علوم نوین امیرکبیر

کلاس آنلاین LIVE WEBINAR

آموزش برنامه نویسی بلاکچین و قرارداد هوشمند

سید مجید شبیری

کارشناسی ارشد IT، گرایش شبکه

از دانشگاه صنعتی امیرکبیر

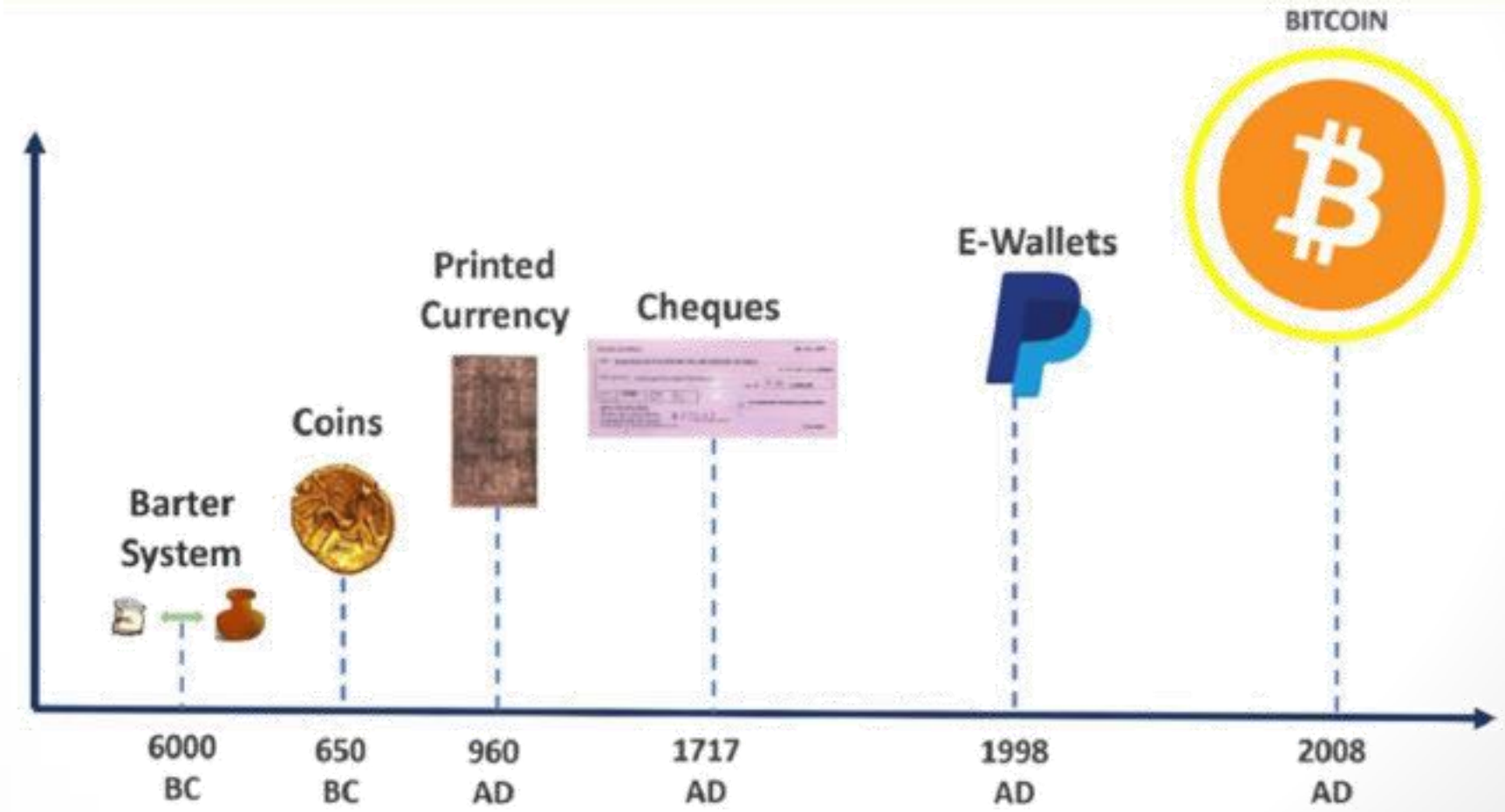
ETHEREUM SOLIDITY

TRUFFLE WEB3.JS Ganache

مروری بر مفاهیم شبکه بلاکچین

سرفصل مطالب

روند تکامل پول

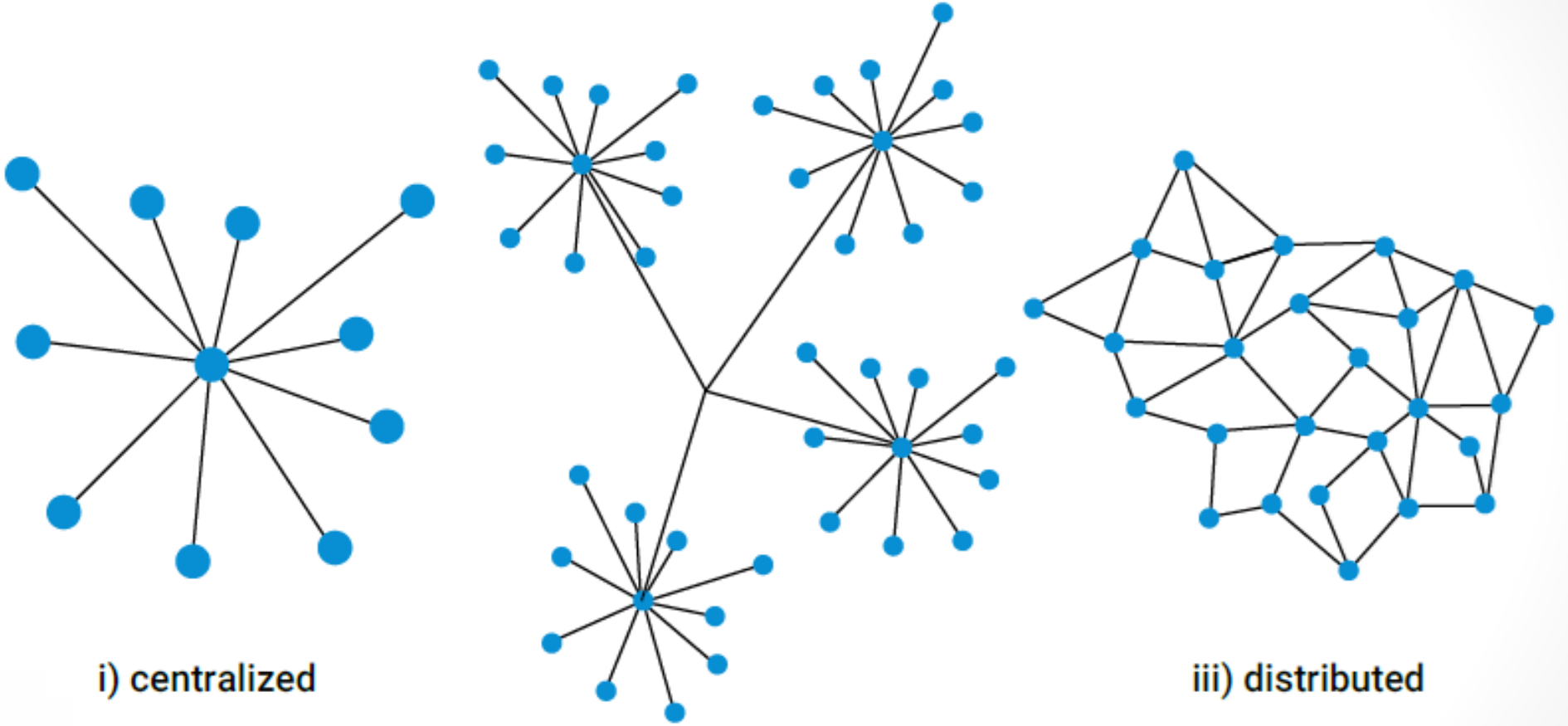


Amirkabir-Science
علوم نوین امیرکبیر

بیتکوین (Bitcoin)

- بیتکوین اولین **ارز دیجیتال** (Digital Currency) پیاده‌سازی شده در بستر **بلاکچین** است.
- **غیرمتمرکز** (Decentralized)
- بدون **واسطه** (Disintermediated)
- بدون نیاز به **اعتمادسازی** (Trustless)

Amirkabir-Science
علوم نوین امیرکبیر



Amirkabir-Science
علوم نوین امیرکبیر

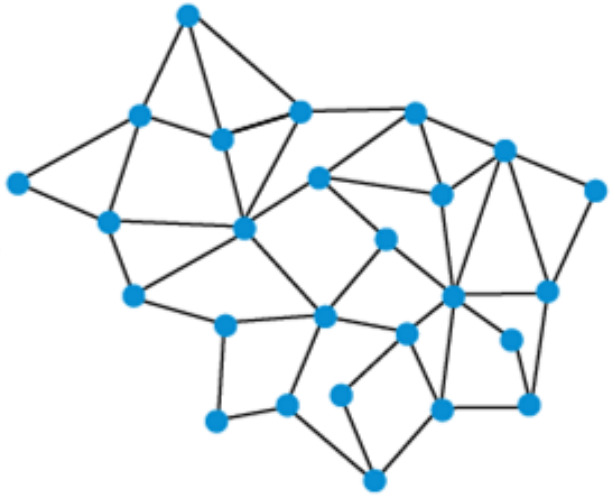
- دارای یک Authority مرکزی بوده و فرایندها و تصمیم‌گیری‌ها در یک نقطه انجام می‌شود.
- چنین سیستمی به سادگی می‌تواند از کار بیفتد

Centralized

- **مزایا**
  - سهولت پیاده‌سازی
  - مقیاس‌پذیری
- **معایب**
  - از کار افتادن سیستم با اختلال در نقطه مرکزی (SPF)
  - عدم شفافیت
- **مثال**
  - سرورهای محاسباتی
  - سیستم بانکی

Amirkabir-Science
علوم نوین امیرکبیر

- دارای چندین Authority بوده و پردازش تراکنش در یک نقطه انجام نمی‌شود.
- چنین سیستمی به سختی ممکن است از کار بیفتد.

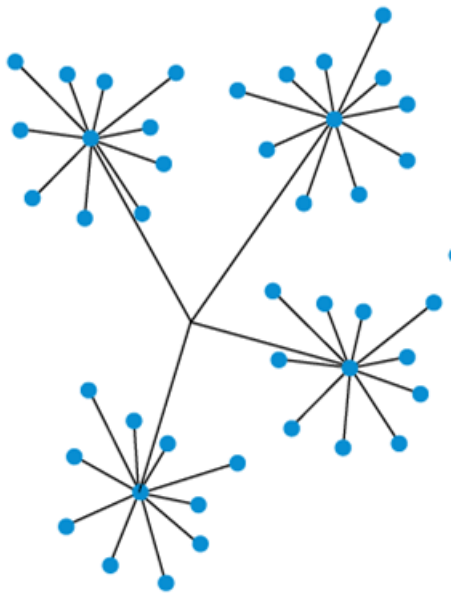


Distributed

- **مزایا**
  - تصمیم گیری ها در نزدیکی مشتری صورت می گیرد
  - اختلال در این سیستم خیلی بعید است
- **معایب**
  - غیراقتصادی بودن در مقیاس‌های بالا
  - عدم برقراری کامل امنیت
- **مثال**
  - پایگاه داده کلود
  - دولت‌ها

Amirkabir-Science
علوم نوین امیرکبیر

- بدون Authority است یا می‌توان گفت همه Authority دارند (No/All Authorities)



Decentralized

مزایا

- کم هزینه بودن به خاطر نبود واسطه
- از لحاظ اقتصادی هک سیستم به صرفه نبوده و دور از امکان است
- دارای شفافیت کامل

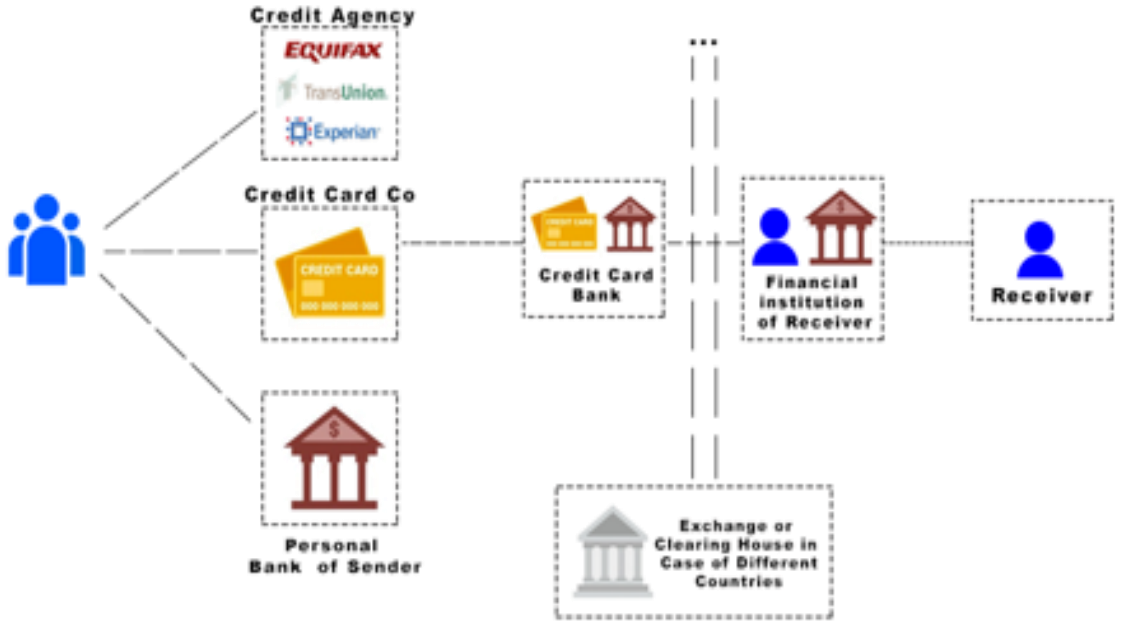
معایب

- تکنولوژی نوظهور
- هزینه بر است

مثال

- ارزهای دیجیتال
- بلاکچین‌ها

Amirkabir-Science
علوم نوین امیرکبیر



Traditional Centralized System

1: Decentralization

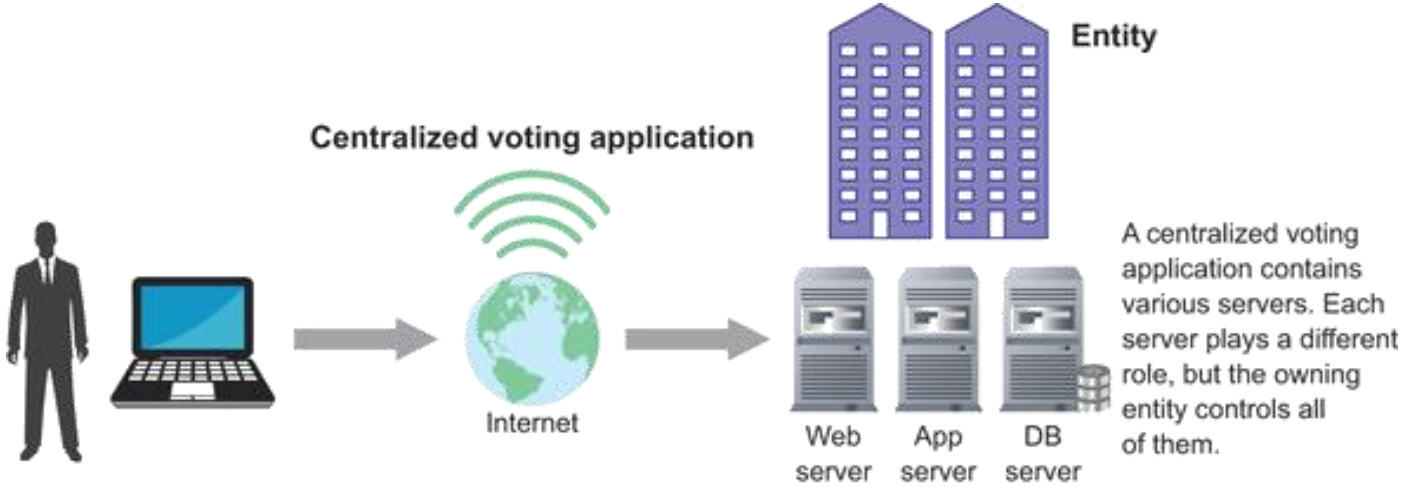
Decentralized System

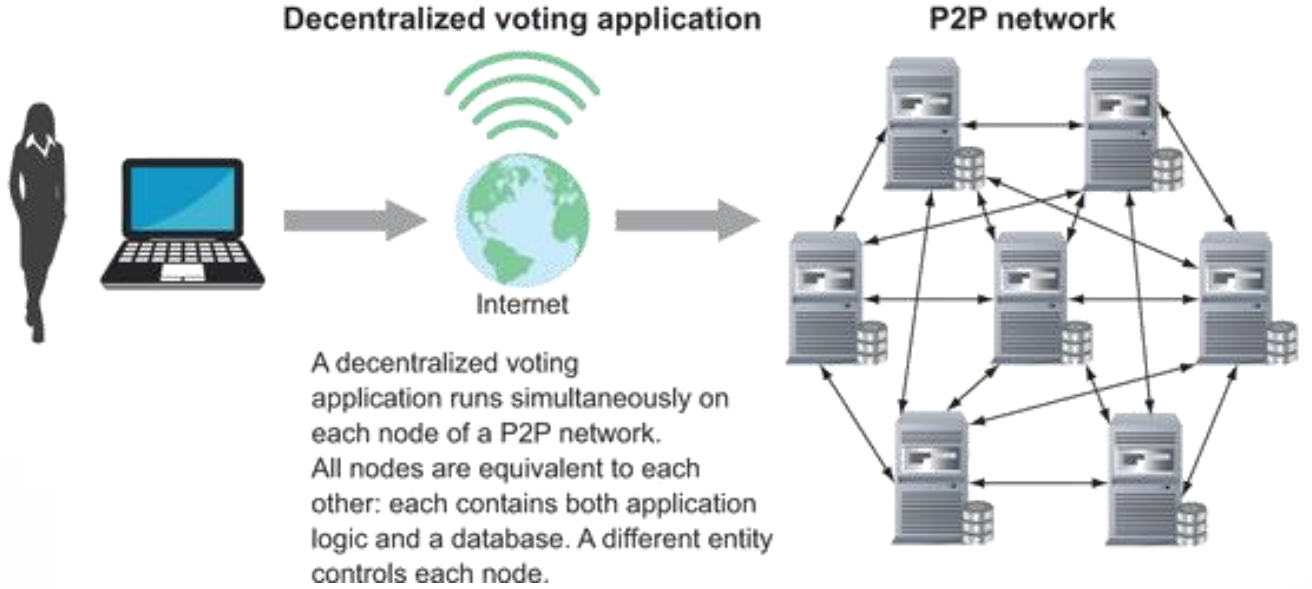
Functions of the intermediaries are shifted to the peer participants and the blockchain nodes:
Disintermediation: validation, recording, verification using blockchain software

8/26/2021

Amirkabir-Science
علوم نوین امیرکبیر

مقایسه رأی گیری در سیستم‌های متمرکز و غیرمتمرکز





Amirkabir-Science
علوم نوین امیرکبیر

- بلاکچین یک دیتابیس توزیع شده است و اطلاعات ثبت شده در آن، تغییرناپذیر (immutable) است.
- یک لجر(Ledger) نظیر به نظیر (P2P) توزیع شده (DLT)
- هر نود از شبکه یک نسخه کامل (کپی محلی) از دیتابیس را دارد و این کپی در همه گره‌ها یکسان است.
- نودها به طور مرتب کپی محلی خودشان را بروزرسانی می کنند.
- هر تراکنش وقتی معتبر خواهد بود که اکثریت نودهای شبکه آن را بپذیرند (51%)
- وقتی بلاک جدیدی تولید می‌شود بلاک‌های جدید در شبکه Broadcast می‌شود.
- با اجرا و راه‌اندازی Client هر کسی می‌تواند یک نود به شبکه بلاکچین اضافه کند.
- توسط اتریوم، انتقال هرگونه ارزشی (اعم از ارز، توکن، مالکیت و ...) بین نودهای شبکه امکانپذیر است.

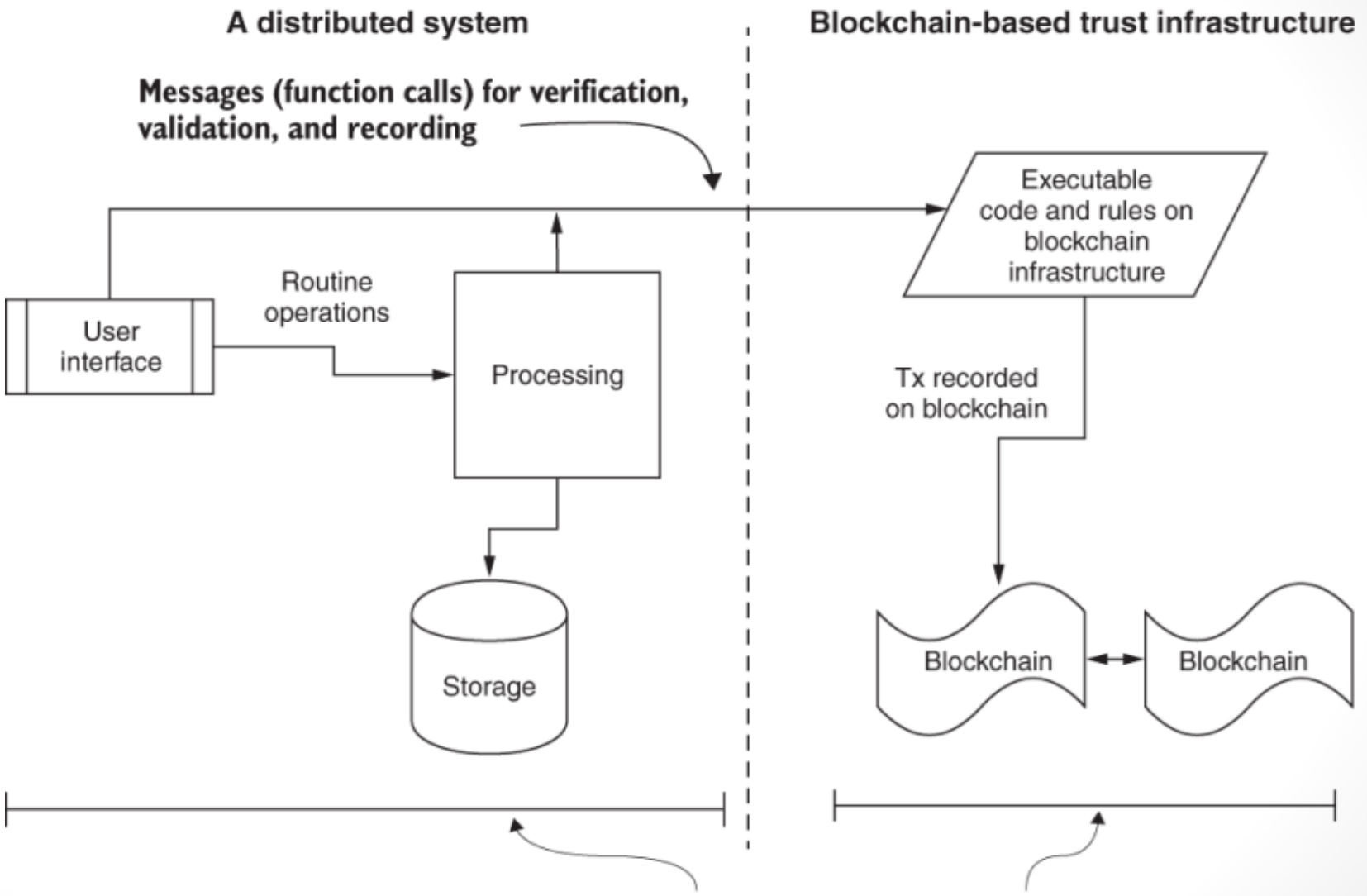
Amirkabir Science
علوم نوین امیرکبیر

- **Private**
  - کاربرد توسط کمپانی‌ها و ارگان‌های **دولتی**
  - برپایی این نوع شبکه به **تعداد نود کمتری** نیاز دارد
  - سطح **تمرکززدایی** در این نوع شبکه **پایین‌تر** بوده و بیشتر در معرض **حمله ۵۱٪** قرار می‌گیرد
  - بلاکچین‌های خصوصی معمولا **permissioned** هستند
- **Public**
  - Bitcoin و Ethereum شناخته‌شده ترین بلاکچین‌های عمومی هستند
  - بلاکچین‌های عمومی اغلب **permissionless** هستند ولی می‌تواند **permissioned** هم باشد

Amirkabir-Science
علوم نوین امیرکبیر

- **مشکلاتی که بلاک‌چین حل می‌کند ولی دیتابیس قادر به حل آن نبود!**
  - بلاکچین کاملا توزیع‌شده است - تحمل‌پذیری خطای بالای دارد
  - بدون تمرکز قدرت
  - عدم نیاز به اعتماد به شخص ثالث
  - عدالت و بهره‌مندی همه افراد جهان از بلاک‌چین بدون اهمیت دادن به مرزهای جغرافیایی
  - ناممکن بودن Double Spending (فروش یک کالا یا خدمات به دو نفر)
  - هزینه معالات پایین‌تر (حذف واسطه ها)

Amirkabir-Science
علوم نوین امیرکبیر



Blockchain programming: you don't replace an existing system but enhance it with code for trust intermediation.

Amirkabir-Science
علوم نوین امیرکبیر

توابع هش یا درهم‌ساز (Hash)

- تابعی است که یک داده دیجیتال با طول دلخواه را به یک داده با سایز ثابت نگاشت می کند.
- توابع هش، یک طرفه بوده و مقدار هش به هیچ روشی قابل تبدیل به مقدار اولیه نخواه بود.
- هش‌های بیتکوین از نوع Sha256 است که بصورت ۲۵۶ بیت یا ۶۴ کاراکتر هگزا دسیمال هستند.
- طول دیتای ورودی هیچ تاثیری روی طول خروجی هش نداشته و سایز خروجی همواره ثابت است.
- ابزارهای آنلاین تولید هش

https://passwordsgenerator.net/sha256-hash-generator/

https://www.tools4noobs.com/online_tools/hash/

Amirkabir-Science
علوم نوین امیرکبیر

توابع هش یا درهم‌ساز (Hash)

- کوچک‌ترین تغییر در ورودی، منجر به تغییرات چشم‌گیری در خروجی می شود.

‘Hello World’ = a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

‘Hello World!’ = 7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069

- تا زمانیکه یک مقدار ورودی تغییر نکند، هش آن ثابت خواهد ماند.
- از ویژگی بالا برای بررسی جامعیت (Integrity) و اصالت دیتا استفاده می‌شود.
- برای حفظ امنیت، معمولاً کلمات عبور به صورت هش شده نگهداری می‌شود.
- آدرس کیف پول (Account Address) در بلاک‌چین از هش کلید عمومی کاربران تولید می‌شود.

Amirkabir-Science
علوم نوین امیرکبیر

آدرس (Address)

- آدرس بلاکچین، مقدار هش شده کلید عمومی کاربر است.
- هر فرد می‌تواند تعداد زیادی آدرس داشته باشد.
- برنامه کیف پول (Wallet) تمام پرداختی‌های صورت گرفته به آدرس شما را نگهداری می‌کند

Amirkabir-Science
علوم نوین امیرکبیر

- در این روش برای رمزنگاری بین دو کاربر یک جفت کلید (Key Pair) تولید می‌شود.
  - کلید عمومی : Public Key
  - کلید خصوصی : Private Key
- کلید عمومی و خصوصی تولید شده در این روش رمزنگاری، با هم جفت (pair) هستند.

Amirkabir-Science
علوم نوین امیرکبیر

- کلید عمومی بدون نگرانی در اختیار عموم قرار می‌گیرد تا بتوانند با مالک کلید ارتباط داشته باشند.
- کلید خصوصی به منزله دسترسی به کیف پول بوده و نباید آن را در اختیار کسی قرار داد.
- وقتی دیتا با یکی از این کلیدها رمز شده باشد فقط از طریق کلید دیگر قابل رمزگشایی خواهد بود.

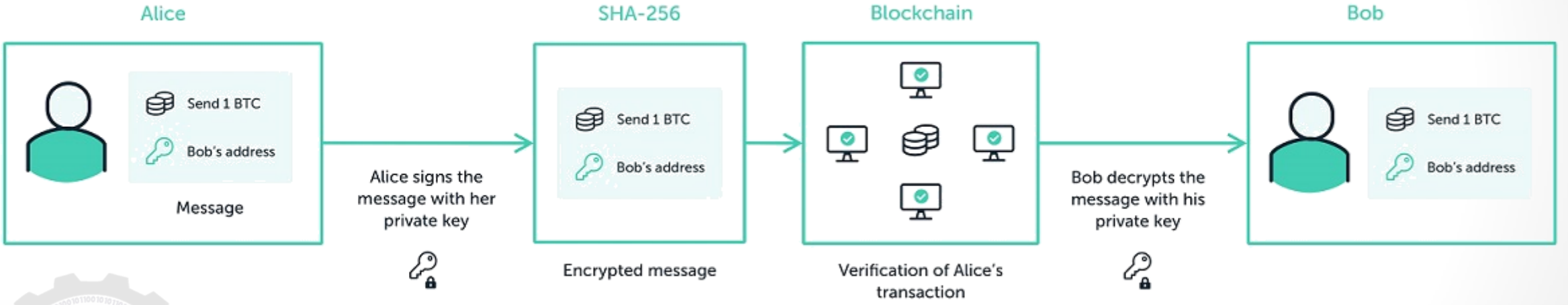
Amirkabir-Science
علوم نوین امیرکبیر

تراکنش (Transaction)

- تراکنش در واقع انتقال مبلغ بین فرستنده و گیرنده را انجام می‌دهد.
- برای اینکه فرستنده مقداری را به گیرنده واریز کند باید آدرس گیرنده را داشته باشد.
- آدرس، همان کلید عمومی (Public Key) گیرنده است.
- اگر گیرنده بتواند ثابت کند که کلید عمومی و خصوصی منطبق با تراکنش وارد شده را دارد اجازه پیدا می‌کند که مقدار ارسالی را دریافت کند.
- هر تراکنش دارای یک برنامه شرطی (در بیتکوین) است که برای انتقال ارز باید برقرار باشد.

Amirkabir-Science
علوم نوین امیرکبیر

- **امضای دیجیتال** به عنوان مهر تایید تراکنش استفاده می‌شود.
- **کلید خصوصی** هر شخص، امضاء دیجیتال آن شخص محسوب می‌شود (با درج امضا روی تراکنش خودش را ثابت می‌کند)



Amirkabir-Science
علوم نوین امیرکبیر

بلاک (Block)

- بلاک‌ها در شبکه بلاکچین واحدهای بسته بندی تراکنش‌ها هستند.
- شماره‌گذاری بلاک‌ها از 0 شروع شده و با گام 1 افزایش می‌یابد.
- به شماره بلوک، ارتفاع بلوک (Height) نیز گفته می‌شود.
- هر بلاک به بلاک قبلی متصل است (از طریق نگهداری هش بلاک قبلی به آن لینک می‌شود).
- هر بلاک به محض ذخیره در بلاکچین غیرقابل تغییر (immutable) می‌شود.

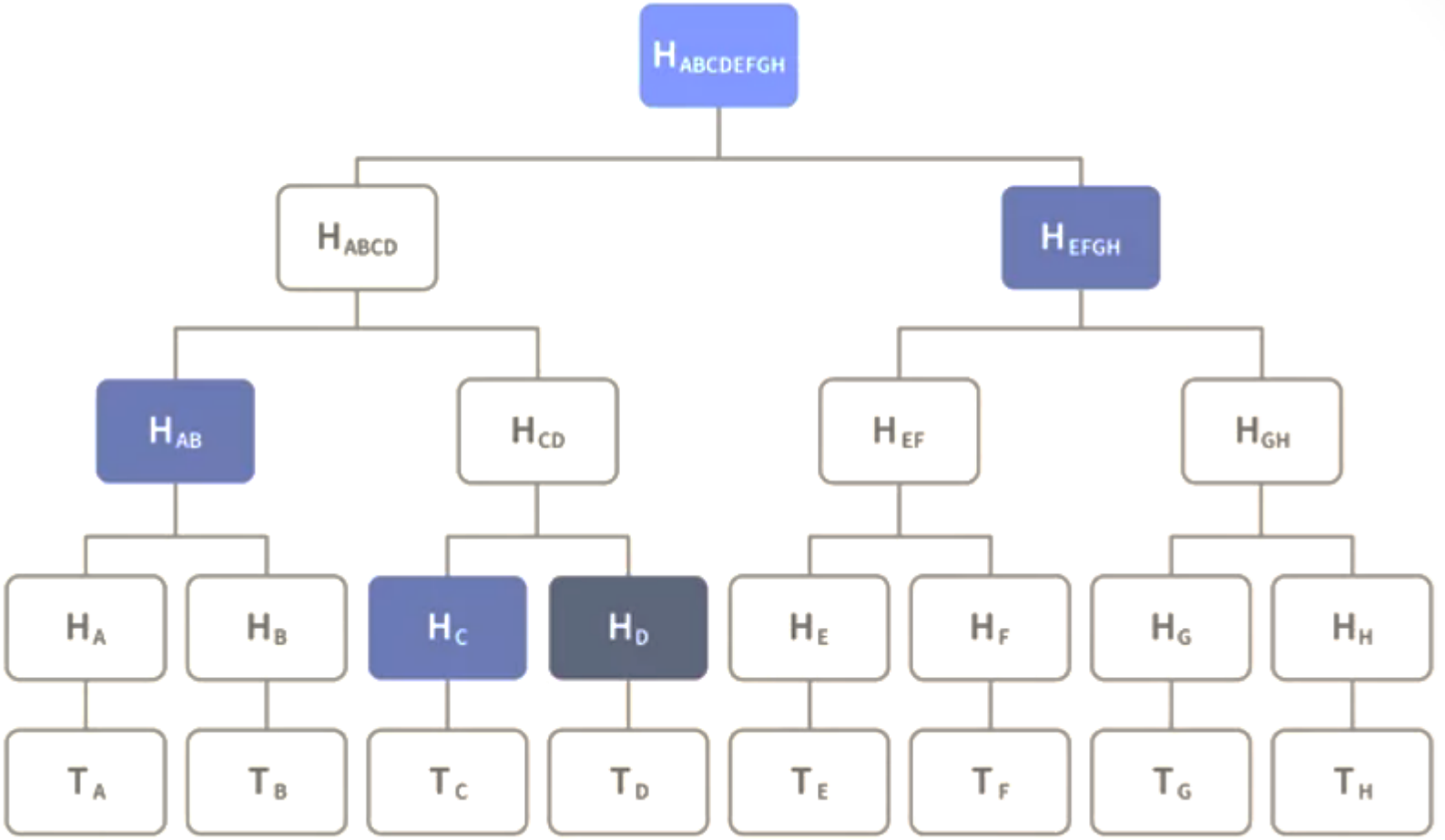
Amirkabir-Science
علوم نوین امیرکبیر

معرفی برخی از فیلدهای بلاک

- **فیلد Timestamp :** برچسب زمانی ساخته شدن بلاک
- **فیلد Transactions :** تمام تراکنش‌های رکورد شده در این بلاک
- **فیلد Difficulty :** سختی ماینینگ
- **فیلد Size :** نشان دهنده حجم دیتای بلاک
- **فیلد Metadata :** ریشه درخت Merkle تراکنش‌های این بلاک
- **فیلد Hash :** هش اطلاعات بلاک که از هش کردن بخش metadata بلاک بدست می‌آید
- **فیلد Parent Hash :** هش بلاک قبلی که یک لینک به بلاک قبلی محسوب می‌شود
- **فیلد Magic Number (0xD9B4BEF9) :** در شبکه بیتکوین این فیلد نشان می‌دهد این بلاک مربوط به شبکه بیتکوین است
- ریشه درخت Merkle تراکنش‌های این بلاک
- **فیلد Nonce :** در الگوریتم pow کاربرد دارد

Amirkabir-Science
علوم نوین امیرکبیر

درخت مرکل (Merkle Tree)



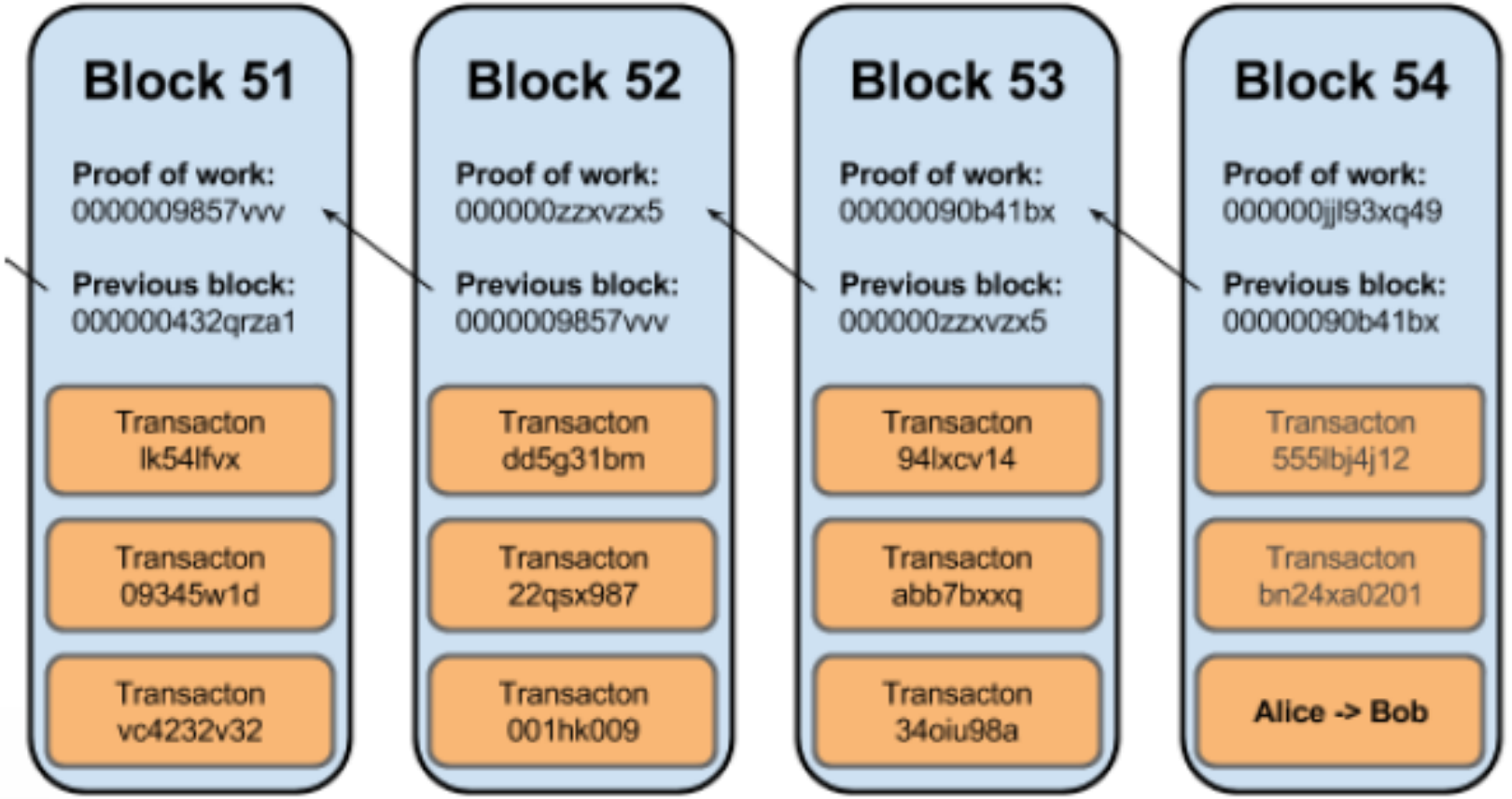
مرجع: www.investopedia.com

Amirkabir-Science
علوم نوین امیرکبیر

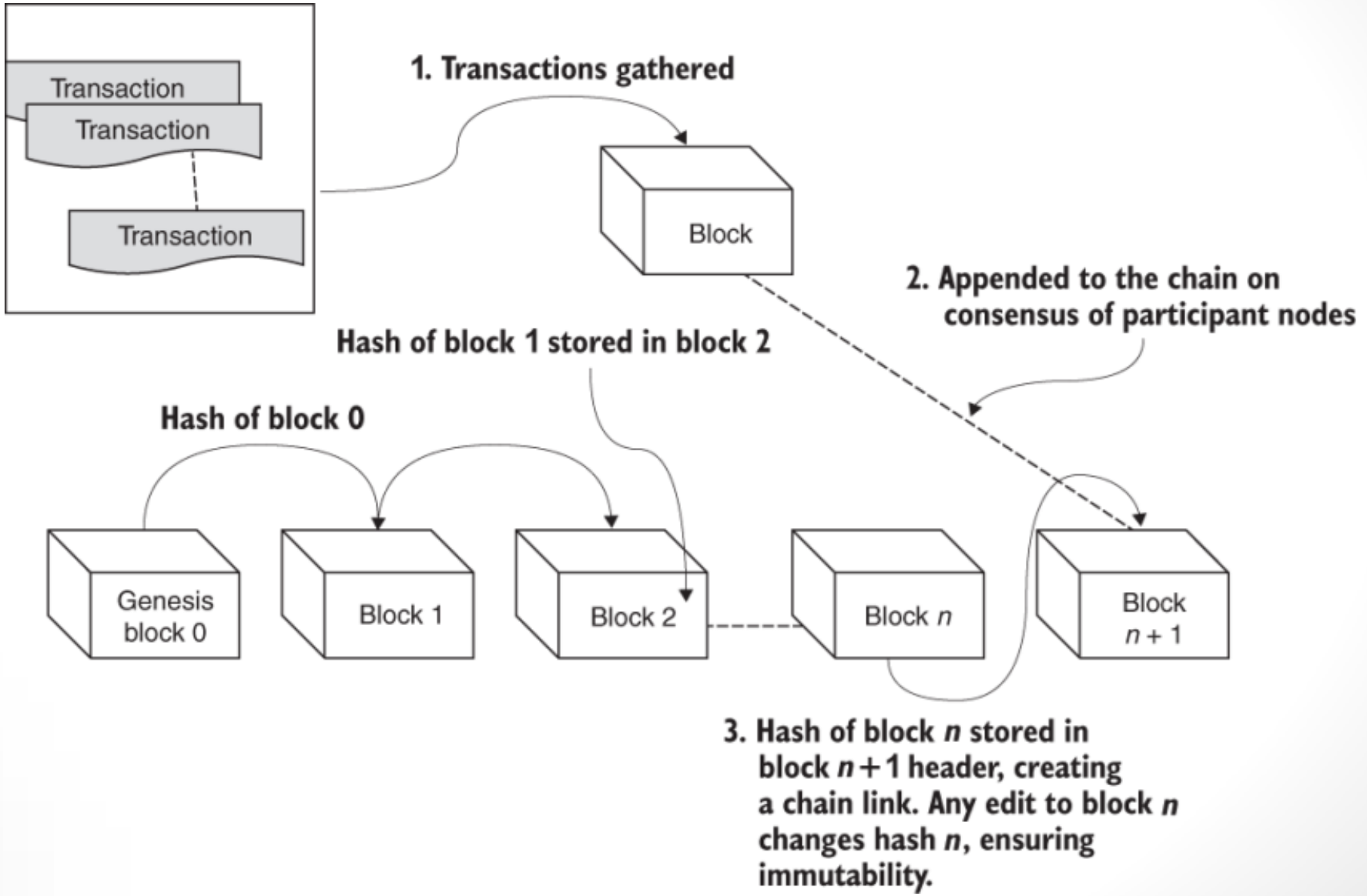
بلاک (Block)

- در بیتکوین از هر ۱۰ دقیقه یک بار، یک بلاک تشکیل می‌شود.
- فرآیند تشکیل بلاک از تراکنش‌ها Mining نامیده می‌شود.
- مشخصه اصلی یک بلاک (شناسه بلاک)، **هش** دیتای داخل آن بلاک (hash) است نه شماره بلاک!
- شناسه بلاک (هش متادیتای بلاک) را می‌توان به عنوان اثرانگشت دیجیتال بلاک در نظر گرفت.
- با کوچکترین تغییر در محتوای تراکنش، **هش ریشه درخت مرکل** تغییر خواهد کرد.
- این موضوع موجب تغییر یافتن **هش متادیتا** و متعاقباً تغییر **هش بلاک** خواهد شد.
- با تغییر **هش بلاک** ، ارتباط زنجیرگونه (**chain**) بین بلاک و بلاک‌های دیگر، قطع خواهد شد (**Broken Chain**)
- گرفتن **هش بلاک**، ساده ترین و سریع ترین راه برای چک کردن **صحت و جامعیت** (**validity and Integrity**) محتوای بلاک است.

Amirkabir-Scient
علوم نوین امیرکبیر



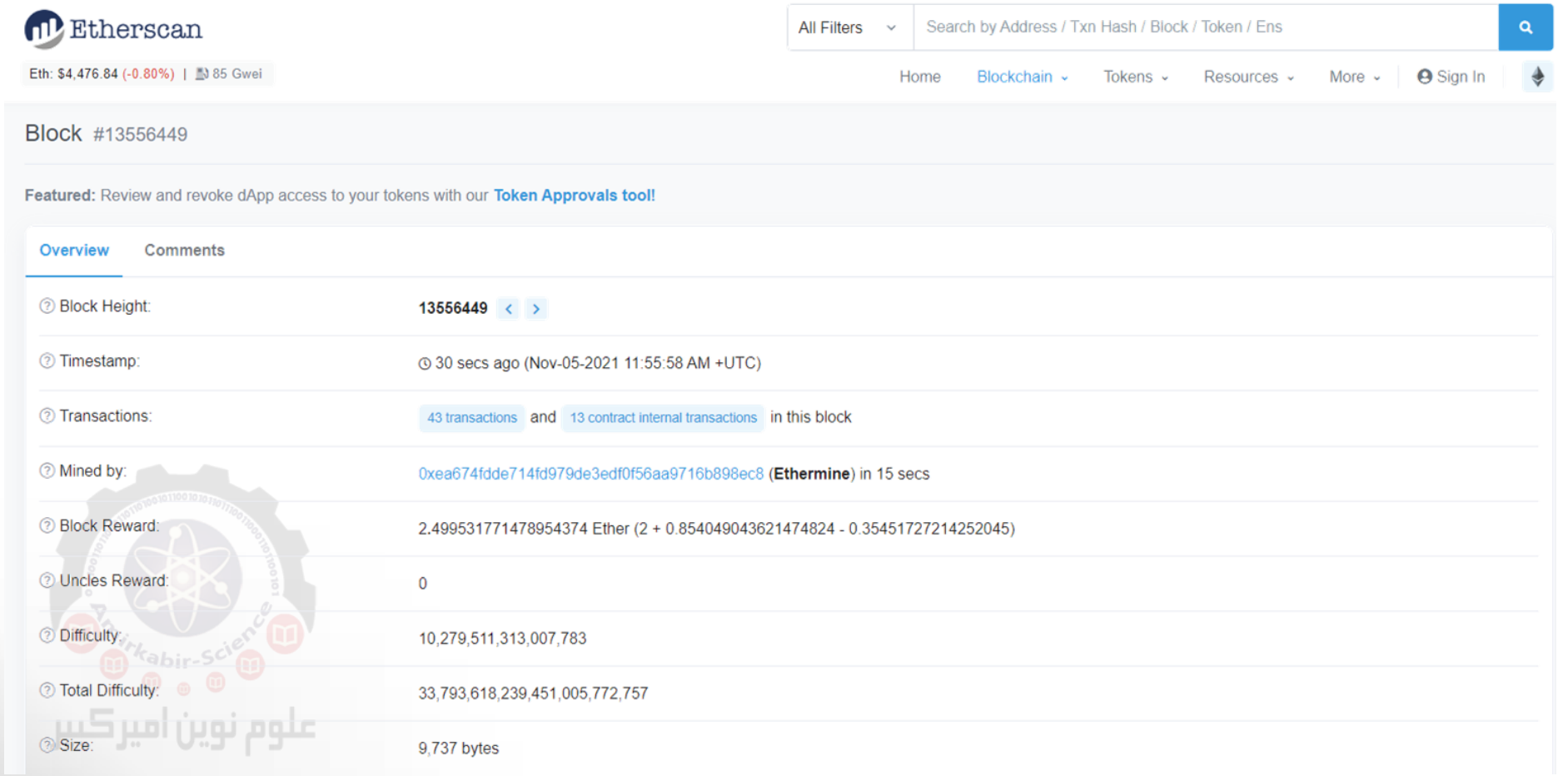
Amirkabir-Science
علوم نوین امیرکبیر



Amirkabir-Science
علوم نوین امیرکبیر

Block Scanner

https://etherscan.io/



- ابتدا شبکه بلاکچین مورد نظر را انتخاب می کنیم.
- سپس ابزار مربوط به Client آن بلاک‌چین را دانلود و نصب می کنیم.
- برنامه Client را اجرا کرده و به کمک آن، بلاکچین مورد نظر را دانلود می کنیم.

Amirkabir-Science
علوم نوین امیرکبیر

Light Weight Client

- این نوع کلاینت، تمام بلاکچین را دانلود نمی‌کند، بلکه به نودهای دیگر متصل شده و تنها اطلاعات تراکنش‌هایی را جمع‌آوری می‌کند که به آدرس خودش مربوط باشد.

Full/Core Client

- به عنوان Full Node در شبکه اجرا شده و کل شبکه را دانلود خواهد کرد.

Amirkabir-Science
علوم نوین امیرکبیر

دانلود برنامه Bitcoin Client

https://bitcoin.org/en/download

- با توجه به سیستم‌عامل، نسخه مناسب را انتخاب و دانلود کنید.
- لینک دانلود کلاینت بیتکوین برای ویندوز

https://bitcoin.org/en/choose-your-wallet?step=5&platform=windows

Amirkabir-Science
علوم نوین امیرکبیر

- دانلود هسته بیت‌کوین

https://bitcoin.org/en/download

https://github.com/bitcoin/bitcoin

Amirkabir-Science
علوم نوین امیرکبیر

بازیگران فضای بلاکچین

Blockchain Companies & Startups

Applications

difacturo, Lenzing, SALZBURG AG, REALEST8, ERSTE Group, Post, WIEN ENERGIE, Verbund

Consulting

accenture, Arthur D Little, hackabu, db, IBM HYPERLEDGER, Catalysts, CryptoRobby, GraphSense, DANUBE TECHCMS, DIGITAL SUNRAY, ROTHARIUM, DIE CRYPTO BERATER, insticore, weavs, SYNERCON, EY, SEEKYOU STRATEGY CONSULTANCY

Crypto Mining

APOLLON CORE GROUP, Coin Factory Austria, CRYPTOUNIVERSE, HYDROMINER, Bitfly, Bitkern

Development & Software

0bsnetwork, baumann.at, BLOCKSERV, SAP, capacity, blocklancer, lab10, iov42, os Alliance, chainlock, Salamantex, Crypto Consulting, iteratec, 4YI, BLOCK42, Riddle & Code

Exchange, Trading, Investing

BITPANDA, COINNECTING, BitPocket, COIN300VEST, coinfinity, BLACK MANTA, CRYPTO Management, APOLLON NETWORK, AUTOWHALE, e-Bitstore, cobra, Trever, FairCoin, SCYTALE VENTURES, iQCashNow

Legal & Tax

AKARION Innovating Trust, STADLER VOLKEL, JP JAROLIM PARTNER, KUNZ WALLENTIN, KPMG, HERBST KINSKY, CMS, WRIP, blockpit, enzinger, HELLER CONSULT, BDO, BINDER GRÖSSWANG, schönherr, BRANDL & TALOS RECHTSANWÄLTE · ATTORNEYS AT LAW, DLA PIPER, WOLF THEISS

Startup

Minerva, finnoq, AVINOC, element36, YOUNIQX, ELYP, helpar, HERSPHERE, CONDA, ARTIS, grapevine WORLD, CRYPTIX, experio.at, lin4, JAROONA, Singularity

Enablers & Extended Ecosystem

Universities & Educational Institutions

Donau Universität Krems, universität wien, ANITA POSCH, BITFANTASTIC, FH Salzburg, fhstp st.pölten, CRYPTO SKILLS ACADEMY, TU WIEN TECHNISCHE UNIVERSITÄT WIEN, FinTech Blockchain Academy, WU, VOMTOM.AT, eigenheads academy, UNI GRAZ, TECHNIKUM WIEN ACADEMY, ÖAW, MODUL UNIVERSITY VIENNA PRIVATE UNIVERSITY, universität innsbruck

Research

ABC Austrian Blockchain Center, AIT Austrian Institute of Technology TOMORROW TODAY, RIAT Institute for Future Cryptoeconomics, SBA Research

Organisations

bitcoin austria, AUSTRIAN STANDARDS, CITY OF BLOCKCHAIN, DIGITAL CITY WIEN, IoT AUSTRIA, AUSTRIA BLOCKCHAIN, smartBlockchain, BlockchainHub, blockchainers.at

Public

ADVANTAGE AUSTRIA, BRZ, HANDELS VERBAND, StaDt Wien

Media

addendum das, was fehlt, der brutkasten, Die Presse, DECENTRALBOX, derStandard.at, futurezone TECHNOLOGY NEWS, TRENDING TOPICS

Accelerators & Incubators

FACTORY 300, weXelerate, ELEVATOR LAB

Conferences

B19, Block & Wine, ANON BLOCKCHAIN SUMMIT AUSTRIA 2019

Presented by enliteAI & CryptoRobby

© EnliteAI GmbH, supported by CryptoRobby.com - Vienna - v2.1 27.6.2019, Licensed under CC BY-ND 4.0

www.enlite.ai **contact:** blockchain@enlite.ai

مطالعه بیشتر

- آشنایی با دائو | سازمان های خودگردان غیرمتمرکز
- آشنایی با فناوری بلاکچین | بزرگترین اختراع قرن ۲۱ بعد اینترنت
- آشنایی با DLT – فناوری دفتر کل توزیع شده - تکنولوژی زیرین بلاکچین
- آشنایی با ارز دیجیتال بیتکوین
- حمله ۵۱ درصد (حمله اکثریت) در بلاکچین
- آشنایی با انواع نود و کلاینت در بلاکچین
- آشنایی با متامسک – کیف پول بلاکچین
- فورک چیست | تفاوت هارد فورک و سافت فورک بلاکچین
- شبکه های بلاکچین | بهترین پلتفرم های توسعه در بستر بلاکچین
- نوجوان ۱۹ ساله کانادایی، خالق ارز دیجیتال اتریوم
- ترایورجنس | بلاکچین ، هوش مصنوعی و اینترنت اشیاء
- کاربرد بلاک چین، هوش مصنوعی و اینترنت اشیا در حوزه سلامت

Amirkabir-Science
علوم نوین امیرکبیر

برنامه نویسی بلاکچین و قرارداد هوشمند

سید مجید شبیری

کارشناسی ارشد IT، گرایش شبکه

از دانشگاه صنعتی امیرکبیر

ETHEREUM SOLIDITY

TRUFFLE WEB3.JS Ganache