



Volume 1, Issue 3, 2020

## An overview of the history of block chain and crypto currencies in e-commerce

Mehran Bahram Arjavand <sup>1\*</sup> Ali Kalantari <sup>2</sup> Yeganeh Kharat <sup>3</sup> Fatemeh Kamalinejad <sup>4</sup>

1. BS student in Financial Management, Sari Branch, Islamic Azad University, Sari, Iran.
2. BS student in Business Management, Sari Branch, Islamic Azad University, Sari, Iran.
3. BS student in Financial Management, Sari Branch, Islamic Azad University, Sari, Iran.
4. BS student in Business Management, Sari Branch, Islamic Azad University, Sari, Iran.

### ARTICLE INFORMATION

**Type of Article:**

**Original Research**

**Pages: 65-79**

**Corresponding Author's Info**

**Email:**

mehranbahramarjavand2@gmail.com

**Article history:**

**Received:** 22 May 2020

**Revised:** 08 July 2020

**Accepted:** 01 August 2020

**Published online:** 23 September 2020

**Keywords:**

digital currency, block chain, bit  
coin, decentralization, security

### ABSTRACT

Following the financial crisis and distrust of central institutions in 2002, the world's financial markets were confronted with a new phenomenon called virtual currencies or cryptocurrencies, which rapidly engulfed and transformed the world. Digital currency or cryptocurrency is a special form of digital money that is based on the science of cryptography. The currency code is not managed by any bank and can be used to buy and sell worldwide. These cryptocurrencies are produced in the context of a special network called the Chinese block chain. The Chinese block chain is hailed as a technological innovation that makes it possible to revolutionize the way trade and society interact in today's era. In this article, we are going to explain how cryptocurrencies and the Chinese block chain came into being, their advantages, disadvantages and efficiencies.



This is an open access article under the CC BY license.

© 2020 The Authors.

**How to Cite This Article:** Bahram Arjavand, M & Kalantari, A., Kharat, Y., Kamalinejad, F (2020). "An overview of the history of block chain and crypto currencies in e-commerce" . *Journal of Management, economics and Entrepreneurship* , 1(3): 65-79.



دوره اول، شماره سوم، پاییز ۱۳۹۹

## مروری بر تاریخچه ی بلاک چین و رمزارز ها در تجارت الکترونیک

مهران بهرام ارچاوند<sup>۱\*</sup> علی کلانتری<sup>۲</sup> یگانه خراط<sup>۳</sup> فاطمه کمالی نژاد<sup>۴</sup>

۱ دانشجوی کارشناسی مدیریت مالی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران. mehranbahramarjavad2@gmail.com

۲ دانشجوی کارشناسی مدیریت بازرگانی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

۳ دانشجوی کارشناسی مدیریت مالی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

۴ دانشجوی کارشناسی مدیریت بازرگانی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

### چکیده

در پی بحران مالی و بی اعتمادی به نهادهای مرکزی در سال ۲۰۰۲ بازارهای مالی جهان با پدیده نوینی به نام ارزهای مجازی و یا رمز ارزها مواجه شدند که جهان را به سرعت در بر گرفتند و متحول کردند. ارز دیجیتال یا رمز ارز شکل خاصی از پول دیجیتال است که بر پایه علم رمزنگاری ایجاد شده است. رمز ارزها تحت مدیریت هیچ بانکی نبوده و می توان از آن برای خرید و فروش در سراسر دنیا استفاده کرد. این رمز ارزها در بستر شبکه ی خاصی به نام بلاک چین تولید می شوند بلاک چین به عنوان یک نوآوری تکنولوژیکی مورد ستایش قرار می گیرد که امکان ایجاد انقلابی در نحوه تجارت و تعامل جامعه را در عصر امروزی فراهم می کند. در این مقاله قصد بیان چگونگی به وجود آمدن رمز ارزها و بلاک چین، مزایا، معایب و کارایی های آنها را داریم.

### اطلاعات مقاله

نوع مقاله: علمی - پژوهشی

صفحات: ۶۵-۷۹

اطلاعات نویسنده مسئول

ایمیل:

mehranbahramarjavad2@gmail.com

### سابقه مقاله:

تاریخ دریافت: ۱۳۹۹/۰۴/۲۸

تاریخ ویرایش: ۱۳۹۹/۰۶/۰۱

تاریخ پذیرش: ۱۳۹۹/۰۶/۰۸

تاریخ انتشار: ۱۳۹۹/۰۷/۰۱

واژگان کلیدی: ارز دیجیتال، بلاک

چین، بیت کوین، عدم تمرکز، امنیت

خوانندگان این مجله، اجازه توزیع، ترکیب مجدد، تغییر جزئی و کار روی حاضر به صورت غیرتجاری را دارند.



## مقدمه

در این قسمت، مبانی نظری دربارهٔ بلاکچین و رمز ارزها بررسی می‌شود. بهنکه و همکاران (۲۰۲۰): به این نتیجه رسیدند که بلاکچین، فناوری مفیدی است؛ زیرا به اشتراک‌گذاری داده‌های بیشتر میان اعضای زنجیره تأمین منجر می‌شود. با این حال، شرایط مرزی باید پیش از استفاده از فناوری بلاکچین برآورده شود. این یافته‌ها نشان می‌دهد زنجیره تأمین پیش از استفاده از بلاکچین باید سازمان‌دهی شود. حسین کاکاوند کاست دورس نیکولت چپلتون برت (۲۰۱۷): به این موضوع پی بردند که بلاک چین یک پلتفرم دیجیتالی است که کل تاریخچه را ذخیره و تأیید می‌کند پایگاه داده ای که به عنوان مخزن غیرقابل برگشت و ناپایدار عمل می‌کند بلاک چین به عنوان یک معماری غیرمتمرکز در حال ظهور و الگوی محاسباتی توزیع شده است. جی و همکاران (۲۰۲۰): به این نتیجه رسیدند که پشتیبانی و تحریک توسعه برنامه‌های کاربردی فناوری بلاکچین، به‌عنوان بخشی از استراتژی دیجیتال‌سازی، برای بهبود شفافیت، کارایی، رقابت‌پذیری و پایداری بازار جهانی است.

تپسکات و تپسکات (۲۰۱۶): در مقاله‌ی خود بیان کردند که بلاک چین می‌تواند نه تنها برای ثبت تراکنش‌های مالی، بلکه برای ثبت هر شی با ارزش ذاتی استفاده شود و این مزیت باعث تحول بزرگ دنیای دیجیتال و حتی آثار مختلف می‌گردد. یوان ونگ (۲۰۱۸): بر طبق بیان این محققان همانند دیگران با به اتفاق نظر رسیدن بیان کردند که مزیت اصلی این فناوری در این واقعیت نهفته است که امکان استقرار اکوسیستم‌های مستقل امن، قابل اعتماد و غیرمتمرکز را برای سناریوهای مختلف، به ویژه برای استفاده بهتر از دستگاه‌ها، زیرساخت‌ها و منابع قدیمی فراهم می‌کند. دیلان یاگا پیتر مل نیک رابی کارن اسکارفونه (۲۰۱۸): همانند دیگر محقق‌ها به این نتیجه رسیدند که شبکه‌ی بلاک چین یک شبکه‌ی وسیع و امن و بدون نیاز به واسطه است که عامل به وجود آمدن رمز ارزها نیز است. جیک فرانکن فیلد (۲۰۲۱): براساس مقاله و بیان فرانکن فیلد

طی چند دهه گذشته، فعالیت اقتصادی جهانی به دلیل آزادسازی تجارت و سرمایه‌گذاری، ظهور اقتصادهای نوظهور و پیشرفت در فناوری‌ها به طور قابل توجهی تغییر کرده است (کانو<sup>۱</sup>، ۲۰۱۸). و باعث انقلاب دیجیتال شده است. انقلاب دیجیتال تغییری از فناوری آنالوگ<sup>۲</sup> و الکترونیکی به فناوری دیجیتال است و در حال حاضر در اوج خود قرار دارد. از آنجایی که ما در عصر دیجیتال زندگی می‌کنیم، منطقی است که شکل دیجیتالی پول، یعنی ارز دیجیتال، باید ظاهر شود. ارز دیجیتال به عنوان شکل دیجیتالی پول با کمک تکنیکی به نام رمزنگاری عمل می‌کند. رمزنگاری فرآیندی است که اطلاعات خوانا را به کدهایی تبدیل می‌کند که به هیچ وجه قابل شکستن نیستند. پایه و اساس تمام تراکنش‌های کریپتو<sup>۳</sup> بلاک چین است. بلاک چین تراکنش‌های فردی و مالکیت تمام ارزهای دیجیتال در گردش را ثبت می‌کند و این سیستم توسط به اصطلاح «ماینها»<sup>۴</sup> بلاک چین مدیریت می‌شود که باید تمام تراکنش‌های رخ داده را به روز کنند و از صحت اطلاعات اطمینان حاصل کنند (مونیا میلیوتینوویک<sup>۵</sup>، ۲۰۱۸). محبوبیت فناوری بلاک چین و گستره وسیع کاربرد آن، نتایج تحقیقات مداوم بسیاری در زمینه‌های مختلف عملی و علمی است. اگرچه بلاک چین هنوز جدید و در مرحله آزمایشی است، به عنوان یک راه حل انقلابی در نظر گرفته می‌شود که به نگرانی‌های فناوری مدرن مانند تمرکززدایی، اعتماد، هویت، مالکیت داده‌ها و تصمیمات مبتنی بر داده‌ها رسیدگی می‌کند (النا کارافیلوسکی<sup>۶</sup> آناستاس میشو<sup>۷</sup>، ۲۰۱۷).

## مبانی نظری

<sup>1</sup> Kano

<sup>2</sup>: Analog Technology

<sup>3</sup>: CryptoCurrency

<sup>4</sup>: Miner

<sup>5</sup> Monia Milutinović

<sup>6</sup> Elena Karafiloski

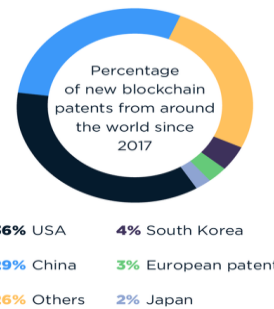
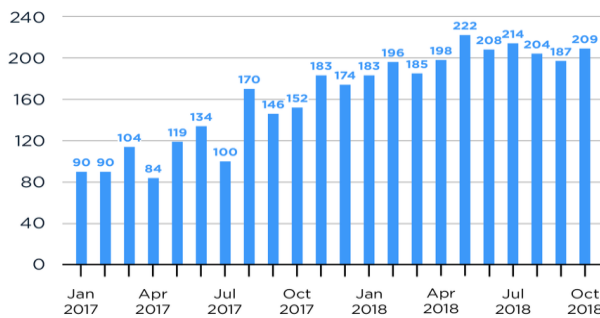
<sup>7</sup> Anastas mishev

فناوری بلاکچین و رمز ارز ها در دنیای دیجیتال صورت نگرفته است بنابر این، این مقاله به دلیل تازگی و عدم وجود مقاله جامع در رابطه با بلاک چین و رمز ارز ها نوشته شده است . که باعث می شود خلأ مطالعاتی موجود از بین برود و موجب غنی شدن منابع علمی موجود در این زمینه شود.

پی میبریم که ارز دیجیتال نوعی رمز ارز دیجیتالی است که انواع مختلفی دارد و تراکنشاتش بر روی بلاک چین ذخیره میشود که باعث به وجود آمدن امنیت زیادی برای تراکنشات می شود و مشکل اعتماد را از بین می برد با این حال همچنان به عنوان ارز رسمی شناخته نمی شوند. با توجه به دانش و اطلاعات نویسندگان، تاکنون، پژوهشی کامل درباره

### Blockchain is becoming more popular despite the bear market

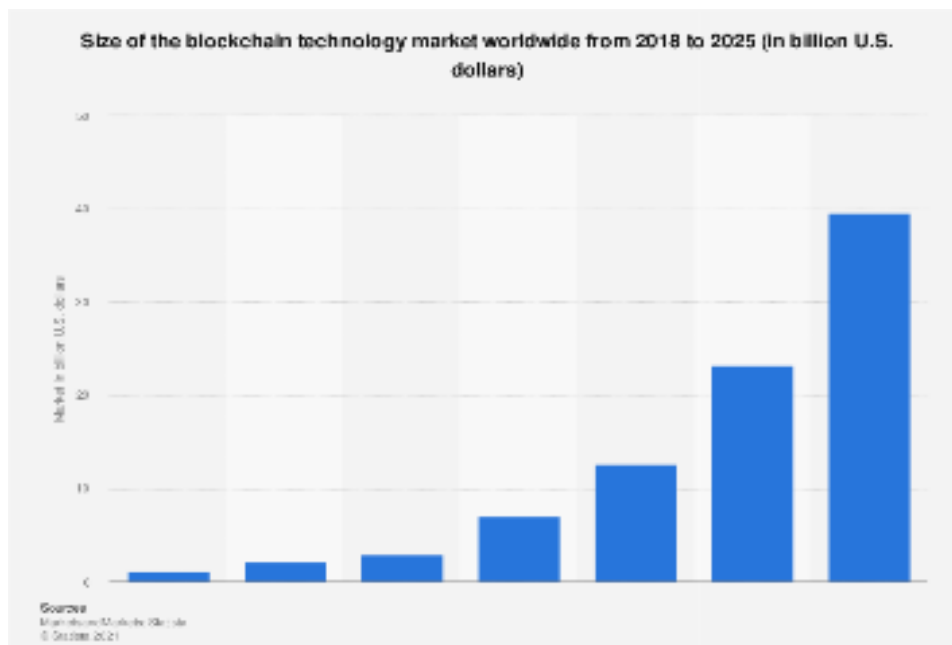
Total number of blockchain patents since 2017



Source: Google Patents



شکل ۱- محبوبیت بلاک چین در بازار نزولی افزایش می یابد



## شکل ۲- محبوبیت بلاک چین و پیش بینی آن از ۲۰۱۸ تا ۲۰۲۵

بدنه

### ۱- بلاک چین

#### ۲- فناوری بلاک چین چیست؟

در سطح اولیه خود، آنها جامعه ای از کاربران را قادر می سازند تا تراکنش ها را در یک دفتر کل مشترک در آن جامعه ثبت کنند، به طوری که تحت عملکرد عادی شبکه بلاک چین، هیچ تراکنش پس از انتشار قابل تغییر نیست. این سند یک نمای فنی سطح بالا از فناوری بلاک چین ارائه می دهد (دیلان یاگا پیتر مل نیک رابی کارن اسکارفونه، ۲۰۱۸).

فناوری بلاک چین از بین بردن هزینه های مضاعف را تضمین می کند. (کتاب مارک پیلینگتون<sup>۱۲</sup>)

### ۳- ساز و کار بلاک چین

این فناوری تراکنش های آنلاین بین طرفین را بدون تکیه بر یک موسسه مالی متمرکز تسهیل می کند (ناکاموتو، ۲۰۰۸). این مفهوم جدید روش های سنتی تبادل ارزش توکن شده بین طرف ها (گره ها) را در یک محیط بی اعتماد و توزیع شده متحول کرده است. بسته به هدف و ظرفیت بلاک چین بکار گرفته شده، چنین تراکنش هایی می توانند برای مبادله دارایی های نامشهود مانند ارزهای دیجیتال، پرداخت حق امتیاز موسیقی، رای دادن یا خرید خانه انجام شوند. در واقع، هر دارایی دیجیتالی را می توان مبادله کرد، مانند توکن های غیر قابل تعویض مانند GIF<sup>۱۳</sup>، آثار هنری یا مقاله. بلاک چین به عنوان زنجیره ای از بلوک های مرتب شده زمانی و رمزنگاری مرتبط تعریف می شود (پرپولی<sup>۱۴</sup> موسو<sup>۱۵</sup> روسانو<sup>۱۶</sup>، ۲۰۱۸).

فناوری بلاک چین (BCT) اطلاعات یکسانی را در گره های مختلف ذخیره می کند و اطلاعات تنها زمانی اضافه می شوند که گره ها به توافق برسند. تراکنش های جدید را می توان اضافه کرد، اما اطلاعات قبلی را نمی توان حذف کرد و تمام

مدت ها قبل از معرفی بیت کوین، بلاک چین یک فناوری دفتر کل توزیع شده بود که در سال ۱۹۹۱ توسط هابر و استورنتتا (۱۹۹۱) توسعه یافته بود. هفده سال بعد، ناکاموتو (۲۰۰۸) اولین مورد استفاده در مقیاس بزرگ و کاربردی از بلاک چین با بیت کوین را پیشنهاد کرد، این ارز دیجیتال بدون واسطه قابل اعتماد کار می کند (ژانگ<sup>۱</sup>، ۲۰۱۹).

فناوری بلاک چین در اصل نامی است که به طراحی زیربنای عملیات دیجیتال داده شده است. خالق بیت کوین هرگز از واژه بلاک چین در وایت پیپر<sup>۲</sup> خود و خواندن آن استفاده نکرد اما بلاک چین باپا به عرصه گذاشتن بیت کوین به وجود آمد (دکتر سیف الدین آموس<sup>۳</sup>، ۲۰۱۶).

بلاک چین ها دفترهای دیجیتالی قابل تشخیص و مقاوم در برابر دستکاری هستند که به صورت توزیع شده (به عنوان مثال، بدون مخزن مرکزی) و معمولاً بدون یک مرجع مرکزی (یعنی بانک، شرکت یا دولت) اجرا می شوند (دیلان یاگا<sup>۴</sup> پیتر مل<sup>۵</sup> نیک رابی کارن اسکارفونه<sup>۶</sup>، ۲۰۱۸).<sup>۸</sup> BCT به عنوان یک فناوری بالقوه مخرب و همه منظوره برای شرکت ها و دولت ها برای حمایت از تبادل اطلاعات و تراکنش هایی که نیاز به احراز هویت و اعتماد دارند، ظهور کرده است (یلی هومو<sup>۹</sup> پارک چوی کو<sup>۱۰</sup> اسمولندر<sup>۱۱</sup>، ۲۰۱۶).

<sup>1</sup> zhang

<sup>2</sup> White Paper

<sup>3</sup> Dr. Saifedean Ammous

<sup>4</sup> Dylan Yaga

<sup>5</sup> Peter Mell

<sup>6</sup> Nik Roby

<sup>7</sup> Karen Scarfone

<sup>8</sup> Blockchain

<sup>9</sup> Yli-Huumo

<sup>10</sup> Ko-Choi Park

<sup>11</sup> Smolander

<sup>12</sup> mark Pilkington book

<sup>13</sup> a lossless format for image files that supports both animated and static images.

<sup>14</sup> Perboli

<sup>15</sup> Musso

<sup>16</sup> Rosano

کند که تراکنش های موجود در بلوک جدید معتبر هستند و توسط اکثر گره ها تایید شده اند. این فرآیند اعتبارسنجی به پروتکلی به نام «مکانیزم اجماع» نیاز دارد که باید توسط همه گره های شرکت کننده دنبال شود. (Proof-of-Stake و PoS<sup>۵</sup>) و (Proof-of-Work (PoW<sup>۶</sup>) رایج ترین مکانیسم ها برای اجماع بلاک چین هستند (سعد<sup>۷</sup> کین<sup>۸</sup> رن<sup>۹</sup> نیانگ<sup>۱۰</sup> محایسن<sup>۱۱</sup>، ۲۰۲۱). اگرچه اثربخشی ثابت شده آنها در اعتبارسنجی بلوک ها، هر دو دارای کاستی هایی هستند. از یک طرف، PoS ممکن است منجر به تمرکز، ناعادلانه و قابلیت اطمینان کمتر شود (نیر<sup>۱۲</sup> سعد و همکاران<sup>۱۳</sup> ۲۰۲۱، ژانگ<sup>۱۴</sup> چان<sup>۱۵</sup>، ۲۰۲۰). برای به روز رسانی زنجیره بلوکی، پروتکل PoS گره اعتبارسنجی را با توجه به سهم آن از سهام تخمین زده شده به عنوان کسری از سکه های متعلق به آن انتخاب می کند که احتمال انتخاب آن را مشخص می کند (روسو<sup>۱۶</sup> صالح<sup>۱۷</sup>، ۲۰۲۱).

هر چه سهام بالاتر باشد، احتمال بیشتری وجود دارد که گره برای ضرب کردن بلوک جدید و دریافت پاداش انتخاب شود. در نتیجه، PoS ممکن است منجر به تمرکز و تمرکز ثروت مانند فرآیند حراج شود (روسو صالح سعد و همکاران<sup>۱۸</sup>، ۲۰۲۱). از سوی دیگر، PoW متکی به داشتن گره هایی برای رقابت محاسباتی در حل یک معمای ریاضی است که حل کردن آن سخت است اما تأیید راه حل آن آسان است. PoW شامل یافتن یک مقدار رشته ای به نام "nonce" است که وقتی با محتویات بلوک و هش<sup>۱۸</sup> بلوک قبلی هش

گره ها را قادر می سازد تا تاریخچه را ردیابی کنند. ذخیره سازی اطلاعات تراکنش در گره های مختلف دفتر کل توزیع شده نامیده می شود. این امر وابستگی به یک بازیگر مرکزی و خطر دستکاری یا خرابی سیستم را کاهش می دهد زیرا همه گره ها اطلاعات کامل را دارند. BCT می تواند برای هرگونه تغییر مالکیت و ذخیره اطلاعات و اسناد مهم مانند گواهی ها، مجوزها، تصمیمات دولتی و قوانین استفاده شود. به طور معمول، اطلاعات ذخیره شده در BCT داده های معاملاتی مانند مالکیت ثبت زمین، گواهی تولد و ازدواج، ثبت وسایل نقلیه، مجوزهای (تجاری)، گواهی های آموزشی، وام های دانشجویی، مزایای اجتماعی و آرا هستند (پال فریمن<sup>۱</sup>، ۲۰۱۵).

BCT دارای پتانسیل ارائه منافع برای دولت و جامعه است و می تواند گام بعدی را در توسعه دولت الکترونیکی ارائه دهد، زیرا آنها هزینه ها و پیچیدگی را کاهش می دهند، فرآیندهای قابل اعتماد مشترک را به اشتراک می گذارند، قابلیت کشف آزمایشات حسابرسی را بهبود می بخشند و از نگهداری سوابق قابل اطمینان، اطمینان می دهند (پال فریمن<sup>۱</sup>، ۲۰۱۵).

هر بلوک یک رکورد تغییرناپذیر از مجموعه ای از تراکنش ها است که توسط گره های شرکت کننده در آن شبکه بلاک چین تعیین و تایید شده است. تغییر ناپذیری با پیوند دادن بلاک ها به صورت متوالی تضمین می شود به طوری که هر بلوک شامل امضا (معروف به هش) بلوک قبلی باشد. بنابراین، تغییر در یک بلوک مستلزم اصلاح تمام بلوک های بعدی است. بقیه بلوک مجموعه ای از تراکنش های بین گره ها را همراه با مهر زمانی ثبت می کند (سینگهال<sup>۲</sup> دهامجا<sup>۳</sup> پاندا<sup>۴</sup>، ۲۰۱۸). هنگامی که یک بلوک قرار قرار است به بلاک چین الحاق شود، مکانیسم اعتبارسنجی خاصی توسط گره ها مورد نیاز است. این مرحله تضمین می

<sup>5</sup> Proof of stake

<sup>6</sup> Proof of work

<sup>7</sup> Saad

<sup>8</sup> Qin

<sup>9</sup> Ren

<sup>10</sup> Nyang

<sup>11</sup> Mohaisen

<sup>12</sup> nayer

<sup>13</sup> saad et al

<sup>14</sup> zhang

<sup>15</sup> chan

<sup>16</sup> Roşu

<sup>17</sup> Saleh

<sup>18</sup> Hash

<sup>1</sup> Palfreyman

<sup>2</sup> Singhal

<sup>3</sup> Dhameja

<sup>4</sup> Panda

(بال<sup>۱۰</sup> رز<sup>۱۱</sup> سابین<sup>۱۲</sup> واسودوان<sup>۱۳</sup>، ۲۰۱۷). PoW بود که در آن به اصطلاح اثبات کار مفید (PoW) توسعه یافت. این ایده شامل حل مسائل ریاضی با پیوستن سختی به سودمندی و در عین حال جلوگیری از استفاده مخرب بلاک چین است. مکانیسم PoW پیش‌بینی شده ما نه تنها به کاهش اتلاف انرژی کمک می‌کند، بلکه مشکلات مربوط به کاربرد بلاک چین را نیز حل می‌کند که برای اکوسیستم آن مفید است. در مورد استفاده خود، ما بر روی PoW تمرکز می‌کنیم تا با معرفی یک PoW جدید که خروجی های مفیدی برای یک بلاک چین، حمل و نقل دریایی ارائه می‌کند، تمرکززدایی شبکه را حفظ کنیم (بال رز سابین واسودوان، ۲۰۱۷).

#### ۵- بلاک‌ها<sup>۱۴</sup> از اجزای جدایی ناپذیر بلاک چین

یک شبکه بلاک چین بدون سرور متمرکز کار می‌کند. تراکنش‌های انجام شده در چنین شبکه‌ای توسط گره‌های غیرمتمرکز (سیستم‌های کاربر) تأیید می‌شوند (ابراهام<sup>۱۵</sup> مخلفی<sup>۱۶</sup>، ۲۰۱۷ ژنگ و همکاران<sup>۱۷</sup>، ۲۰۱۷) و در بلاک‌های به اصطلاح با مهر زمانی ذخیره می‌شوند (گپ و همکاران<sup>۱۸</sup>، ۲۰۱۵ لیاو لین<sup>۱۹</sup>، ۲۰۱۷). محدودیت اندازه بلاک‌ها می‌تواند بین بلاک چین‌های مختلف متفاوت باشد. بلاک‌ها به ترتیب زمانی به هم مرتبط می‌شوند، زیرا هر یک از آنها (به جز اولین بلاک "تولید") حاوی هش رمزنگاری قبلی است، بنابراین یک زنجیره تشکیل می‌دهند (بک و همکاران<sup>۲۰</sup>، ۲۰۱۶ کراسبی و همکاران<sup>۲۱</sup>، ۲۰۱۶). هش بلاک

می‌شود، یک مقدار هش ایجاد می‌شود که دارای تعداد معینی از صفرهای ابتدایی است. سودمندی یافتن یک nonce معتبر به شدت محدود به اهداف اعتبارسنجی بلوک است که از هرگونه استفاده بیشتر حذف شده است (بالدومینوس<sup>۱</sup> و ساعز<sup>۲</sup>، ۲۰۱۹).

#### ۴- مصرف انرژی بلاک چین برای محاسبات و انجام تراکنش‌ها

رقابت شدید در قدرت محاسباتی ناشی از PoW، زنجیره بلوکی را از نظر منابع محاسباتی و انرژی الکتریکی بسیار گران می‌کند (درشر<sup>۳</sup>، ۲۰۱۷). که منجر به اتلاف عظیم منابع و تأثیرات شدید بر محیط‌زیست می‌شود، به‌ویژه که مشکل به تناسب، با استفاده‌کنندگان افزایش می‌یابد (دهیلون<sup>۴</sup> متکالف<sup>۴</sup> (دهیلون<sup>۳</sup> متکالف<sup>۴</sup> (دهیلون<sup>۳</sup> متکالف<sup>۴</sup> هوپر<sup>۵</sup>، ۲۰۱۷). در واقع، پروتکل‌های PoW برای حفظ نرخ ثابت ایجاد بلوک، دشواری مشکل را خود تنظیم می‌کنند. طبق یک مطالعه در سال ۲۰۱۴، کل انرژی مصرف شده توسط کل صنعت استخراج بیت کوین حدود ۰٫۱ تا ۱۰ گیگاوات است در مقایسه با میانگین مصرف برق ایرلند که ۳ گیگاوات<sup>۶</sup> برآورد شده است (درشر<sup>۷</sup>، ۲۰۱۷ ۲۰۱۷ اوادوایر<sup>۸</sup> مالون<sup>۹</sup>، ۲۰۱۴). با این وجود، مکانیسم اجماع فرآیندی ضروری در بلاک چین است و ثابت شده است که یک روش اعتبارسنجی موثر است. بر این اساس، انگیزه این مقاله تصحیح کردن قدرت محاسباتی لازم برای حفظ ویژگی اعتبارسنجی ضروری بلاک چین، برای حل مشکلاتی است که می‌تواند فراتر از یافتن مقادیر هش بی‌معنی کمک کنند. این کار عملکردهای بلاک چین را گسترش می‌دهد و یکی از بدترین کمبودهای آن را به یک مزیت تبدیل می‌کند. در این زمینه، اولین کار مربوط به بهبود

<sup>10</sup> Ball

<sup>11</sup> Rosen

<sup>12</sup> Sabin

<sup>13</sup> Vasudevan

<sup>14</sup> Blocks

<sup>15</sup> Abraham

<sup>16</sup> makhlfy

<sup>17</sup> zheng et al

<sup>18</sup> Gip et al

<sup>19</sup> Lin liao and

<sup>20</sup> Beck et al

<sup>21</sup> Crosby et al

<sup>1</sup> Baldominos

<sup>2</sup> Saez

<sup>3</sup> Dhillon

<sup>4</sup> Metcalf

<sup>5</sup> Hooper

<sup>6</sup> Gigawatt

<sup>7</sup> derscher

<sup>8</sup> Odwier

<sup>9</sup> Malon

بخشی از یک اکوسیستم مبتنی بر فناوری بلاک چین هستند (فنگ<sup>۱</sup> و نتر<sup>۲</sup> باسیوس و همکاران<sup>۳</sup>، ۲۰۲۲).

## ۷- ارزش های دیجیتال (cryptocurrency)

### ۸- رمزارز چیست؟

کریپتوکارنسی یک رسانه غیرمتمرکز مبادله است که از توابع رمزنگاری برای انجام تراکنش های مالی استفاده می کند (دوران<sup>۴</sup>، ۲۰۱۴). ارزش های دیجیتال از فناوری بلاک چین برای برای دستیابی به تمرکززدایی، شفافیت و تغییر ناپذیری استفاده می کنند (معونیر<sup>۵</sup>، ۲۰۱۸).

در بالا، نحوه پیاده سازی فناوری بلاک چین برای ارزش های دیجیتال را مورد بحث قرار داده ایم.

به طور کلی، امنیت ارزش های دیجیتال بر اساس رمزنگاری ساخته شده است، نه توسط افراد و نه بر اساس اعتماد (نارایانان و همکاران<sup>۶</sup>، ۲۰۱۶). به عنوان مثال، بیت کوین از روشی به نام «کریپتوگرافی منحنی بیضی» برای اطمینان از ایمن بودن تراکنش های مربوط به بیت کوین استفاده می کند (Wang et al. ۲۰۱۷). رمزنگاری منحنی بیضی نوعی رمزنگاری با کلید عمومی است که برای اطمینان از امنیت تراکنش ها بر ریاضیات متکی است. هنگامی که کسی تلاش می کند تا طرح رمزگذاری فوق را با زور وحشیانه دور بزند، زمانی که در هر ثانیه ۲۵۰ میلیارد احتمال را امتحان می کند، یک دهم سن جهان طول می کشد تا مطابقت ارزشی پیدا کند (گری بلاک<sup>۷</sup>، ۲۰۱۸). با توجه به استفاده از آن به عنوان عنوان ارز، ارز دیجیتال دارای ویژگی هایی مشابه ارزش های فیات است. دارای عرضه کنترل شده است. اکثر ارزش های

نه تنها داده های ساختاری یک بلوک خاص، بلکه محتوای آن را نیز مانند تراکنش ها در نظر می گیرد.

## ۶- از بلاک چین تا ارزش های دیجیتال

تایید یک مفهوم، مهم در ارزش های دیجیتال است. فقط ماینرها می توانند تراکنش ها را تایید کنند. ماینرها بلوک هایی را به بلاک چین اضافه می کنند. آنها تراکنش های بلوک قبلی را بازبینی می کنند و آن را با هش بلوک قبلی ترکیب می کنند تا هش آن را به دست آورند و سپس هش مشتق شده را در بلوک فعلی ذخیره می کنند. ماینرها در بلاک چین تراکنش ها را می پذیرند، آنها را به عنوان قانونی، علامت گذاری می کنند و در سراسر شبکه پخش می کنند. پس از اینکه ماینر تراکنش را تایید کرد، هر گره باید آن را به پایگاه داده خود اضافه کند. به زبان ساده، به بخشی از بلاک چین تبدیل شده است و ماینرها این کار را برای به دست آوردن توکن های ارزش های دیجیتال، مانند بیت کوین، انجام می دهند. برخلاف بلاک چین، ارزش های دیجیتال با استفاده از توکن ها بر اساس فناوری دفتر کل توزیع شده مرتبط هستند. هر معامله ای که شامل خرید، فروش، سرمایه گذاری و غیره باشد، شامل یک توکن یا زیر توکن بومی بلاک چین است. بلاک چین پلتفرمی است که ارزش دیجیتال را هدایت می کند و فناوری است که به عنوان دفتر کل توزیع شده برای شبکه عمل می کند. شبکه وسیله ای برای تراکنش ایجاد می کند و امکان انتقال ارزش و اطلاعات را فراهم می کند. رمزارزها توکن هایی هستند که در این شبکه ها برای ارسال ارزش و پرداخت برای این تراکنش ها استفاده می شوند. آنها را می توان به عنوان ابزاری در بلاک چین در نظر گرفت و در برخی موارد می تواند به عنوان منابع یا ابزارهای کاربردی نیز عمل کند. در موارد دیگر، از آنها برای دیجیتالی کردن ارزش دارایی ها استفاده می شود. به طور خلاصه، ارزش های دیجیتال

<sup>1</sup> Fang

<sup>2</sup> F., Ventre

<sup>3</sup> C., Basios, M. et al

<sup>4</sup> Doran

<sup>5</sup> Meunier

<sup>6</sup> Narayanan et al

<sup>7</sup> Grayblock



از مقالات از سال ۲۰۱۸ ظاهر شده‌اند که ظهور تجارت ارزهای دیجیتال را به عنوان یک حوزه تحقیقاتی جدید در تجارت مالی نشان می‌دهد. فاصله زمانی نمونه گیری این نظرسنجی از سال ۲۰۱۳ تا ژوئن ۲۰۲۱ می باشد ( فنگ و نتر<sup>۱</sup> باسیوس و همکاران، ۲۰۲۲).

رمزپایه در دسترس بودن حجم ارز خود را محدود می کنند. به عنوان مثال. برای بیت کوین، عرضه به مرور زمان کاهش می یابد و در حدود ۲۱۴۰ به مقدار نهایی خود خواهد رسید (فنگ و نتر<sup>۱</sup> باسیوس و همکاران، ۲۰۲۲).

یکی از مهم‌ترین ویژگی‌های ارزهای رمزنگاری شده، حذف واسطه‌های مؤسسات مالی است (هارویک<sup>۱</sup>، ۲۰۱۶). فقدان "واسطه" هزینه‌های مبادله را برای معامله‌گران کاهش می‌دهد. برای مقایسه، اگر پایگاه داده بانکی هک یا آسیب ببیند، بانک برای بازایی اطلاعات از دست رفته یا به خطر افتاده، به طور کامل به پشتیبان خود متکی خواهد بود. با ارزهای دیجیتال، حتی اگر بخشی از شبکه به خطر بیفتد، بقیه همچنان می‌توانند تراکنش‌ها را به درستی تأیید کنند. رمزارزها همچنین دارای ویژگی مهمی هستند که توسط هیچ مقام مرکزی کنترل نمی‌شوند. (رز<sup>۲</sup>، ۲۰۱۵): ماهیت غیرمتمرکز بلاک چین تضمین می‌کند که ارزهای دیجیتال از نظر تئوری در برابر کنترل و دخالت دولت مصون هستند.

دارایی دیجیتال خالص هر چیزی است که در قالب دیجیتال وجود داشته باشد و حق استفاده از آن را به همراه داشته باشد. در حال حاضر، دارایی‌های دیجیتال شامل اسناد دیجیتال، تصاویر متحرک و غیره است. بازار دارایی‌های دیجیتال در واقع از زمان شروع آن در سال ۲۰۰۹ با اولین دارایی دیجیتال "Bitcoin"<sup>۳</sup> تکامل یافته است. به همین دلیل، ما رمزارز را "اولین دارایی خالص دیجیتال"<sup>۴</sup> می‌نامیم. (کال<sup>۴</sup>، ۲۰۲۰) (فنگ و نتر<sup>۱</sup> باسیوس و همکاران، ۲۰۲۲).

به عنوان یک بازار نوظهور و جهت تحقیق، ارزهای دیجیتال و معاملات ارزهای دیجیتال پیشرفت قابل توجهی داشته‌اند و رشد قابل توجهی در علاقه و فعالیت داشته‌اند (فارل<sup>۵</sup>، ۲۰۱۵). از شکل زیر، مشاهده می‌کنیم که بیش از ۸۵ درصد

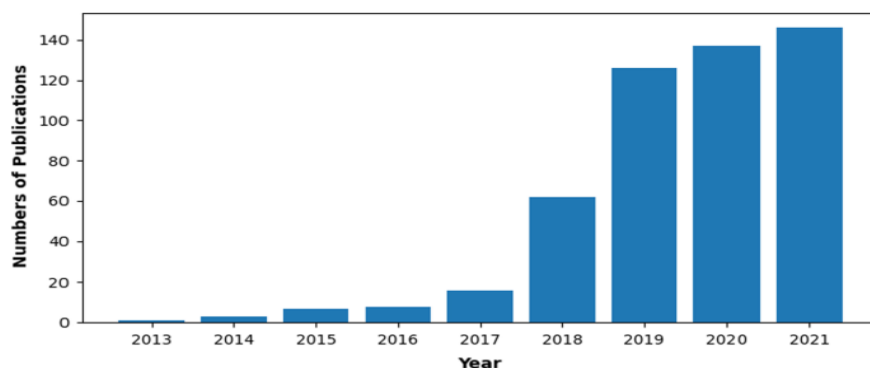
<sup>1</sup> Harwick

<sup>2</sup> Rose

<sup>3</sup> BITCOIN: First of Crypto

<sup>4</sup> Kaal

<sup>5</sup> Farrell



شکل ۳- مقالات منتشر شده در عرصه ارز دیجیتال در طول سال‌های ۲۰۱۳-۲۰۲۱

## ۹- نقطه ی شروع

قدیمی ترین و شناخته شده ترین ارز رمزنگاری شده که به طور گسترده مورد استفاده قرار می گیرد بیت کوین است. این اولین بار در مقاله ای در سال ۲۰۰۸ منتشر شد که با نام ساتوشی ناکاموتو بود - نام مستعاری که برای پنهان کردن هویت خالق استفاده می شود، یا یک فرد یا احتمالاً یک جمع. هویت ساتوشی ناکاموتو تا به امروز یک راز باقی مانده است. نرم افزار متن باز<sup>۱</sup> بیت کوین یک سال بعد منتشر شد و در سال ۲۰۰۹، زمانی که بلوک پیدایش بلاک چین بیت کوین استخراج شد، شبکه راه اندازی شد. بیت کوین از ابتدای پیدایش خود شکوفا شد، رشد اولیه آن توسط برنامه های وب تاریک که معروف ترین آنها وب سایت جاده ابریشم است، انجام شد. ماهیت اساساً ناشناس معاملات و فقدان اقتدار مرکزی، آن را برای تجارت غیرقانونی و تجارت مجرمانه مناسب ساخته است. اما در طول پنج سال گذشته، ارزش بیت کوین تا حد زیادی توسط سفته بازی به جای جنایت هدایت شده است و این ارز به طور فزاینده ای در زمینه های تجاری اصلی استفاده می شود. بیت کوین، یا ارزهای بسیار شبیه به آن، ممکن است به خوبی به بخش اصلی محیط مالی روزمره ما در قرن بیست و یکم تبدیل شوند. این البته تعدادی چالش در مورد مقررات، امنیت و نقش دولت ملی ایجاد می کند (لوک تردینیک ، ۲۰۱۹) (ناکاموتو<sup>۲</sup> ، ۲۰۰۸).

## ۱۰- معاملات بیت کوین و حفظ امنیت آنها

وقتی بیت کوین خرج می کنید، یک شیء فیزیکی را منتقل نمی کنید، بلکه یک قطعه کد را منتقل می کنید که از یک کیف پول دیجیتالی به کیف پول دیجیتالی دیگر منتقل می شود. این تراکنش ها متکی به شبکه های همتا به همتا هستند. به طور معمول، حجم کار توزیع فایل ها در یک شبکه دیجیتال توسط سرورها مدیریت می شود. در شبکه های همتا به همتا حجم کار بین دستگاه های متصل به شبکه توزیع می شود که هر کدام از آنها سهمی از سربار پردازش را می گیرند. در نتیجه، هیچ مرجع واحدی بر آن توزیع وجود ندارد، و هیچ سابقه مرکزی، از معاملاتی که انجام شده است. اما اگر هیچ مرجع مرکزی وجود نداشته باشد، پس وضعیت منحصر به فرد هر بیت کوین چگونه حفظ می شود؟ چه چیزی باعث می شود کسی یک بیت کوین را دو بار خرج نکند؟ این مشکل به عنوان مشکل دوگانه خرج کردن شناخته می شود و با نوآوری واقعی بیت کوین: بلاک چین حل شد (لوک تردینیک ، ۲۰۱۹).

ارزهای رمزپایه مانند بیت کوین بر روی ساختار شبکه همتا به همتا انجام می شوند. هر همتا تاریخچه کاملی از تمام تراکنش ها دارد، بنابراین مانده هر حساب را ثبت می کند. به عنوان مثال، یک تراکنش فایللی است که می گوید " X, A, بیت کوین به B می پردازد" که توسط A با استفاده از کلید خصوصی آن امضا شده است. این رمزنگاری با کلید عمومی اولیه است، اما همچنین بلوک ساختمانی است که ارزهای

<sup>1</sup> Open Source Software

<sup>2</sup> Nakamoto

## ۱۱- انواع ارزهای دیجیتال

موفقیت بیت کوین (نوع اول رمز ارز) مسیری را برای آنچه به نام «آلت کوین<sup>۲</sup>» (نوع دوم رمز ارز) خوانده می شود ایجاد می کند این عبارت به معنای تمام ارزهای رمزپایه ای است که پس از پیروزی به حرکت در می آیند بیت کوین، این سکه<sup>۳</sup> های خود را به عنوان بهترین جایگزین برای بیت کوین می فروشند (فرانکن فیلد<sup>۴</sup>، ۲۰۲۰). انواع مختلفی برای آلتکوین وجود دارد. نوع سوم از رمز «ارز توکن» نامیده می شود برخلاف بیت کوین و آلت کوین، توکن ها قادر به فعال سازی به طور مستقل نیستند. و وابسته به شبکه یک ارز دیجیتال دیگر هستند این معنی می دهد که آنها شبکه ی خاص بلاک چین و یا DLT<sup>۵</sup> خود را ندارند و در عوض بر روی شبکه ی بلاک چین cryptocurrency دیگری اجرا می شوند. (انواع ارزهای دیجیتال: توضیح انواع عمده رمز ارزها<sup>۶</sup>، ۲۰۱۹)

## ۱۲- چند ارز دیجیتال مشابه و بوجود آمده پس از

### بیت کوین

بیت کوین اولین ارز دیجیتالی است که توسط شخص یا گروهی از افراد ناشناس با نام مستعار ساتوشی ناکاموتو ایجاد شد و یک سیستم انتقال پول غیرمتمرکز را با استفاده از بلاک چین ایجاد کرد (ناکاموتو<sup>۷</sup>، ۲۰۰۸). متعاقباً، ارزهای دیجیتال دیگری که معمولاً به آنها آلت کوین گفته می شود، با افزودن قابلیت های بیشتر و ارائه معیارهای طراحی جایگزین ایجاد شدند. اتریوم<sup>۸</sup> توسط Vitalik Buterin در سال ۲۰۱۵ معرفی شد و اولین پلتفرم محاسباتی توزیع شده مبتنی بر بلاک چین است که مفهوم قراردادهای هوشمند<sup>۹</sup> قابل اجرا را در نظر گرفته است (باترین<sup>۹</sup>، ۲۰۱۴). این یکی از

رمزنگاری شده بر اساس آن است. پس از امضا، تراکنش در شبکه پخش می شود. هنگامی که یک همتا تراکنش جدیدی را کشف می کند، بررسی می کند تا مطمئن شود که امضا معتبر است. اگر تأیید معتبر باشد، بلوک به زنجیره اضافه می شود. تمام بلوک های دیگر اضافه شده پس از آن تراکنش را "تأیید" می کنند. به عنوان مثال، اگر یک تراکنش در بلوک ۵۰۲ وجود داشته باشد و طول بلاک چین ۵۰۷ بلاک باشد، به این معنی است که تراکنش دارای ۵ تأییدیه (۵۰۲-۵۰۷) است (جوهار<sup>۱</sup>، ۲۰۱۸).

امنیت بیت کوین از طریق استفاده از یک دفتر کل توزیع شده - بلاک چین - حفظ می شود که تراکنش ها را در سراسر شبکه بیت کوین ثبت می کند و اکنون بیش از ۱۵۰ گیگابایت داده است. هویت منحصر به فرد هر بیت کوین با شفافیت کامل در معاملات تضمین می شود که از طریق آن می توان هر بیت کوین را تا لحظه ایجاد آن ردیابی کرد. تصور کنید که هر اسکناس در گردش با سوابق هر فرد و سازمانی همراه باشد که آن را مدیریت کرده است و نسخه های به روز آن سوابق نیز در کتابخانه ها و توسط افراد در سراسر جهان نگهداری می شود. تصور کنید که هر بار خریدی با استفاده از پول نقد انجام می شود، این سوابق بررسی می شوند تا هر اسکناس را با فردی که به عنوان آخرین مالک آن ثبت شده، تطبیق دهد. اسکناس های جعلی یا دزدیده شده بلافاصله شناسایی می شوند زیرا سوابق با هم جمع نمی شوند. این در اصل نشان می دهد چگونه بلاک چین هویت منحصر به فرد هر بیت کوین در شبکه را ایمن می کند. به دلیل سرعت شبکه های دیجیتال، تطبیق بسیار سریع و البته نه کاملاً آبی انجام می شود - معمولاً حدود ۱۰ دقیقه طول می کشد تا یک تراکنش تأیید شود (لوک تردینیک<sup>۱</sup>، ۲۰۱۹).

<sup>2</sup> ALTCoin

<sup>3</sup> Coin

<sup>4</sup> FRANKENFIELD

<sup>5</sup> Distributed ledger technology (DLT)

<sup>6</sup> Types of cryptocurrencies: explaining the major types of cryptos

<sup>7</sup> Ethereum

<sup>8</sup> Smart Contracts

<sup>9</sup> Buterin

<sup>1</sup> Johar

### نتیجه گیری

ما در این مقاله سعی کردیم یک نگاه کلی از دنیای بلاک چین و رمز ارزها داشته باشیم و نکات کلیدی آنها را بازگو کنیم با خواندن این مقاله به این درک میرسیم که رمز ارزها چگونه پا به عرصه ی وجود گذاشته اند و کارایی آنها برای ما چیست. ما با بررسی دنیای دیجیتال به فرصت های فراوان پیش روی خود پی میبریم. به اتفاق نظر محققین امروزه بابه وجود آمدن بلاک چین فرصت های بسیار زیادی در بستر معاملات دیجیتال به وجود آمده است که منحصر به دارایی خاصی نیست و می تواند حتی عکس و یا فیلم باشد که این فناوری موجب تحول در جهان امروزه شده است که هم می تواند مفید و هم مضر باشد. در این جا هدف بلاک چین ارائه ناشناس بودن، امنیت، حریم خصوصی و شفافیت برای همه کاربران است. با این حال، این ویژگیها چالشها و محدودیت های فنی زیادی را ایجاد می کنند که باید برطرف شوند. فناوری بلاک چین یک فناوری نوپا است که هر روز در حال پیشرفت است. بلاک چین از طریق تکرارهای متعدد توسعه خواهد یافت و به ناچار از آن عبور خواهد کرد (آزمایشات، تکامل، شکست ها و در نهایت پذیرش گسترده).

حال به نظر می رسد ارزهای دیجیتال از مرحله پذیرش اولیه که فناوری های جدید تجربه می کنند گذشته است. موضوعات مورد بررسی در مورد بیت کوین و ارزهای دیجیتال بسیار زیاد است. مطالعات گسترده ای باید انجام شود. جامعه بیت کوین در تلاش است تا از طریق نوآوری و حل مشکلات قدیمی وارد جریان اصلی شود (هافمن<sup>۹</sup>، ۲۰۱۴). توانایی برای ارز دیجیتال برای انجام تراکنش های خرد ممکن است به آن اجازه دهد تا شکاف اقتصادی حالت سنتی را پر کند که ارزهای حمایت شده قادر به حل آن نیستند، اما نیاز به بازار و تحلیل اقتصادی بسیار عمیق تری دارد. همچنین، فناوری

از تاثیرگذارترین و پرکاربردترین ارزهای دیجیتال است که پس از بیت کوین معرفی شده است. لایت کوین<sup>۱</sup> نیز یکی از اولین ارزهای رمزنگاری شده است که از نظر فنی بسیار شبیه بیت کوین است و تنها تفاوت های جزئی با آن دارد (لایت کوین<sup>۲</sup>، ۲۰۱۹). به عنوان مثال، لایت کوین از تابع هش Scrypt به جای SHA-۲۵۶ برای اثبات کار استفاده می کند و تراکنش ها را در بلاک چین چهار برابر سریعتر از بیت کوین ثبت می کند. لایت کوین به عنوان هارد فورک بیت کوین ایجاد می شود و یک بلاک چین مجزا دارد. دش<sup>۳</sup> یکی دیگر از ارزهای دیجیتال است که کاملاً شبیه بیت کوین است و از الگوریتم هش ۱۱X برای اثبات کار استفاده می کند (دیفیلد<sup>۴</sup> دیاز<sup>۵</sup>، ۲۰۱۴). مشابه لایت کوین، دش دارای یک بلاک چین مجزا است که سرعت تراکنش ها ۴ برابر بیشتر از بیت کوین است. Cash-Z یک ارز دیجیتال بسیار امن است که از شواهد دانش صفر استفاده می کند، در نتیجه حریم خصوصی و ناشناس بودن کاربران به طور قابل توجهی افزایش می یابد (هوپ وود و همکاران<sup>۶</sup>، ۲۰۱۸؛ معتمد<sup>۷</sup> بهارک<sup>۸</sup>، ۲۰۱۹).

در تمامی ارزهای رمزنگاری شده ذکر شده، قابلیت انتقال پول، قابلیت اصلی و رایج اصلی است. با استفاده از داده های بلاک چین هر یک از این ارزها، می توان به تراکنش هایی که در آن رخ می دهند دسترسی داشت. در نتیجه می توان معاملات این ارزها را از جنبه های مختلف تحلیل کرد و انواع تحلیل های آماری را روی آنها انجام داد. به طور خاص، امکان بررسی یک شبکه واقعی از تراکنش های مالی برای هر ارز دیجیتال وجود دارد (معتمد بهارک<sup>۸</sup>، ۲۰۱۹).

<sup>1</sup> Lite Coin

<sup>2</sup> Litecoin

<sup>3</sup> Dash

<sup>4</sup> defild

<sup>5</sup> diaz

<sup>6</sup> Hopwood et al

<sup>7</sup> Motamed, A

<sup>8</sup> P., Bahrak

<sup>9</sup> Hofman

زنجیره بلوکی که به عنوان ستون فقرات بیت‌کوین عمل می‌کند، از راه‌های دیگری نیز استفاده می‌کند به اسم قراردادهای هوشمند (هیلمن<sup>۱</sup>، ۲۰۱۶). در نهایت، ارز دیجیتال یک محصولی است که با استفاده از رمزنگاری برای ایجاد یک ویژگی دیجیتال است. توسط انواع مختلف رسانه‌ها سایر اشکال اموال دیجیتال ممکن است مانند موسیقی و ارزهای دیجیتال محبوب شوند. رمزنگاری، علم ریشه‌ای در پشت بیت‌کوین و همه ارزهای دیجیتال، ممکن است مکانیسمی باشد که مرزی برای اختراعات دیجیتال جدید و هیجان‌انگیز به وجود بیاورد (پیتر د دوریس<sup>۲</sup>، ۲۰۱۶). در پایان با بررسی این مقاله به بخشی از جنبه‌های بلاک‌چین و رمز ارزها در دنیای دیجیتال پرداختیم و سعی کردیم یک بررسی شفاف برای خوانندگان این مقاله به وجود بیاوریم.

**ملاحظات اخلاقی:** موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماماً رعایت گردید.

**تعارض منافع:** تدوین این مقاله، فاقد هرگونه تعارض منافی بوده است.

**سهام نویسندگان:** نگارش مقاله تماماً توسط نویسندگان بصورت مشترک و برابر انجام گرفته است.

**تشکر و قدردانی:** از تمام کسانی که ما را در تهیه این مقاله یاری رسانده‌اند، سپاسگزاریم.

**تأمین اعتبار پژوهش:** این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

## منابع و مأخذ

- A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

- Ammous, Saifedean, Blockchain Technology: What is it Good for? (August 8, 2016). Available at SSRN: <https://ssrn.com/abstract=2832751> or <http://dx.doi.org/10.2139/ssrn.2832751>

- Baldominos, Alejandro, and Yago Saez. 2019. "Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain-Based Distributed Deep Learning" Entropy 21, no. 8: 723. <https://doi.org/10.3390/e21080723>

- Behnke, Kay & Janssen, Marijn. (2019). Boundary conditions for traceability in food supply chains using blockchain technology. International Journal of Information Management. 52. [10.1016/j.ijinfomgt.2019.05.025](https://doi.org/10.1016/j.ijinfomgt.2019.05.025).

- DeVries, Peter D. "An analysis of cryptocurrency, bitcoin, and the future." International Journal of Business Management and Commerce 1, no. 2 (2016)

- F. Xavier Olleros and Majlinda Zhegu. Creator/Contributor: Olleros, F. Xavier, editor Zhegu, Majlinda, editor Edward Research handbook on digital transformations / edited by Elgar Publishing Publisher: Cheltenham, UK ; Northampton, MA, USA : Edward Elgar Publishing, [2016]

- Fang, F, Ventre, C, Basios, M, Kanthan, L, Martinez-Rego, D, Wu, F & Li, L 2022, 'Cryptocurrency Trading: A comprehensive Survey', Financial Innovation, vol. 8, 13. <https://doi.org/10.1186/s40854-021-00321-6>

<sup>1</sup> Hilman

<sup>2</sup> Peter D. DeVries

- TY - BOOK AU - Koteska, Bojana AU - Karafiloski, Elena AU - Mishev, Anastas PY - 2017/09/11 SP Blockchain Implementation Quality Challenges: A Literature Review
- Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>
- Singhal, Bikramaditya & Dhameja, Gautam & Panda, Priyansu. (2018). Beginning Blockchain. 10.1007/978-1-4842-3444-0.
- Saad, M., Qin, Z., Ren, K., Nyang, D. H., & Mohaisen, D. (2021). E-PoS: Making Proof-of-Stake Decentralized and Fair. *IEEE Transactions on Parallel and Distributed Systems*, 32(8), 1961-1973. [9312484]. <https://doi.org/10.1109/TPDS.2020.3048853>
- Nair, P. & Dorai, D.. (2021). Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain. 279-283. 10.1109/ICICV50876.2021.9388487.
- Stankevičius, Mikas. (2018). BLOCKCHAIN WITHIN AN ENTERPRISE CONTEXT: technological fit and adoption process. 10.13140/RG.2.2.11724.72327.
- Ball, M., Rosen, A., Sabin, M., & Vasudevan, P.N. (2017). Proofs of Useful Work. *IACR Cryptol. ePrint Arch.*, 2017, 203.
- Hossein Kakavand .Stanford University Nicolette Kost De Sevres Mayer Brown; DLA Piper; University of Montreal - Faculty of Law; NYSE Euronext Bart Chilton DLA Piper Date Written: January 1, 2017 [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2849251](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251)
- 2016. Dan Tapscott and Alex Tapscott. New York: Penguin Random House. 348 pages Nicole Radziwill (Reviewed by)Pages 64-65 , Published online: 18 Jan 2018 <https://doi.org/10.1080/10686967.2018.1404373>
- Fantazzini D, Calabrese R. Crypto Exchanges and Credit Risk: Modeling and Forecasting the Probability of Closure. *Journal of Risk and Financial Management*. 2021; 14(11):516. <https://doi.org/10.3390/jrfm14110516>
- Farrell, Ryan. "An Analysis of the Cryptocurrency Industry." (2015). *Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey* by Sumaira Johar 1,\*ORCID,Naveed Ahmad 1,Warda Asher 1,Haitham Cruickshank 2 andAmad Durrani
- G. Perboli, S. Musso and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," in *IEEE Access*, vol. 6, pp. 62018-62028, 2018, doi: 10.1109/ACCESS.2018.2875782.
- Harwick, Cameron. (2017). Cryptocurrency and the problem of intermediation. 20. 569-588.
- Hileman, G. (2016, January 28). State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass. Retrieved from Coindesk Website: <http://www.coindesk.com/state-of-bitcoin-blockchain-2016/>
- Hofman, A. (2014, March 6). The Dawn of the National Currency – An Exploration of Country-Based Cryptocurrencies. Retrieved from Bitcoin Magazine Website: <https://bitcoinmagazine.com/articles/dawnnational-currency-exploration-country-based-cryptocurrencies-1394146138>
- Huumo, Deokyoong Ko, Sujin Choi ,Sooyong Park ,Kari Smolander Where Is Current Research on Blockchain Technology?—A Systematic Review , Jesse Yli-Published: October 3, 2016 <https://doi.org/10.1371/journal.pone.0163477>
- Monia Milutinovic, (2018), Cryptocurrency, *Ekonomika, Journal for Economic Theory and Practice and Social Issues*, 64,

- Roşu, Ioanid and Fahad Saleh. "Evolution of Shares in a Proof-of-Stake Cryptocurrency." *Manag. Sci.* 67 (2021)
- O'Dwyer, Karl J. and Malone, David (2014) Bitcoin Mining and its Energy Footprint. In: Proceedings of the 25th Joint IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)
- Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress.
- Lin, I.C. and Liao, T.C. (2017) A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, 19
- R. Beck, J. Stenum Czepluch, N. Lollike, S. Malone Blockchain – The gateway to trust-free cryptographic transactions 24th European Conference on Information Systems, ECIS 2016 (2016)
- Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., 2016. *Blockchain technology: beyond bitcoin*. *Appl. Innovation* 2,.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University Press.
- Richmond, S. "Ellen Rose, "On Reflection: An Essay on Technology, Education, and the Status of Thought in the Twenty-First Century."". *Philosophy in Review*, Vol. 35, no. 1, Feb. 2015, pp. 38-40, <https://journals.uvic.ca/index.php/pir/article/view/13379>.
- Vikram Dhillon, David Metcalf, und Max Hooper (2017), *Blockchain Enabled Applications, Understand the Blockchain Ecosystem and How to Make it Work for You* Fachbuch Buch. Softcover 2017, Bibliographie.
- Tredinnick, Luke. "Cryptocurrencies and the Blockchain." *Business Information Review* 36, no. 1 (March 2019) <https://doi.org/10.1177/0266382119836314>.
- Internet of Things, Artificial Intelligence and Blockchain Technology :edited by R.Lakshmana Kumar, Yichuan Wang, T. Poongodi, Agbotiname Lucky Imoize
- Ethereum White Paper A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM By Vitalik Buterin 2014
- Motamed, A.P., Bahrak, B. Quantitative analysis of cryptocurrencies transaction graph. *Appl Netw Sci* 4, 131 (2019). <https://doi.org/10.1007/s41109-019-0249-6>
- INVESTO PEDIA Cryptocurrency . By JAKE FRANKENFIELD Updated January 11, 2022. Reviewed by ETHAN VERA . Fact checked by VIKKI VELASQUEZ <https://www.investopedia.com/terms/c/cryptocurrency.asp>
- P. Wang, W. Zhang, X. Li, D. Shen Is cryptocurrency a hedge or a safe haven for international indices? A comprehensive and dynamic perspective *Finance Res. Lett.*, 31 (2019),
- Article Source: Where Is Current Research on Blockchain Technology?—A Systematic Review Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE* 11(10): e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- Palfreyman, J. (2015). *Blockchain for government?* Retrieved from <https://www.ibm.com/blogs/insights-on-business/government/blockchain-for-government/>

NIST Interagency/Internal Report (NISTIR),  
National Institute of Standards and Technology,  
Gaithersburg, MD, [online],  
<https://doi.org/10.6028/NIST.IR.8202>.

Book.In englischer Sprache APRESS L.P..  
ISBN 978-1-4842-3080-0

- Yaga, D. , Mell, P. , Roby, N. and Scarfone, K.  
(2018), Blockchain Technology Overview,