International Journal of Multidisciplinary Trends

E-ISSN: 2709-9369
P-ISSN: 2709-9350
www.multisubjectjournal.com
IJMT 2021; 3(1): 34-37
Received: 13-12-2020
Accepted: 16-01-2021

روهید شکورزاده
دانشجو دیپارتمنت تکنالوژی معلوماتی
دانشکده کمپیوتر ساینس
دانشگاه پروان، افغانستان

Corresponding Author:
روهید شکورزاده
دانشجو دیپارتمنت تکنالوژی معلوماتی
دانشکده کمپیوتر ساینس
دانشگاه پروان، افغانستان

چین، فناوری رو به رشد - سروی‌بلاک

روهید شکورزاده

چکیده
این مقاله در باره بلاک‌چین به پژوهش می پردازد. بلاک‌چین یا رنسانس پول ، پروتکلی که همراه با ارز دیجیتالی بیت‌کوین یکجا به جهان عرضه شد، این فناوری پشتوانه‌ای نزدیک به دو هزار ارز دیجیتالی کنونی هست، که تنها امروز 16.5میلیون بیت‌کوین در سراسر جهان مبادله می‌شود، فناوری بلاک‌چین با قدرت و سیستم غیرقابل ردیابی، به پروژه‌های در حال کار اکثر شرکت‌ها و غول‌های فناوری دنیا مبدل شده است. به ذکر هست که می‌توان از این فناوری در انتخابات افغانستان نیز استفاده کرد. در این مقاله از میتود تحقیق کتابخانه‌ای و دیگر مقاله های علمی استفاده شده و برای دانشجویان کمپیوتر ساینس و علاقمندان ارز های دیجیتالی مناسب هست. بلاک‌چین از فناوری های قدرتمند بشمار رفته و من آنرا در مورد سیستم انتخابات الکترونیکی مناسب یافتم، کسانی که میخواهند در باره (بلاک‌چین و انتخابات الکترونیکی) تحقیق بکنند، این مقاله مناسب آنها هست.

واژگان کلیدی: بلاک‌چین، ارز دیجیتالی، بیت‌کوین، تراکنش، رمزنگاری، عدم دخالت

مقدمه
فناوری بلاک‌چین (Blockchain) امروزه در حال گسترش سریع هست، از ارزهای دیجیتالی گرفته تا خدمات بیمه و انتخابات، صحت و ادویه، عصر جدید شفافیت و سهولت را بمیان آورده است، بلاک‌چین یک فناوری با امنیت فوق‌العاده و بدون رهبری مرکزی هست [1]، اطلاعات بلاک‌چین غیر قابل ردیابی و تقریباً غیر قابل هک شدن هستند، نظریه‌های اولیه در مورد رمزگذاری بلاک-های اطلاعات توسط استوارت هابر (Stuart Haber) و سکات استورنیتا (Scott Stornetta) در سال 1991 م. بوجود آمد و به تعقیب آن بایر (Bayer)، استوارت و استورنیتا در سال 1992 م. درخت مرکل (چندین بلاک بهم پیوسته) را دیزاین کردند، اما اولین بلاک‌چین در سال 2008 م. توسط شخصی یا گروهی به اسم ساتوشی ناکاموتو (Satoshi Nakamoto) ساخته شد و به تعقیب آن ناکاموتو از این دیزاین منحیث یک هسته مرکزی برای ساخت بیت‌کوین (Bitcoin) استفاده کرد [2]. این فناوری ساختار ارزهای مشهور دیجیتالی نظیر بیت‌کوین (سیستم ارز الکترونیکی یک به یک) را تشکیل می‌دهد [3]، ارزی با نوسانات بسیار زیاد که مارکیت های بزرگ جهانی را تحت تاثیر قرار داده هست. اما ساختار بلاک‌چین چگونه هست و سازنده آن کیست؟ چرا بلاک‌چین قدرتمند هست؟ و چگونه می‌توان از بلاک‌چین در عرصه‌های دیگر استفاده کرد؟
این مقاله پژوهشی کتابخانه‌ای بوده و از منابع مختلف خارجی (ژورنال‌های انگلیسی زبان) تهیه شده و در صدد یافتن پاسخ به سوالات فوق هست.
متن:
با به وجود آمدن بیت‌کوین (ارز دیجیتالی)، در سال 2008 م. توسط ساتوشی ناکاموتو، یک پروتکل جالب به اسم بلاک‌چین هم به معرفی گرفته شد که منحیث هسته اصلی بیت‌کوین کار می-کرد، این پروتکل با منبع باز (Open Source) در اختیار همه قرار داده شد.

1. ساختار:
بلاک‌چین یک کتابخانه (Ledger) نامتمرکز، توزیع شده و اغلب عمومی هست که سابقه (Record) تراکنش‌های (معاملات) بانکی را نگه می‌دارد [4]، این پروتکل به افراد اجازه می‌دهد بدون دخالت شخص ثالث (Third Party)، معاملات بانکی خود را سریع، مطمین و به قیمت ارزان انجام دهند، ساختار بلاک‌چین به افراد اجازه نمی‌دهد تا یک مقدار پول را دوبار یا بیشتر (Double Spending)

توسط کلیدهای محرمانه رمزگذاری می‌شود، که تنها توسط احمد قابل کدگشایی هست، حالا محمود مطمین هست که این پیام فقط توسط احمد دیده خواهد شد، اگر فرضاً کسی دیگر به این پیام دسترسی پیدا کند، پیام را باز کرده نمی‌تواند، چرا که فقط توسط کلید خصوصی احمد و محمود نشانه‌گذاری شده است. با استفاده از این دو عملکرد، پ.ک.ای یک سیستم با امنیت خیلی خوب و با اطمینان را شکل می‌دهد. مشهورترین الگوریتم‌های پ.ک.ای: ر.س.ا(RSA) و ای.سی.اس.دی.ا (ECSDA) هست و بیت‌کوین از الگوریتم دومی استفاده می‌کند.

5. هشینگ (Hashing):

هشینگ یکی از عمکردهای مهم الگوریتم پ.ک.ای هست، با استفاده از این عملکرد، دیتای با اندازه دلخواه (Arbitrary size) به دیتای با اندازه ثابت (Fixed size)، تبدیل می‌شود، مانند:

(Message... From: Ahmad, To: Mahmoud, Msg: I send you 100 Afghanis towards the price of your book+100Af)

این پیام احمد هست که بعد از عملیه هش به پیام ذیل تبدیل می-شود:

(100101010 xx... 01010) (32byte hash)

بیت‌کوین از هش (SHA-256) استفاده می‌کند، که خروجی دیتا را بصورت هش سی و دو بایتی (32 byte) نمایش می‌دهد. اگر پیام تغییر کند، قیمت هش نیز تغییر می‌کند، که در آن صورت پیام قابل بازسازی نخواهد بود، قیمت هش یک بلاک نظر به بلاک-های قبلی تعیین می‌شود و در صورتی که شما هش یک بلاک را تغییر بدهید مجبور به تغییر این قیمت در سراسر بلاک‌چین هستید، که یک کار تقریباً غیرممکن هست.

6. ماینینگ (Mining):

زمانی که احمد به محمود پول می‌فرستد، پیام او تنها به محمود نه، بل در کل کمپیوترهای متصل به شبکه توزیع می‌شود، بعضی از این کمپیوترها به نام ماینر (Miner) یاد می‌شوند، هر ماینر قسمتی از سافت‌ویر (Software) مورد نیاز برای ماینینگ را انجام می‌دهد. اما عملیه ماینینگ چیست؟

7. عملیه ماینینگ (Mining Process):

به هر ماینر در شبکه انتظار می‌رود که تا پیام‌های زیادی را از فروشنده‌های مختلف دریافت بکند (پیام احمد یکی از این-هاست)، کاری که ماینر می‌کند، این است که این پیام‌ها را در یک بلاک واحد یکجا بسازد [9]، بعد از یکجا کردن، ماینر یک هش برای این بلاک تشکیل می‌دهد، ضمناً هر بلاک مهر زمانی (Time Stamp) می‌خورد، و کسی قادر به تغییر آن نیست، در صورتی که مهر زمانی تغییر کند، قیمت هش نیز تغییر می-کند، که بلاک فوق را بی اعتبار می‌سازد.

8. بلاک‌های زنجیرشده (Chaining Blocks):

بلاک‌ی که قبلاً توسط ماینر بوجود آمد، هش بلاک قبلی را در خود دارد، که با این هش به آن بلاک وصل می‌شود و این پروسه ادامه می‌یابد و همین‌طور بلاک‌ها به زنجیره اصلی اضافه می‌شوند، که در کل بلاک‌چین را تشکیل می‌دهند.

به مصرف برسانند، هیچ سازمان دولتی و یا حکومتی نظارت بر معاملات بانکی ندارد [5]، سرور بلاک‌چین شبکه خودگران یک به یک و سرور تایم استمپینگ (Timestamping) توزیع شده دارد، معاملات ارزی شما از طریق کلید عمومی (Public Key) در انظار همگان هست و در واقع بلاک‌های حاوی معاملات بانکی در کل سرور وجود دارد و مانع ایجاد مصرف مضاعف یا دوبرابر می‌شود.

2. بلاک (Block):

هر بلاک حاوی دسته‌ای از معاملات یا تراکنش‌های معتبری که کودگذاری و هش (Hash) شده هستند، می‌باشد و این بلاک‌ها درون درخت مرکل قرار دارند، همچنان هر بلاک دارای هش رمزگذاری شده بلاک قبلی هست، که بلاک فعلی را به بلاک قبلی وصل می‌سازد و این پروسه یک زنجیره را به وجود می-آورد که همه بلاک‌ها به آن متصل هست [6]. این زنجیره بنام بلاک‌چین یاد می‌شود و در واقع حاوی همه تراکنش‌های موجود در جهان هست.

رمزنگاری کلید عمومی یا (Public Key Cryptography): پ.ک.ای که هم چنان بنام رمزنگاری نامتقارن یاد می‌شود، شیوه رمزنگاری‌ی هست که از دو کلید (خصوصی و عمومی) برای رمزنگاری استفاده می‌کند، کلید یک رشته دراز اعداد باینری هست مانند (8fd1f12b-e79e-46d0-926a-2739066ffc9f)، کلید عمومی همانطوری که از نامش پیداست، عمومی بوده و در انظار همگان هست، برعکس کلید مخفی فقط در اختیار یک نفر هست و شدیداً توصیه می‌شود که آنرا فراموش نکنید. پ.ک.ای از طریق میکانیزم کدگذاری/کدگشایی وظیفه شناسایی (Authentication) و پوشیده‌گی پیام (Message Privacy) را انجام می-دهد، که در ذیل هریک به معرفی گرفته می‌شود [7].

3. شناسایی (Authentication):

در نظر بگیرید که احمد میخواهد به محمود به مقدار 100 افغانی پول بفرستد، و کتاب‌ی انلاین را از او خریداری کند، این پول باید دقیقاً محمود برسد، و احمد هم از رسید پول مطمین شود، اما چگونه؟

در قدم اول، زمانی که احمد می‌خواهد پول بفرستد، کلید عمومی و خصوصی احمد یکجا بوجود می‌آید، احمد یک پیام ایجاد می‌کند که شامل: کلید عمومی احمد، کلید عمومی محمود و مقدار 100 افغانی هست، یک پیام کوتاه "من می‌خواهم کتاب را از شما خریداری کنم"، نیز به این مجموعه اضافه می‌شود، اکنون این پیام با کلید خصوصی احمد امضا گذاری می‌شود و زمانی که محمود این پیام را دریافت می‌کند، با استفاده از الگوریتم شناسایی امضا پ.ک.ای و کلید عمومی احمد مطمین می‌شود این پیام مربوط به احمد هست [8]. این‌ها تمام مراحل شناسایی توسط الگوریتم پ.ک.ای هست.

4. پوشیده‌گی پیام (Message Privacy):

زمانی که پول با پیام یکجا به محمود رسید، او می‌خواهد آدرس انترنتی کتاب الکترونیکی اش را به احمد بفرستد، لذا محمود یک پیام با متن "این آدرس کتاب درخواستی شما هست". و کلید عمومی احمد که به او رسیده امضا می‌کند، و همچنان این پیام

2. ثبت و نگه‌داری از اسناد: می‌توان اسناد و سوابق را به راحتی ذخیره کرد.
3. اوراق بهادار: اوراق بهادار یا سهام شرکت‌ها، به خوبی حفظ می‌شوند.
4. انترنت اشیا (Internet of Things): انترنت اشیا و بلاک‌چین، لازم و ملزوم یکدیگر شده‌اند.
5. روی بیمه، بانکداری و طبابت پروژه‌های مختلف با ساختار بلاک‌چین در جریان هست [12].
6. ایستگاه‌های شارژ موترهای برقی: چند صد عدد از این ایستگاه‌ها در کلیفرونیا با فناوری بلاک‌چین مجهز اند.
7. مدیریت زنجیره مارکیت‌ها: می‌توان از این فناوری در عیب‌یابی کالاهای یک شرکت، از زمان تولید تا مصرف استفاده کرد.
8. مسایل حقوقی: همه کشورهای عضو شورای امنیت، در حال بررسی این فناوری، برای تطبیق قوانین و برگزاری انتخابات شفاف در کشورهای شان هستند [13].
9. غول فناوری ای.ب.ام (IBM) و سیستم یونین پی چین (UnionPay)، در حال ایجاد این فناوری در سیستم ابری (Cloud) خود هستند [14].

سرمایه گذاری روی بیت‌کوین در سال 2013 م. 29 ام ماه می، چیزی در حدود 1,457,815,292$ بوده هست.
ضمناً گزارش مجمع جهانی اقتصاد از سپتامبر 2015 پیش بینی کرده که تا سال 2025، ده درصد تولید ناخالص داخلی جهان بروی تکنالوژی بلاک‌چین ذخیره خواهد شد .
در پهلوی این همه موارد و از آن جای که پروسه انتخابات در افغانستان، یک پروسه جنجالی و دوامدار هست، می‌توان با ایجاد یک سرور بلاک‌چین شخصی افغانستان و تذکره الکترونیکی، این پروسه را به شفافیت و بهره دهی بالا رساند، انتخابات می‌شود که تنها در عرض یک روز اجرا شده و نتایج آن فقط در عرض چند ساعت اعلان شود، با امنیت بلاک‌چین دیگر امکان رای تقلبی نیست و اعلان نتایج هم چندین ماه در پی نخواهد گرفت، اما ایجاد چنین سرور نیاز به سرمایه‌گذاری و تیم متخصص دارد، که البته با درنظر گرفتن نواقص بوجود آمده از انتخابات کاغذی خیلی بهتر هست، لازم هست تا یکبار روی این فناوری سرمایه‌گذاری شود و نتایج آن در بهبودی افغانستان سهم بزرگی خواهد داشت، لازم هست تحقیق روی این موضوع (بلاک‌چین و انتخابات افغانستان) صورت بگیرد و نتایج آن با دولت افغانستان شریک ساخته شود، تا یک معضل بزرگ دیگر را توسط تکنالوژی و فناوری بتوانیم حل کنیم.

نتیجه گیری

فناوری بلاک‌چین که همزمان با روی‌کار آمدن ارز دیجیتالی بیت‌کوین عرضه شد، یک پروتکل قوی در امر مبادلات ارزی در سراسر جهان می‌باشد، بلاک‌چین تراکنش‌ها را غیرقابل ردیابی ساخته و آنرا از دسترسی غیرمجاز نگه‌می‌دارد، با روی کار آمدن این فناوری تراکنش‌های ارزی یک جهش فوق-العاده بسوی نیرومندی داشته و ثبت این تراکنش‌ها را اسان ساخته هست. فناوری بلاک‌چین امروزه در ساحات مختلف قابلیت استفاده را دارا بوده و شرکت‌ها ، سازمان‌ها و حکومت-های مختلف از این فناوری در موارد جداگانه استفاده می‌کنند. شما می‌توانید در اکثر سایت‌های فروش اجناس، رستورانت‌ها،

9. اثبات کار (Proof of Work):
زمانی که تمام تراکنش‌ها مهر زمانی خورده‌اند، نیاز هست که یک سرور تایم استامپینگ توزیع شده در کل شبکه اضافه شود، این اضافه کاری بنام الگوریتم اثبات کار یاد می‌شود [10]. و یک عنصر جدید به بلاک اضافه می‌شود که بنام نانس (Nonce) یاد می‌شود، که هر دو در پایین توضیح داده می‌شوند.

10. نانس:
هش هر بلاک یک معیار خاص دارد، مانند: هش بلاک سوم قسمی هست که چهار عدد شروعی آن باید صفر باشند (00001010001xxx)، این معیار بنام نانس یاد می‌شود، حالا ماینر عملیه هش را از عدد صفر آغاز می‌کند و همین‌طور به هش اضافه می‌کند تا به معیار فوق برسد، قابل ذکر هست که عملیه هش بصورت تصادفی بوده و کسی نمی‌تواند هش دلخواه را به وجود بی‌آورد، و این عملیه توسط دستگاه‌های قوی با سرعت بالا (چند تریلیون هش در یک ثانیه) انجام می‌شود، زمان متوسط برای تولید یک بلاک در سیستم بیت‌کوین 10 دقیقه هست [11]، زمانی که ماینر موفق به تولید بلاک می‌شود، این بلاک در سیستم رها می‌شود که اخرین بلاک زنجیره را تشکیل می‌دهد. چندین ماینر همزمان کوشش می‌کنند تا بلاک معتبر را تشکیل بدهند، و سیستم به اولین نفر موفق بیت‌کوین (در حدود 12.5بیت‌کوین) جایزه می‌دهد. اگر چندین ماینر همزمان موفق با ساخت چندین بلاک معتبر شده‌اند، سیستم فقط درازترین زنجیره ایجاد شده را می‌پذیرد. این الگوریتم فوق بنام الگوریتم اثبات کار یاد می‌شود و ناگفته نباید گذاشت که چندین الگوریتم دیگر نظیر اثبات موجودی (Proof of Stock) نیز وجود دارند.

11. چرا بلاک‌چین قدرتمند هست؟
زمانی که به کسی بخواهید پول بفرستید، از او تقاضای کلید عمومی‌اش را می‌کند، این کلید می‌تواند مستعار باشد و وابسته بودن این کلید عمومی به شخص مورد نظر در هیچ جای ثبت نمی‌شود و شخص ثالث فقط همین قدر می‌فهمد که این مقدار پول به این کلید عمومی ارسال شده است. جهت امنیت بیشتر می‌توانید در هر بار معامله کلید عمومی خود را تغییر دهید که اینکار ردیابی شما را غیر ممکن می‌سازد.
مثل هر سیستم انلاین دیگر امکان حمله به این سیستم نیز وجود دارد که با تدابیر می‌توان جلوی آنرا گرفت و تدبیر مهم این است که قبل از ارسال کالا در مقابل پول رسید، تا تایید شش بلاک در سیستم صبر کنید.
بلاک‌چین با امکانات فوق، زمینه را برای عدم دخالت شخص سوم (نظیر بانک‌ها یا دولت)، برای شما فراهم ساخته، و می-توانید میلیون‌ها دالر پول را بدون دخالت به هر حسابی که خواستید منتقل کنید.
همچنان بلاک‌چین یک پروتکل با منبع باز است و وجود این دو دلیل، بلاک‌چین را قدرتمند ساخته هست.

12. موارد استفاده:
بلاک‌چین در عرصه‌های مختلف قابلیت استفاده دارد، که از آن به مختصر یاد می‌شود:

1. ارز دیجیتلی: که مهمترین مثال آن بیت‌کوین هست.

کافی شاپ‌ها یا دوکان‌ها به جای پول بیتکوین بپردازید. می-توان از این فناوری در انتخابات افغانستان نیز استفاده کرد، تا مانع این همه جنجال‌ها و مصارف گزاف در این پروسه شویم.

منابع:

1. Popper, Nathan. A Venture Fund with Plenty of Virtual Capital, but No Capitalist. The New York Times. Archived from the original on 22 May 2016.
2. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System (PDF). bitcoin.org. Archived (PDF) from the original on 20 March 2008-2014.
3. https://www.tutorialspoint.com/blockchain/blockchain-quick-guide.html
4. Morris, David Z. Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting. Fortune. Archived from the original on 21 May 2016.
5. Catalini Christian, Gans Joshua S. Some Simple Economics of the Blockchain (PDF). doi:10.2139/ssrn.2874598. S2CID 46904163. SSRN 28 74598. Archived (PDF) from the original on 6 March 2020.
6. https://www.wikipedia.com/Blockchain.html
7. Janathan Warren. Bitmessage: A peer-to-peer message Authentication and Delivery System 2017. https://bitmessage.org/bitmessage.pdf.
8. Bheemaiah, Kariappa. Block Chain 2.0: The Renaissance of Money. Wired. Archived from the original on 14 November 2015-2016.
9. Antonopoulos, Andreas. Bitcoin security model: trust by computation. Radar. O'Reilly. Archived from the original on 31 October 2016. "Blockchains: The great chain of being sure about things". The Economist. 31 October 2014-2015.
10. Lee, Timothy. Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%. Arstechnica. Archived from the original on 22 April 2013.
11. Wang Kevin, Safavi Ali. Blockchain is empowering the future of insurance. Tech Crunch. AOL Inc. Archived from the original on 7 November 2016.
12. Iansiti Marco, Lakhani Karim R. The Truth About Blockchain. Harvard Business Review. Harvard University. Archived from the original on 18 January 2017.
13. Arnold, Martin. IBM in blockchain project with China UnionPay. Financial Times. Archived from the original on 9 November 2013-2016.
14. Brito Jerry, Castillo Andrea. Bitcoin: A Primer for Policymakers (PDF) (Report). Fairfax, VA: Mercatus Center, George Mason University. Archived (PDF) from the original on 21 September 2013.