بسم الله الرحمن الرحيم

مبانی فنی ، اقتصادی و فقهی رمزارزها

مورد مطالعه بیت کوین

7/15/2019

فهرست مطالب

- ✓ نحوه شکل گیری رمز ارزها و فناوری بلاکچین
- ✓ نحوه انجام یک تراکنش در بیت کوین
- ✓ معرفی اجمالی برخی از کوین ها مانند اتریوم، تتر و...
- ✓ تحلیل اقتصادی رمز ارزها با توجه به اقتصاد ایران
- ✓ بررسی فقهی رمز ارزها

مقدمه

- مکاتب اقتصادی
- کلاسیک
  - آزادی فردی
  - دست نامرئی آدام اسمیت
  - حفظ حریم شخصی
  - مخالف رگولاتوری
  - مخالف نهاد مرکزی
  - بازار آزاد
- غیر کلاسیک
  - ضرورت وجود رگولاتور و نهاد مرکزی
  - بازار کارا توسط دخالت شخص ثالث

مقدمه

- ایده اصلی اینترنت: راهی برای آزادی فردی و حفظ حریم شخصی برای انتقال **داده**
  - در زمان های بعد، واسطه های ارائه دهنده خدمات این معنا را تغییر دادند.
- مکتب اتریش و مصاحبه «هایک»
  - غیرمتمرکز سازی پول
- پیدا کردن راهی برای آزادی فردی و حفظ حریم شخصی برای انتقال **ارزش**
  - تفاوت ارزش و داده
  - مساله اصلی: مشکل دوبار خرج کردن (کپی کردن داده)

مقدمه

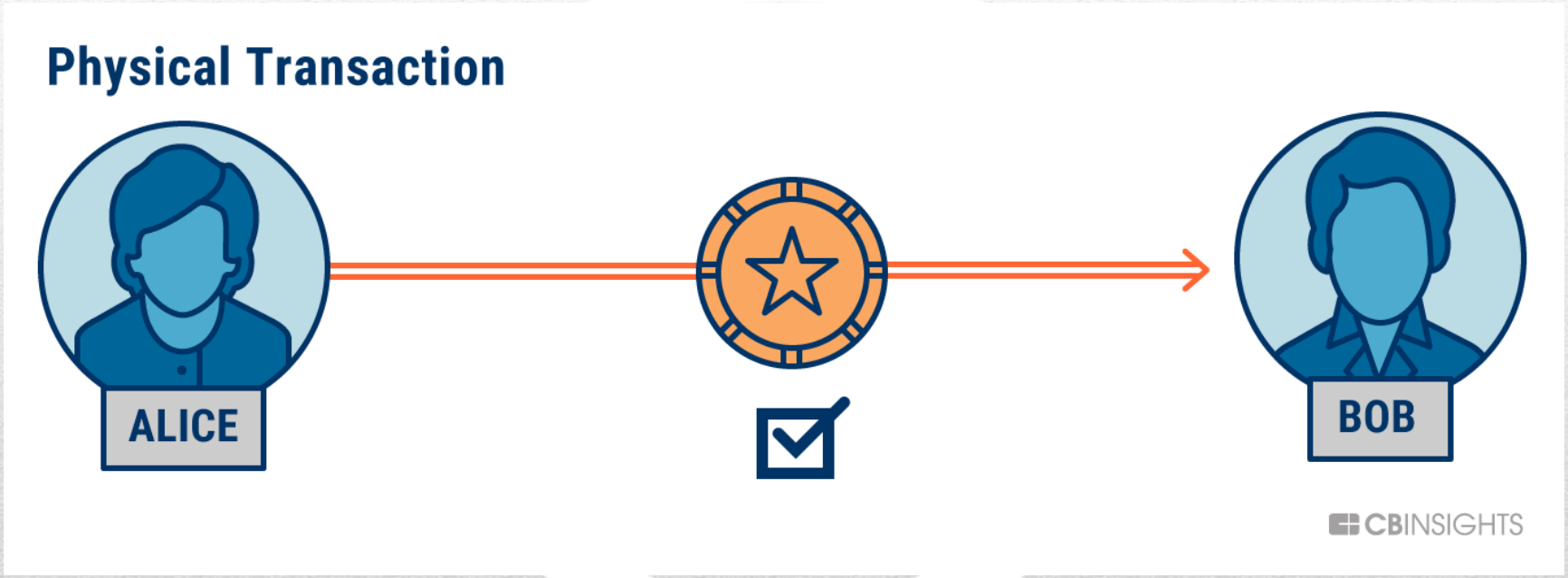
- مشکل دوبار خرج کردن
  - تلاش هایپرپانک ها (عاشقان رمزنگاری)
  - هال فینی
- بحران مالی ۲۰۰۸ و ۲۰۰۹ و تشدید دغدغه
- حل مشکل دوبار خرج کردن با فناوری بلاک چین در قالب بیت کوین
  - ایده اصلی بیت کوین حذف سلطه بانک ها و یک پول فرد به فرد (آزادی)
  - پیام اصلی بلاک پیدایش:
    - روزنامه The Times در تاریخ ۳ ژانویه ۲۰۰۹: رئیس خزانه‌داری [انگلستان] در آستانه‌ی اهدای کمک مالی دوم به بانک‌ها است!

بلاک چین چیست؟

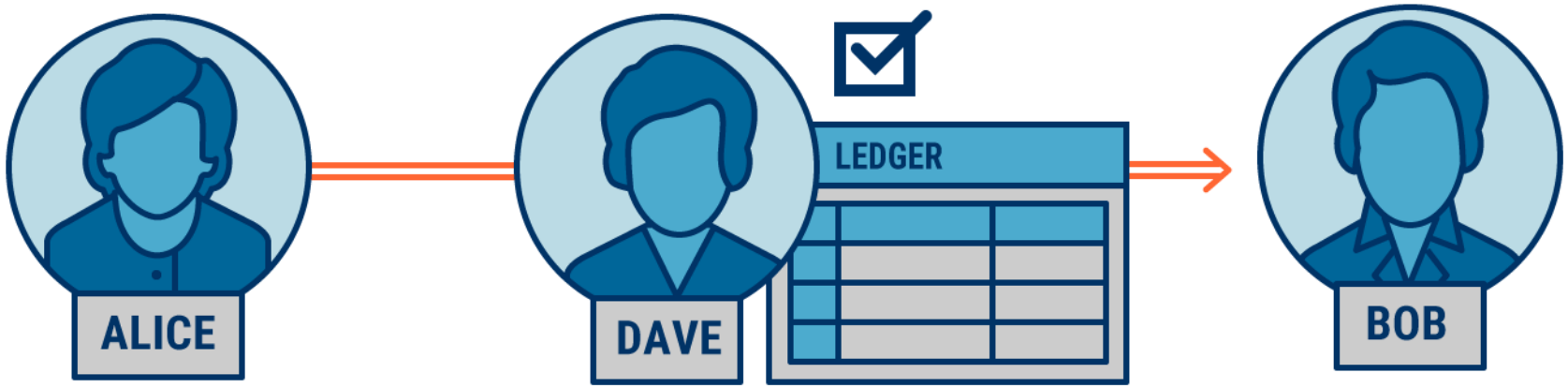
- ✓ یک مفهوم سهل و ممتنع
- ✓ بلاک چین چیزی جز یک دفتر کل ثبتی نیست!
- ✓ بلاک ها هر صفحه دفتر و زنجیره ها همان مهر و سیم نگهدارنده دفتر است.
- ✓ نوآوری اصلی : حذف واسطه در تبادلات و در عین داشتن کارکرد آن
  - ❖ حل مشکل دوبار خرج کردن از طریق مکانیزم اجماع

دو کارویژه نهاد واسط و ثالث

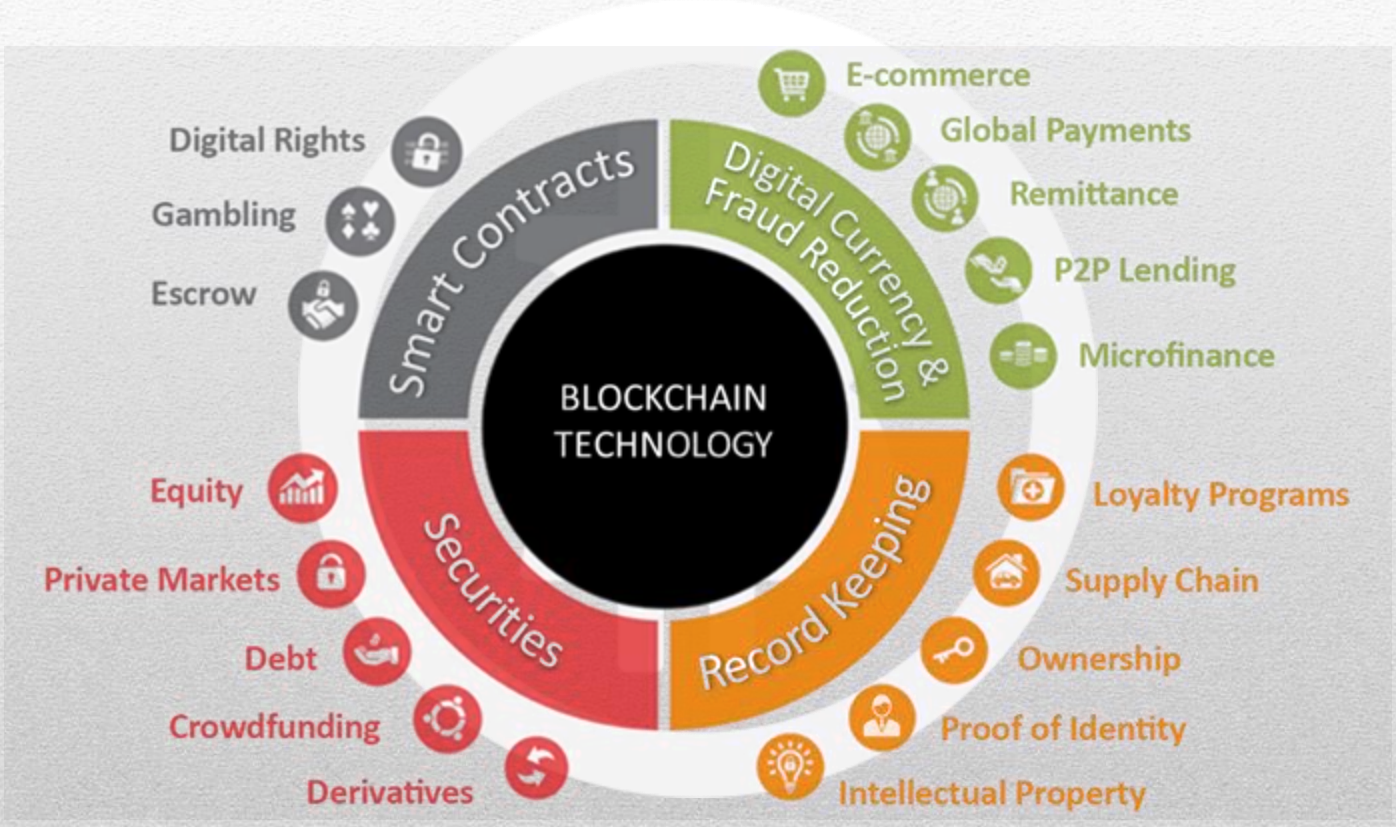
- ✓ نگهداری دفتر کل و ثبت تراکنش ها – مساله اعتماد
- ✓ تایید اصالت تراکنش ها – مساله اعتماد


Physical Transaction
ALICE
BOB
CBINSIGHTS

Digital Transaction: Ledger




Decentralized Ledger
ALICE
BOB
CBINSIGHTS


BLOCKCHAIN TECHNOLOGY
Smart Contracts
Digital Currency & Fraud Reduction
Securities
Record Keeping
Digital Rights
Gambling
Escrow
E-commerce
Global Payments
Remittance
P2P Lending
Microfinance
Equity
Private Markets
Debt
Crowdfunding
Derivatives
Loyalty Programs
Supply Chain
Ownership
Proof of Identity
Intellectual Property

بیت کوین اولین نمونه بلاک چین

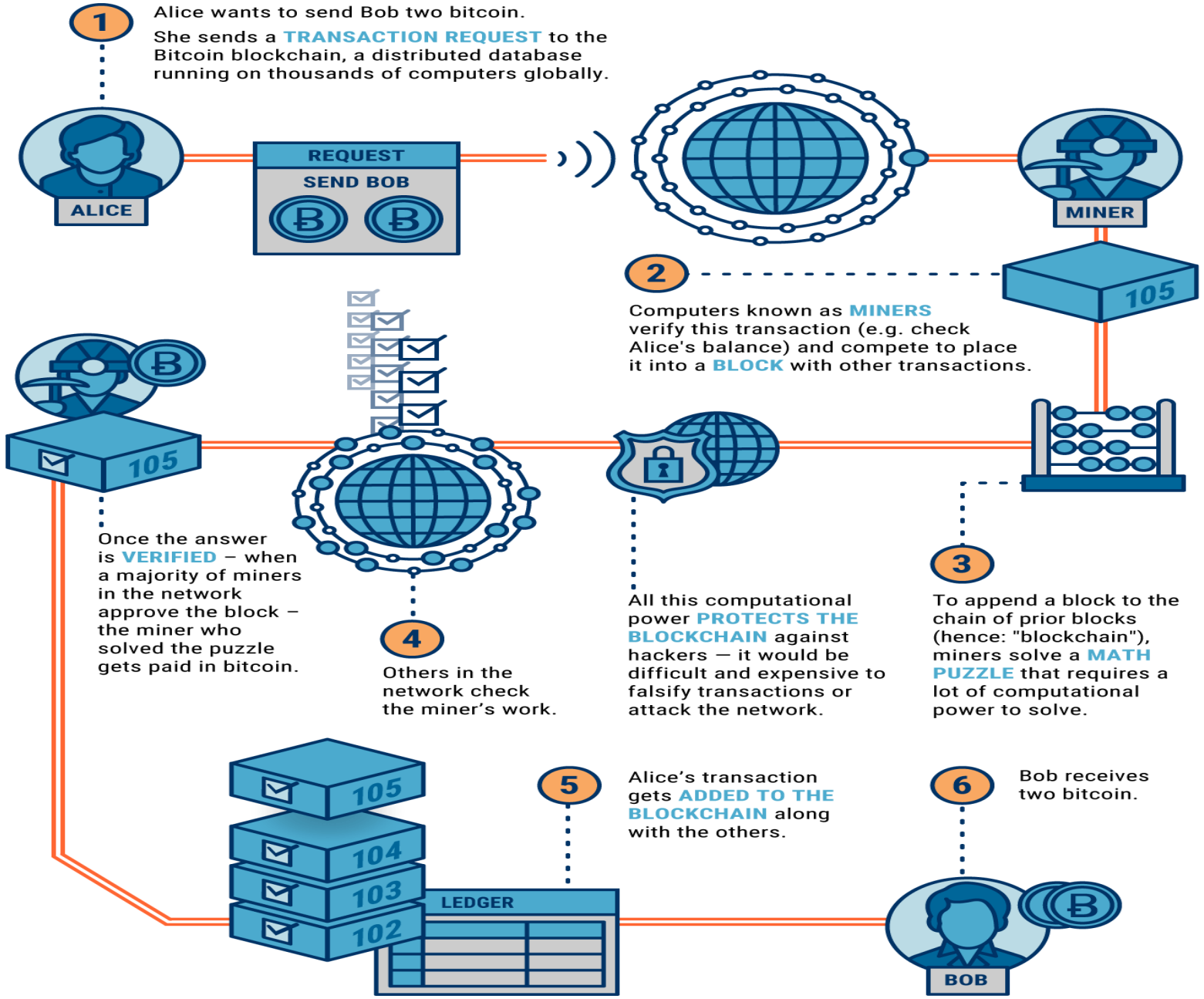
- ✓ رای گیری
- ✓ زنجیره تامین
- ✓ قرارداد هوشمند
- ✓ پرونده سلامت
- ✓ و هر کار ثبتی...

نحوه انجام یک تراکنش در بیت کوین

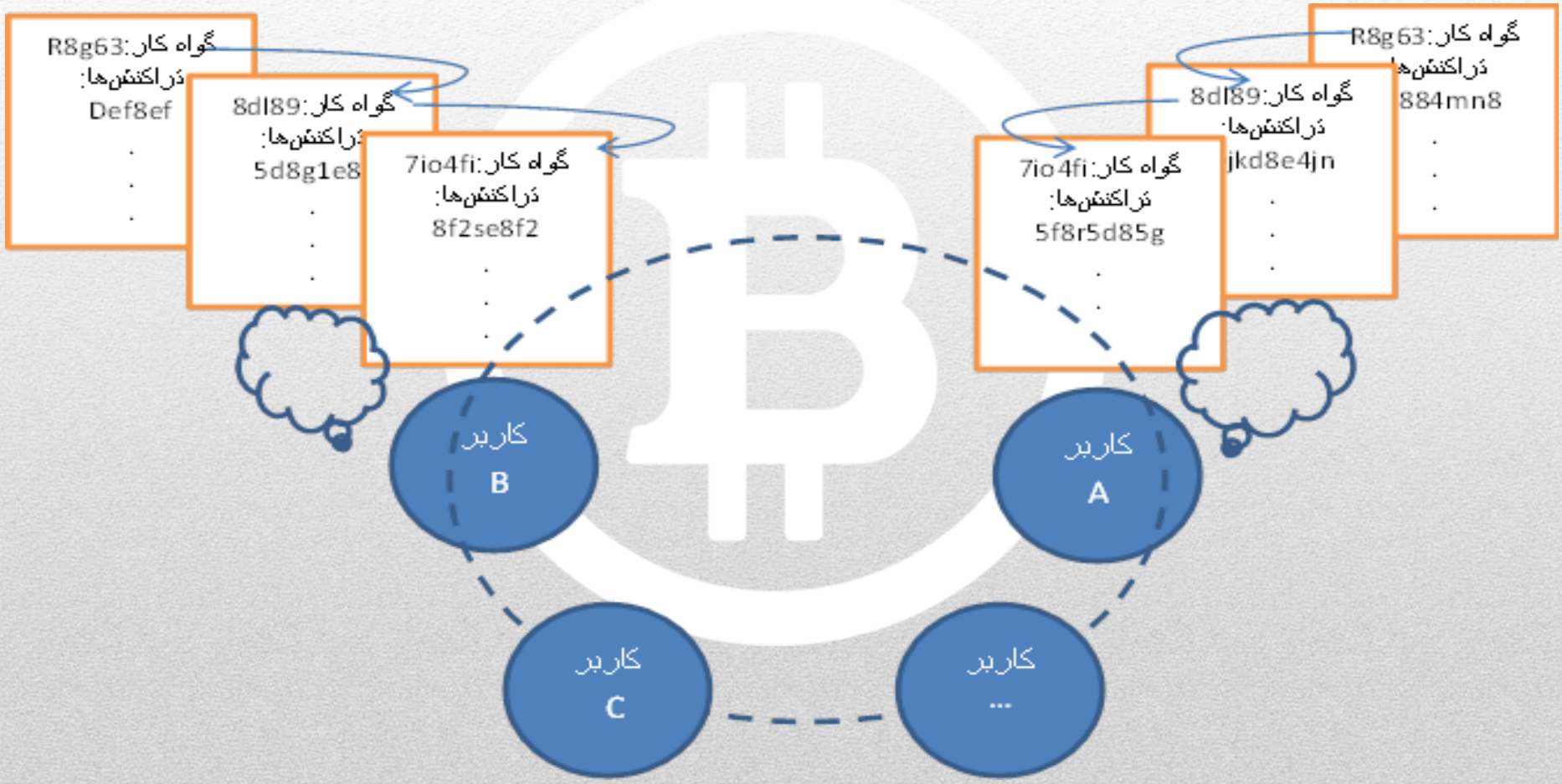
- ✓ مفهوم بلاک (Block)
- ✓ تابع Hash
- ✓ کلید خصوصی و عمومی(Private key and Public Key)
- ✓ معدن کاوی(Mining)
- ✓ اجماع (Consensus)
- ✓ حمله ۵۱ درصدی
- ✓ مشکل دوبار خرج کردن(Double Spending Problem)

Understanding a bitcoin transaction

HOW BLOCKCHAIN TECHNOLOGY POWERS BITCOIN



بستر عملیاتی پول رمزنگاری شده – زنجیره بلوکی



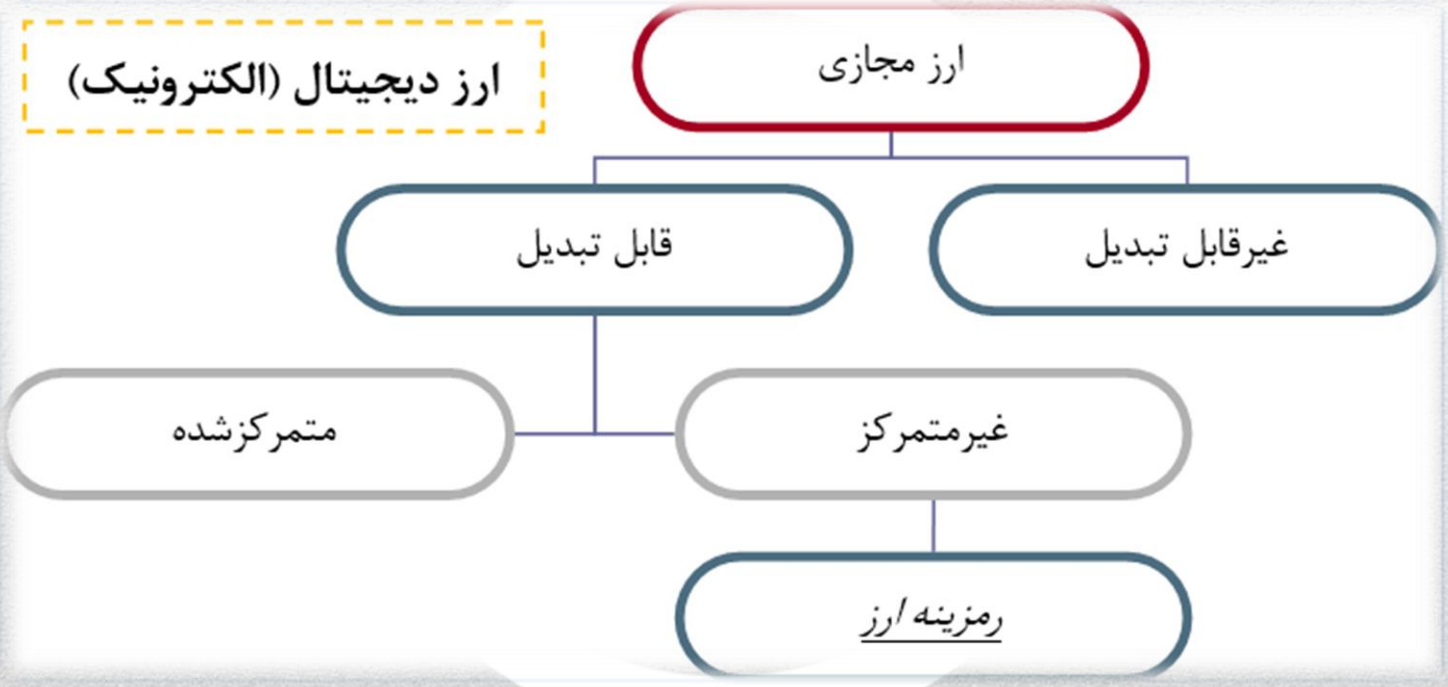
ماینینگ چیست؟

- ✓ **کارکرد ماینرها در شبکه**
- ✓ **نحوه پاداش دهی در بیت کوین**
- ✓ **مساله ای که باید ماینرها حل کنند چیست؟**
- ✓ **انواع مکانیزم های اجماع:**
  - ❖ POW: اصالت کار
  - ❖ POS: اصالت سرمایه
  - ❖ اصالت افراد (تعاونی)
  - ❖ هش گراف
  - ❖ Stellar Consensus Protocol (SCP) و ...

چند مفهوم

- ✓ هش
- ✓ کیف پول و انواع آن
- ✓ کلید عمومی و خصوصی
- ✓ نحوه مبادله و ذخیره

واژه شناسی


ارز دیجیتال (الکترونیک)
ارز مجازی
قابل تبدیل
غیرقابل تبدیل
متمرکزشده
غیرمتمرکز
رمزینه ارز

موضوع شناسی

	متمرکز	غیرمتمرکز
قابل‌تبدیل	این پول دارای یک نهاد مرکزی است و استفاده‌کنندگان از این پول می‌تواند آن را از طریق صرافی‌ها به اسکناس بانکی تبدیل نمایند. مثال: وب مانی (Web Money)	این پول هیچ نهاد مرکزی ندارد و نیاز به اعتماد به شخص ثالث نیست و استفاده‌کنندگان از این پول می‌توانند آن را از طریق صرافی‌ها به اسکناس بانکی تبدیل نمایند. (ارز رمزگذاری شده) مثال: بیت‌کوین، لایت‌کوین(Litecoin)
غیرقابل‌تبدیل	این پول دارای یک نهاد مرکزی است و استفاده‌کنندگان از این پول نمی‌تواند آن را به اسکناس بانکی تبدیل نمایند. مثال: سکه بازی World of Warcraft	در حال حاضر وجود ندارد

مقایسه پول رمزنگاری شده با پول حاکمیتی و طلا

تفاوت با پول بانکی	شباهت با طلا
عدم نیاز به نهاد مرکزی برای جابه‌جایی پول (پول خصوصی)	عدم وجود نهاد مرکزی، واسط و ناظر
عدم توانایی دخالت دولت در تولید و خلق پول	محدود بودن منابع
مخفی ماندن هویت فرستنده و گیرنده (در بیت کوین)	تولید پول به‌وسیله عملیات استخراج
تحت حمایت دولت نیست و پشتوانه دولتی ندارد	دولت هیچ دخالتی در خلق آن ندارد
هزینه عملیاتی ناچیز (در سطح بین‌المللی)	قیمت آن به‌وسیله عرضه و تقاضا کشف می‌شود
سرعت انتقال بالا (در سطح بین‌المللی)	

برخی از انواع رمزارزها

- **بیت کوین**
- **ریپل**
- **تتر**
  - رمزارزهای با ثبات
- **اتریوم و قرارداد هوشمند**
  - عرضه اولیه سکه (ICO)

تحلیل اقتصادی رمز ارزها

- ✓ **ماهیت اقتصادی رمزارزها**
  - ❖ پول
  - ❖ کالا
  - ❖ اوراق بهادار

مزایا

- آزادی در پرداخت و دسترسی بین‌المللی
- هزینه عملیاتی پایین
- سرعت بالا در انتقالات بین‌المللی و فرامرزی
- عدم خلق پول بی‌رویه در اقتصاد و کنترل تورم
- استفاده از پول های رمزنگاری شده در شرایط تحریمی ایران
- عدم توانایی دولت‌ها در مصادره و بلوکه کردن
- امکان رهگیری و شفافیت
- امکان انشعاب و ارتقای پروتکل
- عرضه اولیه سکه
- قراردادهای هوشمند

چالش ها

- نوسانات قیمتی و عدم ثبات
- فقدان قوانین و مقررات مشخص
- تهدید اقتصاد واقعی
- مشخص نبودن هویت فرستنده و گیرنده
- تضعیف بانک مرکزی و نهادهای واسط
- امکان فرار مالیاتی، پول‌شویی و گسترش بخش غیررسمی اقتصاد
- بروز مشکلات امنیتی
- مشکل وراثت
- ابهام در ماهیت پول های رمزنگاری شده
- عدم حفظ ارزش

چالش ها

- برگشت‌ناپذیری وجه
- تهدید رقبا
- فقدان مستند قانونی و توانایی طرح دعوی و پیگیری حقوقی
- تأمین مالی گروه‌های تروریستی و معاند سیاسی
- نقدشوندگی پایین در اقتصاد ایران
- ناآشنایی عموم مردم با پول های رمزنگاری شده
- عدم امکان تجهیز و تخصیص منابع به فعالان اقتصادی
- امکان انشعاب و شکستن محدودیت
- زمان بالای تایید تراکنش در مبادلات داخلی
- خروج ارز از کشور
- مصرف بالای انرژی
- کامپیوترهای کوانتومی

رویکردها

- **فقه فردی**
  - احکام ثمن و مثمن (مالیت، معلوم و معین، ملک طلق فروشنده، قدرت بر تسلیم و تحویل)
  - اصول چهارگانه معاملات (ممنوعیت ضرر، غرر، اکل مال به باطل و ربا)
  - حفظ حریم شخصی، مالکیت و سرمایه افراد
- **فقه حکومتی**
  - اصل کلی «لا ضرر و لا ضرار»
  - اصل کلی «نفی سبیل»
  - اصل کلی «رعایت مصلحت مسلمین»
  - اصل کلی «عدالت و مبارزه با ظلم»
  - اصل کلی «امانتداری»
- **مقایسه ای**
  - با طلا
  - با پول بانکی و بدون پشتوانه

سطوح

- معاملات بر روی پول های رمزنگاری شده به عنوان کالا و سرمایه گذاری
- انجام معاملات بوسیله پول های رمزنگاری شده به عنوان پول
- معدن کاوی و ایجاد پول رمزنگاری شده

تعیین ابعاد فقهی

	فقه فردی	فقه حکومتی
استخراج	اکل مال به باطل	اسراف انرژی هدر رفت منابع
معامله	احکام ثمن و مثمن اصول چهارگانه معاملات حفظ مالکیت و سرمایه افراد	لا ضرر و لا ضرار امانتداری نفی سبیل عدالت

تعیین ماهیت

پول
زنجیره بلوکی خصوصی
مانند ریپل

کالا
زنجیره بلوکی عمومی
مانند بیت کوین

اوراق بهادار
عرضه اولیه سکه (ICO)
مانند اتریوم

چالش ها و سوالات فقهی

- ✓ آیا رویکرد فقه شیعه در مواجهه با پول، تأییدی و امضایی است؟ آیا صرف اینکه مردم به چیزی به‌عنوان وسیله مبادله اعتبار دهند و آن شی مخالفتی با اصول اسلامی نداشته باشد کافی است؟

چالش ها و سوالات فقهی

- ✓ آیا پول مورد تأیید فقه شیعه فقط منحصر به نقدین می‌باشد؟
- ✓ از منظر فقه، ارزش و مالیت ناشی از چیست؟

چالش ها و سوالات فقهی

- ✓ آیا پول رمزنگاری‌شده مالیت دارد؟

چالش ها و سوالات فقهی

- ✓ آیا بحث «پشتوانه» جایگاهی در مباحث فقهی دارد؟ آیا لازم است پول رمزنگاری شده پشتوانه داشته باشد؟

چالش ها و سوالات فقهی

- ✓ آیا معامله با بیت کوین از مصادیق معاملات غرری محسوب می گردد؟ شبهه غرر از این منظر که اصل وجود، اعتباردهنده، هدف از انتشار و ارزش آن همگی مبهم است

چالش ها و سوالات فقهی

- در سیستم بیت‌کوین راه برای مصادیق «اکل مال به باطل» همانند پولشویی و باج‌افزارها و همچنین تأمین مالی گروه‌های معاند (در تضاد با قاعده نفی سبیل) باز است و این امور را تسهیل می‌بخشد. همچنین فرار مالیاتی از جمله کارکردهایی است که با بیت‌کوین می‌توان به راحتی انجام داد و در سرتاسر دنیا این مسأله مشاهده می‌شود. اگر چنانچه فرض شود سیستم أخذ مالیات عادلانه است و در صورت عدم پرداخت آن، امور مسلمین مختل می‌گردد، آیا استفاده از این پول با ویژگی‌های فوق‌الذکر از منظر فقه شیعی جایز است؟

چالش ها و سوالات فقهی

- یکی از شبهات مهم در رابطه با پول رمزنگاری‌شده، شبهه ضرر و عدم رعایت مصلحت عامه است. بدین معنا که اولاً این احتمال را می‌دهند که شاید برنامه به‌گونه‌ای طراحی شده باشد که پس از رسیدن به مرحله‌ای به طور کامل منحل شود.
- ثانیاً مطرح می‌شود که شاید این پول توسط دولت آمریکا درست شده و بیش از ۵۰ درصد شبکه دست آمریکا باشد و با رشد قیمتی آن درصدد تسویه بدهی‌های جهانی خود است. آیا این مسأله از منظر فقه دارای اشکال است؟

چالش ها و سوالات فقهی

- برخی ادعا می‌کنند که احتمال دارد یکی از انواع پول‌های رمزنگاری‌شده مثلاً بیت‌کوین خریداری شود و بعد از مدتی این نوع پول توسط دولت‌ها غیرقانونی اعلام شود و یا یک نوع پول رمزنگاری‌شده جذاب‌تری عرضه شود و دیگر کسی بیت‌کوین را نپذیرد و چون بیت‌کوین ارزش ذاتی فیزیکی ندارد در این حالت کل سرمایه دارندگان بیت کوین نابود شده و متضرر می‌شوند. آیا این مسأله مصداق ضرر و ضرار است؟.

چالش ها و سوالات فقهی

- ✓این شبهه مطرح است که در پول رمزنگاری‌شده دولت نمی‌تواند سیاست‌های پولی و مالی خود را پیاده نماید و این مساله به ضرر عامه مردم تمام می‌شود.آیا این شبهه وارد است؟

چالش ها و سوالات فقهی

- ✓ آیا در عملیات اثبات گواه کار شبهه قمار وجود دارد؟

چالش ها و سوالات فقهی

- ✓ آیا مهم است که مخترع پول رمزنگاری‌شده کیست و هدف او چه بوده است؟ مثلاً اسرائیل برای اهداف مجرمانه؟

چالش ها و سوالات فقهی

- ✓ آیا وجود نهاد ناظر و واسط در فقه الزامی است؟ بدون وجود چنین نهادی دولت نمی‌تواند بر اموال مردم نظارت داشته باشد و از آنان مالیات اخذ کند.

چالش ها و سوالات فقهی

- ✓ آیا اینکه امکان هک شدن سیستم وجود دارد مشکل شرعی ایجاد می‌نماید؟

چالش ها و سوالات فقهی

- ✓ آیا حکم فقهی پول‌های رمزنگاری‌شده به لحاظ تعلق زکات، کنز، خرید و فروش، وقف، به عنوان سرمایه در مضاربه و تعلق خمس به افزایش ارزش اسمی آن با پول‌های بانکی فرق دارد؟

با تشکر