به نام خدا

پروژه زنجیره بلوکی درس رمزنگاری پیشرفته – بهار ۱۴۰۲

موعد اعلام گروه‌بندی: چهارشنبه ۲۳ فروردین ساعت ۲۳:۵۵

موعد آپلود گزارش و فایل ارائه: ۱۴ اردیبهشت ساعت ۲۳:۵۵

یکی از مهم‌ترین کاربردهای زنجیره‌ی بلوکی در دنیای اقتصاد است. از آن‌جایی که از اصلی‌ترین ارکان دنیای اقتصاد، عدم اعتماد هستارها به یکدیگر است، فناوری زنجیره‌ی بلوکی خیلی سریع جای خود را در بازارهای مالی پیدا کرد، با این تفاوت که دیگر موانع بوروکراسی، قضایی و گاهاً انحصارطلبی بانک‌ها و دولت‌ها مانع ایده‌پردازان نبود و هر فرد، تنها با داشتن دسترسی به اینترنت می‌توانست ایده‌های مالی خود را عملی کند. در واقع شبکه‌ی زنجیره‌ی بلوکی Ethereum، مانند یک کامپیوتر جهانی مطمئن، قادر به اجرای هر ایده‌ی جدیدی در این حوزه بود که این باعث رشد و شکوفایی شگرف دنیای اقتصاد در قرن ۲۱ شد و اقتصاد مدرن یا توزیع‌شده (Defi[1])، به سرعت در حال پیشی گرفتن از اقتصاد سنتیِ مرکزگرا می‌باشد.

هدف از طرح این پروژه، آشنایی با گوشه‌ای از دنیای Defi و تحلیل و بررسی چند پروژه‌ی بین‌المللی است که بر بستر شبکه‌ی Ethereum راه‌اندازی شده‌اند. از جمله‌ی پروژه‌های موفق در دنیای Defi می‌توان به صرافی‌های توزیع‌شده یا DEX[2]، سیستم‌های قرض دارایی[3]، بازارهای پیش‌بینی[4]، سامانه‌های ضد پولشویی یا شناسه-محور (KYC)[5] شرکت‌های توزیع‌شده‌ی بیمه، سپرده سرمایه‌گذاری روی POS ، توکن‌کردن دارایی و ... اشاره کرد.

در این پروژه از هر کدام از موارد ذکر شده در بالا یک پروژه پیشنهاد می‌شود و افراد باید طی مدتی معین، پروژه‌ی مورد نظر خود را انتخاب کنند و برای آن **گزارش** و **ارائه** تهیه نمایند. این پروژه‌ها عبارتند از:

نوع پروژه	نام پروژه	لینک‌های مفید
DEX	UniSwap	Source Code + White Paper
Lending & Borrowing	Lendroid	Source Code + White Paper
Prediction Markets	Augur	Source Code + White Paper
KYC	Hydro	Source Code + White Paper

[1] Decentralized Finance
[2] Decentralized Exchange
[3] Lending Protocols
[4] Prediction Markets
[5] Know Your Costumer

Source Code + White Paper	NexusMutual	Insurance
Source Code	Stakefish	Staking
Source Code + White Paper	Polymath	Asset Tokenization

نکته: ممکن است برخی از پروژه‌های بالا روی لایه‌ی اول اتریوم راه اندازی نشده باشند، بلکه روی یکی از راه‌حل‌های لایه دویی اتریوم مانند Polygon راه اندازه شده باشند، به همین دلیل Source Code آن با زبان Solidity نباشد. از آن‌جایی که در این پروژه نیازی نیست Source Code را خط به خط و دستور به دستور مطالعه بفرمایید، مشکلی پیش نمی‌آید. صرفا لازم است عملکرد پروتکل را به شکل سیستمی ارائه بدهید.

خواسته‌های پروژه:

گزارش و ارائه‌ی شما آنالیز کاملی از پروتکل منتخب شما باشد. به طور کلی باید به سئوالاتی اعم از سئوالات زیر پاسخ داده باشید:

۱- هدف از این پروژه چیست؟
۲- مدل سیستمی آن چگونه است؟
۳- Source Code را آنالیز کنید و قراردادهای هوشمند مهم آن را شرح دهید. این قراردادها چه منطقی دارند؟ راجع به Interfaceهای این قراردادها بحث کنید.
۴- آیا این قراردادها audit[۶] شده اند؟ نتایج این audit ها را شرح دهید.
۵- پروژه‌های رقیب چه پروژه‌های هستند؟
۶- آیا در متن قرارداد هوشمند از اولیه‌ی رمزنگاری دیگری نیز استفاده شده؟ آن‌ها را شرح دهید.
۷- چه ایده‌ای برای بهبود این پروژه دارید؟

و ...

پس از انتشار صورت پروژه، لطفا نام و نام خانوادگی اعضای گروه به همراه اسم پروژه را در گروه تلگرامی درس اعلام بفرمایید و در صورت داشتن هرگونه سئوال به شناسه khamOsh98 در تلگرام پیام بدهید.

توجه: به دلیل اینکه تعداد اعضای کلاس ۱۱ نفر است، ۴ گروه ۲ نفره و ۱ گروه ۳ نفره خواهد بود.

موفق باشید

---

[۶] راجع به audit قرارداد هوشمند تحقیق کنید.