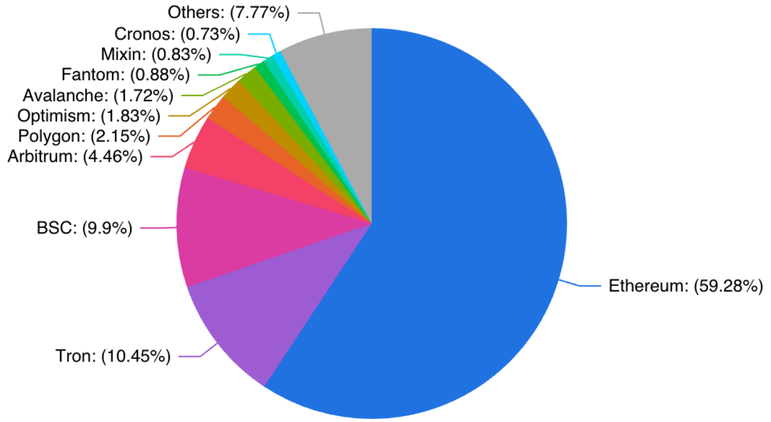
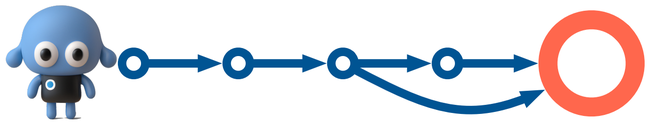
멀티체인으로의 확장을 위한 기술의 이슈들

가천대학교 & Bifrost
이종협

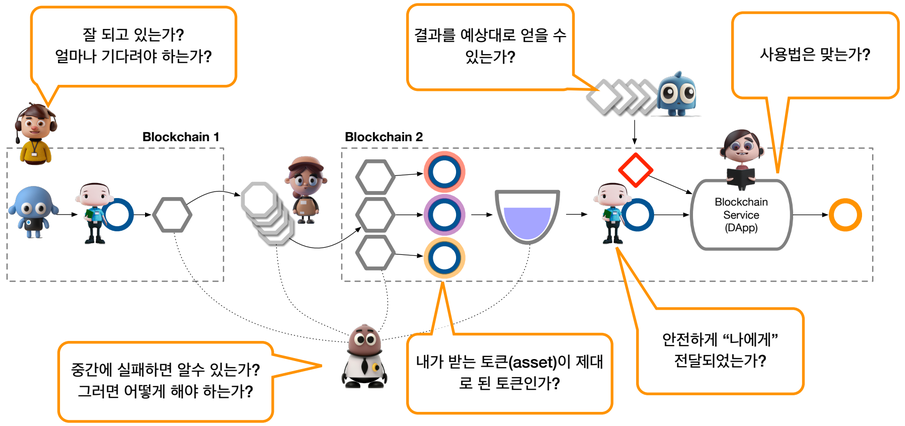
요약



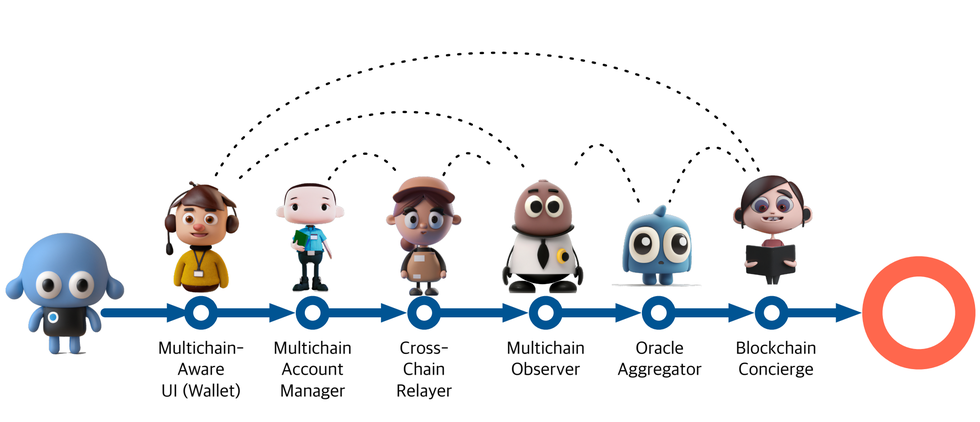
이미 블록체인은 멀티체인과 대연결의 시대로 접어 들었습니다.



서비스가 확장되어갈수록, 사용자의 관점에서는
더 불안하고 생소한 일들을 해내야 합니다.

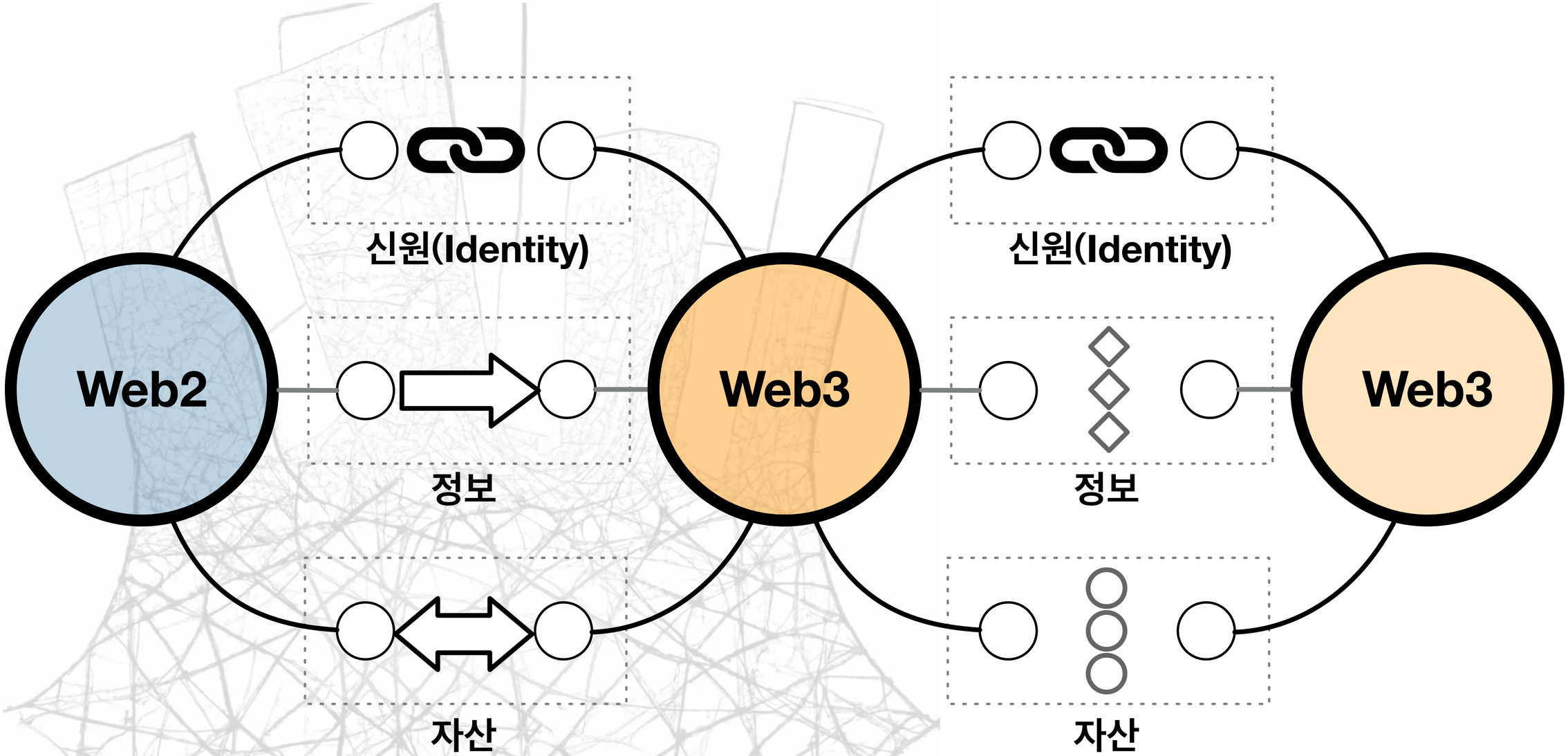


게다가 사용자가 멀티체인에서 겪어야 하는 고충은
복합적인 문제들로 가득차 있습니다.



다른 역할의 컴포넌트로 구성된 service stack (team)을 완성하여
사용자가 안전한 멀티체인 환경을 만들어야 합니다.

블록체인 대연결의 시대



Web3 대중화의 가장 큰 장애물

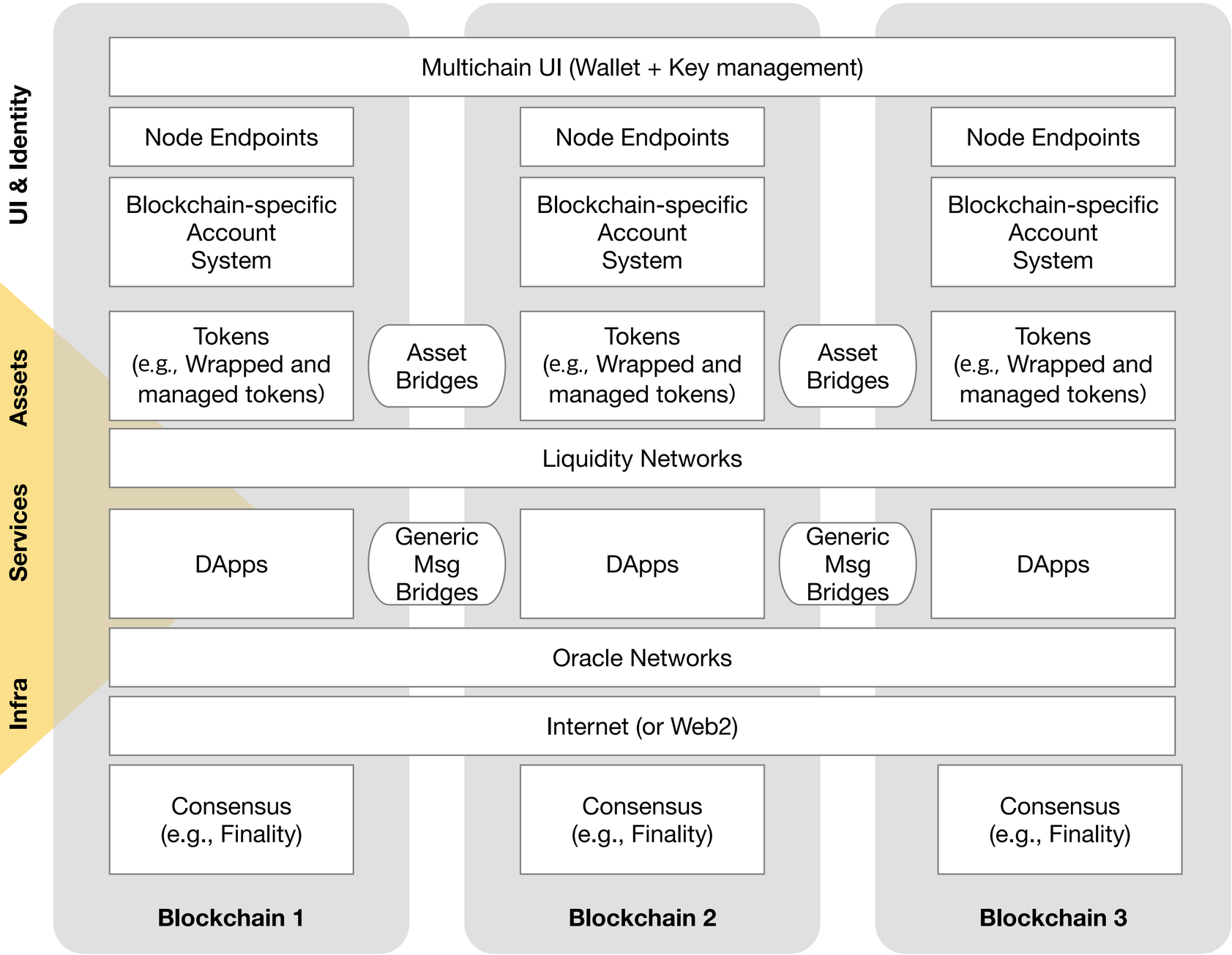
- Real Utility
- Regulatory Framework
- UX and UI
- Interoperability and Collaboration
- Security and Privacy

오히려 Web2가 Web3의 문제의 해결사가 될 수 있을까요?

- Real Utility - 인터넷(web2)의 무궁무진한 활용처
- Regulatory Framework - 소유자 특정하여 제도적 해결책과 연결 (모색)
- UX and UI - 친숙한 web2의 PKI 인프라 활용
- Interoperability and Collaboration - (거래소를 통한) 동일 소유자의 자산 연결
- Security and Privacy - 기존 web2에서의 신용도를 활용

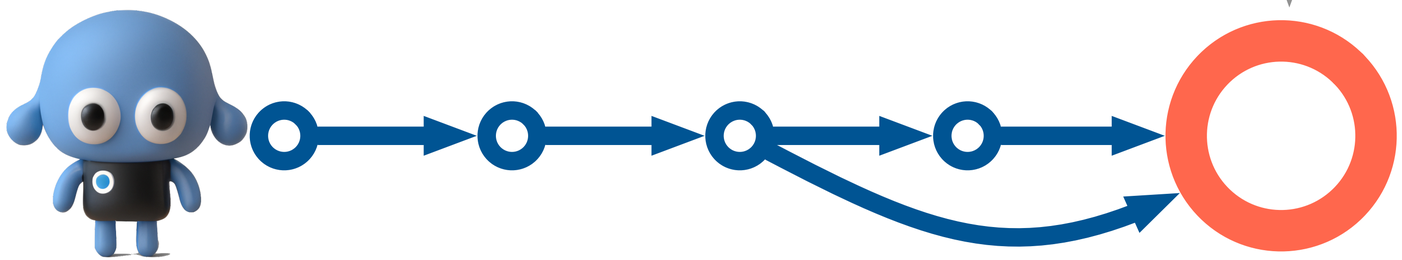
Web3의 연결

기존 인프라적인 입장에서
Multichain
(+ cross-chain)의
구성을 그려보자면,

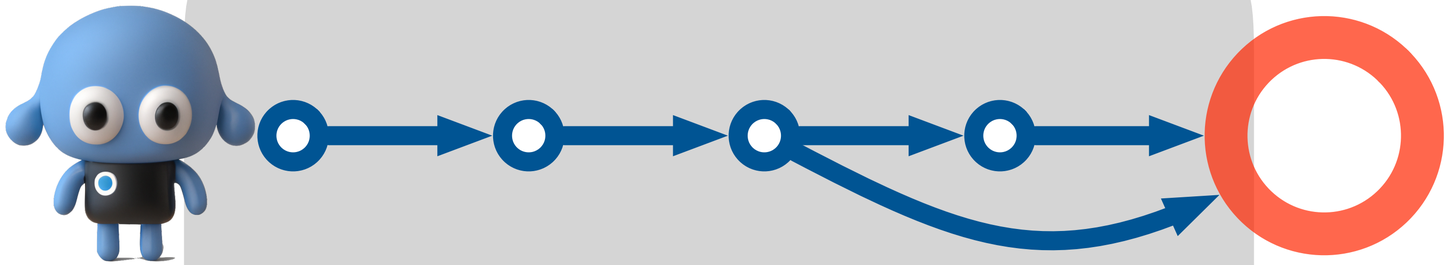


“Jobs to be Done”

하지만 Web3라고, 멀티체인이라고, 사용자가 필요로 하거나 하고싶어 하는 일이 근본적으로 변하지는 않습니다.



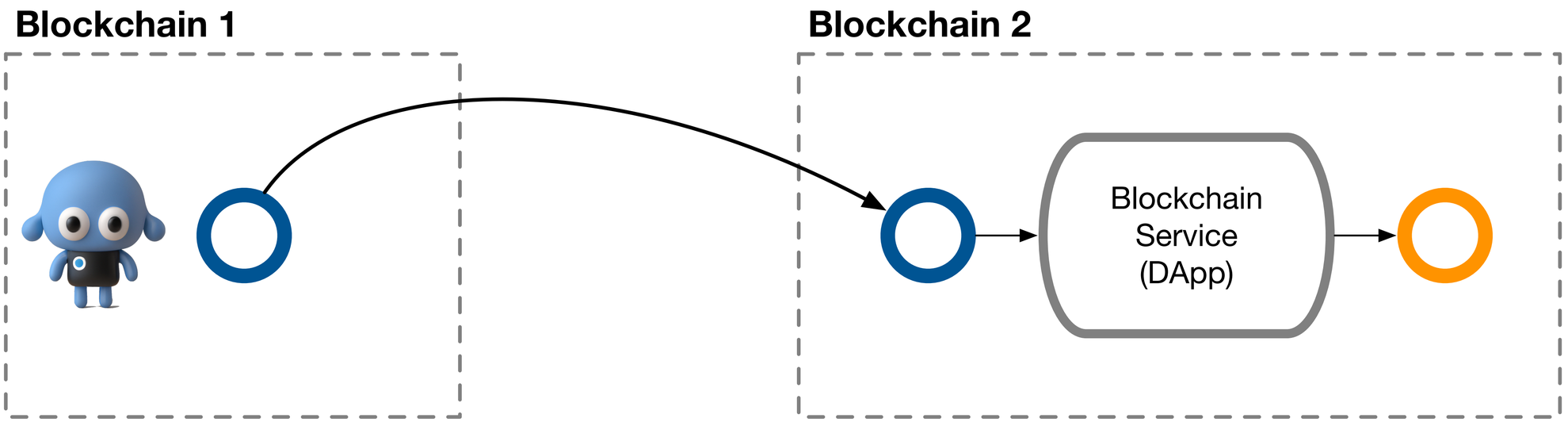
기술이 1차적으로 해결해야 하는 영역



“사용자가 멀티체인 서비스에서
자신의 의도를 명확하게 정할 수 있고,
결과에 대한 명확한 기대를 가지고,
수행하려던 작업을 완수할 수 있는 것”

Usable + Software + Network Security

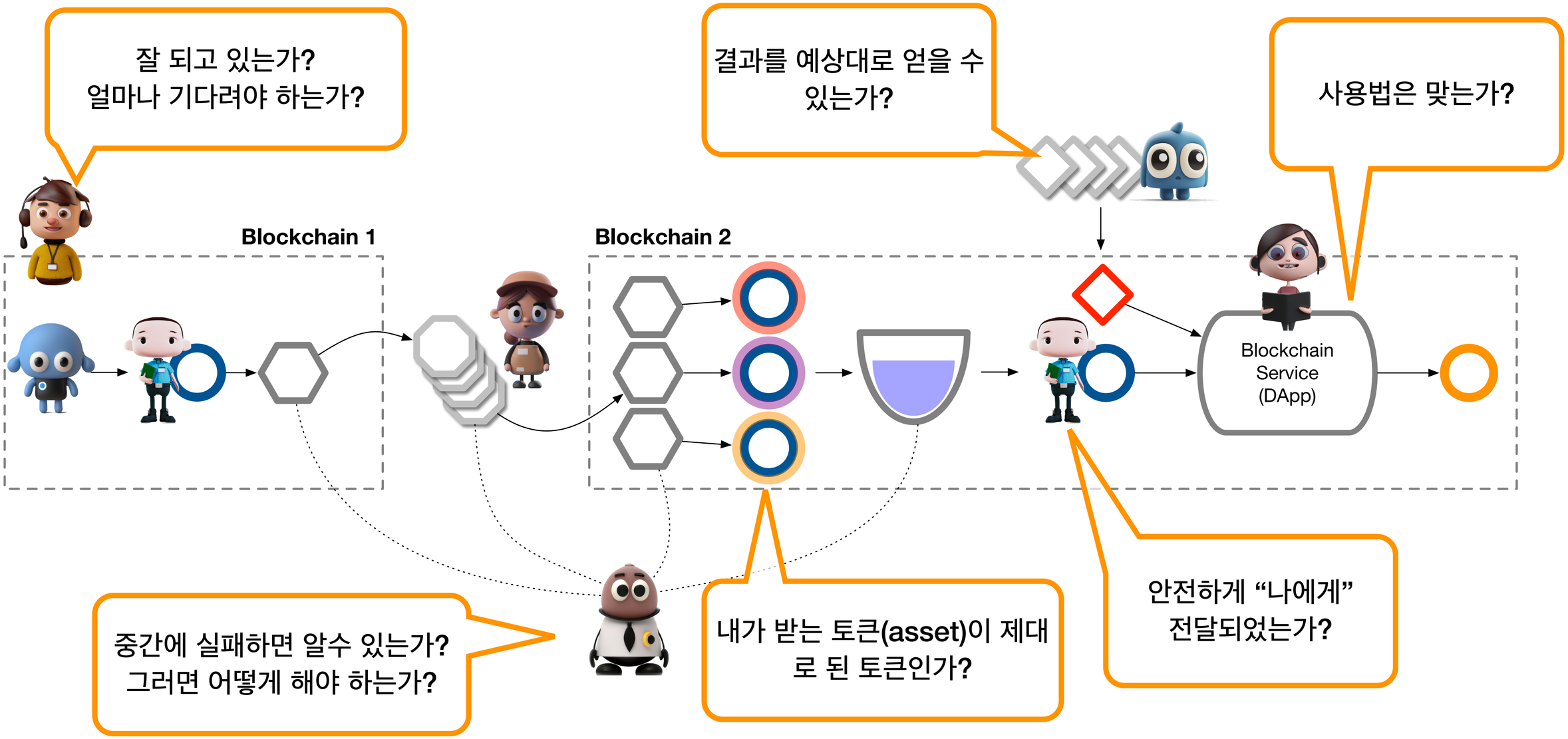
Running Example



멀티체인 사용자의 시점과 고충

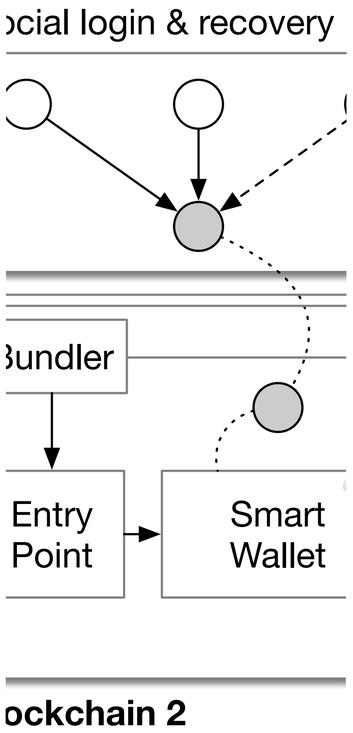
- 생소한 서비스들을 서로 다른 규칙이 적용되는 환경에서 사용하고 있습니다.
- 도전적이지만, 생소하기 때문에 당연히 어렵고 두렵습니다.
  - 내가 수행하는 과정이 어떠한 효과를 내는지, 그리고 어느 순간에 일어나는지를 걱정합니다.
- 결과에 예민하기 때문에 지속적인 정보 업데이트를 기대합니다.

Running Example



안전하게 “나에게” 전달되었는가?

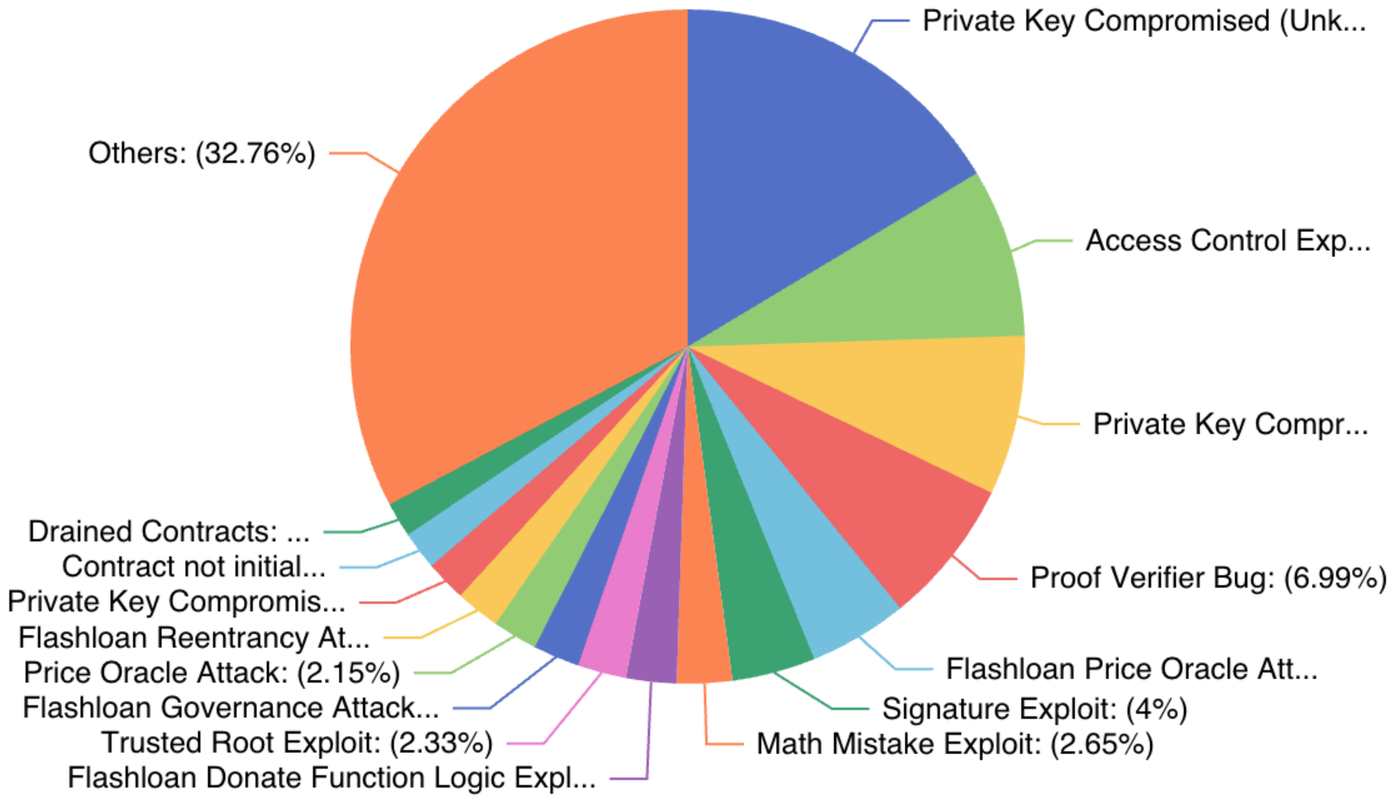
- 멀티체인 환경에서, 여기에서의 ‘나’와 저기에서의 ‘나’는 누구인가?
- Account management의 변화
  - 특히 멀티체인에서는 블록체인 본연의 기능(EoA, Smart Contract)만으로 account를 관리를 구현해야 합니다.
  - Social login + Smart Wallet (EIP-4337, EIP-3074)
- Smart Wallet (또는 Account Abstraction)은 장점이 많아서 무시하기 어렵습니다.
  - 하지만 blockchain-dependent 합니다.



안전하게 “나에게” 전달되었는가?

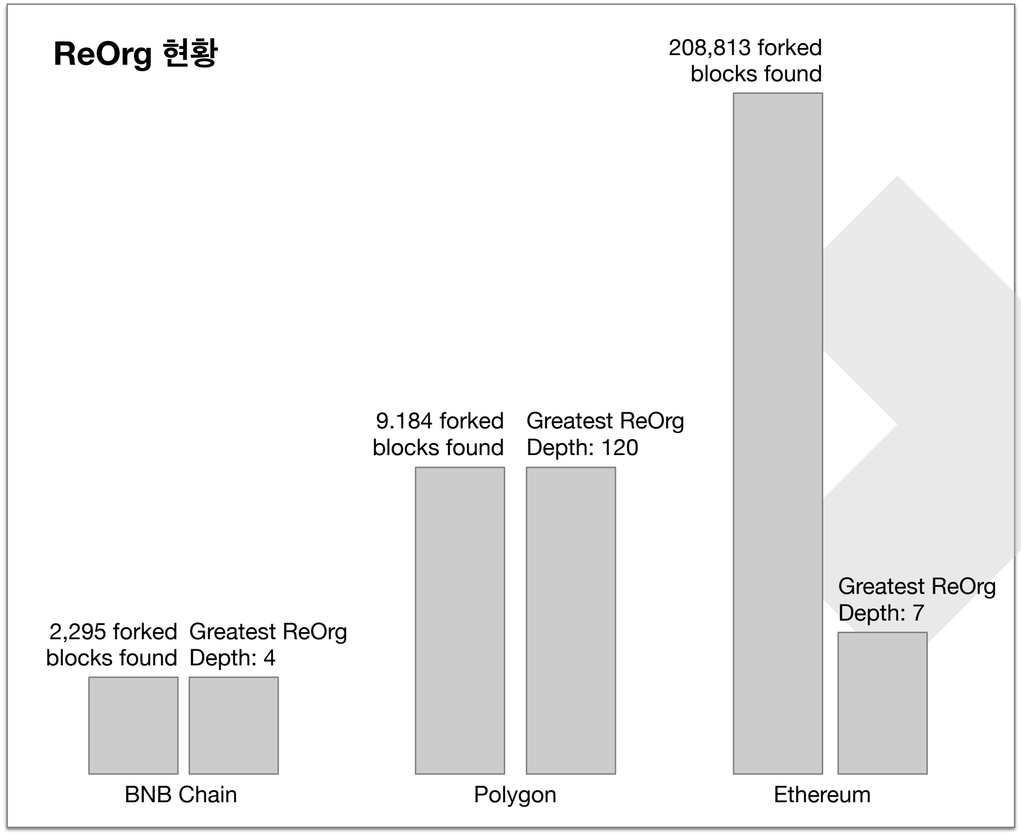
rekt

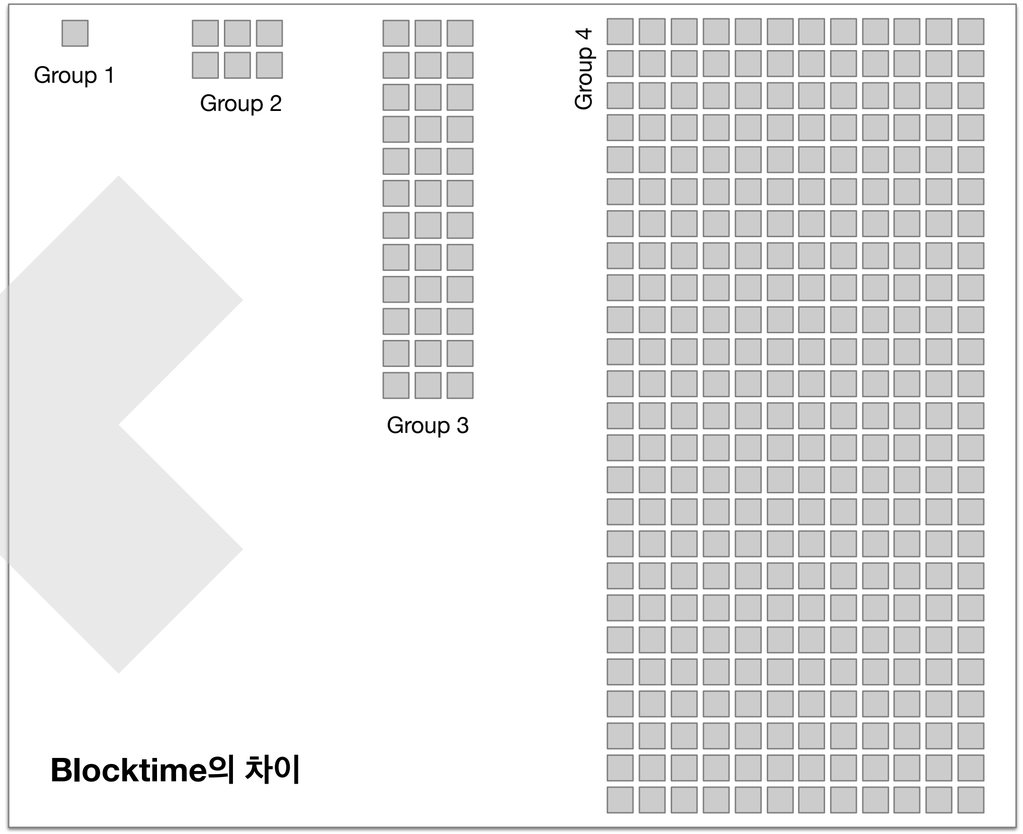
1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **BNB Bridge - REKT** *Unaudited*
   $586,000,000 | 10/06/2022
4. **SBF - MASK OFF** *N/A*
   $477,000,000 | 11/12/22
5. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
6. **Euler Finance - REKT** *Sherlock*
   $197,000,000 | 03/13/2023
7. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
8. **Nomad Bridge - REKT** *N/A*
   $190,000,000 | 08/01/2022
9. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
10. **Wintermute - REKT 2** *N/A*
    $162,300,000 | 09/20/2022



제대로 되고 있는가? 얼마나 오래 기다려야 하는가?

- 지금 어떠한 단계에 있는지 상황에 있는지 누가 알려줄까요?
- 그리고 엮여 있는 블록체인들에서, 안정적으로 결정이 날 때까지 얼마나 기다려야 할까요?

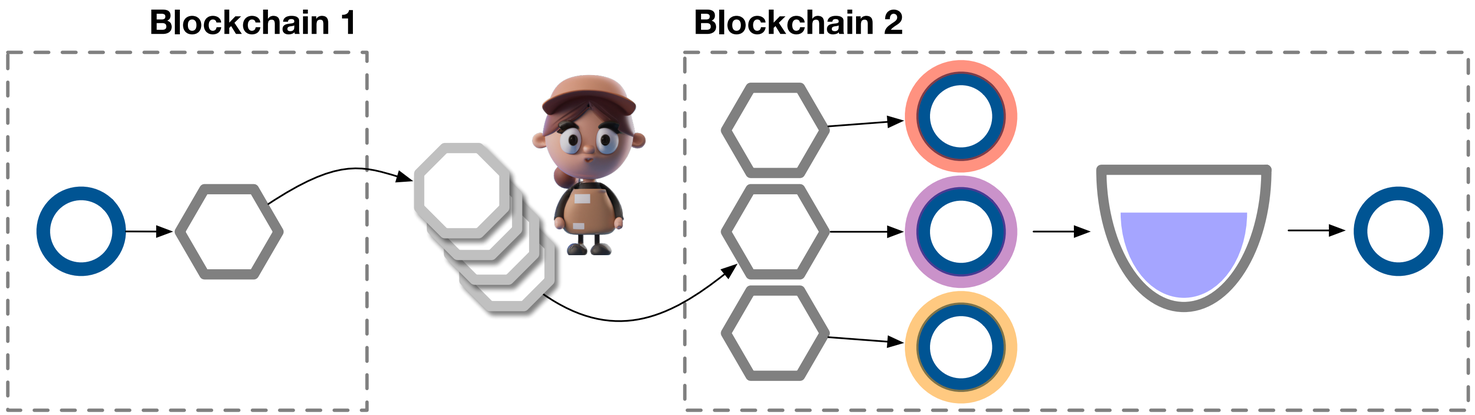




ReOrg 통계 참조 : https://andrecronje.medium.com/frustrations-of-a-dapp-developer-35701700e325

내가 받은 토큰이 제대로 된 토큰인가?

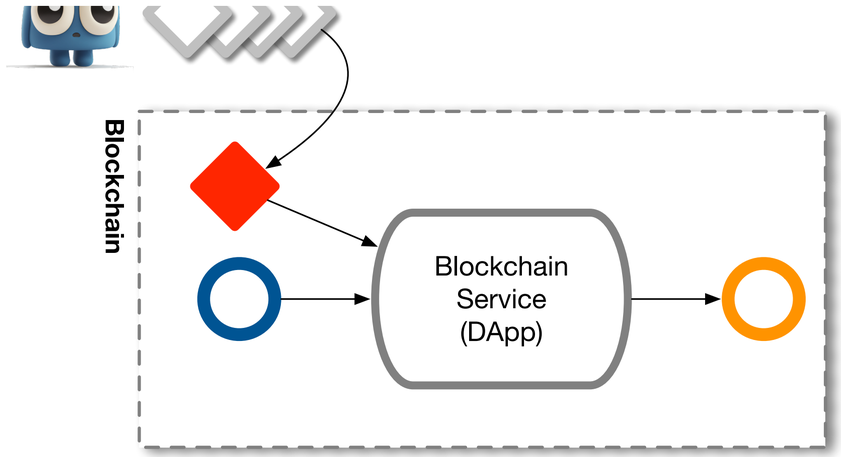
- 같은 토큰(asset)의 다른 버전들 (e.g., Wrapped tokens)
  - + “Lock and mint” 방식의 bridge



- 누가 확인하고 알려줄 것인가?

결과를 예상대로 얻을 수 있는가?

- 일치된 정보(일치된 context)를 가지고 동작한다고 예상할 수 있을까요?
- 예를 들어, Price Oracle은?
  - 멀티체인에서는 모두 동일한 price oracle이 제공되지 않습니다.
    - 우선, price oracle 자체가 없는 곳도 많습니다.
  - 서로 다른 해상도, 정보 source, 정책 등이 사용됩니다.
  - 게다가 서비스마다 원하는 방식도 다릅니다.

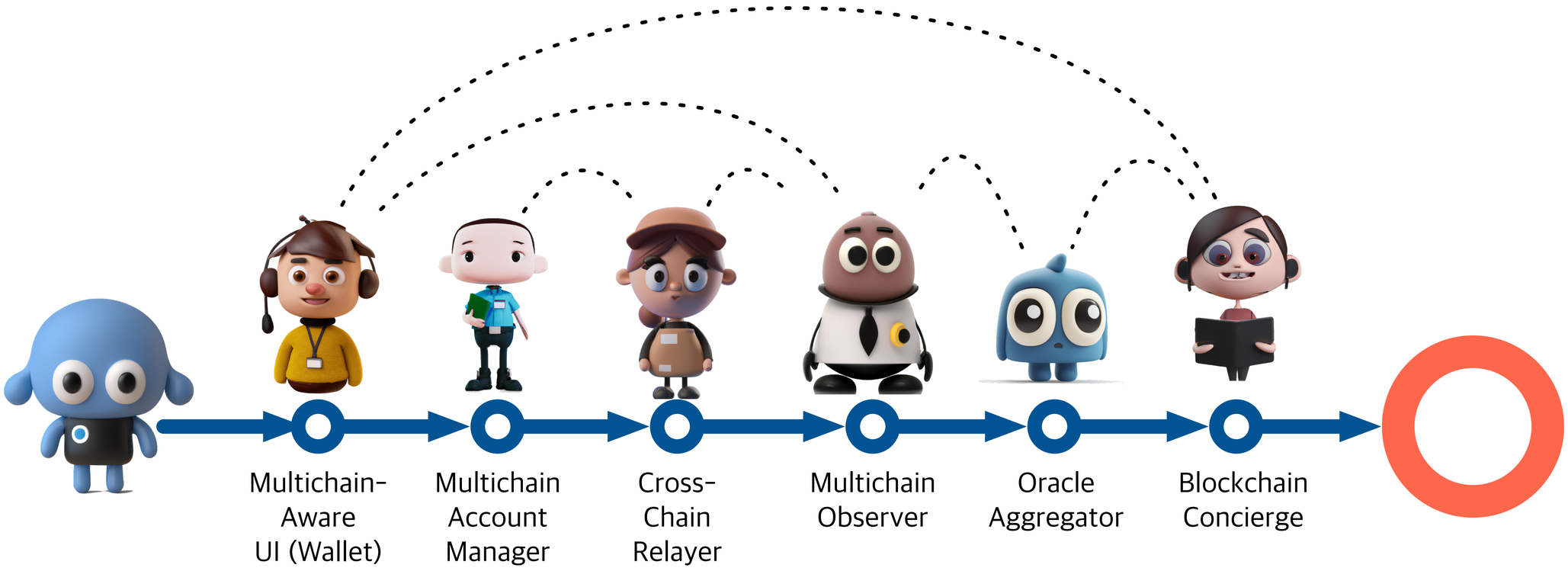


…그래서 ‘안전하다’는 느낌

여러 보안기술들을 종합하여 우선 실제로 안전하고,
사용자가 안전한 선택을하고,
안전하게 느낄 수 있는 환경을 만들어야 합니다.

Multichain Service Component의 “Team”

인프라보다 사용자를 먼저 생각하는 멀티체인 서비스에서는,
“사용자가 멀티체인 서비스에서 **자신의 의도를 명확하게** 정할 수 있고,
결과에 대한 명확한 기대를 가지고, **수행하려던 작업을** 완수”하기 위해서 각 역할을 담당하는 component들로 구성된 team이 필요합니다.



감사합니다.