ARX - Arcium

Arcium é uma rede de computação confidencial descentralizada que visa resolver a vulnerabilidade dos dados quando estão em uso, um problema que a criptografia tradicional não aborda completamente. Ao alavancar a Multi-Party Computation (MPC), Arcium permite que várias partes executem computações em dados encriptados sem que nenhum participante tenha acesso aos dados brutos. Isso cria um ambiente de computação confiável e verificável, tornando-o adequado para uma ampla gama de aplicações que exigem privacidade.

A arquitetura da Arcium é concebida como um supercomputador global, onde os nós (Arx Nodes) formam clusters para executar tarefas de MPC. A rede utiliza um mecanismo de orquestração on-chain para gerenciar tarefas, incluindo a criação de Ambientes de Execução Multi-Partidária (MXEs). Uma característica notável é o uso de processamento paralelo para eficiência. A Arcium é projetada para ser agnóstica em relação a blockchains, permitindo que os desenvolvedores implantem contratos inteligentes confidenciais em várias redes.

O token ARX é o pilar econômico e de governança da rede Arcium. Sua principal utilidade reside em:

- **Segurança da Rede:** Operadores de nós apostam (stake) tokens ARX como garantia para participar da infraestrutura computacional da rede e garantir sua integridade. Quanto mais computação um nó oferece, mais ARX ele deve apostar.
- **Pagamento de Taxas:** Embora as taxas de computação sejam pagas em tokens nativos da blockchain em que a Arcium opera (como SOL na Solana), o ARX está intrinsecamente ligado à demanda por esses serviços. A demanda por computação confidencial se traduz em demanda real pelo ARX.
- **Governança:** Detentores de ARX participam das decisões de governança da rede, com mecanismos que recompensam detentores de longo prazo.
- **Alocação de Recompensas:** Os operadores de nós recebem taxas da rede em proporção ao seu desempenho, e nós subperformantes podem perder delegação.

A Arcium oferece uma gama diversificada de casos de uso, incluindo:

- **Finanças Descentralizadas (DeFi):** Criação de dark pools para negociações privadas, empréstimos e empréstimos confidenciais, e negociação de leilões de lance selado. Isso ajuda a mitigar riscos como MEV (Maximal Extractable Value) e front-running.
- **Inteligência Artificial (IA):** Permite o treinamento e inferência de IA sobre dados confidenciais, protegendo dados sensíveis em aplicações de IA.
- **Gerenciamento da Cadeia de Suprimentos:** Protege dados comerciais sensíveis durante toda a cadeia de suprimentos, permitindo colaboração.
- **Saúde:** Permite o processamento seguro de dados de saúde sensíveis para pesquisa colaborativa sem comprometer a confidencialidade do paciente.
- **Sistemas de Votação Seguros:** Garante a integridade e a confidencialidade dos dados dos eleitores em sistemas de votação.
- **DePIN (Decentralized Physical Infrastructure Networks):** Gerencia dados de uso sensíveis e computações de gerenciamento de rede.

A tokenomics do ARX prevê um suprimento total de 1 bilhão de tokens. No lançamento, aproximadamente 20,88% do suprimento estava em circulação. A distribuição visa alinhar os incentivos entre os principais stakeholders, incluindo a comunidade, investidores anjo, validadores, contribuintes principais e capitalistas de risco. A Arcium implementa um mecanismo de suprimento dinâmico que pode ajustar a inflação e as estratégias de queima com base na demanda da rede, com inflação controlada para compensar os operadores de nós durante períodos de baixo volume de trabalho e queima de tokens quando a demanda aumenta.

As vantagens da Arcium incluem confidencialidade total e sem confiança para os usuários, aplicativos mais capazes de operar sobre dados confidenciais, e integração de baixa fricção com poucas linhas de código. A rede se destaca por sua capacidade de executar computações arbitrárias sobre dados confidenciais de forma confiável e verificável.

As limitações potenciais podem incluir a complexidade técnica inerente à computação confidencial e ao MPC, e desafios com operações de entrada/saída (I/O) em computações de larga escala. A arquitetura também precisa gerenciar o risco de colusão entre nós anônimos.

As perspectivas para a Arcium envolvem o desenvolvimento contínuo de sua infraestrutura de computação confidencial, visando tornar-se o padrão para aplicações que exigem privacidade e segurança de dados na era descentralizada. Sua abordagem agnóstica de

blockchain e foco em casos de uso do mundo real, como DeFi e IA, posicionam-na como um player promissor no ecossistema cripto.