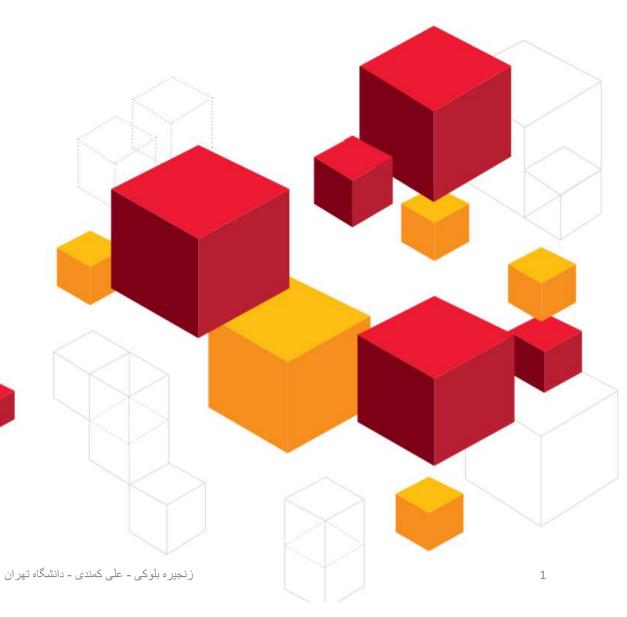
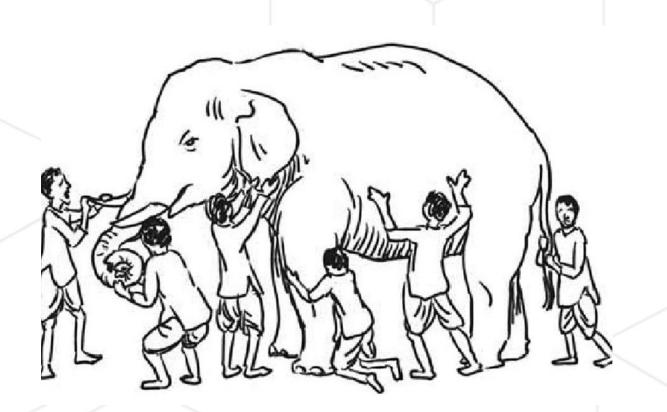


بلاكچين

دکتر علی کمندی عضو هیات علمی دانشگاه تهران





زنجیره بلوکی و ارز دیجیتال

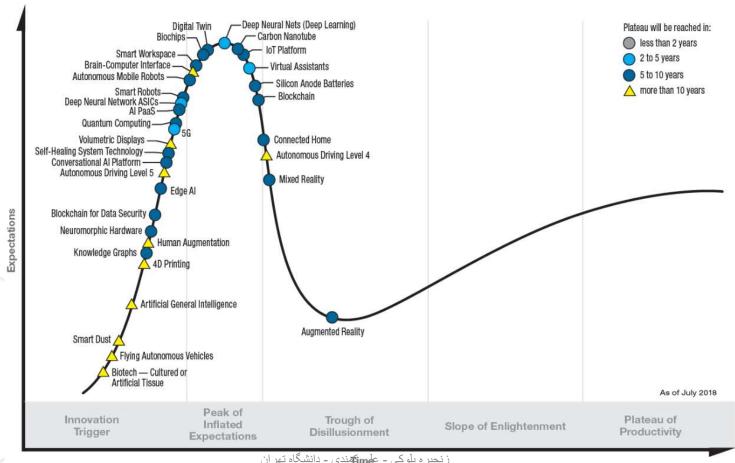






به گزارش Bitinfocharts.com تا کنون ۸۰۰ ارز دیجیتالی متفاوت اختراع شده است. به گزارش صندوق بین المللی پول در سال ۲۰۱۸، ۴۵۲ ارز دیجیتالی جدید معرفی شده است.

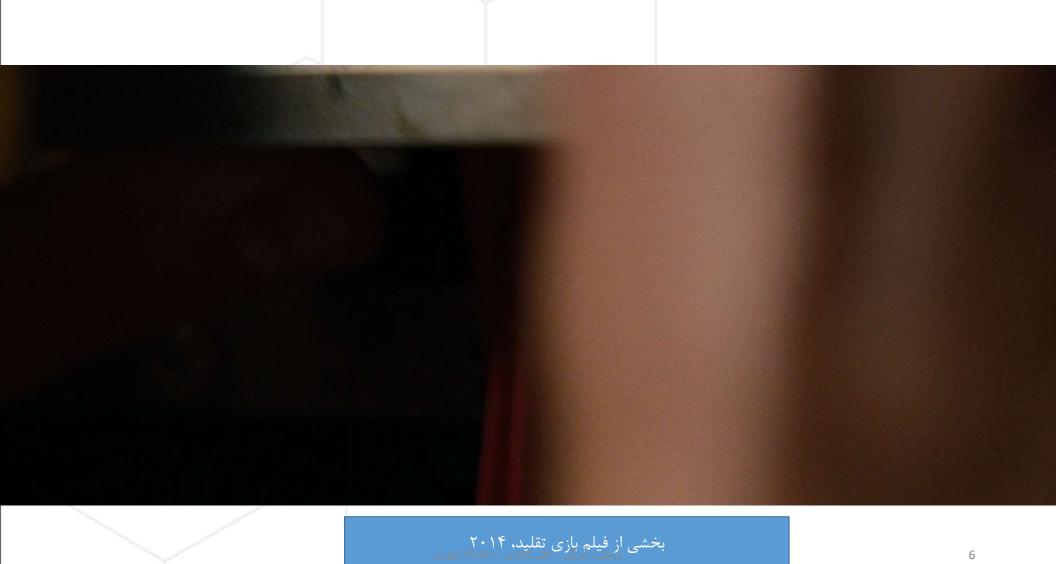
Hype Cycle for Emerging Technologies, 2018



اهداف بلاكچين

اطمینان از نگهداری اطلاعات به نحوی که به هیچ وجه قابل حذف، تغییر، دست کاری و انکار نباشد.

راهکار ۱: استفاده از کد چکیده اطلاعات به کمک تکنیک های رمزنگاری



ماده ١- اساس قرارداد

این بیمه نامه براساس قانون بیمه مصوب اردیبهشت ماه سال ۱۳۱۶ و پیشنهاد کتبی بیمه گذار (که جزء لاینفك بیمه نامه می باشد) تنظیم گردیده است و مورد توافق میباشد. آن قسمت از پیشنهاد کتبی بیمه گذار که مورد قبول بیمه گر واقع نگردیده و کتبا" به بیمه گذار همزمان با صدور بیمه نامه اعلام گردیده است جزء تعهدات بیمه گر محسوب نمدگردد.

ماده ۲- بیمه گر

بیمه گر شرکت بیمه ایست که مشخصات آن در این بیمه نامه قید گردیده و جبران خسارت احتمالی را طبق شرایط مقرر در این بیمه نامه بعهده میگیرد.

ماده ٣- سمه گذار

بيمه گذار شخص حقيقي يا حقوقي مذكور در اين بيمه نامه است كه بيمه را خريداري نموده و متعهد يرداخت حق بيمه آن ميباشد.

ماده ۴- نینفع

ذينفع هر شخص حقيقي يا حقوقي مذكور در اين بيمه نامه اعم از بيمه گذار ميباشد كه در تمام يا قسمتي از موضوع بيمه نفع داشته باشد.

ماده ۵- مورد سمه

مورد بيمه اموال مندرج در جدول مشخصات اين بيمه نامه است كه متعلق به بيمه گذار و يا در تصرف وي در محل مورد بيمه باشد.

اموال ساير اشخاص تا حدودي كه با نوع اشتغال بيّمه گذار ارتباط دارد و همچنين اثاثيه منزل و ساير اموال متعلق به اعضاء خانواده بيمه گذار يا كارگراني كه در منزل وي به سر ميبرند , مشروط بر اين كه بهاي آنها در سرمايه بيمه شده منظور و در محل مورد بيمه مستقر باشد بيمه شده محسوب ميشود.

SHA-256 hash

34bd8ea71995b8bae3f02d049eb72dcf8c4b6a8cb77f9da2ff09bdec8df51bda

Data

ماده ۱- اساس قرارداد این بیمه مصوب اردیبهشت ماه سال ۱۳۱۶ و پیشنهاد کتبی بیمه گذار (که جزء لاینقك بیمه نامه می باشد) تنظیم گردیده است و مورد توافق میباشد. این بیمه نامه براساس قانون بیمه مصوب اردیبهشت ماه سال ۱۳۱۶ و پیشنهاد کتبی بیمه گذار همزمان با صدور بیمه نامه اعلام گردیده است جزء تعهدات بیمه گر محسوب ماده ۲- بیمه گر میرک بیمه گر میرک بیمه گر واقع نگردیده و کتبا" به بیمه گذار همزمان با صدور بیمه نامه اعلام گردیده است جزء تعهدات بیمه گر محسوب ماده ۲- بیمه گر مرکت بیمه ایست که مشخصات آن در این بیمه نامه قید گردیده و جبران خسارت احتمالی را طبق شرایط مقرر در این بیمه نامه بعهده میگیرد. ماده ۳- بیمه گذار شخص حقیقی یا حقوقی مذکور در این بیمه نامه است که بیمه را خریداری نموده و متعهد پرداخت حق بیمه آن میباشد. ماده ۴- نینفع می شخص حقیقی یا حقوقی مذکور در این بیمه نامه است که بیمه گذار میباشد که در تمام یا قسمتی از موضوع بیمه نفع داشته باشد. ماده ۵- مورد بیمه اموال مندرج در جدول مشخصات این بیمه نامه است که متطق به بیمه گذار و یا در تصرف وی در محل مورد بیمه باشد. مورد بیمه اموال مندرج در جدول مشخصات این بیمه گذار ارتباط دارد و همچنین اتاثیه منزل و سایر اموال متطق به اعضاء خانواده بیمه گذار یا کارگرانی که در منزل وی به سر میبرند , مشروط بر این که بهای آنها در سرمایه بیمه شده منظور و در محل مورد بیمه مستقر باشد بیمه شده محسوب میشرد. , مشروط بر این که بهای آنها در سرمایه بیمه شده منظور و در محل مورد بیمه مستقر باشد بیمه شده محسوب میشرد.

SHA-256 hash

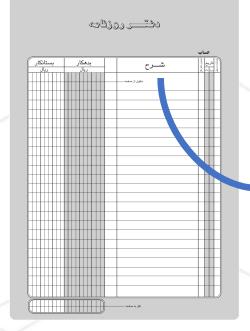
49b3c49fbf680ef62b24c3faac1802730de1a41c766a181629a73b31201eaa71

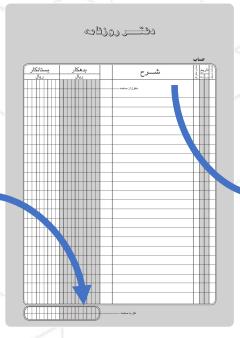
34bd8ea71995b8bae3f02d049eb72dcf8c4b6a8cb77f9da2ff09bdec8df51bda

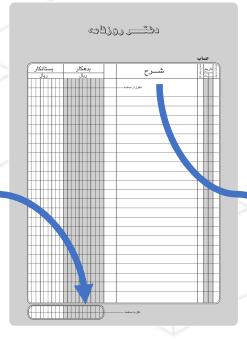


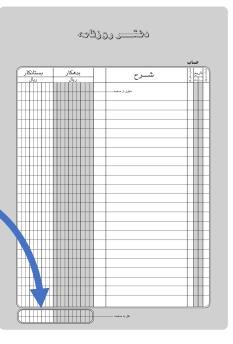
(11)	بامه	دفتر روز
	بدهكار	C
بستانكار	ريال	
July 1	THE PROPERTY AND A STATE OF THE PARTY AND A ST	منقول از صفحه
NOTE & SOUTH AND	Tempores.	gie de mont part you
	10000000	aut fundament
	~ ~ ~ ·	Various Ser 10
	14-01/4/	wyor W
	Men. WAA.	good of the at
	a savea	JUBBOIN W
	Argy A	de any w
	VV-10-K11	in tops
Personal M		are provide care
tra 64		energial see
15011101		- with the state of the state o
124606 ACOV		100
44-11-611		1,400
1884.78		San Your Street
		" Company
	6111611V	- 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	ETNATETY.	& with the EN
	114.404	, ielyin w
MUQUE BERNE	14. 444.19.	الما عنقار الديراض منه مناه
		, Jugo in
CELTELDE		13.20,12
YVYNAIN_		Significant Company
TETA. VAL.		Just marging sent sent 107
evanen .		
		0,-
		13 in less
	YTANIT VIE	we win it, we at x
		03.0%
医眼视器 對岸陰縣 医巩膜层	東部男子の単名を見り	ز نجر و بلوکی - علی کمندی - دانشگاه

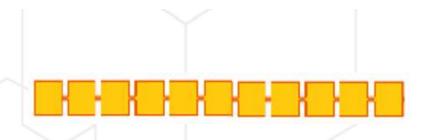
				حساب	
بستانکار ریال	بدهكار ريال		شب ح	کل اور	شماره ر
ريال	ريال			ا روز ماه کلا	ر ديغ
			شـرح		
					╝
					\int
			نقل به صفحه		
		انشگاه تهران	ز نجیره بلوکی - علی کمندی - د	11	

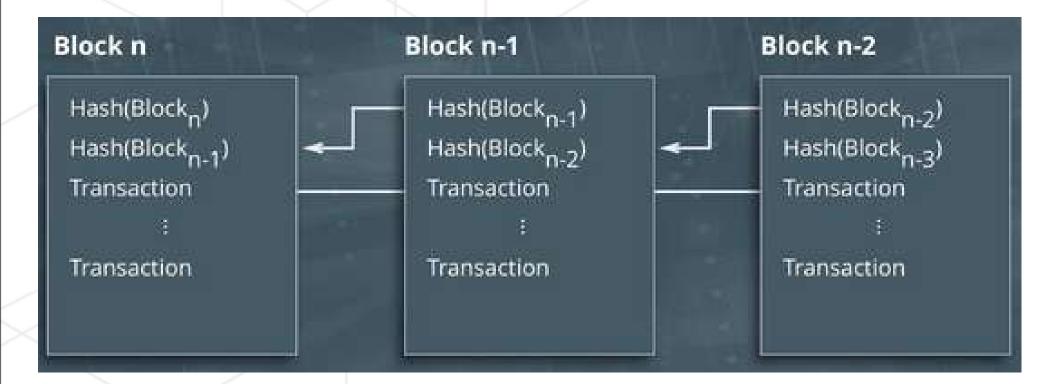




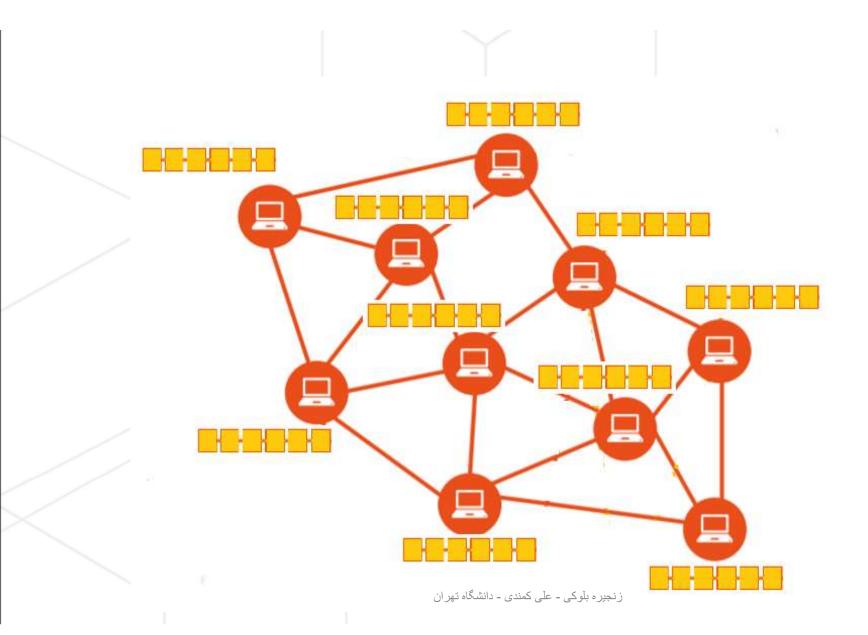


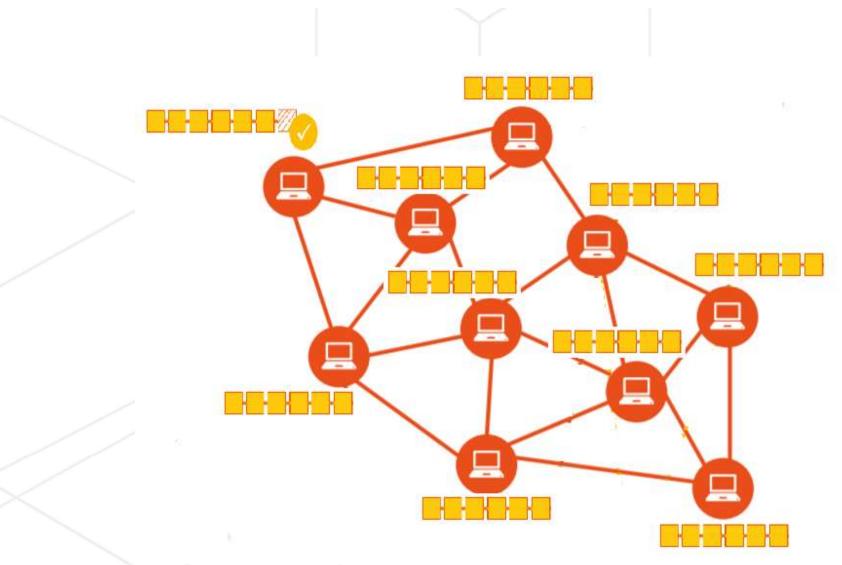




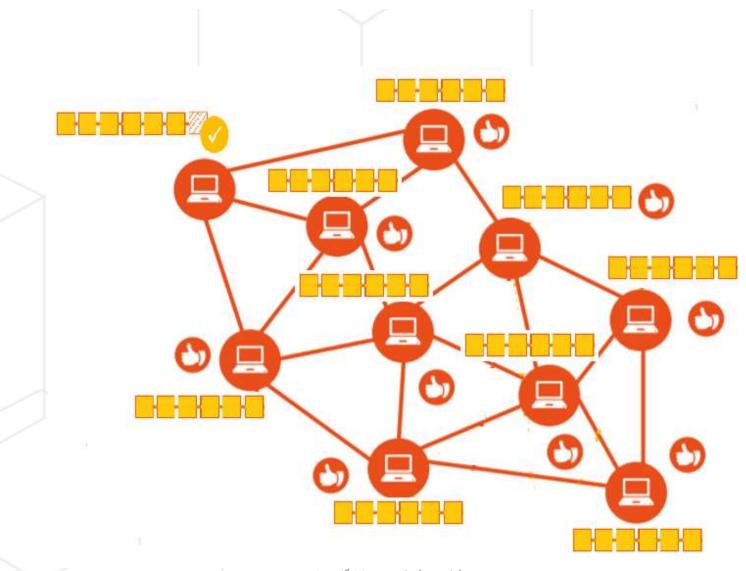




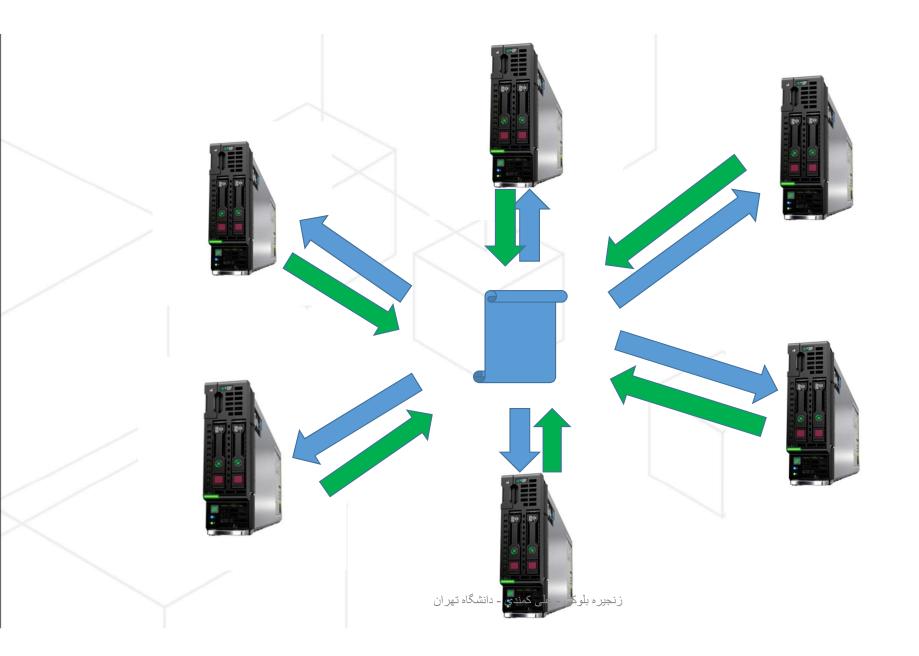


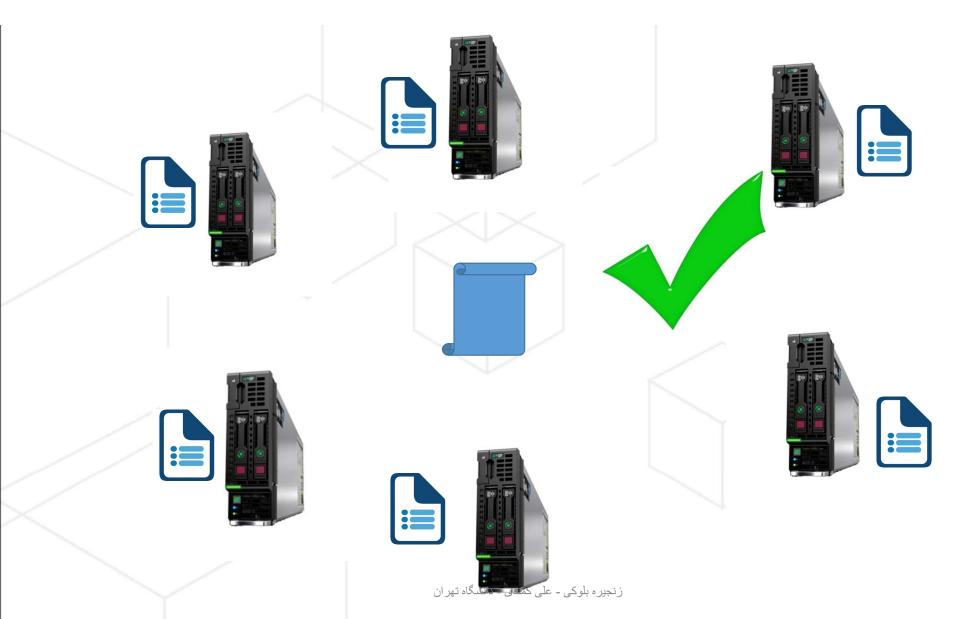


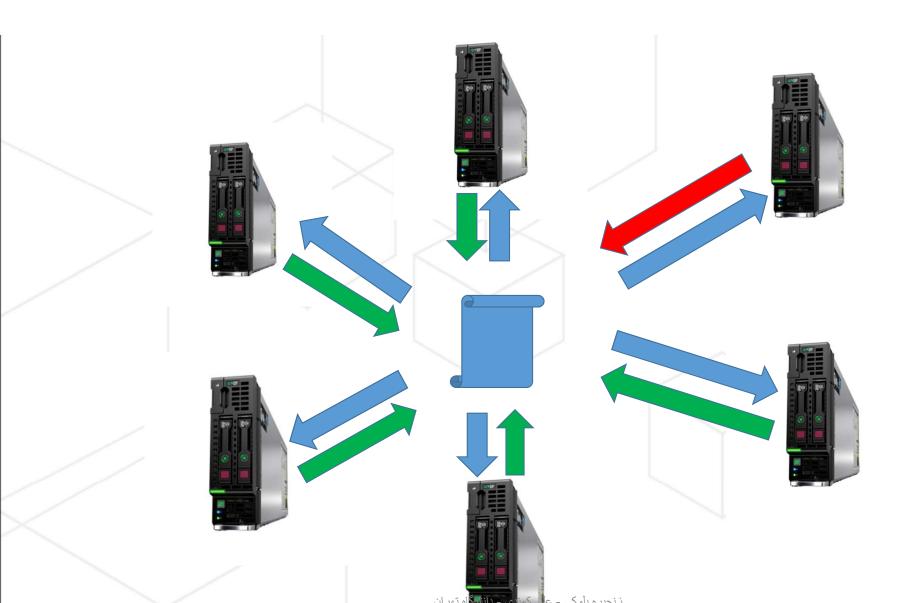
زنجیره بلوکی - علی کمندی - دانشگاه تهران



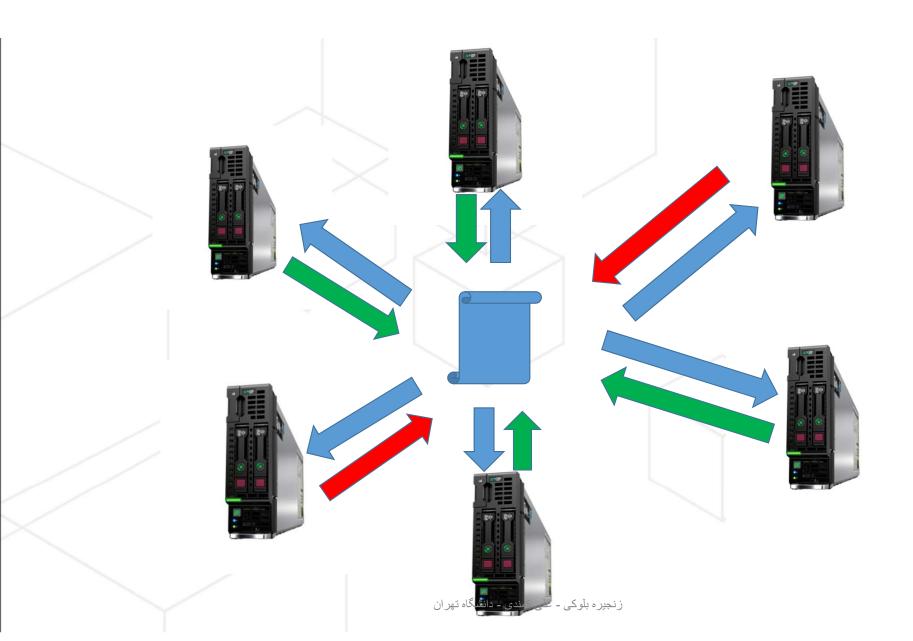
زنجیره بلوکی - علی کمندی - دانشگاه تهران

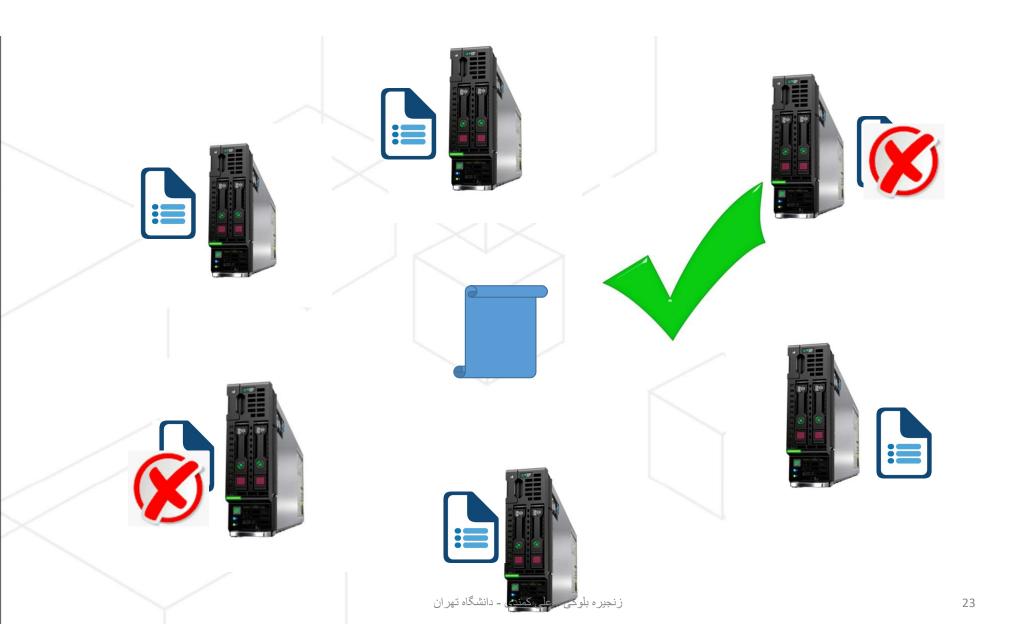


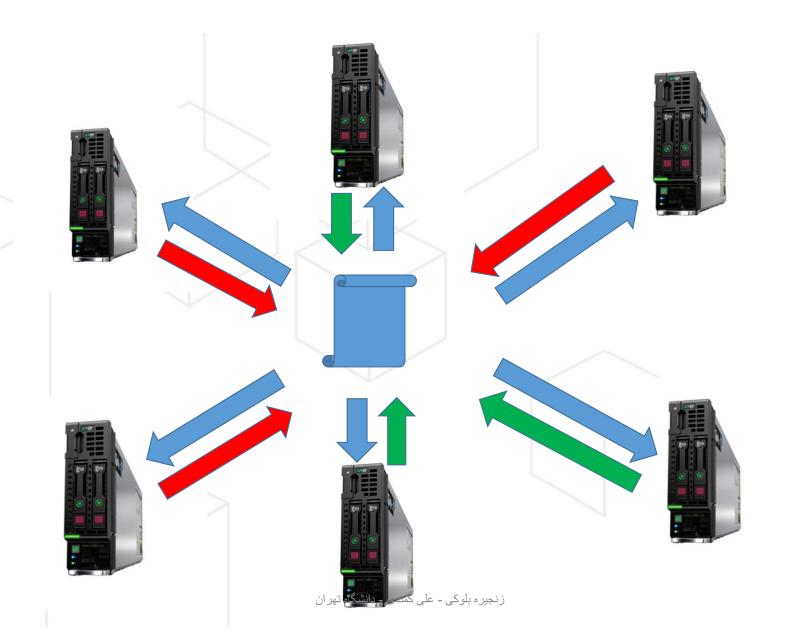








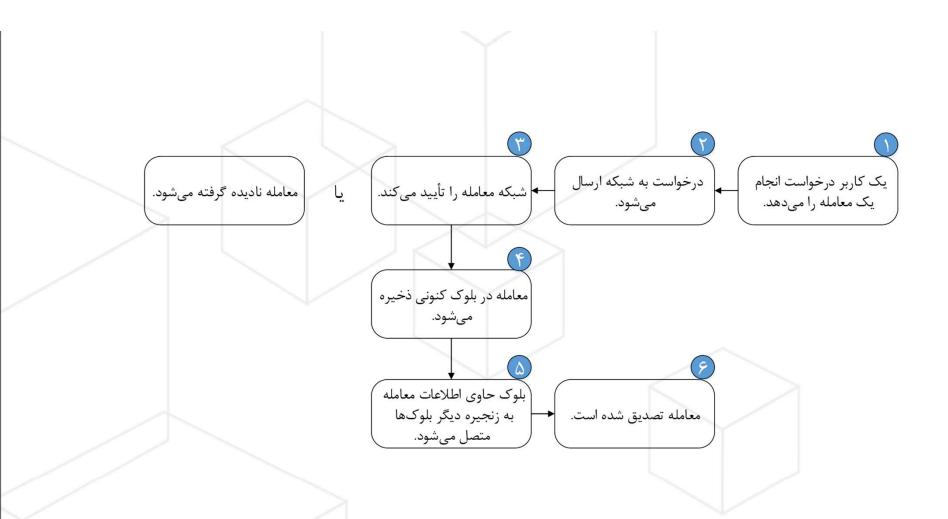












بیت کوین

• بیت کوین رمز-ارز، ارز دیجیتالی یا پول مجازی است که در اکتبر ۲۰۰۸ اختراع شد. در همان سال فردی ناشناس با نام مستعار ساتوشی ناکاموتو در مقالهای بیت کوین را بهعنوان یک سامانه ی پرداخت الکترونیکی نظیربهنظیر معرفی کرد. سپس در ژانویه ی ۲۰۰۹ کدهای آن بهصورت متنباز در اختیار عموم مردم قرار گرفت. ناکاموتو تا سال ۲۰۱۰ با تعداد زیادی از برنامهنویسان برای توسعه بیت کوین بهصورت متنباز همکاری می کرد.













































































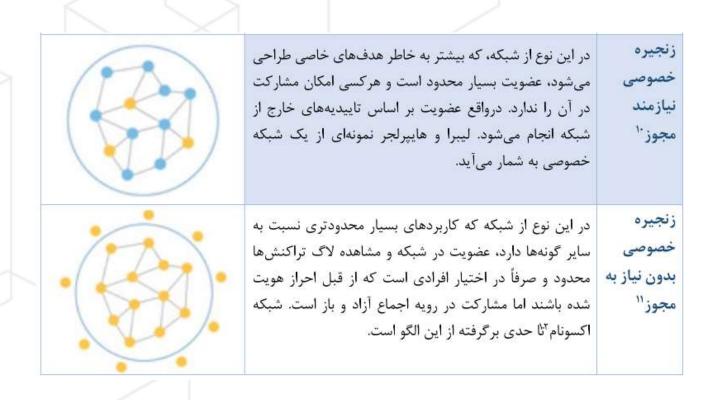








تصوير نمادين	توضیحات و نمونهها	نوع شبكه
	مشارکت همه در زنجیرههای عمومی آزاد است و هرکسی می تواند هم در مشاهده و هم در تأیید تراکنشها و پیشبرد اهداف کل شبکه تلاش کند. کد شبکههای عمومی به صورت متنباز در دسترس عموم قرار می گیرد. بیت کوین، لایت کوین و اتریوم نمونههایی از یک شبکه عمومی به شمار می آیند.	زنجیره بلوکی عمومی ^۷
	نقشهای تعریفشده در این شبکه زنجیرهای کنترلشده هستند و می توانند در طول زمان توسط توسعه دهندگان اصلی تغییر پیدا کنند. به عبارت دیگر هرکسی در شبکه می تواند لاگ تراکنشها را مشاهده کند اما تنها گرههای خاصی می توانند در فرایند رأی گیری و اجماع شرکت کنند که باید از قبل احراز هویت شده باشند. کد منبع مربوط به هسته پیاده سازی شده در این نوع از شبکه ها، معمولاً به صورت متن باز در دسترس است. ریپل و شبکه ها، معمولاً به صورت متن باز در دسترس است.	زنجیره عمومی نیازمند مجوز^
	سبکهها، معمولاً به صورت متن باز در دسترس است. ریپل و نسخه خصوصی اتریوم نمونهای از شبکههای عمومی مبتنی بر مجوز است.	

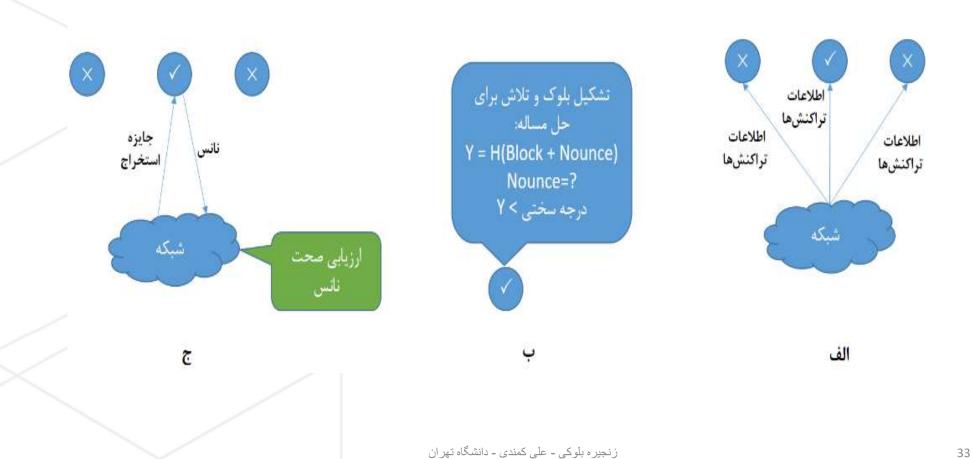


روش اثبات کار

- این پروتکل در پلتفرم بیت کوین به عنوان الگوریتم اجماع استفاده می شود.
- برای جلوگیری از ورود گرههای غیرقابلاعتماد و یکسانسازی دفتر کل به کار گرفته میشود.
- بزرگترین زنجیره از بلوکها را که تعداد نود بیشتری در ایجاد آن دخالت دارند به عنوان زنجیره اصلی در نظر می گیرد.
- معمولاً برای جلوگیری از خطاهای بیزانس و هزینه مجدد توسط نودهای غیرقابلاعتماد استفاده می شود.

كنترل تراكنش ها

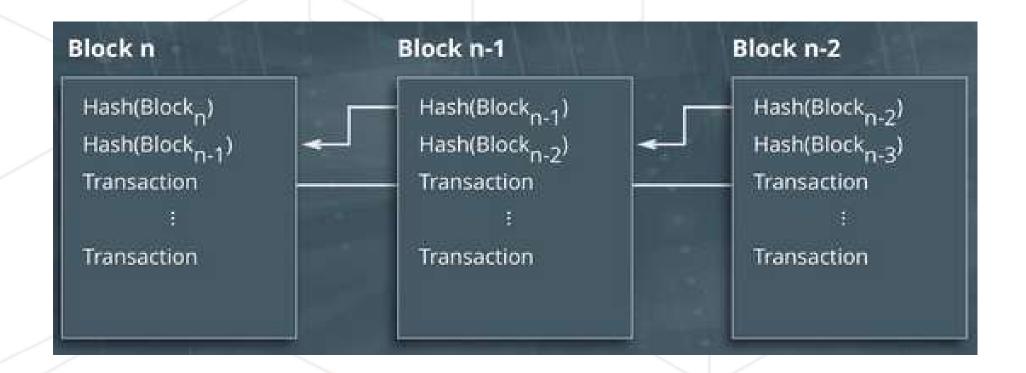
- موارد زیر برای هر تراکنش بررسی میشوند:
- لیست ورودیها و خروجیها بههیچعنوان خالی نباشد.
- تعداد بایتهای یک معامله نباید از حداکثر اندازه تعیینشده برای بلوک کمتر باشد (بزرگتر یا مساوی با ۱۰۰ باشد).
 - هر مقدار خروجی باید در محدوده تعیینشده قرار داشته باشد (کمتر از ۲۱ میلیون سکه).
 - تعداد امضاهای تأیید هر معامله نباید کمتر از حدنصاب مشخص باشد.



```
>>> import hashlib
>>> print (hashlib.algorithms guaranteed)
{'blake2b', 'sha224', 'sha3 384', 'shake 128', 'sha512', 'sha3 224', 'sha256',
'sha1', 'sha384', 'sha3 256', 'shake 256', 'sha3 512', 'blake2s', 'md5'}
>>> str="زنجيره بلوكي"
>>> nonce=["1","2","3","4","5","6","7","8","9","10","11","12","13","14","15"]
>>> for i in range (15):
       strh=str+nonce[i]
       result = hashlib.sha256(strh.encode())
       print(strh+ "--->"+"Hash value: "+result.hexdigest())
--->Hash value: d0f2291136006086f164f02208947558a390cfc19a0dd323a5
a9de77c08cc295
6e8ffbcd06505a
Hash value: 7401167b3c4af42414f95d6dd96657819064f0e495e120c104---زنجيره بلوكي3
ae4c5591d23605
4--->Hash value: 5bdeaab509011709c500639475b85909eab1724a38fe92d047
1a3e3028b9458f
Hash value: 5e3dcae512e224e43f2c4b182e83b3656c04307453622917cb---زنجيره بلوكي5
8d7e04cc485e45
Hash value: efb11ce73c9bfd81eed3e9896ecd74d427504982db5e44e11e---زنجيره بلوكي6
554e314b1c0958
Hash value: 11186f0a62a3b3e949c221f96bea14d82679c896145d2c6e06---زنجيره بلوكي7----
bd2342f673b94e
7--زنجيره بلوكي8-hash value: 34525c38ed4cd16592231bff8e53e8f4e573eacc36829334c7-رنجيره بلوكي8
098112cef407b7
Hash value: 0b54b83edac4f7ddf1196c82370af9b41e116bce2f203c123c--;نحيره بلوكي9
65bf925ca8270b
10رنجيرة بلوكي100-hash value: d3ff201c19f903278e59d92490acde0a7259c5134155389b0=رنجيرة بلوكي
8ed80c1d708988c
11.خبره سلوكي11--->Hash value: 63c33e1df91f6bd0429d2b3e2397a824040ec980241de0899
21c74c3374f3f4b
12...->Hash value: 4d716f433a3d7ef5dd9fbb6fbcef480851443ccdc9c36f421
c1e34a433cc4fd1
13--->Hash value: 7ae1d06b356b8bdf53f926374b93a977ca473ae21f98182bf
a2e29d450b60f84
14وكي14 --->Hash value: eb6c4b55827e48408c7fee099043e549b2d3af29bd034a517
60dbe6fc05fd04b
25. Hash value: 178be63cf100221aba13bcd05484aa130606a9a788c1d98ac--زنجيره بلوكي
977c25d8e51eca1
```

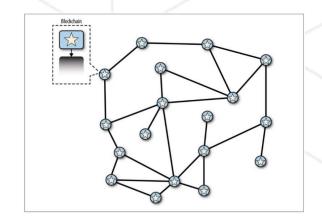
بهروزرساني درجه سختي الگوريتم

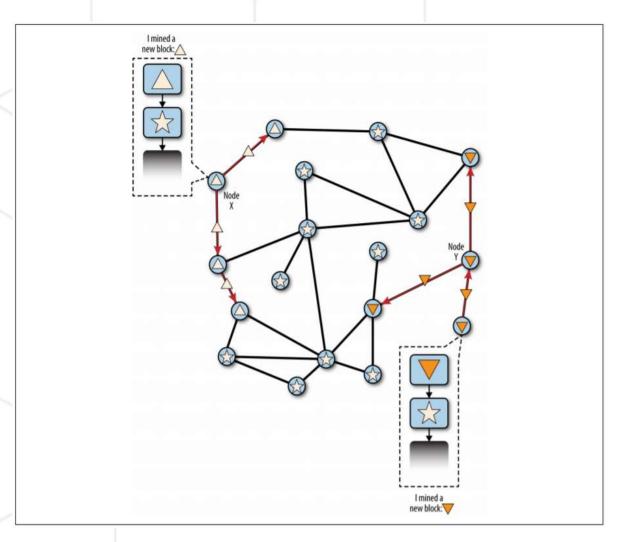
- در پروتکل بیت کوین به منظور جلوگیری از ایجاد همزمان بلوکها که می تواند مشکلاتی را در شبکه ایجاد کند و باعث افت کارآیی شبکه شود (این مشکلات در ادامه تشریح شده است)، شبکه طوری تنظیم می شود که تقریباً هر ۱۰ دقیقه یک بلوک جدید تولید شود.
- برای ثابت نگه داشتن سرعت تولید بلوکهای جدید در حد ۱۰ دقیقه، سختی الگوریتم بهطور منظم و پس از تولید هر ۲۰۱۶ بلوک توسط استخراج کنندگان به روز می شود.
- مقدار جدید درجه سختی استخراج برابر است با زمان واقعی صرف شده برای استخراج ۲۰۱۶ بلوک نسبت به زمان مورد انتظار یعنی ۲۰۱۶۰ (۱۰ دقیقه به ازای هر بلوک)، هر چه این مقدار بزرگتر باشد، میزان سختی استخراج بیشتر است.



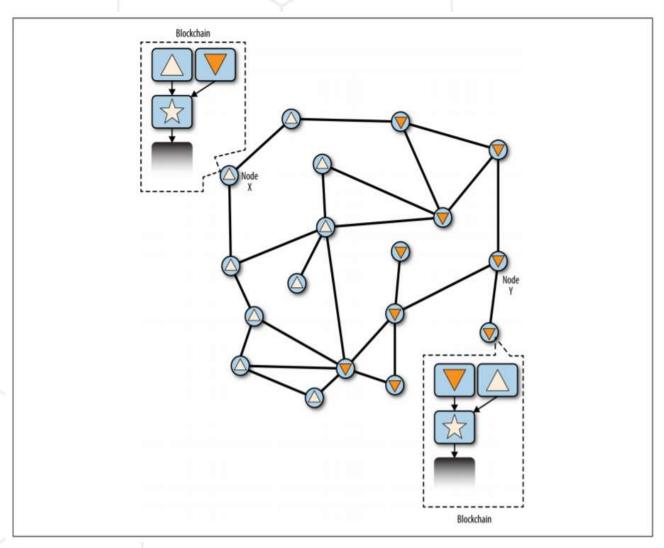
چندشاخه شدن زنجیراه

• ممکن است همزمان بیش از یک گره موفق شوند بلوک جدیدی را به زنجیره اضافه کنند. اگرچه تأخیر ۱۰ دقیقهای که در شبکه تعبیه شده است، تا حد زیادی شانس اینکه همزمان دو گره به جواب برسند و هر یک بخواهند بلوک متفاوتی را به زنجیره اضافه کنند کاهش میدهد، ولی کماکان احتمال این امر وجود دارد.

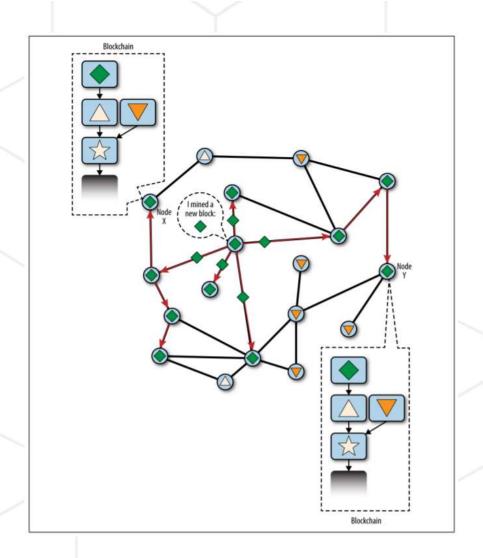




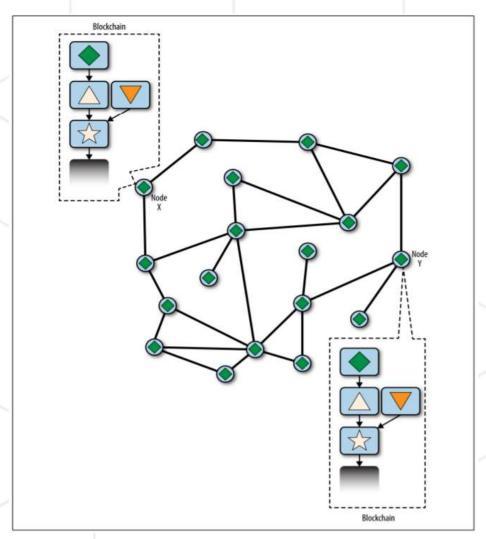
زنجیره بلوکی - علی کمندی - دانشگاه تهران



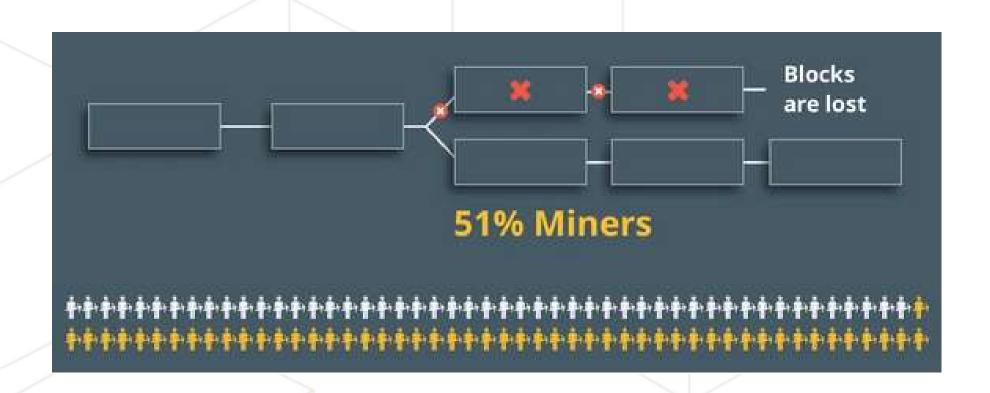
زنجیره بلوکی - علی کمندی - دانشگاه تهران



زنجیره بلوکی - علی کمندی - دانشگاه تهران



زنجیره بلوکی - علی کمندی - دانشگاه تهران



گواه اثبات سهام وثيقه

- اگر یک گره بخواهد در مرحله بعد استخراج کننده (تشکیل دهنده بلوک بعدی) باشد، بخشی از سهم (اعتبار) خود را بلوکه می کند و به شبکه اطلاع می دهد.
- هر گره معاملات ارسال شده از سمت کلاینتهای خود را انتشار میدهد. زمانی که تعداد کافی تراکنش تأیید شد، گرههای کاندید، گرهای را که بیشترین میزان اعتبار را بلوکه کرده بهعنوان گره رهبر اعلام میکنند. در گونههای تصادفی، علاوه بر میزان سهام بلوکه شده، انتخاب گره برنده تا حدی به صورت تصادفی انجام می شود.
 - گره رهبر بلوک جدید را ساخته و آن را در شبکه انتشار میدهد.
- هر گره بلوک ساختهشده توسط رهبر را معتبر اعلام کرده و آن بلوک به همراه تمامی تراکنشهای درون آن را به زنجیره خود اضافه میکند.
- گره رهبر مبلغی را بهعنوان کارمزد دریافت میکند. این کارمزد در تراکنشها مشخصشده است (برخلاف الگوریتم اثبات کار، رمز-ارز جدیدی ساخته نمیشود).

انتخاب تصادفي

- روش ساده: ترکیب سهام و کد هش
- روش زمانی (روزشمار): وزن زمان انتظار سهام

• ريسك الگوريتم: افراز

روش اثبات سهام وكالتي

- در این الگوریتم گرهها از طریق رأی گیری از بین خودشان تعدادی را به عنوان نماینده یا و کیل انتخاب می کنند.
- معمولاً حدود ۲۰ الی ۱۰۰ گره با رویکردی کاملاً دموکراتیک بهعنوان نماینده انتخاب میشوند. این نمایندگان بهطور دورهای تغییر میکنند.
- تمام تصمیمات توسط این گروه از نمایندگان اخذ می شود. این سازوکار درعین حال که رویکرد توزیع شدگی را حفظ می کند و به نحوی همه گرهها را در فرایند تصمیم گیری دخیل می کند، باعث می شود زمان لازم برای رسیدن به توافق بسیار کاهش پیدا کند. در عمل در پروتکلهایی نظیر بیت شیر این زمان در حد ۱ ثانیه است (مقایسه کنید با ۱۰ دقیقه در بیت کوین).
 - اگر یک نماینده نتواند فعالیت خود را بهطور مؤثر به انجام رساند، صاحبان سهام آن را از سیستم خارج نموده و نماینده بهتری را جایگزین میکنند.

گواه اثبات ظرفیت

- روش کار این الگوریتم مانند الگوریتم گواه اثبات کار است، در الگوریتم گواه اثبات کار، هر یک از گرهها با توجه به میزان توان سختافزاری قادر به تولید بلوک جدید در زنجیره هستند. درنتیجه گرهی که قدرت محاسباتی بالاتری داشته باشد، از شانس بیشتری برای موفقیت و ایجاد بلوک جدید برخوردار است.
- در این الگوریتم گرههایی توانایی ساخت بلوک جدید را دارند که میزانی از حافظه بلندمدت (دیسک) خود را به اشتراک بگذارند. هرچقدر یک گره امکانات سختافزاری (دیسک) بیشتری فراهم کند و به اشتراک بگذارد، از شانس بیشتری برای ساخت بلوک جدید برخوردار میشود.
- تمرکزگرایی در این الگوریتم نسبت به الگوریتم گواه اثبات کار کمتر است و عادلانهتر عمل می کند. علاوه بر این گرههای شبکه در ذخیرهسازی اطلاعات دخیل بوده و تمایل به انجام این کار دارند.

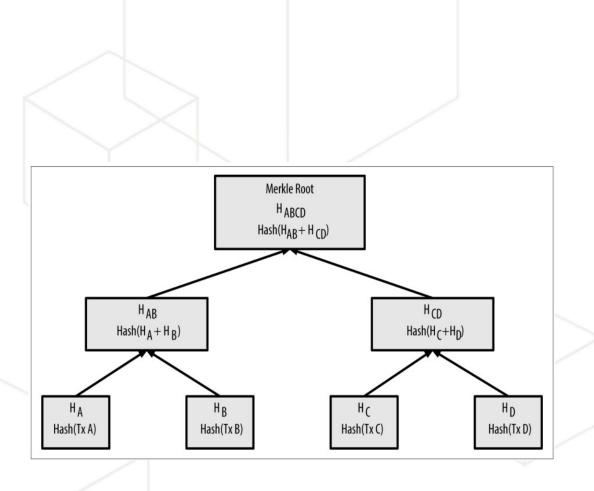
گواه اثبات زمان سپریشده

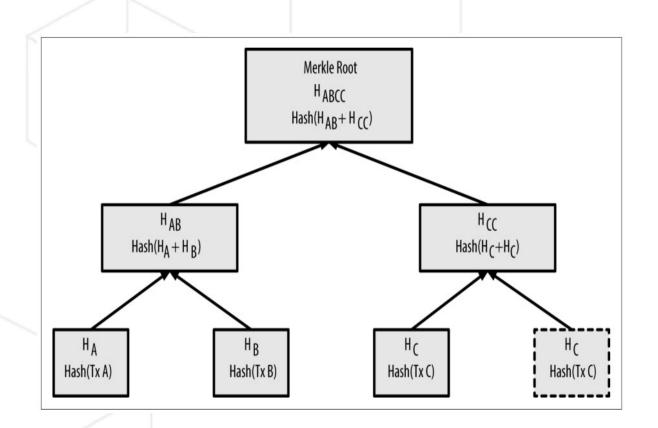
- گره استخراج کننده در هر مرحله از طریق قرعه کشی انتخاب می شود. برای تعیین گره استخراج کننده بلوک، زمان مشخصی در نظر گرفته می شود و انتظار می رود که در کوتاه ترین زمان ممکن این گره از طریق قرعه کشی انتخاب شود. انتخاب گره استخراج کننده بلوک جدید به طور تصادفی و از میان کلیه گرههای موجود در شبکه انجام می شود و هیچ گرهی نمی داند که چه زمانی برای استخراج بلوک انتخاب می شود. الگوریتم در سطح بالا از دو بخش تشکیل می شود:
 - هر یک از شرکتکنندگان (گرههای شبکه) باید به اندازه یک زمان تصادفی منتظر بمانند.
 - اولین گرهای که زمان انتظارش به سر برسد، به عنوان رهبر انتخاب می شود و می تواند یک بلوک به زنجیره اضافه کند.
- Trusted execution environment (TEE)

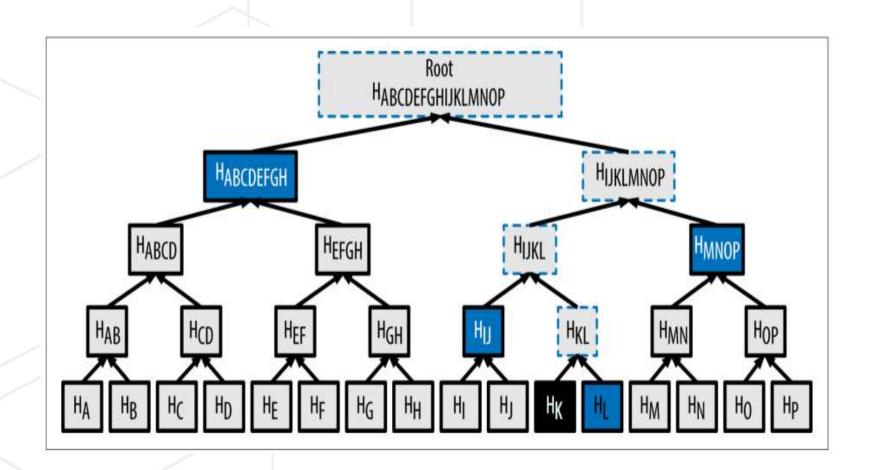
. گواه اثبات فعالیت

- این الگوریتم بر مبنای الگوریتمهای گواه اثبات کار و گواه اثبات سهام وثیقه کار می کند.
- همانند الگوریتم گواه اثبات کار، استخراج کنندگان باید مقدار مناسب نانس را پیدا کنند که مقدار تابع درهمسازی آن کمتر از حدنصاب خاصی باشد. اما به جای تراکنشهای واقعی، یک بلوک خالی با کد درهمسازی بلوک قبلی را در نظر گرفته و نانس مناسب آن را پیدا می کنند.
- وقتی یک گره موفق به حل مسئله شد، به صورت تصادفی تعداد Nگره را انتخاب می کند. بلوک جدید برای همه گرههای شبکه ارسال می شود. هر گره شبکه وقتی این پیام را دریافت کند ابتدا چک می کند N که بلوک به درستی ایجاد شده باشد و قواعد را رعایت کند. سپس کنترل می کند که آیا جزء یکی از گره انتخابی هست یا خیر. اگر یکی از آن ها بود بلوک را امضا می کند. گره شماره Nوقتی امضای همه را دریافت کرد، تراکنش های موردنظر را به بلوک اضافه می کند و عملاً بلوک جدید تشکیل می شود.
- پاداش استخراج بین همه گرههایی که مشارکت داشتهاند (گرهای که استخراج را انجام داده و الاگره دیگر) تقسیم میشود. عملاً بلوک توسط گره آخر ایجاد میشود و گره آغازکننده یا همان گرهای که استخراج را انجام داده صرفاً یک بلوک خالی و بدون تراکنش ایجاد میکند.

• یکی از موضوعات مهم این الگوریتم نحوه انتخاب Nگره بهصورت شبه تصادفی است. روش کار به این صورت است که تعداد Nعدد تصادفی بین ۱ و حداکثر تعداد ساتوشیهای موجود در شبکه تولید می شود. ساتوشی کوچک ترین واحد پول شبکه است که مورداستفاده قرار می گیرد. سپس لیست تراکنشهای زنجیره توسط هر گره کنترل می شود تا ببینند هر یک از ساتوشیهای Nگانه در اختیار کدام گره است. از آنجاکه ممکن است یک ساتوشی بارها معامله شده باشد، گرهای در نظر گرفته می شود که آخرین مالک آن باشد.







Buying a house on Ethereum

BUYER LAWYERS, BROKERS, INSURANCE SELLER

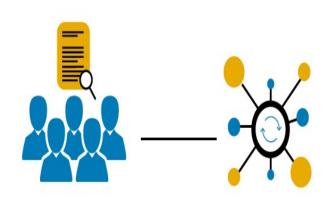
SMART CONTRACTS "CODE AS LAW" BUYER SELLER

قرارداد هوشمند

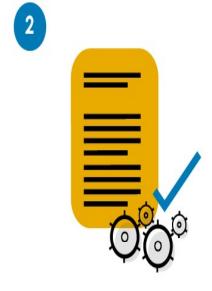








نهاد ناظر با استفاده از زنحیره بلوکی بر کلیه اتفاقات و تراکنشها نظارت خواهد داشت. در عین حال حریم خصوصی هر یک از افرادی که در قرار داد نقش دارند حفظ میشود.



چنانچه رویدادی اتفاق بیفتد و شرایط مندرج در قرارداد برقرار شود، تعهدات طرف دیگر نیز به طور خودکار جاری می شود. هیچ کس قادر نخواهد بود جلوی اجرای قرارداد را بگیرد و این فرایند به طور خودکار اتفاق میفتد.



قرارداد مورد نظر بین طرفین بصورت کد زنحیره بلوکی نوشته میشود. قرارداد به صورت دفتر کل توزیع شده در شبکه زنجیره بلوکی نگهداری میشود.

Source: Deloitte University Press, DUPress.com

بيمه پارامتريک

بیمه پارامتریک یا بیمه مبتنی بر شاخص جبران خسارت را به فراهم شدن شرایط خاصی منوط می کند.

مثال

- · اگر زلزله ای با قدرت بیش از ۷ ریشتر رخ دهد، مبلغ مشخصی به بیمه شده پرداخت می شود.
 - اگرطوفان مرتبه ۴ روی دهد آنگاه مبلغ مشخصی به بیمه شده پرداخت می شود.
- اگر میزان بارش سالانه از حد مشخصی کمتر شود، مبلغ مشخصی به بیمه شده پرداخت می شود.

تفاوت بیمه پارامتریک با بیمه سنتی:

- پرداخت مبلغ توافق شده به وقوع خسارت ربطی ندارد. ممکن است خانه کسی در زلزله آسیب نبیند ولی خسارت دریافت کند.
 - روال پرداخت سریع و قابل پیش بینی است و نیازی به کارشناسی هم ندارد.

راههای پیادهسازی

- Microsoft Azure
- Hyperledger
- IBM Blockchain

پروژه

- هایبرلجر فابریک را نصب و راه اندازی نمایید و به کمک آن یک زنجیره بلوکی با تنظیمات دلخواه تعریف کنید. شاخص های اصلی نظیر زمان ایجاد بلوک جدید، الگوریتم اجماع، میزان مقاومت در برابر خطا را اندازه گیری و گزارش نمایید. اندازه و تعداد تراکنش ها را به دلخواه تعیین کنید. سعی کنید در زنجیره انشعاب ایجاد کنید و گزارش دهید واکنش زنجیره نسبت به تلاش شما چه بوده است.
 - پروژه در گروه های ۳ نفری انجام شود.
 - موعد تحویل گزارش نهایی پروژه و ارائه حضوری آن طبق برنامه اعلامی خواهد بود.