Private & Permissioned Blockchains

Outline

- Introduction
- Differentiation
- Benefits and Drawbacks
- Applications

Introduction

- The main Ethereum blockchain is public and permissionless - also called Mainnet
- Ethereum has multiple public testnets like Görli, Kovan, Rinkeby, and Ropsten
- Anyone can create a private blockchain
  - For testing and development
  - For specific use cases, generally within a domain
- Has no direct connection with the mainnet
  - Same node/client can connect to mainnet and your private chain
  - No common accounts, state, or value transfer
- Why use Ethereum (or any other public blockchain) protocol then?
  - Dependable, tested, and secure protocol, node implementations, and tools
  - Availability of developers and administrators with deep knowledge
  - Benefit from new updates and feature/tool development
  - Similar to using open source libraries in a closed source product

Differentiation

- Public
  - Inherently assumed to be permissionless
  - All the popular ones like bitcoin, ethereum mainnet, etc.
  - Account identity is private but transactions are transparent
- Fully Private
  - Owned by one single entity and used within their system
  - A distributed decentralized ledger with cryptographic immutability, but not really a blockchain
  - Controlled joining and identity sharing - creator can control mining, transaction type, etc.
  - Useful for development and testing
  - Useful within a large organization or a group to store demonstrably immutable data
- Permissioned Private
  - Mix of both worlds
  - Generally run by a domain-based consortium or a federation
  - Different roles based on identity verification
  - Account identity is public (to creators) but transactions are private (from the outside world)

  Ripple (real-time settlement between banks),
  - Quorum (finance-domain, consortium-based)

Benefits and Drawbacks

- Benefits
  - Low transaction fees - Creator can set any level for transaction/gas fees
  - Better efficiency and throughput - Can choose protocols other than PoW to reduce computation cost and increase block creation rate
  - Less congestion - Controlled network will have fewer and more controlled transactions
  - Enterprise-preferred - Strikes a balance between transparency and regulation
  - Access control levels - Creators can define different levels of access, limit mining to a specific group, limit type and value of transactions based on levels, etc.
  - Can regulate and hence disallow illegal activity based on various regional laws
  - Limits identity and transaction transparency - Required in some domains
- Drawbacks
  - Not trustless - Controlled by the creator group, creates inherent trust dependency
  - Limits transparency leading to reduced trust by individuals
  - Immutability is not guaranteed
  - More prone to be manipulated by a bad actor with sufficient permissions

Applications

- **Financial Services**
  - Controlled financial interactions between equivalent players - gross bank settlement, P2P transaction settlement, efficient global payments, trade finance, federation (Bankchain)
  - User information with privacy - credit ratings, loan proofs, lending platforms, data exchange
- **Supply chain**
  - Raw material and goods tracing across the chain - tracking and prediction
  - Combined with IoT for faster and more accurate worldview
  - Applies to food, clothing, precious metals/gems, electronics, and more
- **Media and Entertainment -** In-game currency, music royalty platform, content verification
- **Identity -** Digital encrypted identity docs with controlled access and audit trail, deep integration with Govt, Education, Banking & Insurance, Healthcare, Employers, etc.
- **Insurance -** Data validation, automated claim processing, KYC and money laundering protection, high-value item tracker, etc.
- **Healthcare -** Secure patient data sharing, digital record management
- **Other domains -** Employment, Education, Manufacturing, Real Estate

greatlearning

Power Ahead

Happy Learning !