



عنوان ارائه:

بررسی ساختار زنجیره بلوکی رمزارز کاردانو

A Review on Cardano Blockchain System

توسط: علیرضا صادقی نسب

استاد: دکتر وحید رافع

تاریخ ارائه: 1400/10/18

فهرست مطالب

- مقدمه
- الگوریتم اجماع
- مقایسه PoS و PoW
- ساختار لایه‌ای
- آمار و ارقام در تراکنش‌ها و بلاک‌ها

مقدمه

■ انتشار اولیه سکه (ICO)

★ انتشار اولیه کاردانو در چهار مرحله از سپتامبر 2015 تا ژانویه 2017 انجام شد

★ 95 درصد خریداران این سکه اصلیت ژاپنی، 2.56 درصد اصالت کره‌ای و 2.39 درصد اصالت چینی داشتند

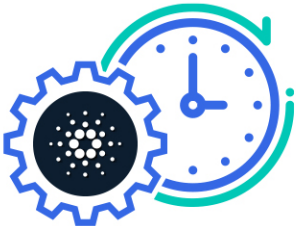
★ در این انتشار، تقریباً 26 میلیارد توکن ADA فروخته شد. تعداد کل توکن‌های ADA برابر 45 میلیارد می‌باشد

★ در پایان ICO، در مجموع حدود 63 میلیون دلار جمع‌آوری شد و قیمت هر واحد ADA به صورت

میانگین 0.00242 دلار قرار داده شد. بعد از ICO نیز مقدار 5,185,414,108 توکن ADA نیز به

شرکت‌های IOHK، Emurgo و Cardano Foundation توزیع شد. باقی توکن‌ها

(13,887,515,354) به عنوان پاداش‌های بلاک در نظر گرفته می‌شوند



مقدمه

■ اطلاعات بیشتر

★ کوچکترین واحد ADA، یک Lovelace نامیده می‌شود. هر یک میلیون Lovelace یک ADA محسوب می‌شود. این اسامی از اولین برنامه‌نویس تاریخ، Ada Lovelace اقتباس گرفته شده‌اند

★ از زبان Haskell برای پیاده‌سازی این رمزارز استفاده شده است، همچنین بعضی از کدهای جدید این رمز ارز در حال حاضر به زبان Rust پیاده‌سازی می‌شوند. از زبان Plutus نیز برای پیاده‌سازی قراردادهای هوشمند استفاده شده است



الگوریتم اجماع

■ الگوریتم اجماع

★ از الگوریتم Ouroboros برای اجماع استفاده می‌شود. Ouroboros یک الگوریتم ایمن مبتنی بر PoS

است که توسط کمپانی IOHK توسعه داده شده است. این الگوریتم 5 نسخه دارد: Classic، BFT،

Genesis، Praos و Hydra. هم‌اکنون در فاز Genesis قرار دارد

★ در مقایسه با بیتکوین می‌توان گفت که به یک اندازه هر دو امن هستند ولی Ouroboros مصرف انرژی بسیار کمتر و عملکرد بهتری دارد. Ouroboros به دارندگان توکنی که ADA خود را در شبکه به اشتراک می‌گذارند و به اطمینان از اجماع شبکه کمک می‌کنند، پاداش می‌دهد

★ این پروتکل از یک تابع رمزنگاری به نام تابع تصادفی قابل تایید (VRF) استفاده می‌کند. VRF در ابتدا

توسط برنده جایزه تورینگ، Silvio Micali که در حال حاضر استاد دانشگاه MIT است و در حال کار بر

روی یک ارز دیجیتال به نام Algorand است، اختراع شد



الگوریتم اجماع

▪ الگوریتم اجماع – ادامه

👤 پردازش Ouroboros به صورت زیر پیش می‌رود:

★ شبکه به طور تصادفی چند گره را انتخاب می‌کند تا فرصت استخراج بلوک‌های جدید را داشته باشد.
این گره‌ها به عنوان slot leaders شناخته می‌شوند



★ زنجیره بلوکی به شکاف‌هایی تقسیم می‌شود که به هر کدام یک دوره یا epoch می‌گویند



الگوریتم اجماع

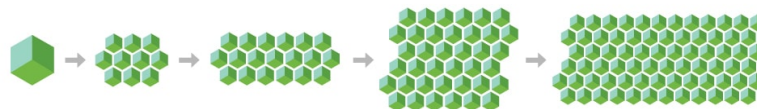
■ الگوریتم اجماع – ادامه

👤 پردازش Ouroboros به صورت زیر پیش می‌رود (ادامه):

★ رهبران slot این توانایی را دارند که epoch خاص خود یا زیر پارتیشن یک epoch را استخراج کنند. هر شرکت‌کننده‌ای که به استخراج یک دوره یا بخشی از یک دوره کمک کند، برای خدمات خود پاداشی دریافت می‌کند



★ یک دوره را می‌توان تا بی‌نهایت تقسیم کرد. این بدان معناست که بلاکچین کاردانو، در تئوری، بی‌نهایت مقیاس پذیر است و امکان اجرای هر تعداد تراکنش مورد نیاز را بدون برخورد با گلوگاه ممکن می‌سازد



الگوریتم اجماع

■ الگوریتم اجماع – ادامه

- ★ اگر یک slot leader به نحوی شانس خود را از دست بدهد و بلوک را انتخاب نکند، فرصت خود را از دست می‌دهد و باید منتظر بماند تا دوباره رهبر slot شوند. خالی ماندن یک یا چند slot (بدون بلوک‌های تولید شده) مشکلی ندارد، اما اکثر بلوک‌ها (حداقل $1 + 50\%$) باید در طول یک دوره تولید شوند
- ★ رهبران slot نقش بسیار مهمی در اکوسیستم دارند. برای احراز صلاحیت، باید 2 درصد از سهام کاردانو را در اختیار داشت. این ذینفعان انتخاب‌کننده نامیده می‌شوند و آن‌ها کسانی هستند که در دوره فعلی رهبران دوره بعدی را انتخاب می‌کنند. هر چه ذینفعان سهم بیشتری در سیستم داشته باشند، شانس بیشتری برای انتخاب شدن به عنوان رهبران slot دارند



الگوریتم اجماع

■ الگوریتم اجماع – ادامه

- ★ اکنون، از آنجایی که رهبران slot قدرت زیادی دارند، باید مراقبت ویژه‌ای انجام شود تا انتخابات تا حد امکان بی‌طرفانه برگزار شود. باید مقداری تصادفی وجود داشته باشد. به همین دلیل است که یک محاسبه چند جانبه (MPC) برای دستیابی به نوعی از تصادفی بودن انجام می‌شود
- ★ در این رویکرد MPC، هر انتخاب‌کننده یک عمل تصادفی به نام "پرتاب سکه" را انجام می‌دهد و پس از آن نتایج خود را با انتخاب‌کنندگان دیگر به اشتراک می‌گذارد. اگر چه نتایج به طور تصادفی توسط هر انتخاب‌کننده ایجاد می‌شود، اما در نهایت بر روی همان مقدار نهایی توافق می‌کنند



الگوریتم اجماع

■ الگوریتم اجماع – ادامه

- ★ بزرگترین مزیت Ouroboros امنیت ریاضی آن در انتخاب اعتبارسنجی بلاکچین است
- ★ Ouroboros یک راه قابل اثبات برای انتخاب تصادفی اعتباردهنده ارائه می‌کند و اطمینان حاصل می‌کند که همه دارندگان توکنی که ADA را در بلاکچین کاردانو به اشتراک می‌گذارند، شانس مناسبی برای استخراج یک بلوک و دریافت پاداش مربوطه دارند
- ★ این امر نیاز به توان محاسباتی بیش از حد رایج در شبکه‌های بلاکچین اثبات کار (PoW) را از بین می‌برد و یک مدل سهامداری منصفانه را تضمین می‌کند که در هیچ پروتکل بلاکچین PoS دیگری یافت نمی‌شود



الگوریتم اجماع

▪ الگوریتم FTS

★ نام این الگوریتم از ساتوشی ناکاموتو، خالق ناشناخته بیتکوین گرفته شده است

★ FTS اساساً یک سکه تصادفی را از سهام انتخاب می‌کند. هر کسی که صاحب آن سکه باشد، رهبر slot می‌شود. به همین سادگی!!

★ به همین دلیل است که هر چه سهام بیشتری در سیستم داشته باشد، شانس بیشتری برای برنده شدن در این قرعه کشی خواهد داشت. رهبران slot همچنین این قدرت را خواهند داشت که نه تنها بلوک‌های موجود در بلاکچین اصلی را انتخاب کنند، بلکه بلاک‌هایی را در سایر بلاکچین‌های داخل اکوسیستم کاردانو نیز انتخاب کنند.

```
+-----+  
SEED --->| FTS |---> ELECTED_SLOT_LEADERS  
+-----+
```

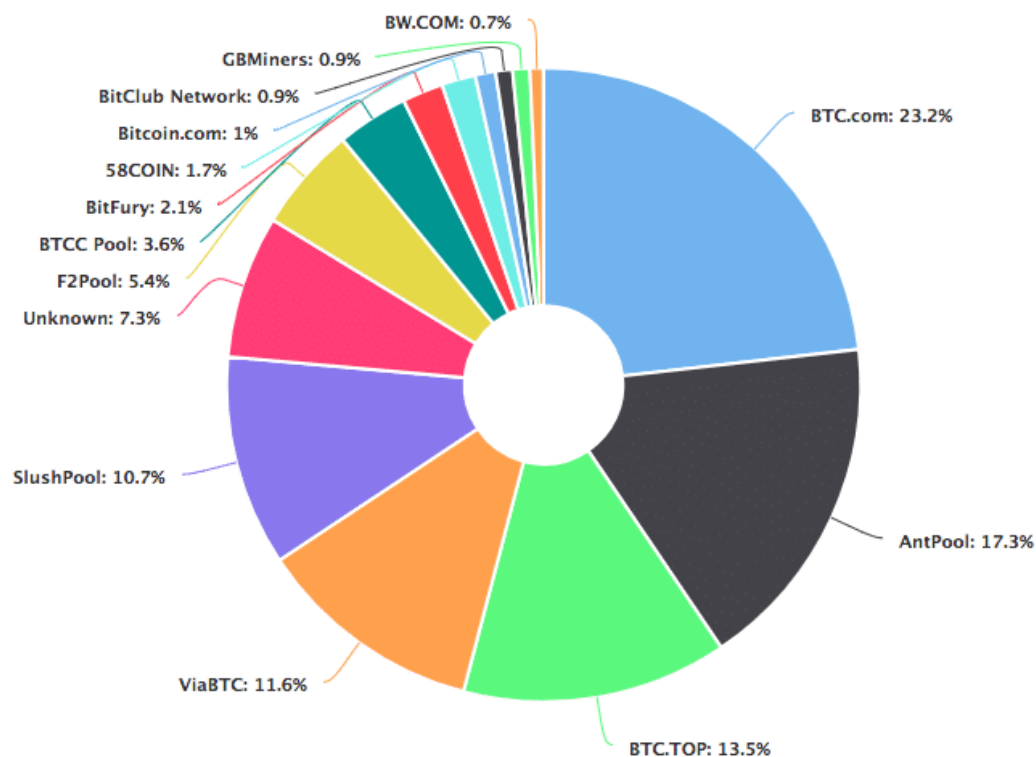
مقایسه PoW و PoS

■ مقایسه PoW و PoS

- * پروتکل PoW به خوبی آزمایش شده و در بسیاری از پروژه‌های ارزهای دیجیتال استفاده می‌شود. حملات DDoS به یک بلاکچین با استفاده از این الگوریتم با فناوری محاسباتی امروزی غیرممکن است. با این حال، هزینه بالای انرژی، افزایش فشار بر محیط زیست، تمرکز بیشتر عملیات استخراج، و توان عملیاتی پایین تراکنش‌ها احتمالاً آن را در درازمدت غیرقابل دوام می‌کند. جوامع به طور فزاینده‌ای نگران هزینه‌های انرژی بالای استخراج بیت‌کوین هستند. برای مثال، چین رسماً تمام این عملیات‌ها را ممنوع کرده است
- * هدف غیرمتمرکز بودن در این پروتکل ممکن است محقق نشود. برای مثال در بیت‌کوین، ۷۵ درصد hashrate بین ۵ استخر تقسیم شده است. در نتیجه از نظر تئوری این امکان وجود دارد که این استخرهای ماین، دست به یکی کرده و مشکل ۵۱ درصد را به وجود آورند

مقایسه PoS و PoW

■ مقایسه PoS و PoW – ادامه



مقایسه PoS و PoW

■ مقایسه PoS و PoW – ادامه

* الگوریتم PoS یک بلاکچین مقیاس‌پذیرتر با توان تراکنش بالاتر را فراهم می‌کند. چند پروژه قبلاً این الگوریتم را اتخاذ کرده‌اند، به عنوان مثال، ارز دیجیتال DASH. با این حال، نسبت به الگوریتم PoW کاملاً غیرمتمرکز از امنیت کمتری برخوردار است

* این امکان وجود دارد که اکثریت سکه‌های شبکه را خریداری کنید، سهامدار انتخاب شوید و تراکنش‌های اشتباه را به عنوان بخشی از یک حمله تأیید کنید. با این حال، اقتصاد بازار یک سوپاپ اطمینان طبیعی برای این کار دارد، زیرا زمانی که فردی بخواهد چنین حجم انبوهی از سکه‌ها را بخرد، قیمت سکه به میزان قابل توجهی افزایش می‌یابد و کار مهاجمان را بسیار دشوارتر می‌کند

* همچنین این امکان وجود دارد که یک سهامدار دغل‌باز شود و تراکنش‌های اشتباه را تأیید کند. پروژه اتریوم، به عنوان بخشی از انتقال برنامه‌ریزی شده خود به PoS، پروتکل «Casper» را طراحی کرده است که در آن چنین سهامداران دغل‌بازی با مصادره ارزهای رمزنگاری شده سهام خود و ممانعت از اشتراک‌گذاری مجدد مجازات می‌شوند

مقایسه PoS و PoW

■ مقایسه PoS و PoW – ادامه



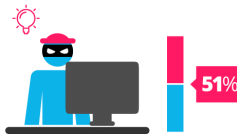
Proof of Work vs **Proof of Stake**



proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



Proof of Stake currencies can be several thousand times more cost effective.

ساختار لایه‌ای

■ ساختار لایه‌ای

★ پلتفرم کاردانو بر روی یک پشته نرم‌افزاری لایه‌لایه بلاک‌چین ساخته می‌شود. این ساختار مقیاس‌پذیری و انعطاف‌پذیری همه رویه‌های تراکنش را بهبود می‌بخشد و نگهداری آن را بسیار آسان‌تر می‌کند. از آنجایی که ساختار لایه‌ای دسترسی بهتری به ویژگی‌های مختلف پلتفرم فراهم می‌کند، فضای بیشتری برای ارتقا از طریق soft fork ها وجود خواهد داشت. soft fork تغییر در پروتکل‌های نرم‌افزار است که در آن، تراکنش‌های معتبر قبلی نامعتبر می‌شوند. بنابراین، به شرکت‌کنندگان اجازه می‌دهد تا انواع تراکنش‌های جدید را اضافه کنند

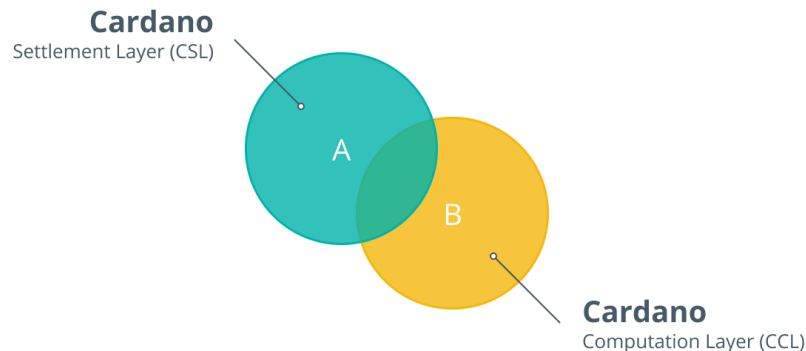
★ لایه Settlement کاردانو برای مدیریت جابه‌جایی ارزش (یا ارز) بین فرستنده و گیرنده طراحی شده است. به عبارت دیگر لایه نشست لایه مسیریابی برای تمامی لایه ها و سیستم های کنترلی است. CSL از دو زبان برنامه نویسی اختصاصی Plutus و Marlowe برای انتقال ارزش و افزایش پشتیبانی از پروتکل شبکه همپوشانی استفاده می‌کند

ساختار لایه‌ای

■ ساختار لایه‌ای – ادامه

★ لایه محاسباتی رگ حیاتی شبکه است. مسئولیت حفظ امنیت زنجیره را بر عهده دارد، به عنوان زمین صفر برای استقرار قراردادهای هوشمند عمل می‌کند و همچنین به هدف خود یعنی چارچوبی که برای اطمینان از انطباق مقررات با حوزه‌های قضایی مختلف طراحی شده است، عمل می‌کند

Two layers of the Cardano blockchain



آمار و ارقام در تراکنش‌ها و بلاک‌ها

▪ ظرفیت تراکنش

* میزان گذردهی میانگین کاردانو، ۱۰ الی ۱۵ تراکنش بر ثانیه می‌باشد. در نسخه Hydra الگوریتم اجماع این رمزارز، با رسیدن به اهداف گذردهی بالا، تاخیر کم و ذخیره کمینه به ازای هر گره، امکان مقیاس‌دهی افقی فراهم شده و شبیه‌سازی‌های اولیه نشان می‌دهد که هر head می‌تواند تا TPS 1000 عملکرد داشته باشد. این مقدار با head 1000 به یک میلیون تراکنش بر ثانیه می‌رسد

▪ مدت زمان تایید تراکنش

* مدت زمان تایید یک تراکنش به عوامل متعددی بستگی دارد و به ازای هر رمزارز، تقریباً متفاوت است. در کاردانو، هر تراکنش به طور متوسط، ۱۰ دقیقه طول می‌کشد تا تایید شود. میزان confirmation هایی که در این رمزارز مورد بررسی قرار می‌گیرد، ۱۵ می‌باشد. در بیتکوین، میزان تاییدیه‌ها ۴ و مدت زمان تایید به طور متوسط، ۴۰ دقیقه می‌باشد. این مقدار برای اتریوم نیز، ۲۰ عدد و ۵ دقیقه می‌باشد

آمار و ارقام در تراکنش‌ها و بلاک‌ها

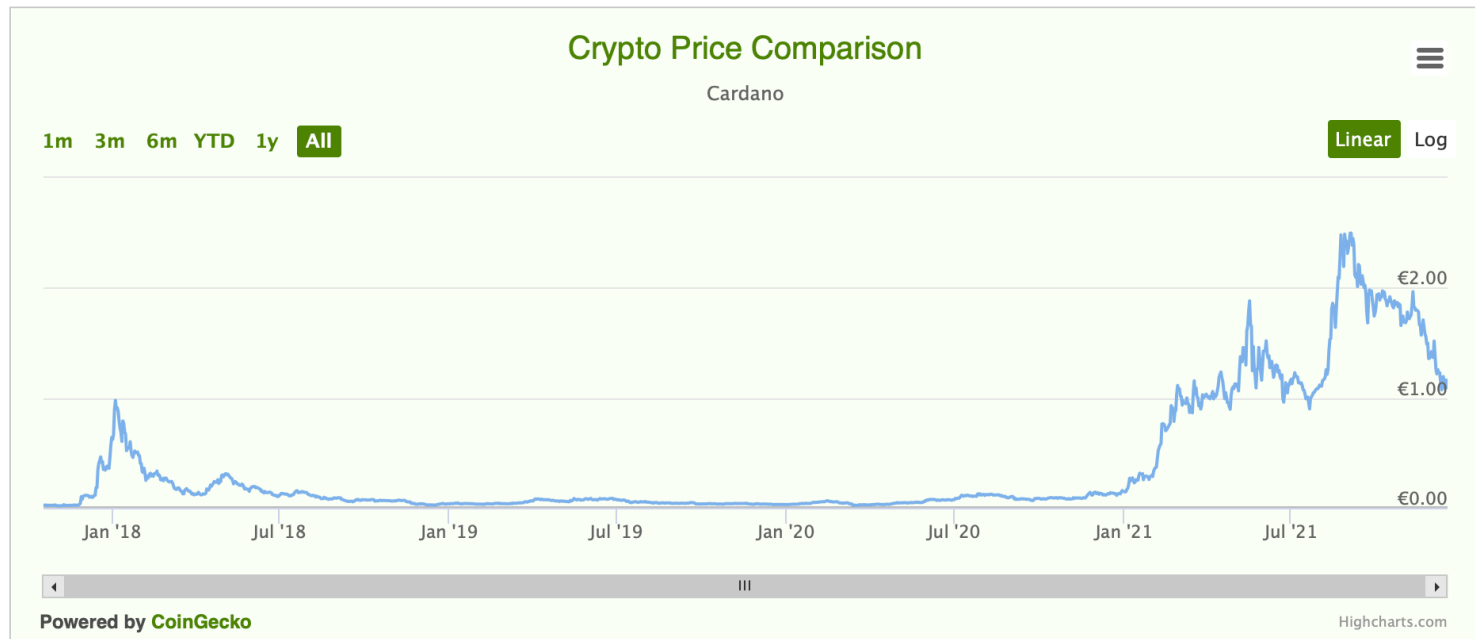
▪ مدت زمان ساخت یک بلاک

* این مدت زمان نیز به ازای هر رمزارز متفاوت است و به ساختارهای آن رمزارز بستگی دارد. در شبکه کاردانو، گره‌های اپراتورهای استخر، وظیفه تولید بلوک‌های جدید را بر عهده دارند. هر اپراتور استخر باید چند جفت کلید تولید کند و خود را به عنوان تولیدکننده بلوک ثبت کند تا بتواند به یک رهبر slot تبدیل شود. زمان به epoch ها و هر epoch به slot ها تقسیم می‌شود. یک slot یک ثانیه طول می‌کشد. در هر دوره slot 432000 وجود دارد، بنابراین epoch 5 روز طول می‌کشد. این امکان وجود دارد که هر چند وقت یک‌بار یک بلوک جدید توسط پارامتر d ایجاد شود. در حال حاضر، مقداری تنظیم شده است که به شبکه اجازه می‌دهد تقریباً هر 20 ثانیه یک بلوک جدید ایجاد کند. این بدان معنی است که تقریباً هر 20 ثانیه یک گره رهبر slot می‌شود و می‌تواند یک بلوک جدید ایجاد کند. در هر epoch، تقریباً 21600 بلوک ایجاد می‌شود. به دلیل تصادفی بودن که در پروتکل پیاده‌سازی می‌شود، در واقع می‌توان بلوک‌های بیشتر یا کمتری ایجاد کرد. اندازه هر بلاک در حال حاضر، 72KB می‌باشد

با تشکر از توجه شما






پیوست

■ نمودار قیمت کاردانو



پیوست

■ انواع کیف پول در رمزارزها

Types of cryptocurrency wallets		
Online	 Pros <ul style="list-style-type: none">+ Free+ Easy to set up+ Easy to access	Cons <ul style="list-style-type: none">- Prone to scams- Limited options- No access private key*
Software	 Pros <ul style="list-style-type: none">+ Free+ Easy to use+ Private key access	Cons <ul style="list-style-type: none">- Less secure- Manual updates
Mobile	 Pros <ul style="list-style-type: none">+ Free+ Easy to set up+ Easy to access	Cons <ul style="list-style-type: none">- Less secure- Limited options- No access private key*
Full node	 Pros <ul style="list-style-type: none">+ Free+ Very safe+ Full control	Cons <ul style="list-style-type: none">- Hard to set up- Requires disk space
Hardware	 Pros <ul style="list-style-type: none">+ Safest option+ Advanced options	Cons <ul style="list-style-type: none">- Expensive- Less accessible

* Exceptions may occur