

# جزوه جلسه ۱: فراتر از ترید

## ریشه‌های پول، بحران اعتماد و تولد بیت کوین



### ایده محوری

بیت کوین صرفاً یک دارایی دیجیتال برای نوسان‌گیری یا یک فناوری کامپیوتری جدید نیست؛ بلکه یک پاسخ انقلابی به قدیمی‌ترین مشکل اقتصاد بشر یعنی «اعتماد» است. بیت کوین توانست برای اولین بار در تاریخ، مشکل جابه‌جایی ارزش در دنیای دیجیتال را بدون نیاز به هیچ واسطه یا نهاد مرکزی (مثل بانک‌ها و دولت‌ها) حل کند.

### مفاهیم کلیدی

#### ۱. تکامل پول از کالا تا فیات

پول در طول تاریخ برای حل مشکلات تجاری بشر دچار تحول شده است:

نمودار	تکامل	تاریخی	پول
		۱. مبادله پایاپای؛ معامله کالا با کالا (مشکل: عدم تطابق نیازهای دو طرف)	



۲. پول کالایی<sup>۲</sup>: صدف، نمک، طلا و نقره (ویژگی: کمیاب، بادوام و باارزش ذاتی)



۳. پول نماینده<sup>۳</sup>: رسیدهای کاغذی صرافان (متکی به پشتوانه طلا در گاو صندوق)



۴. پول فیات<sup>۴</sup>: دلار، یورو، ریال (بدون پشتوانه فیزیکی - متکی بر دستور دولت و اعتماد جامعه)



۵. بیت کوین<sup>۵</sup>: دفتر کل توزیع شده (حذف واسطه - متکی بر اعتماد ریاضیاتی و رمزنگاری)

• مبادله پایاپای<sup>۶</sup>: معامله مستقیم کالا با کالا که نیازمند «تطابق دقیق نیازهای دو طرف»<sup>۷</sup> بود.

Bitcoin<sup>۵</sup>

Barter<sup>۶</sup>

Coincidence of Wants<sup>۷</sup>

Commodity Money<sup>۲</sup>

Representative Money<sup>۳</sup>

Fiat Money<sup>۴</sup>

- پول کالایی و فلزی: استفاده از اشیای باارزش ذاتی، کمیاب و بادوام (مثل صدف، نمک، طلا و نقره) برای تسهیل تجارت. (نکته جالب: کلمه Salary به معنی حقوق از Salt به معنی نمک گرفته شده است).
- پول نماینده: رسیده‌های کاغذی صرافان و زرگران که پشتوانه طلا داشتند. ارزش از خود کالا به «اعتبار صادرکننده» منتقل شد.
- پول فیات: پول‌های امروزی (مثل دلار، یورو، ریال) که هیچ پشتوانه فیزیکی ندارند و ارزش آن‌ها صرفاً ناشی از دستور دولت‌ها و اعتماد عمومی جامعه است. (سال ۱۹۷۱ توسط ریچارد نیکسون اتصال دلار به طلا رسماً قطع شد).

## ۲. بحران کپی‌رایت پولی<sup>۸</sup>

بزرگ‌ترین چالش برای ساخت پول دیجیتال این بود که فایل‌های دیجیتال به راحتی و با هزینه صفر کپی می‌شوند. «مشکل دوبار خرج کردن» یعنی: چطور می‌توانیم جلوی یک فرد را بگیریم تا یک «فایل پول» را همزمان برای دو نفر متفاوت ارسال نکند؟

## ۳. راهکار سنتی در برابر راهکار ساتوشی ناکاموتو

برای حل مشکل دوبار خرج کردن، دو رویکرد تاریخی وجود دارد:

---

Double Spending<sup>8</sup>

راهکار ساتوشی ناکاموتو (غیرمتمرکز) 	راهکار سنتی (سیستم مالی متمرکز): 	ویژگی
استفاده از دفتر کل توزیع شده <sup>9</sup>	استفاده از یک واسطه معتمد (بانک یا شرکت پرداخت)	مکانیزم حل مشکل
کپی یکسان روی هزاران کامپیوتر در سراسر جهان	سرورهای خصوصی و گاوصندوق بانک	محل نگهداری دفتر حساب
بی‌نیاز از اعتماد (Trustless) / اتکا به ریاضیات و کد	اعتماد به قول، صداقت و مدیریت انسان‌ها/دولت‌ها	نوع اعتماد
مقاومت در برابر سانسور، تغییرناپذیر و شفاف	نقطه شکست مرکزی، کارمزد، کندی، تورم و سانسور	آسیب‌پذیری‌ها

### نگاه پادیا: گذر از اعتماد انسانی به اعتماد ریاضیاتی

سیستم‌های متمرکز در طول تاریخ نشان داده‌اند که می‌توانند نقطه ضعف بزرگی برای اقتصاد باشند. چاپ بی‌رویه پول کاغذی و بحران مالی سال ۲۰۰۸

<sup>9</sup> Blockchain

(فروپاشی بانک‌هایی مثل لیمن برادرز) نشان داد که اعتماد مطلق به نهادهای متمرکز چقدر شکننده است.

ساتوشی ناکاموتو با قرار دادن تیترو روزنامه تایمز بریتانیا (مبنی بر کمک مالی دولت به بانک‌های ورشکسته) در «بلاک پیدایش»<sup>۱</sup>، پیام روشنی به جهان داد: سیستم پولی مبتنی بر برنامه‌ریزی مرکزی شکست خورده است. بیت‌کوین پارادایم اقتصاد را از «اعتماد به قول سیاستمداران و بانکداران» به «شفافیت کدهای برنامه‌نویسی و قوانین تغییرناپذیر ریاضی» (Trustless) تغییر داد.

### ابزارها و مراجع کاوش (برای کنجکاوان)

• تیترو تاریخی بلاک پیدایش: در تاریخ ۳ ژانویه ۲۰۰۹، ساتوشی تیترو روزنامه The Times را در اولین بلاک بیت‌کوین حک کرد:

"The Times ۰۳/Jan/۲۰۰۹ Chancellor on brink of second bailout for banks"

• برای مشاهده اطلاعات اولین بلاک تاریخ بیت‌کوین می‌توانید در کاوشگرهای بلاک چین به دنبال Block #۰ بگردید.

### واژه‌نامه انگلیسی به فارسی

اصطلاح انگلیسی	معادل فارسی	توضیح کوتاه
Barter	مبادله پایاپای / تهاتر	معامله مستقیم کالا با کالا بدون استفاده از پول

<sup>۱</sup> Genesis Block

<p>پولی که خودش ارزش ذاتی دارد (مثل نمک، طلا و نقره)</p>	<p>پول کالایی</p>	<p>Commodity Money</p>
<p>پول قانونی که اعتبارش فقط از دستور دولت و اعتماد مردم است</p>	<p>پول فیات (بدون پشتوانه)</p>	<p>Fiat Money</p>
<p>خرج کردن همزمان یک سکه/فایل دیجیتال در دو مکان مختلف</p>	<p>دوبار خرج کردن</p>	<p>Double Spending</p>
<p>سیستمی که کنترل آن در دست یک فرد، شرکت یا سرور واحد است</p>	<p>متمرکز</p>	<p>Centralized</p>
<p>سیستمی که کنترل و داده‌های آن بین تمام اعضا توزیع شده است</p>	<p>غیرمتمرکز</p>	<p>Decentralized</p>
<p>سیستمی که برای کار کردن نیازی به اعتماد به نیت خیر انسان‌ها ندارد</p>	<p>بی‌نیاز از اعتماد</p>	<p>Trustless</p>

بلاک شماره صفر و اولین

بلاک ساخته شده در

شبکه بیت کوین

بلاک پیدایش

Genesis Block