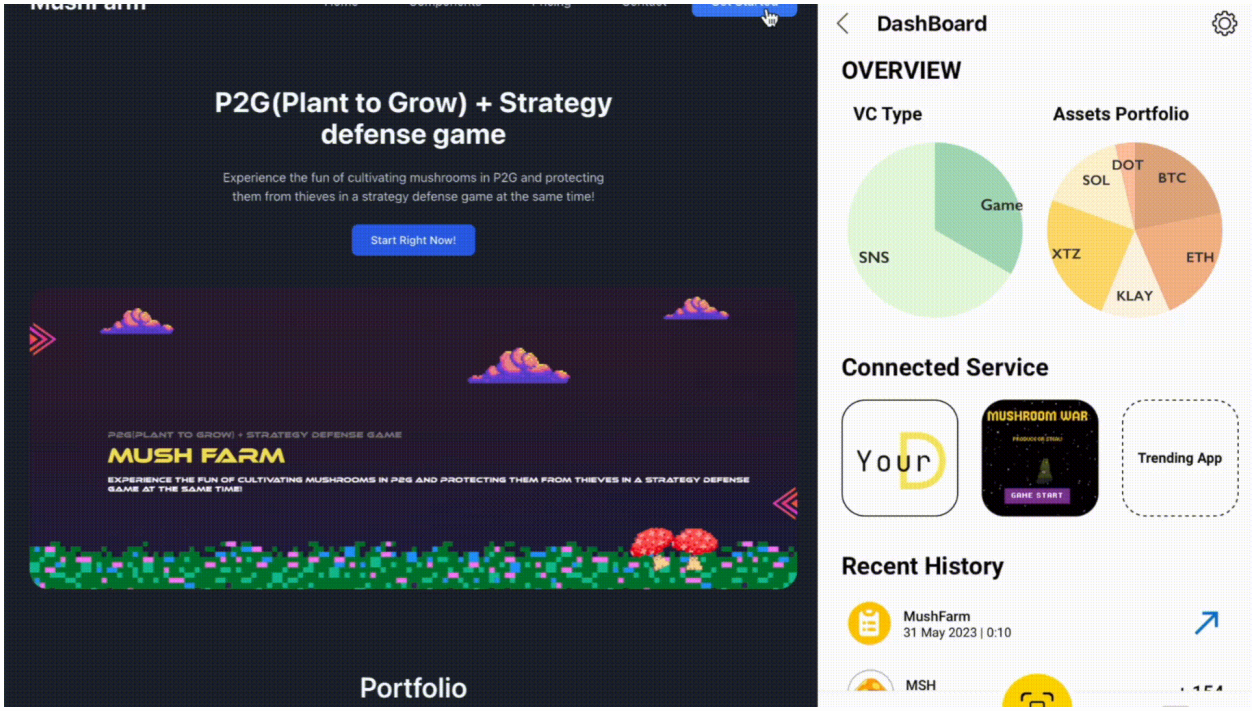
<그림12> YourD 프로젝트의 목표

YourD는 위의 그림 12와 같이 문제들을 해결하기 위해 1) DID의 구현을 통해 사용자의 데이터 소유권과 프라이버시 문제를 해결하고 2) 사용자들의 데이터를 가치있게 활용할 수 있는 광고 프로토콜을 지원 하고 3) 기존 Web3.0 Identity의 어려운 사용을 간편 로그인 Wallet으로 해결합니다. 사용자는 YourD의 디지털 데이터 지갑(Digital Data Wallet)을 통해 자신의 Identity와 데이터의 소유권을 증명하고 Web3.0의 자산들인 Coin,FT/NFT 를 관리할 수 있게 됩니다.

2.2 YourD의 컴포넌트

YourD 서비스의 기술사용자는 YourD의 모바일 클라이언트를 통해 DID생성과 관리, Web 3.0의 디지털 자산들을 관리 할 수 있습니다. 사용자의 DID와 신원인증 관리 정보, 메타 데이터들, 디지털 자산들은 퍼블릭 블록체인인 클레이튼에 기록되며 관리 됩니다. 기존의 사용자들은 Web2.0의 친숙한 모바일 클라이언트의 로그인 방식으로 YourD를 사용할 수 있습니다. YourD는 사용자의 데이터를 활용하기 위하여 광고 프로토콜을 지원하며, 이는 사용자가 직접 자신의 데이터를 판매할 수 있으며, 데이터가 필요한 회사나 서비스에게 제공 할수 있습니다. YourD의 자세한 기술 컴포넌트는 다음과 같습니다.

1) DID 간편 QR 회원가입과 로그인



<그림13> YourD 간편 QR 로그인

YourD는 사용자들에게 편리한 로그인을 제공하기 위해 DID QR 코드 로그인을 지원합니다. QR 코드를 활용하여 간편한 로그인 프로세스를 통해 친숙한 Web2 경험을 선사하고 Web 3.0 및 블록체인 기반 서비스에 보다 쉽게 액세스할 수 있습니다. YourD 간편 로그인 SaaS 서비스에 VC Schema를 등록하여 QR 데이터로 활용할 수 있게 합니다. 이는 유저가 해당 QR을 스캔하여 VC Schema를 확인하고, 유저의 YouD 앱에서 해당 서비스 VC 유무에 따라 로그인 또는 회원가입 절차를 진행합니다 . 회원가입 및 로그인하는 과정에서 지문이나 Face ID를 통해 오직 유저 자신만이 서비스에 빠르게 접근할 수 있도록 합니다.

2) YourD 로그인&데이터 지원

YourD 간편 로그인을 이용하게 되는 서드 파티 서비스들은 YourD가 제공하는 Javascript SDK를 활용해서 로그인 기능을 구현할 수 있습니다. 뿐만 아니라 YourD 간편 로그인 SaaS 서비스에 등록하여

유저 데이터 분석 자료를 받을 수 있습니다. YourD가 제공하는 API를 통해 서비스 전용 VC Schema를 커스텀하고 유저에게 회사 서비스 VC를 발급할 수 있습니다. 그런 다음 유저는 받은 VC를 활용하여 VP를 생성하고 인증 프로세스를 수행합니다. VP 인증이 완료되면 유저는 해당 서비스를 이용할 수 있습니다. 이 SDK를 사용하여 개발된 Web3 서비스는 VC 발급 및 VP 검증을 포함한 인증 프로세스를 통해 로그인이 가능하므로 보다 안전하고 유연한 디지털 ID 관리가 가능합니다.

3) Digital Data Wallet

분산화되어있는 블록체인에 맞게 많은 종류의 Wallet도 생겨났습니다. 이는 유저 입장에서 Wallet 별로 호환되는 자산이 다르고 인터페이스 구성도 다르기 때문에 적절한 Wallet을 선택하는데 어려움이 있습니다. 이는 처음 Web3를 시작하는 유저에게 있어서 특정 Chain, Wallet에만 의존적으로 서비스를 이용하게 만들고 Mass adoption을 힘들게 만듭니다.YourD Data Wallet은 유저의 디지털 ID를 중심으로 새롭게 account를 설계하여 동일한 인터페이스 구성으로 여러 체인에 분산되어있는 디지털 자산을 한 곳에서 관리할 수 있습니다.

4) D-Ad : web3.0 광고 서비스

YourD에서는 개인이 데이터의 소유권을 지키면서, 이를 비즈니스 모델에 활용될수 있도록 광고 서비스를(기존의 Web2.0 에서 데이터가 가장 많이 활용되는 광고 분야를 타켓팅) 제공합니다. 기존 Web 2.0 광고와 달리 개인스스로 데이터를 제어하며 데이터의 가치를 광고를 통해 이익을 얻는 Web3.0 광고 (D-AD) 서비스를 제안합니다. 개인정보호를 보호하기 위해 ZKP (zero-Knowledge Proof)를 기술을 적용하였습니다.

1. 개인정보 보호와 타겟 광고의 조화 : ZKP 기술을 통해 광고주는 개인정보를 노출하지 않고 사용자의 선호도와 관심사에 따라 타깃 광고를 제공할 수 있습니다. 이를 통해 광고주는 효과적인 광고 전략을 구현하고 사용자는 개인 정보를 보호하면서 관련 광고를 수신할 수 있습니다.
2. 사용자 중심 보상 시스템: 사용자가 시청하는 광고를 기반으로 토큰이나 코인 등의 보상을 제공하는 시스템을 도입할 수 있습니다.

결론적으로, ZKP를 활용한 D-Ad 서비스는 Web3 환경에서 새로운 수익모델의 제안과 이를 기반으로 한 Dapp서비스들의 생태계를 확장할 수 있게 해줍니다. 이 서비스는 개인 정보를 보호하면서 표적 광고를 가능하게 하여 기존의 Web2.0의 광고 모델에서 사용자의 데이터 주권을 갖게되는 Web3.0 분산형 광고 모델을 가능하게 합니다.

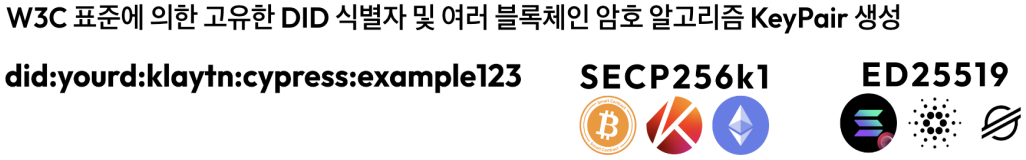
3. YourD는 어떻게 동작하는가?

YourD는 오픈소스 프로젝트이며 클레이튼의 블록체인 위에서 구현을 하였습니다. 본 장에서는 YourD의 주요한 기능들의 구현사항들에만 설명을 합니다. 자세한 오픈소스의 내용들은 YourD 홈페이지에서 공개할 예정이 입니다.

3.1 YourD : DID 구현

1장에서 설명한 W3C 표준의 DID 신원 증명 시스템을 기반으로 YourD의 DID는 블록체인 환경에서 구현하기 위해서 다음과 사항들이 개발되었습니다. 자세한 W3C표준에 등록된 YourD의 DID 스펙은 link 여기서 확인이 가능합니다.

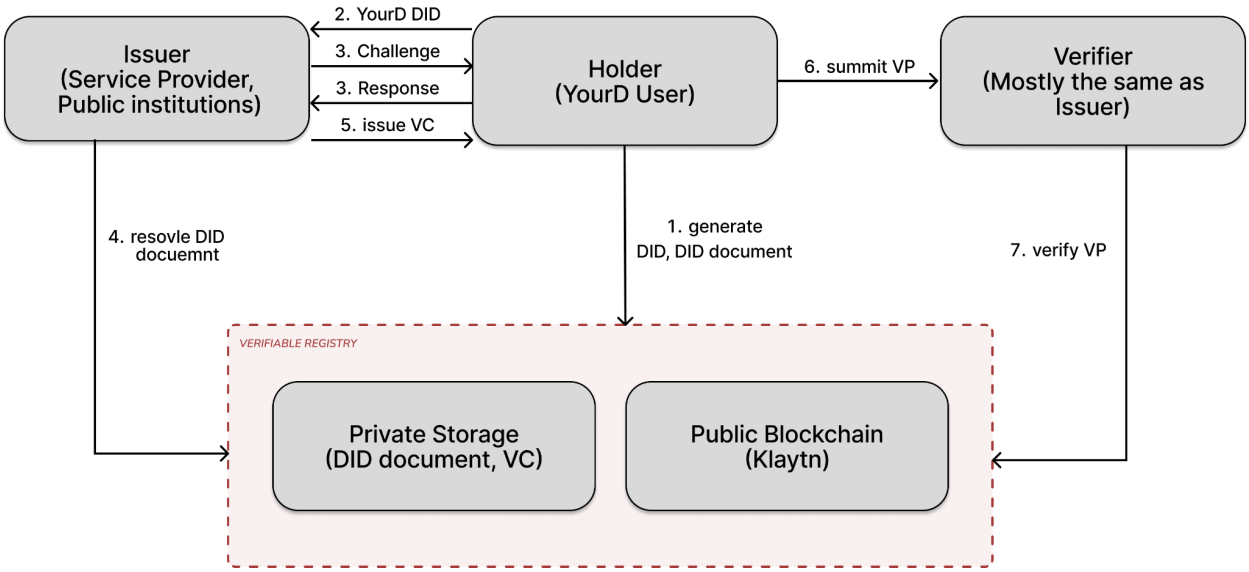
- 사용자에게 W3C 표준에 의한 고유한 DID 식별자 및 알고리즘들의 KeyPair 생성 지원.



- YourD는 KeyPair와 사용되는 알고리즘은 현재 클레이튼과 이더리움 Account를 생성할 때 사용하는 알고리즘인 secp256k1를 사용합니다. 또한 타 체인들의 알고리즘 지원을 위해 p256, ed25519의 알고리즘을 지원하는 KeyPair를 지원합니다

- 블록체인에 의해서 관리되는 DID는 권한이 있는 사용자만이 정보를 조회하고 이에 대한 증명이 되는 접근제어 지원. DID document는 사용자의 DID를 알고 있는 사람만이 조회가 가능.
  - DID document에는 민감한 개인정보가 작성되어서는 안되고 Public blockchain 상에는 DID document 상태에 대한 정보만을 기록합니다.
  - 회사, 기관으로부터 발급받은 VC는 개인정보가 포함되어있으므로 반드시 로컬 스토리지(ex 핸드폰)에서 관리가 됩니다.
  - 현재 YourD 프로젝트는 Klaytn의 Blockchain을 Verifiable Data Registry로 사용하고 있습니다. DID document에는 유저의 인증 방식 뿐만 아니라 편의성을 위해 serviceEndpoint와 같은 개인을 표현하기 위한 수단들도 기록이 되어있습니다.
  - 블록체인에 기록된 개인의 정보가 공개되어도 문제가 없는 정보들이지만 이를 조합해놓았을 때, 유저를 특정하여 추측을 할 수있는 가능성이 있습니다. 따라서 YourD는 DID document를 private storage에 저장하고 blockchain상에는 documentMetadata만을 기록하여 무분별한 document 조회를 방지하고자 합니다.
  - 마지막으로 발급받은 VC는 개인정보가 포함되어있으므로 이 또한 private storage에 저장하여 관리하도록 합니다.

3.2 Your 간편 QR 로그인



<그림14> YourD 간편 QR로그인 Flow

1) Entity

위 그림14는 주요 사안들을 반영하여 구현한 YourD의 DID 간편 로그인 WorkFlow입니다. 먼저 Entity들에 대한 설명입니다.

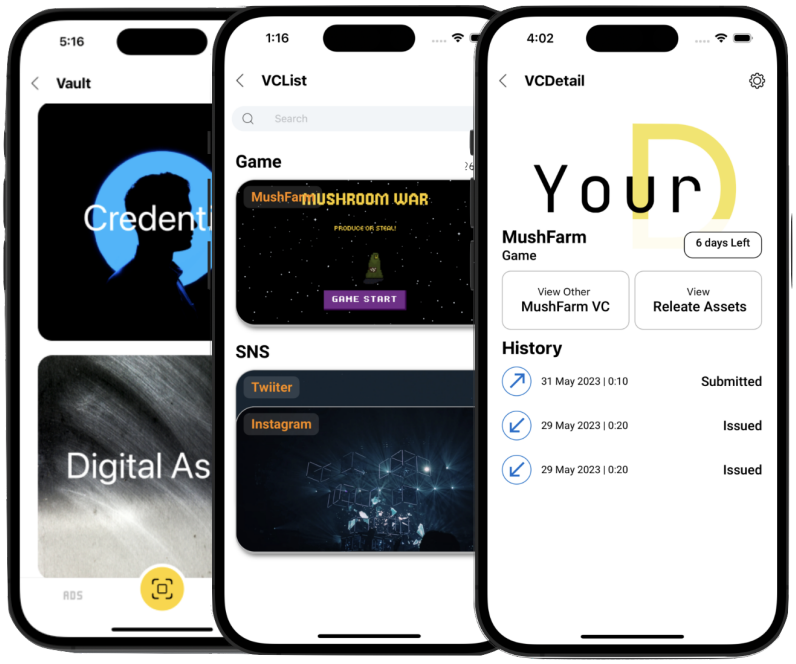
- Issuer : Holder로부터 DID를 받아 해당 DID document를 조회하여 유저를 검증하고 이후 요청한 VC를 발급합니다. Issuer는 자격을 증명하는 주체로서, 일반 서비스에서의 자격 증명이나 정부, 공공기관등에서도 전자 문서를 발급할 수 있습니다.
- Holder : Service에 로그인하는 주체로 로그인 시에 필요한 정보들을 Holder의 private storage에서 관리합니다. Private storage에서는 DID document와 Issuer로부터 발급받은 VC들을 관리합니다.
- Verifier : Holder로부터 받은 VP를 검증합니다. 대부분의 경우 Issuer와 동일하지만 VP에 담을 정보에 따라 Issuer와 Verifer가 다른 시나리오가 발생할 수도 있습니다.

2) YourD 간편 QR 로그인의 프로세스

1. YourD 로그인을 위해 유저는 YourD APP(Digital Data Wallet)을 통해 DID와 DID document를 생성합니다.
2. 이후 YourD QR 로그인을 지원하는 Service에 회원가입을 하기 위해 유저 자신의 DID를 제출합니다. QR로 이루어진 VC Schema를 스캔하는 동작으로 이루어지는데 해당 VC를 갖고 있지 않다면 회원가입, 갖고 있다면 로그인 과정을 진행합니다.
3. Service(Issuer)와 유저는 Challenge/Response를 통해 검증과정을 거칩니다.
4. 검증이 완료되면 Service(Issuer)는 유저의 DID document를 조회합니다.
5. DID document의 내용을 확인한 후, VC를 발급합니다.
6. 유저는 받은 VC를 핸드폰에서 관리하고 이후, Service(Verifier)에 로그인을 하기 위해 필요한 정보를 조합하여 VP를 생성하고 제출합니다.
7. Service(Verifier)는 받은 VP를 검증합니다. 이 때, 유저를 검증하기 위해 DID document 조회를 해야합니다. DID document를 조회할 때는 항상 클레이튼의 Public Blockchain에 기록되어있는 document 상태를 체크하는 작업이 선행되어야합니다.

3.3. Digital Data Wallet

YourD의 Digital Data Wallet은 DID 신원 증명 시스템을 기반으로 만들어진 SSI Wallet입니다. 기존의 Web3 Wallet의 디지털 자산을 관리하는 기능에 추가로 디지털 자산과 더불어 Digital Data에 대한 소유권을 DID 기반으로 정의하였습니다. 뿐만 아니라 selective disclosure, zkp 등을 활용하여 YourD Data Wallet을 사용하는 유저는 각종 서비스를 이용하기 위해 꼭 필요한 정보만 제공하게 됩니다.

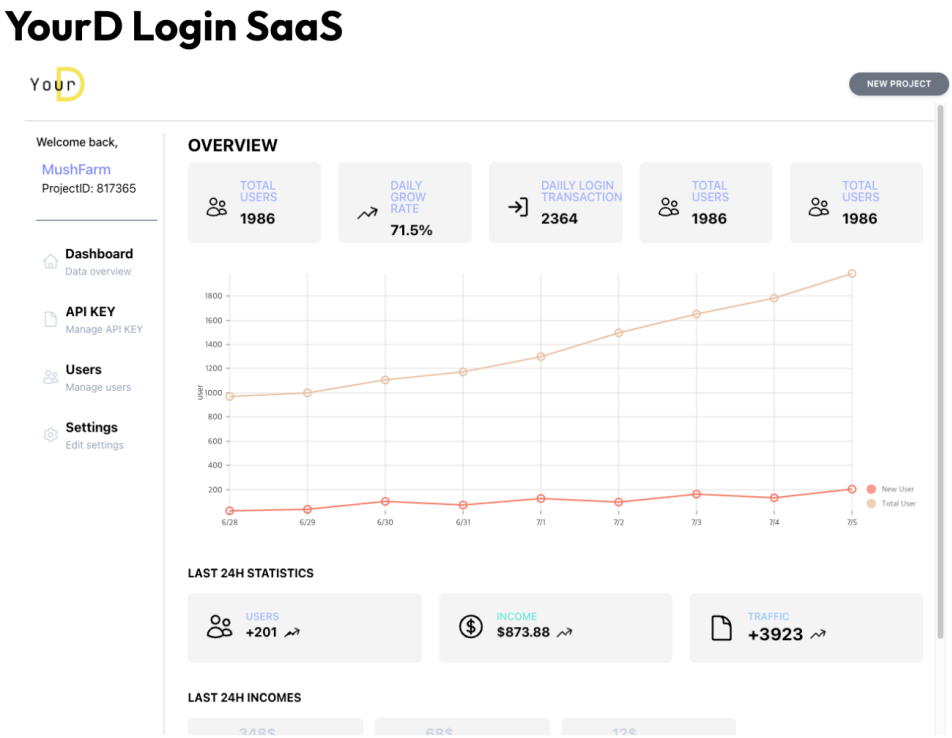


<그림15 VC Card 관리 >

그림 15는 유저가 어떻게 자신의 디지털 데이터를 관리할 수 있는지 보여줍니다. 각종 서비스 뿐만 아니라 신원 데이터도 모두 기본적으로 VC Card 단위로 관리합니다. 그래서 이후에 YourD 간편 QR 로그인을 진행할 시, VC Schema를 스캔하여 Card 존재 여부를 파악하게 됩니다. 로그인 정보를 VC 형태로 관리함으로써, 유효기간, 이용내역 등을 실시간으로 확인할 수 있고 이는 데이터 주권을 개인 중심으로 확립시키는 UX입니다.

3.4 YourD Login SaaS

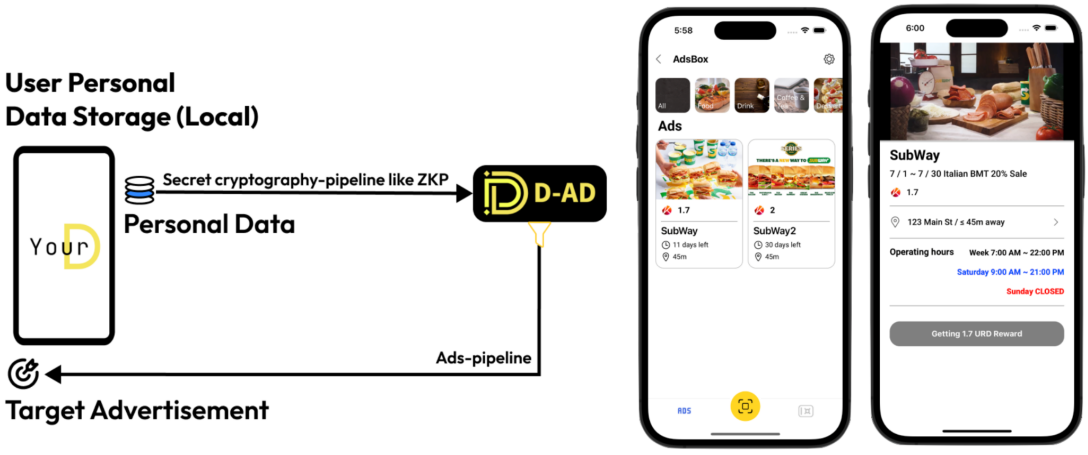
YourD Login SaaS는 YourD 간편 QR 로그인을 지원하기 위해 제공되는 B2B 솔루션입니다. 기업들은 자신의 서비스를 이용하기 위한 로그인 기능을 간편하게 구현함으로써 자신의 서비스 개발에 집중할 수 있습니다. 또한, DID 신원 인증 시스템을 기저로 유저 관리를 함으로써, GDPR과 같은 데이터 보호 법안 문제등에서 자유로워지게 됩니다. 이는 기업이 글로벌 서비스로 확장하는데 있어 진입장벽을 낮춰주고 개인정보보호 강화 흐름 속에서 대응하기 쉬워집니다.



<그림16 YourD Login SaaS >

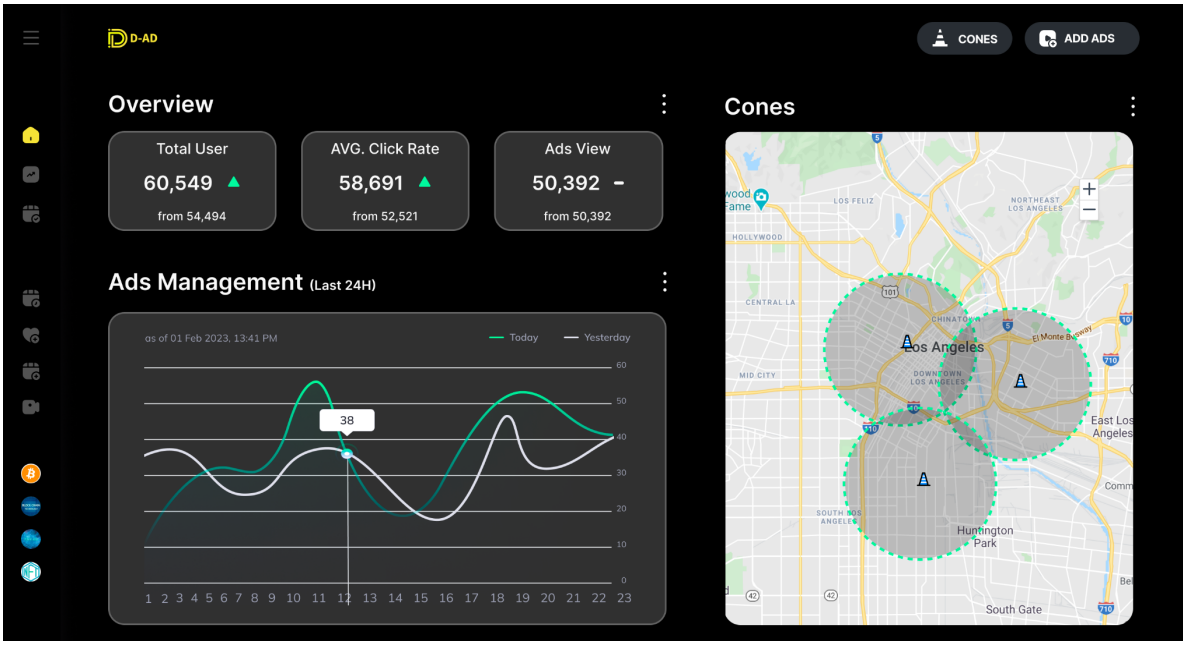
그림 16은 YourD Login SaaS를 이용하는 기업에게 제공되는 유저 분석 툴입니다. YourD 간편 QR 로그인을 이용하는 유저 데이터를 분석하여 기업 서비스에 지속적인 리텐션을 일으킬 수 있는 전략을 세울 수 있도록 도와줍니다. 더 나아가 Web3.0 광고 서비스인 D-Ad를 통한 기업 서비스 자체적으로 광고 수익 모델을 수립할 수 있습니다.

3.5 Web3.0 광고 서비스 : D-Ad



<그림17 D-Ad Flow >

위의 그림 17과 같이 Web3.0 광고 프로토콜인 D-Ad는 유저의 위치, 시간, 관심도를 기반으로 YourD 어플로 타겟 광고를 받아서 볼 수 있도록 합니다. zkp기반인 D-AD 프로토콜은 타겟 광고를 수신하기 위해 분석하는 유저의 개인 데이터들은 모두 ZK proof를 기반으로 수집되므로 개인 정보를 보호함과 동시에 광고주는 효과적인 타켓 광고 전략을 세울 수 있습니다.



<그림18> D-Ad 광고주 Dashboard

광고주는 광고하고 싶은 지역과 시간대를 선택하여 광고를 배치할 수 있습니다. 광고주는 Cone을 구매하여 지역별로 배치되며, Cone에 할당된 광고 개수와 광고 당 보상 코인인 KLAY로 설정할 수 있습니다. Cone은 광고주가 구매하여 배치하는 것으로 거리별로 Cone을 구매하여 원하는 지역에 배치할 수 있습니다. 이를 통해 광고 조건에 맞는 유저에게 광범위하게 광고를 에어드랍할 수 있습니다. 그림18은 광고주가 Cone의 배치 모습과 광고 데이터 분석을 할 수 있는 D-Ad Dashboard 입니다. YourD의 D-Ad Dashboard는 광고 데이터를 분석하여 효율적인 광고 전략을 수립할 수 있도록 도와줍니다.

4. 결론

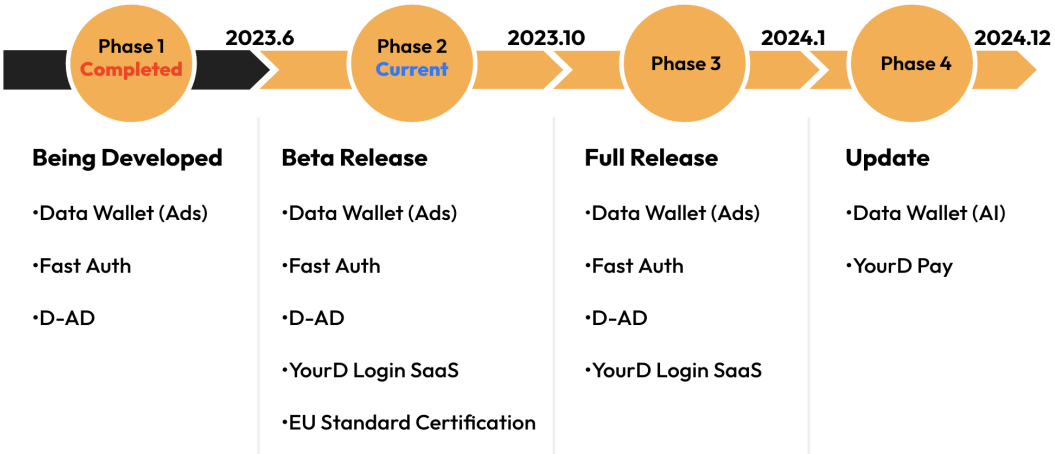
4.1 YourD의 기대 효과

YourD는 다음과 같이 클레이튼 에코시스템의 활성화 효과를 기대합니다.

- **Web3.0 사용자 경험 증대 :** YourD는 “DID 간편 QR 로그인”, “Service 중심의 Digital Data Wallet” 등을 통해 클레이튼 네트워크에서 사용자나 Dapp들에게 보다 편리하고 직관적인 사용자 경험을 제공할수 있습니다. 또한 사용자들의 데이터들을 활용할 수 있게 하여, 더 많은 유의미한 트랜잭션의 발생과 함께 이를 활용한 다른 서비스들이 많이 생길것으로 기대합니다. 또한 YourD의 Saas 서비스를 이용하여, 누구나 손쉽게 yourD 로그인 시스템을 이용할 수 있으며, 유저들을 분석 리포트를 제공받아 볼수 있습니다. 이러한 YourD의 편의성 제공과 데이터들의 가치 활용들은, 클레이튼 위에서 사용자들이 새로운 Web3.0 경험을 증대할수 있을것으로 기대합니다.

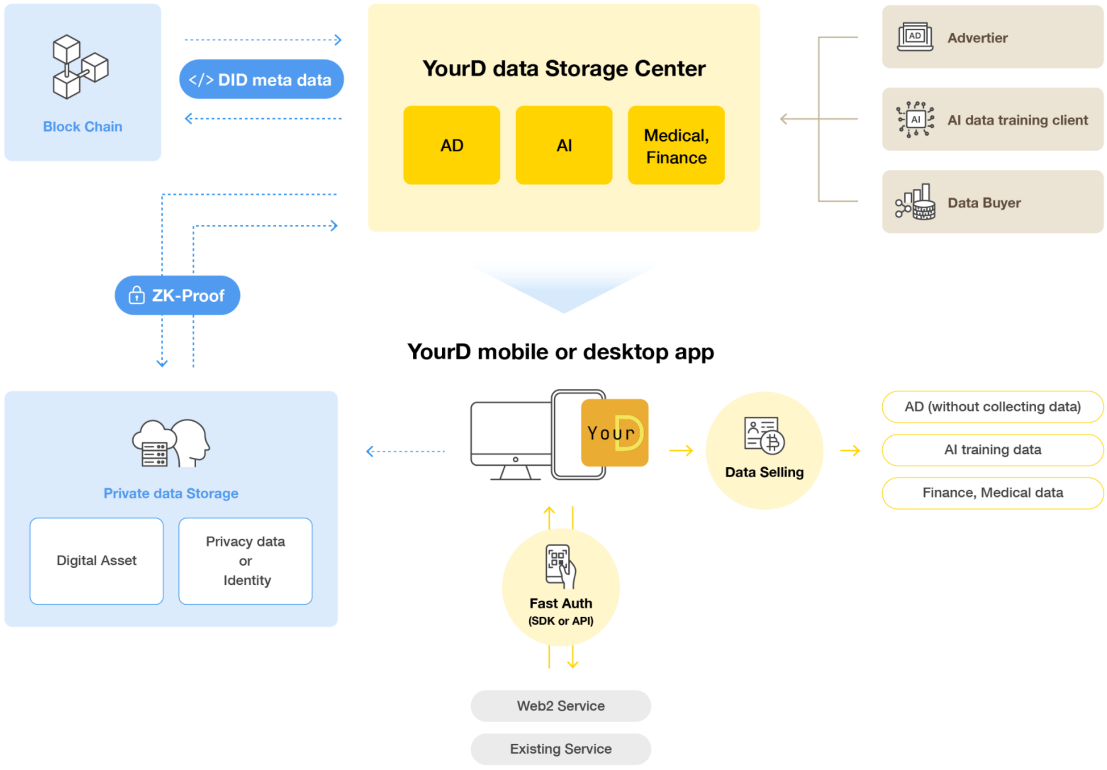
- **KLAY 유틸리티 창출:** YourD의 D-Ad 광고 프로토콜은 광고 수익모델과, 사용자 중심의 보상 모델을 도입 함으로서 많은 사용자들의 활동을 촉진하며, 교환 수단으로서 Klay를 사용하여, 사용성을 높이는데 기여할 수 있습니다.

4.2 YourD 로드맵



<그림19> YourD 마일스톤 계획

YourD는 위의 그림 19와 같은 마일 스톤을 계획하고 있으며, 현재는 3, 4장에서 언급한 모든 기능들을 개발 완료 하였으며, 현재는 10월을 베타 서비스 오픈을 기준으로 서비스화 개발과 운영 준비를 하고 있습니다.



<그림20> YourD 전체 구조도

YourD는 위의 그림 20과 같이 DID를 활용한 개인 데이터 관리 인프라를 구축하고 , YourD는 다양한 서비스에서 개인의 데이터들이 프라이버시를 지키면서 활용될 수 있는 방안을 탐구하고 있습니다. 이는 Advertisement, AI, Medical, Finance 등 모든 서비스를 포함하며, 이를 위한 판매 및 보상 체계를 하나씩 설계하고 구축할 것입니다. 향후 로드맵은 보안을 강화하면서 진정한 데이터 소유권을 실현하는 새로운 데이터 순환 흐름을 만들어 나갈 것입니다. 그리고 사용자 중심의 세상을 만들어나가는 데에 중요한 역할을 하는 모든 서비스들을 재구성하고자 합니다. 사용자의 데이터는 그들 자신에게 속하는 것이며, 이를 이용하여 사회 전체가 혜택을 받을 수 있도록 하는 것이 YourD의 궁극적인 목표입니다. YourD 프로젝트의 업데이트 사항들은 https://www.yourd.xyz/ 에서 확인 하실수 있으며, 많은 관심 부탁드립니다.

5. 부록 : YourD의 W3C 표준 소개

YourD는 W3C 심사를 거쳐 현재 공식 DID Method로 등록되었고, W3C 공식 문서 및 github에서 확인할 수 있습니다. W3C 공식 DID Method 에 등록 되기 위해서 DID Method와 DID document Schema, DID Method의 CRUD(Create, Read, Update, Delete) 방법에 기술 되어 있으며, 프라이버시와 보안사항을 고려한 설계 내용들이 포함 되어 있습니다. YourD DID Method는 [blockchain identifier]:[network identifier]:[blockchain account] 형식으로 Klaytn 네트워크의 경우 아래와 같은 DID를 사용하게 됩니다.

```
- did:yourd:klaytn:cypress:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58
- did:yourd:klaytn:baobab:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58
```

<그림21> YourD DID Identifier Syntax

```
{
   "@context":[
      "https://www.w3.org/ns/did/v1",
      "https://ns.did.ai/suites/secp256k1-2019/v1/"
   ],
   "id":"did:yourd:klaytn:baobab:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58",
   "verificationMethod":[
      {
         "id":"did:yourd:klaytn:baobab:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58#key-default",
         "type":"EcdsaSecp256k1VerificationKey2019",
         "controller":"did:yourd:klaytn:baobab:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58",
         "publicKeyMultibase":"A_Huy4IDtm0reCw0AgvZ-PbOKXaNpjcLbxCdCK3iBzky"
      }
   ],
   "authentication":[
      "did:yourd:klaytn:baobab:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58#key-default"
   ],
   "assertionMethod":[
      "did:yourd:klaytn:baobab:0xA738931B9Dd4019D282D9cf368644fEc52e9ec58#key-default"
   ]
}
```

<그림22> YourD DID document

YourD DID를 이용해 resolve한 YourD DID document는 위의 그림 22와 같습니다. Id : 이것은 고유한 식별자로서, DID document와 연결된 개체를 구분하는 데 사용됩니다. 여기서 사용된 ID는 Klaytn이라는 블록체인 네트워크의 Baobab 테스트넷에 존재하는 특정 블록체인 주소를 가리킵니다.

- verificationMethod: 이 DID가 어떻게 인증될 수 있는지에 대한 방법을 나열합니다. 다양한 공개키와 관련된 메타데이터를 제공하며, 각 방법은 고유한 ID, 관리자(controller), 키 유형(type), 그리고 공개키(publicKeyMultibase)를 포함합니다.
- authentication: DID document를 통해 인증을 받을 수 있는 방법을 나열합니다. 주로 DID의 소유자가 자신이 해당 DID의 주체임을 증명하기 위해서 쓰는 항목입니다. 여기서 제시한 예시에서는 기본 키('#key-default')를 authentication 방법으로 사용합니다.
- assertionMethod: DID가 어떤 주장(assertions)을 수행하는데 사용할 수 있는 방법을 나열합니다. DID의 주체가 다른 DID에게 VC와 엔티티를 넘겨줄 때, 즉 VP를 발행할 때 쓸 수 있습니다. 여기서 제시한 예시에서는 기본 키('#key-default')가 assertion 방법으로 사용됩니다.
- DataSovereignty-YourD라는 organization의 YourD-did-specification에서 더 자세한 YourD DID Method 스펙을 확인할 수 있습니다.

6. YourD 리서치 저자 소개

YourD팀은 여러 유명 블록체인 프로젝트들의 해커톤에서의 수상이력들이 있다.

*해커톤 수상이력들 : Klay Makers22, ETH Seoul, Tron, Tezos Incubating program, Polkadot , EVMOS Covalent

염재경

염재경은 YourD팀의 리더이자, 클레이튼의 Dev ambassador 로서 활동을 하고 있다. 현재는 Blockchain Engineer로서 ZKP, DID등을 개발하며, Iden3와 ZK-SBT 프로젝트에 기여한 적이 있고, YourD의 DID와 SDK를 개발하였다. 또한 현재 De-Butler 블록체인 학회의 Co-Founder로서 블록체인의 발전을 위해 여러 학회 활동을 하고 있다.

차영훈

차영훈은 YourD팀의 멤버이자, 클레이튼의 Dev ambassador 로서 활동을 하고 있다. 현재는 Blockchain Engineer로서 ZKP, DID등을 개발하며, 특히 YourD의 DID와 SDK를 개발하였다. 또한 현재 De-Butler 블록체인 학회의 Co-Founder로서 블록체인의 발전을 위해 여러 학회활동을 하고 있다.

김지황

김지황은 YourD팀의 멤버이자, 클레이튼의 Dev ambassador 로서 활동을 하고 있다. 현재는 Blockchain Engineer로서 Full Stack 개발자로 일을 하고 있으며, 특히 YourD의 Application을 개발하였다. 또한 현재 De-Butler 블록체인 학회의 Co-Founder로서 블록체인의 발전을 위해 여러 학회활동을 하고 있다.