



دانشگاه صنعتی شریف
دانشکده علوم ریاضی

ارزهای پایدار الگوریتمی

Algorithmic Stablecoin

نظریه الگوریتمی بازی‌ها – دکتر مجتبی تفاق

نام تیم:

aGoodTeamName

اعضای تیم:

طیب پورابراهیم

سید عرفان موسویان

پاییز ۱۴۰۰

مقدمه

ایجاد ارزهای تکمیلی در طول تاریخ موضوع جدیدی نیست. امروزه با رشد روز افزون بازار ارزهای دیجیتال توجه بسیاری به این بازار جلب شده است؛ مشکل اصلی این رمز ارزها نوسانات بسیار زیاد آنها می باشد. در این میان به ارزهایی نیاز پیدا می شود که نوسانات کمی داشته باشند و ارزش ثابتی داشته باشند. چنین ارزهایی با نام stablecoin شناخته می شوند. توجه فیسبوک [۱] و J.P. Morgan [۲] و صرافی بزرگ Coinbase [۳] به این نوع ارزها و تلاش آنها برای ایجاد این ارزهای دیجیتال نشان دهنده ی پتانسیل بالای این نوع ارزها است.

یکی از مزیت های اصلی ارزهای دیجیتال نسبت به پول های بدون پشتوانه^۱، غیر متمرکز بودن آنها می باشد [۴] اما stablecoin های موجود در بازار مانند Tether [۵]، برای حفظ ثبات آن ارز، اغلب به صورت متمرکز و سازمانی عمل می کنند. البته الزاماً stablecoin ها به مرکز خاصی برای مدیریت نیاز ندارند و نمونه هایی وجود دارند که به صورت غیر متمرکز می باشند. دسته ای از این ارزها سعی دارند تا با الگوریتم هایی ارزش آن ارز را ثابت نگه دارند؛ به این نوع ارزها Algorithmic Stablecoin می گویند [۶]. تلاش هایی در راستای ایجاد چنین ارزهایی صورت گرفته است، ما تلاش می کنیم با مطالعه و بررسی آنها به مدل کامل تر و بهتری در این زمینه برسیم.

پروژه های پیشین

پروژه Basis [۷] یکی از stablecoin هایی که مورد توجه و مطالعه ما قرار گرفته است. در این پروژه بر مبنای «نظریه مقداری پول»^۲ عملکرد بانک مرکزی را در خلق و نابودی پول به صورت الگوریتمی تقلید کرده اند و به صورت غیر متمرکز آن را پیاده سازی کرده اند و با ساخت دو توکن تکاملی در کنار توکن اصلی و فروش اوراق قرضه^۳ توسط این دو توکن تکاملی، قصد داشتند ارزش این ارز را نسبت به پول بدون پشتوانه ای همچون دلار یا شاخص CPI^۴ ثابت نگه دارند. در این مدل نیاز به دریافت اطلاعات خارجی مثلاً ارزش دلار، قیمت کالا و... وجود دارد که یکی از راه های پیشنهادی استفاده از oracle ها است که می توان به دو روش متمرکز و غیر متمرکز این کار را انجام داد. همچنین در سوی دیگر، در پروژه ی دیگری به نام Ampleforth [۸] رویکردی کاملاً ریاضی محور دارند که نیاز به دریافت اطلاعات خارجی نیست.

هدف ما از این پروژه

ما با مطالعه دقیق روش های استفاده شده در stablecoin ها و با استفاده از نظریه بازی ها و روش های آماری قصد در بهبود مدل های قبلی و یا ایجاد مدل جدید الگوریتمی و غیر متمرکز داریم. ما با ایده گرفتن از ابزارهای موجود مالی و سازوکارهای مورد استفاده بانک مرکزی ها، قصد ایجاد سیستم غیر متمرکز با نوسانات حداقلی نسبت به شاخص های مشخصی را داریم. همچنین به دنبال طراحی سازوکاری برای ایجاد مشوق های کافی برای جذب افراد اولیه و همچنین استفاده دراز مدت از این ارز هستیم. امیدواریم در این ارز روش های بهتری برای کمینه کردن نوسانات ارزش پیدا کنیم که نسبت به اقدامات خصمانه^۵ هم مقاوم باشد.

^۱Fiat Money

^۲Quantity theory of money

^۳Bond

^۵Adversarial

^۴شاخص قیمت مصرف کننده

- [1] Diem (formerly known as Libra) is a permissioned blockchain-based payment system proposed by the American social media company Facebook, Inc. [\[Link\]](#) 1
- [2] J.P. Morgan claims: JPM Coin is a permissioned, shared ledger system that serves as a payment rail and deposit account ledger, enabling participating J.P. Morgan clients to transfer US Dollars held on deposit with J.P. Morgan. JPM Coin facilitates real-time value movement, helping to solve common hurdles of traditional cross-border payments. [\[Link\]](#) 1
- [3] USD Coin is a digital stablecoin that is pegged to the United States dollar and runs on the Ethereum, Stellar, Algorand, Solana, Tron and Hedera Hashgraph system. [\[Link\]](#) 1
- [4] Lipton, A., Sardon, A., Schär, F., & Schüpbach, C. (2020). 11. Stablecoins, Digital Currency, and the Future of Money. In Building the New Economy. [\[Link\]](#) 1
- [5] A digital token backed by fiat currency provides individuals and organizations with a robust and decentralized method of exchanging value while using a familiar accounting unit. [\[Link\]](#) 1
- [6] Kahya A, Krishnamachari B, Yun S. Reducing the Volatility of Cryptocurrencies—A Survey of Stablecoins. arXiv preprint arXiv:2103.01340. 2021 Mar 1. [\[Link\]](#) 1
- [7] Basis was designed to keep prices stable by algorithmically adjusting supply, White Paper: [\[Link\]](#) 1
- [8] Ampleforth running on Ethereum that attempts to incentivize a network of users to maintain a crypto asset with a value equal to the U.S. dollar. The Ampleforth protocol translates price-volatility into supply-volatility. [\[link\]](#) 1