فصل‌نامه مطالعاتی در مدیریت بانکی و بانکداری اسلامی

مؤسسه عالی آموزش بانکداری ایران
تابستان ۱۴۰۴، دوره ۱۱، شماره ۳۱، ۱۰۸-۱۴۷

بانکداری اسلامی در عصر پساکوانتوم: گریز از بلاک‌چین، پیوند با شریعت

سید امید آذرکسب[۱] محمد رجبی[۲] سید حسین خواسته[۳] امیر بهادر مروت[۴]

چکیده

در آستانه ورود به عصر رایانش کوانتومی، بنیان‌های امنیت اطلاعات که بر رمزگذاری نامتقارن و توابع هش کلاسیک استوار هستند، با تهدیدات بی‌سابقه‌ای روبه‌رو شده‌اند. این وضعیت، به‌ویژه برای بانکداری اسلامی که بر صحت، شفافیت و مشروعیت شرعی قراردادها تأکید دارد، چالشی حیاتی محسوب می‌شود. از طرفی در حالی‌که اغلب راهکارهای فناورانه بر زیرساخت بلاک‌چین متکی‌اند، شواهد فقهی و تحلیلی حاکی از آن است که بلاک‌چین با برخی اصول اساسی فقه اسلامی، از جمله منع غَرر و شفافیت مالکیت، سازگاری کامل ندارد. از این‌رو، در این مقاله چارچوبی ترکیبی بلاک‌چین‌گریز برای تقویت امنیت دیجیتال در عقود غیرربوی ارائه شده که مبتنی بر فناوری توزیع کلید کوانتومی و الگوریتم‌های رمزنگاری مقاوم در برابر کوانتوم است. در این چارچوب، سه اصل فقهی احراز اصالت قرارداد، جلوگیری از تحریف و جعل و تضمین شفافیت در توزیع مالکیت به‌صورت لایه‌مند در ساختار رمزنگاری پیاده‌سازی شده است. پس از تحلیل اصول فقه معاملات اسلامی و بررسی فنی الزامات امنیتی آینده‌نگر، الگوی پیشنهادی طراحی و امکان‌سنجی پیاده‌سازی آن در نظام بانکداری اسلامی ایران و سایر کشورهای مسلمان تحلیل شده است. یافته‌های مقاله نشان می‌دهد که می‌توان بدون ورود به تعارضات فقهی، چارچوبی امن، اخلاق‌محور و علمی برای حفاظت از قراردادهای اسلامی در برابر تهدیدات کوانتومی ارائه داد، چارچوبی که بر محدودیت‌های بلاک‌چین فائق می‌آید و می‌تواند اعتماد عمومی و اصالت شرعی را در محیط دیجیتال حفظ نماید.

واژه‌های کلیدی: رمزنگاری مقاوم در برابر کوانتوم، توزیع کلید کوانتومی، عقود غیرربوی دیجیتال، اصالت و تمامیت قراردادها، شفافیت مالکیت در نظام مالی اسلامی.

طبقه‌بندی JEL: G21, D86, O33, Z12

---

۱. دکتری مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه خواجه نصیر الدین طوسی، تهران، ایران(نویسنده مسئول). Sayedomid.azarkasb@email.kntu.ac.ir

۲. کارشناسی ارشد امور بانکی و اقتصادی، پژوهشکده پولی و بانکی، تهران، ایران. rajabi@banksepah.ir

۳. استادیار گروه مهندسی کامپیوتر، دانشگاه خواجه نصیرالدین طوسی، تهران، ایران. khasteh@kntu.ac.ir

۴. دانشجوی دکتری آینده پژوهی، واحد ایوانکی، دانشگاه آزاد اسلامی، سمنان، ایران. morovat@eyc.ac.ir

۱. مقدمه

این مقاله بر خلاف مسیر غالب که بلاک‌چین را ابزار اصلی در ایمن‌سازی قراردادهای اسلامی می‌داند، راه‌حلی منطبق‌تر با اصول فقهی پیشنهاد می‌دهد که مبتنی بر رمزنگاری فیزیکی–کوانتومی و فاقد ابهام مالکیتی است. در دهه‌ی اخیر، هم‌زمان با پیشرفت سریع فناوری‌های کوانتومی، بنیان‌های امنیت اطلاعات که بر رمزگذاری نامتقارن و توابع هش کلاسیک استوارند با تهدیدی جدی روبه‌رو شده‌اند (نیلسن[۱] ۲۰۱۱). این تحول صرفاً فنی نیست؛ بلکه در نظام‌هایی مانند بانکداری اسلامی که بر صحت، شفافیت و مشروعیت شرعی قراردادها استوار است، مخاطره‌ای حیاتی محسوب می‌شود (پرسکیل[۲] ۲۰۱۸). خدشه به اصالت، امانت یا شفافیت مالکیت در فضای دیجیتال می‌تواند مشروعیت عقود اسلامی را تضعیف کند و پیامدهای اقتصادی و اجتماعی گسترده‌ای داشته باشد. در چنین شرایطی، ضرورت دارد چارچوبی نوین برای امنیت دیجیتال قراردادهای شرعی تدوین شود که هم در برابر تهدیدات کوانتومی مقاوم باشد و هم با اصول فقه اسلامی تعارض نداشته باشد. بانکداری اسلامی برخلاف مدل‌های متعارف مبتنی بر بهره و اعتبار ربوی، بر عقودی نظیر مشارکت، مرابحه و صکوک استوار است که باید از منظر فقهی از هرگونه غَرر، ابهام مالکیت و امکان جعل مصون بمانند. اما در محیط‌های دیجیتال جدید، تهدیدهای فنی می‌توانند همان آسیب‌های رفتاری را بازتولید کنند و نقص در زنجیره اطمینان دیجیتال معادل کتمان حقیقت یا جعل در معامله تلقی شود (بونو[۳] ۲۰۱۵). از این منظر، امنیت اطلاعات، بحثی فنی و بخشی از فقه‌المعاملات نوین است، جایی که ابزارهای شرعی باید در بستری قرار گیرند که شفافیت مالکیت، قطعیت قرارداد و منع جعل را تضمین کند حتی در برابر رایانه‌هایی که قوانین فیزیک کلاسیک را در هم می‌شکنند (منه[۴] ۲۰۲۴).

ظهور رایانه‌های کوانتومی با قدرت درهم‌شکنی رمزهای کلاسیک نوعی ابهام ساختاری به قراردادهای دیجیتال تزریق کرده است. پرسش‌هایی مانند اینکه «آیا عقد مرابحه‌ای که با امضای دیجیتال منعقد

---

۱ Nielsen
۲ Preskill
۳ Bonneau
۴ Menne

می‌شود همچنان معتبر است؟» یا «آیا اطمینان از صحت پیام، که شرط اساسی صحت عقد است، با احتمال شنود یا جعل قابل پذیرش خواهد بود؟» (نیدرهاگن[۱] ۲۰۲۵) نشان می‌دهد که امنیت دیجیتال در فقه اسلامی به مسئله‌ای اصولی تبدیل شده است. نبود اجماع فقهی درباره جایگاه ابزارهای رمزنگاری و وابستگی فقه اسلامی به اصالت ابزار و قطعیت در اطلاع‌رسانی، نیاز به چارچوبی نوین برای امنیت دیجیتال شرعی را دوچندان می‌کند (منصور[۲] ۲۰۲۴؛ دانیلز[۳] ۲۰۱۷). این چارچوب باید از تهدیدات کوانتومی مصون باشد و با منطق درونی فقه اسلامی نیز تطابق داشته باشد. در سال‌های اخیر بلاک‌چین به‌عنوان بستر پیش‌فرض برای توسعه سامانه‌های مالی غیرمتمرکز مطرح شده است، اما بررسی‌های فقهی نشان می‌دهد این فناوری در برخی موارد، از جمله احتمال وجود غَرر در فرآیند تولید بلاک‌ها، پیچیدگی مالکیت توکن‌ها، دشواری احراز اصالت در محیط‌های توزیع‌شده و نبود نهاد پشتیبان شرعی، با اصول رایج فقه اسلامی تعارض دارد و حتی می‌تواند زمینه شبه‌ربا یا شبه‌غَرر را فراهم آورد (جهانگیر[۴] ۲۰۲۵؛ محمود[۵] ۲۰۲۵). علاوه بر این، قدرت رایانش کوانتومی مرزهای رمزنگاری سنتی بلاک‌چین را نیز در هم می‌شکند؛ الگوریتم‌های کوانتومی قادرند زیرساخت‌های کلید عمومی متداول را در زمان بسیار کوتاه تخریب کنند (آگراوال[۶] ۲۰۱۷). بنابراین حتی در صورت پذیرش نسبی بلاک‌چین از منظر فقهی، بقای امنیتی آن در عصر پساکوانتومی تضمین‌شده نخواهد بود. بر همین اساس، این مقاله طراحی چارچوبی ترکیبی و بلاک‌چین‌گریز را پی می‌گیرد که با تکیه بر فناوری توزیع کلید کوانتومی[۷] و الگوریتم‌های مقاوم به کوانتوم سه هدف اصلی بانکداری اسلامی را محقق کند: ۱) تضمین صحت و اصالت قرارداد شرعی، ۲) جلوگیری از جعل و تحریف، و ۳) تأمین شفافیت در مالکیت. در این چارچوب به جای اتکا به اعتماد به نهاد ثالث یا اجماع بلاک‌چینی، از مکانیزم‌های فیزیکی–

---

۱ Niederhagen
۲ Mansour
۳ Daniels
۴ Jahangir
۵ Mahmood
۶ Aggarwal
۷ Quantum Key Distribution (QKD)

رمزنگاری برای تولید و انتقال امن کلیدها استفاده می‌شود که با مفاهیم امانت، شفافیت و منع غَرر در فقه اسلامی هم‌راستا است.

پرسش محوری مقاله آن است که آیا می‌توان با بهره‌گیری از فناوری‌های نوین کوانتومی، چارچوبی امن، مشروع و غیرربوی برای ثبت و اجرای قراردادهای اسلامی در محیط دیجیتال طراحی کرد، بدون آنکه متکی به زیرساخت‌هایی باشد که با شریعت در تضادند. این پرسش از دو بُعد اهمیت دارد: نخست، لزوم ارتقای امنیت قراردادهای دیجیتال اسلامی در برابر تهدیدات آتی و دوم، ضرورت انطباق کامل این فناوری‌ها با اصول فقهی، بدون ورود به شائبه‌های ربوی یا غَرری. خدشه به صحت قراردادها هم عملکرد فنی را تضعیف می‌کند و هم مشروعیت شرعی و اعتماد عمومی را تحت تأثیر قرار می‌دهد. فرضیه مقاله این است که ترکیب فناوری توزیع کلید کوانتومی با الگوریتم‌های مقاوم پساکوانتومی می‌تواند چنین چارچوبی را فراهم آورد و نسبت به مدل‌های بلاک‌چینی مشروعیت و اعتمادپذیری بیشتری ارائه دهد. این پژوهش با رویکردی تطبیقی و میان‌رشته‌ای به تحلیل ساختاری و فقهی این چارچوب پرداخته و پس از بررسی چالش‌های فنی و نهادی، امکان‌سنجی پیاده‌سازی آن را در نظام بانکداری اسلامی ایران و سایر کشورها بررسی می‌کند. نوآوری‌های اصلی مقاله عبارت است از: (۱) تدوین چارچوب مفهومی توزیع کلید کوانتومی در عقود اسلامی با تمرکز بر صکوک و مشارکت و حفظ صحت، شفافیت و اصالت قراردادها؛ (۲) تحلیل فقهی–فنی رمزنگاری پساکوانتومی و امکان استفاده از الگوریتم‌های تخصصی این حوزه در چارچوب بانکداری اسلامی؛ (۳) طراحی مدل امن بدون بلاک‌چین و ارائه ساختار جایگزین برای ثبت قراردادهای شرعی بدون نیاز به زیرساخت‌های ناسازگار با فقه. مبنای فقهی این پژوهش بر فقه امامیه (شیعه جعفری) استوار است؛ مکتبی که با تکیه بر قواعدی چون اوفوا بالعقود، لاضرر و لاضرار[۱] و قاعده سلطنت، به‌صورت نظام‌مند به تنظیم روابط معاملاتی در فضای نوین مالی می‌پردازد (موسوی بجنوردی، ۱۳۷۹؛ کمالی[۲]، ۲۰۱۹). با این حال، در تطبیق نظری و تطور فقهی، تطبیقات مقایسه‌ای با دیدگاه‌های فقهی اهل‌سنت به‌ویژه در مکاتب حنبلی و شافعی نیز مورد توجه

---

[۱] قاعده لا ضرر و لا ضرار: اصل عدم ورود زیان به طرفین معامله؛ که در زمینه امنیت سایبری، به معنای جلوگیری از هرگونه آسیب احتمالی ناشی از نقص رمزنگاری یا دستکاری داده‌ها تعبیر می‌شود.

[۲] Kamali

قرار گرفته است (النووی، ۱۴۲۵؛ ابن قدامه المقدسی، ۱۴۴۰) تا چارچوب پیشنهادی قابلیت پذیرش در سطح فراملی نظام بانکداری اسلامی را حفظ نماید.

برای تحقق اهداف فوق، ادامه مقاله به این صورت سازمان‌دهی شده است: در بخش دوم، پیشینه پژوهشی و شکاف تحقیق ارائه می‌شود. بخش سوم به تشریح چارچوب نظری اختصاص دارد و مبانی منطقی و رویکرد میان‌رشته‌ای تحقیق را تبیین می‌کند. در بخش چهارم، تحلیل الزامات فقهی عقود اسلامی و تطبیق آن با ساختارهای رمزنگاری کوانتومی بررسی می‌شود. بخش پنجم به معرفی چارچوب پیشنهادی مقاله اختصاص دارد، در این بخش، با اتکا به نتایج تحلیل‌های پیشین، امکان‌سنجی پیاده‌سازی مدل امنیتی در نظام بانکداری اسلامی مورد بررسی قرار می‌گیرد. بخش ششم به چالش‌های اجرایی، زیرساختی و سیاست‌گذاری در زمینه استقرار فناوری‌های رمزنگاری نوین در ایران و سایر کشورهای اسلامی می‌پردازد. در بخش پایانی (بخش هفتم)، نتیجه‌گیری کلی پژوهش ارائه شده و مسیرهای پیشنهادی برای مطالعات آینده و گام‌های اجرایی آتی مطرح می‌شود.

۲. پیشینه پژوهشی و شکاف تحقیق

تحولات شگرف در حوزه فیزیک کوانتومی در قرن بیستم، زمینه‌ساز پیدایش فناوری‌هایی نوین چون محاسبات کوانتومی، رمزنگاری کوانتومی و توزیع کلید کوانتومی شده‌اند. برخلاف سیستم‌های کلاسیک که بر مبنای بیت‌های دودویی کار می‌کنند، محاسبات کوانتومی بر پایه کیوبیت‌ها بنا شده‌اند که از اصولی اعجاز برانگیزی چون برهم‌نهی ، درهم‌تنیدگی و اصل عدم قطعیت هایزنبرگ بهره می‌برند. این ویژگی‌ها به کامپیوترهای کوانتومی این توانایی را می‌دهند که در حل مسائل پیچیده مانند فاکتورگیری عددی، الگوریتم‌های جستجو و تحلیل رمزنگاری، بسیار سریع‌تر از رایانه‌های کلاسیک عمل کنند (زیگلمن[۱] ۲۰۲۵). یکی از پیامدهای مهم این پیشرفت، تضعیف یا حتی فروپاشی امنیت رمزنگاری متقارن و نامتقارن کلاسیک است. به‌ویژه، الگوریتم شُر توانایی در هم شکستن فاکتورگیری اعداد اول و لگاریتم گسسته را دارد، در حالی که الگوریتم گروور امنیت سیستم‌های متقارن مانند

[۱] Zygelman

استاندارد رمزگذاری پیشرفته را نیز با کاهش توان نمایی، تهدید می‌کند (نرِم[۱] ۲۰۲۳). در این بستر، مفهوم امنیت پساکوانتومی و پروتکل‌های توزیع کلید کوانتومی به‌عنوان دو رهیافت اصلی در مقابله با تهدیدات کوانتومی مطرح شده‌اند.

در پاسخ به این چالش، سازمان ملی استاندارد ایالات متحده در اوت ۲۰۲۴ سه استاندارد رسمی برای رمزنگاری مقاوم به حملات کوانتومی منتشر کرده است (۲۰۳ FIPS، 204 و ۲۰۵) که بر الگوریتم‌هایی مانند تبادل کلید ، امضاهای دیجیتال و امضای مبتنی بر هش استوار هستند و همچنین پیش‌نویس‌هایی مانند RFC 9794 پیشنهاد انتقال تدریجی به رمزنگاری ترکیبی را مطرح می‌سازند (الاگیچ[۲] ۲۰۲۲؛ کویاتکوفسکی[۳] ۲۰۲۵).

به موازات این تلاش‌ها، فناوری توزیع کلید کوانتومی به‌عنوان نخستین راهکار رمزنگاری فیزیکی مطرح شده است (آکینا[۴] ۲۰۲۵). تحقیقات آکادمیک نشان می‌دهند که رمزنگاری مقاوم به کوانتوم باید توسعه‌یافته و فوراً برای نهادهای مالی مورد استفاده قرار گیرد تا از استراتژی برداشت حالا، رمزگشایی در آینده جلوگیری شود (سینگاماننی[۵] ۲۰۲۴). تحلیل‌های نوین نیز به تهدیدات هم‌افزای هوش مصنوعی و کوانتوم در امنیت تراکنش‌های مالی اشاره کرده‌اند (المیسری[۶] ۲۰۲۵). توزیع کلید کوانتومی با اتکا بر اصول اعجازآور بنیادی مکانیک کوانتوم همچون اصل عدم قطعیت و درهم‌تنیدگی کوانتومی، قابلیت ذاتی در تشخیص شنود را فراهم می‌کند و امنیت غیرقابل شکستی را در سطح نظری تضمین می‌نماید (نورالاین[۷] ۲۰۲۵). با وجود چالش‌هایی نظیر نیاز به زیرساخت فیبر نوری، محدودیت فاصله، و هزینه بالا، روش توزیع کلید کوانتومی به‌طور آزمایشی در شبکه‌های مالی برخی کشورها مورد بهره‌برداری قرار گرفته است

---

۱ Nerem
۲ Alagic
۳ Kwiatkowski
۴ Aquina
۵ Singamaneni
۶ Elmisery
۷ Ain (Noor Ul Ain)

- بانک HSBC در سال ۲۰۲۳ نخستین تراکنش امن مالی مبتنی بر توزیع کلید کوانتومی را در مسیر لندن–برکشایر اجرا کرد (اچ‌اس‌بی‌سی[۱] ۲۰۲۴)،
- بانک JPMorgan از توزیع کلید کوانتومی برای تقویت امنیت تراکنش‌های بلاک‌چینی استفاده کرده است (جی‌پی‌مورگان[۲] ۲۰۲۴)،
- در چین، بانک ICBC شبکه فیبر نوری توزیع کلید کوانتومی به طول هزار کیلومتر مسیر پکن–شانگهای و اجرای شبکه بین‌بانکی مبتنی بر آن را بین مراکز اصلی خود راه‌اندازی نموده است (آی‌سی‌بی‌سی[۳] ۲۰۲۳؛ آی‌سی‌بی‌سی، ۲۰۱۷))،
- در اروپا، پروژه‌هایی نظیر توزیع کلید کوانتومی باز با حمایت اتحادیه اروپا، چارچوب‌های عملی برای استقرار توزیع کلید کوانتومی در سیستم‌های بانکی فراهم کرده‌اند (کوانتوم فلگشیپ[۴] ۲۰۲۳)،
- بانک‌های مرکزی فرانسه و ایتالیا در کنار BIS پروژه‌هایی برای آماده‌سازی کوانتومی و مهاجرت تدریجی به فناوری رمزنگاری پساکوانتومی را آغاز کرده‌اند (بانک تسویه‌حساب‌های بین‌المللی[۵] ۲۰۲۳).

سایر کشورها نیز نظیر کره جنوبی اقدام به پیاده‌سازی سیستم‌های توزیع کلید کوانتومی در زیرساخت‌های مخابراتی خود نموده اند (کوانتوم زایت‌گایست[۶] ۲۰۲۵). این اقدامات نشانگر حرکت جهانی به‌سوی امنیت اطلاعات مقاوم به تهدیدات کوانتومی، به‌ویژه در بخش حساس مالی است. در حوزه بانکداری اسلامی، ادبیات پژوهشی بیشتر به مباحث فقهی ابزارهای مالی، قراردادها و تحلیل‌های ساختاری پرداخته‌اند. توجه فناورانه به‌ویژه در بخش امنیت دیجیتال و رمزنگاری پساکوانتومی در این حوزه بسیار محدود بوده است. در یک دسته از پژوهش‌های فناورانه، برخی مطالعات اولیه به بررسی امکان ترکیب فناوری‌های نوظهور

---

[۱] HSBC
[۲] JPMorgan
[۳] ICBC
[۴] Quantum Flagship
[۵] BIS
[۶] Quantum Zeitgeist

مانند بلاک‌چین با بانکداری اسلامی پرداخته‌اند (ماتوندانگ[۱] ۲۰۲۴)، اما غالب آن‌ها تنها به توجیه تئوریک استفاده از بلاک‌چین در قراردادهای اسلامی بسنده کرده‌اند و به چگونگی ترکیب آن با رمزنگاری مقاوم به کوانتوم یا پیاده‌سازی عملی توزیع کلید کوانتومی اشاره‌ای نداشته‌اند. در واقع، در اغلب موارد، مسائل مربوط به امنیت ارتباطات مالی، صحت اصالت قراردادها، مالکیت داده و انکارناپذیری، بدون ارزیابی دقیق از زیرساخت‌های رمزنگاری آینده‌نگر مورد بررسی قرار گرفته‌اند (فوتووا چیکوویچ[۲] ۲۰۲۵). پژوهش‌هایی مانند گزارش تخصصی مرکز تحقیقات اسلامی مالزی، بر این موضوع تأکید دارند که بانکداری اسلامی به‌دلیل اصول خاص فقهی، باید از فناوری‌هایی استفاده کند که نه‌تنها از نظر امنیتی کارآمد باشند، بلکه اصولی مانند عدم‌ربا، شفافیت مالکیت، عدم‌غَرر و وفای به‌عهد را نیز در سازوکارهای خود لحاظ کنند (سلیم[۳] ۲۰۲۰). این موضع در حالی است که برخی تحقیقات دانشگاهی منطقه خلیج فارس، مانند مطالعه انجام‌شده توسط دکتر اندرو ده‌دال از دانشگاه قطر، نشان می‌دهد که بلاک‌چین با وجود افزایش شفافیت، در مواردی مانند مالکیت توکن‌ها و قراردادهای مشارکتی یا مضاربه، به‌ویژه در مواجهه با غَرر، دارای ابهام است و از نظر تطابق شرعی قابل اتکا نیست (دهدل[۴] ۲۰۲۲). از این منظر، استفاده از رمزنگاری پساکوانتومی می‌تواند در صورت طراحی درست، یکی از راهکارهای مهم برای تقویت اصل اصالت قرارداد و جلوگیری از جعل یا تحریف در ساختار قراردادهای شرعی تلقی شود. علاوه بر آن، در برخی پژوهش‌های نوآورانه اخیر پیشنهاد شده است که ترکیب رمزنگاری مبتنی بر توزیع کلید کوانتومی با سامانه‌های تشخیص هویت چندعاملی مقاوم به کوانتوم، می‌تواند مسیر را برای شکل‌گیری هویت دیجیتال اسلامی مبتنی بر مالکیت غیرقابل‌انکار هموار سازد (بابو[۵] ۲۰۲۴). چنین سیستمی، در صورت پیاده‌سازی، قادر خواهد بود اطلاعات هویتی افراد حقیقی و حقوقی را با اصول شرعی همچون مالکیت صریح، عدم‌تزویر و شفافیت قرارداد انطباق دهد، بی‌آنکه نیاز به اعتماد مطلق به نهاد ثالث وجود داشته باشد. اگرچه بانکداری اسلامی با ظرفیت‌های فقهی خاص، پتانسیل بالایی برای همگرایی با فناوری‌های کوانتومی دارد، اما تاکنون نه در

---

[۱] Matondang
[2] Fotova Čiković
[3] Salim
[4] Dahdal
[5] Babu

سطح راهبردی و نه در سطح عملیاتی، چارچوبی منسجم برای بهره‌گیری از فناوری‌های رمزنگاری مقاوم به کوانتوم با رعایت الزامات فقهی و ساختاری تدوین نشده است.

۲-۱. شکاف‌های پژوهشی و انگیزه تحقیق

در نتیجه، شکاف اصلی در ادبیات موجود را می‌توان چنین صورت‌بندی کرد:

– عدم وجود یک چارچوب جامع، تطبیقی و مفهومی که فناوری‌های توزیع کلید کوانتومی و رمزنگاری پساکوانتومی را در قالبی فنی–فقهی برای استفاده در بانکداری اسلامی بررسی و تحلیل کند،

– نبود مطالعات تطبیقی درباره امکان‌پذیری بومی سازی این فناوری در نظام مالی ا سلامی، خ صو صاً در ایران،

– کمبود مدل‌های قابل اجرای عملی بدون نیاز به زیرســـاخت بلاک‌چین پیچیده که امنیت و شـــفافیت قرارداد اسلامی را تضمین کنند،

– بی‌توجهی به محدودیت‌های فناوری، حقوقی و مقرراتی بانکداری اسلامی در کشورهای در حال توسعه.

مطالعه حاضر درصدد است با پر کردن این خلأ، نه‌تنها امکان‌سنجی فقهی و فنی را هم‌زمان در نظر گیرد، بلکه با تبیین الزامات پیاده‌سازی در بستر بانک‌های ا سلامی (به‌ویژه در ایران)، مسیر توسعه امنیت پایدار و شریعت‌محور را هموار سازد. این پژوهش با تمرکز بر ابزارهای شرعی مانند صکوک، مرابحه و مشارکه، چارچوبی را پیشنهاد می‌دهد که سه مؤلفه ا صالت قرارداد، امضای غیرقابل جعل و شفافیت مالکیت را در بســتر کوانتومی تأمین کند و با توجه به فقدان الگویی بومی و غیرمتکی به بلاک‌چین که با ســاختارهای بانکی اسلامی و فقهی ایران سازگار باشد، الگویی عملیاتی و قابل پیاده‌سازی ارائه می‌دهد

۳. چارچوب نظری تحقیق

این پژوهش با رویکردی توصیفی–تحلیلی و میان‌رشته‌ای انجام شده است. چارچوب فقهی این مقاله بر مبنای اصول فقه امامیه (شیعی) تدوین شده است، با تأکید بر قواعد صحت، لزوم، امانت و منع غَرر

که در منابعی همچون «شرایع الاسلام» محقق حلی و «جواهرالکلام» نجفی به‌عنوان ارکان مشروعیت معاملات مطرح شده‌اند. در عین حال، برای تقویت جنبه تطبیقی، دیدگاه‌های فقهی شافعی و حنبلی نیز در موارد خاص مورد مقایسه قرار گرفته‌اند (النووی، ۱۴۲۵؛ ابن قدامه المقدسی، ۱۴۴۰)؛ به‌ویژه در زمینه مفهوم غَرر در معاملات الکترونیکی و مالکیت اعتباری در فضای مجازی که در فقه شافعی با تفسیر مضیّق‌تر از فقه امامیه تحلیل می‌شود. این تلفیق، ضمن حفظ اصالت فقه شیعی، امکان انطباق مدل پیشنهادی با نظام‌های بانکداری اسلامی سایر کشورها را نیز فراهم می‌سازد. روش تحلیل به این صورت بوده است که پس از استخراج اصول فقهی و شناسایی تهدیدات فنی، برای هر اصل فقهی شاخص‌های عملیاتی متناظر تعریف و سپس الگوریتم‌ها و فناوری‌های مقاوم به کوانتوم براساس این شاخص‌ها ارزیابی و تطبیق داده شده‌اند. ارزیابی امنیتی الگوریتم‌ها با تکیه بر مدل‌های رسمی نظیر IND-CPA (تمایزناپذیری تحت حمله‌ٔ متن‌رمز اختیاری) و EUF-CMA (جعل‌ناپذیری امضا تحت حمله انتخابی–انطباقی) صورت گرفت تا از قابلیت پیاده‌سازی بدون تعارض با اصول شریعت اطمینان حاصل شود. از یک‌سو به‌صورت نظام‌مند ادبیات فنی رمزنگاری و امنیت اطلاعات در عصر پساکوانتومی مرور شده است (استانداردهای پیشنهادی NIST و RFCها، شامل تبادل کلید امن، امضای مقاوم به جعل و ساختارهای هش‌محور برای امضای دیجیتال (ناز[۱] ۲۰۲۵؛ الاگیچ[۲] ۲۰۲۵)) و از سوی دیگر اصول فقه معاملات اسلامی شامل امانت، منع غَرر، عدم ربا و شفافیت در مالکیت استخراج و تحلیل تطبیقی شده است. برای تلفیق این دو حوزه، از روش «نگاشت لایه‌به‌لایه» میان مؤلفه‌های فقهی و اجزای رمزنگاری مقاوم استفاده شده تا چارچوب مفهومی طراحی شود. این رویکرد به جای توجیه پسینیِ فناوری، طراحی فناوری را از ابتدا با ملاحظات شرعی آغاز می‌کند.

در حوزه فنی، گذار از ساختارهای کلاسیک به معماری‌های مقاوم در برابر حملات کوانتومی امری اجتناب‌ناپذیر است. الگوریتم‌های کوانتومی مانند شُر و گروور توانایی درهم‌شکستن سازوکارهای فعلی کلید عمومی، امضاهای دیجیتال و حتی رمزنگاری متقارن را دارند. در پاسخ، پروژه استانداردسازی مؤسسه جهانی فناوری و استاندارد مجموعه‌ای از الگوریتم‌های مقاوم به کوانتوم را در قالب اسناد رسمی

---

[۱] Naz

[۲] Alagic

مانند NIST SP 800-208 و RFC 9380 پیشنهاد داده که شامل طرح‌هایی برای تبادل کلید امن، امضای مقاوم به جعل و ساختارهای هش‌محور برای امضای دیجیتال است (ناز، ۲۰۲۵؛ الاگیچ، ۲۰۲۵). همچنین فناوری توزیع کلید کوانتومی با تکیه بر اصول مکانیک کوانتوم مانند اصل عدم قطعیت، برهم‌نهی و قضیه عدم‌کپی‌برداری[۱] امکان تولید و انتقال کلیدهایی را فراهم می‌آورد که به لحاظ نظری شنود یا جعل‌شدنی نیستند و سطحی تازه از اعتماد ایجاد می‌کنند.

در حوزه فقه معاملات، اصول امانت (حفظ اصالت قرارداد)، منع غَرر (ابهام)، عدم ربا و شفافیت در مالکیت نقش بنیادینی در مشروعیت هر قرارداد مالی ایفا می‌کنند. نظریه حاکمیت فقه بر فناوری ایجاب می‌کند که طراحی فناوری از ابتدا با رویکرد انطباق با اصول فقهی آغاز شود. بر این اساس، چارچوب مفهومی این تحقیق مبتنی بر نگاشت مؤلفه‌های فقهی به اجزای رمزنگاری مقاوم طراحی شده است. جدول ۱ ساختار این تعامل را نشان می‌دهد.

جدول ۱: تعامل ساخت‌یافته فقه و فناوری در چارچوب پیشنهادی

مؤلفه رمزنگاری کوانتومی	مؤلفه فقهی متناظر	هدف عملکردی
توزیع کلید کوانتومی	امانت، صحت قرارداد و وفای به‌عهد	جلوگیری از تحریف و دستکاری
امضای دیجیتال مقاوم به کوانتوم (LMS, XMSS)	عدم غَرر، قطعیت قرارداد	تأمین اصالت و مالکیت
الگوریتم‌های مقاوم به حمله (FALCON, CRYSTALS, DILITHIUM)	وضوح طرفین و روابط معاملاتی	شفافیت در مالکیت

علاوه بر تطابق مفهومی، امنیت چارچوب پیشنهادی در سطح نظری نیز بر مدل‌های رسمی مانند تمایزناپذیری تحت حمله با متن‌رمز اختیاری[۲] و جعل‌ناپذیری امضا تحت حمله انتخابی انطباقی[۳] استوار است. این مدل‌ها در تحلیل امنیتی الگوریتم‌های پیشنهادی مؤسسه جهانی فناوری و استاندارد و ساختارهای توزیع کلید کوانتومی نیز نقش محوری دارند (ناز، ۲۰۲۵؛ الاگیچ، ۲۰۲۵). بر پایه این چارچوب، چهار فرض کلیدی تحقیق به شرح زیر شکل گرفته است:

---

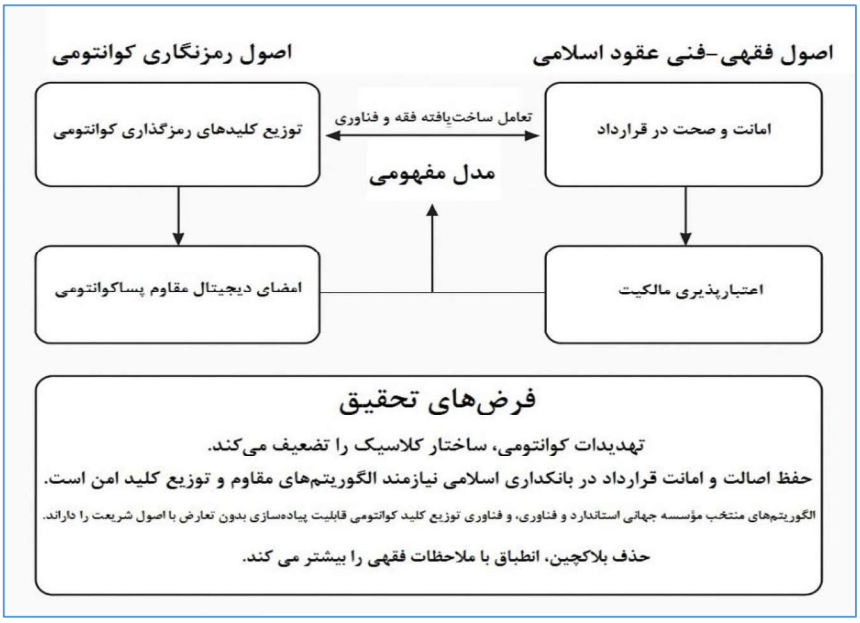
[۱] No-Cloning Theorem

[۲] Indistinguishability Under Chosen-Plaintext Attack (IND-CPA)

[۳] Existential Unforgeability Under Adaptive Chosen-Ciphertext Attack (EUF-CMA)

- ظهور رایانش کوانتومی، ساختارهای رمزنگاری کلاسیک را به‌زودی ناکارآمد خواهد ساخت،
- حفظ اصالت و امانت قرارداد در بانکداری اسلامی نیازمند الگوریتم‌های مقاوم و توزیع کلید امن است،
- الگوریتم‌های منتخب مؤسسه جهانی استاندارد و فناوری، و فناوری توزیع کلید کوانتومی قابلیت پیاده‌سازی بدون تعارض با اصول شریعت را دارند،
- حذف زیرساخت‌هایی چون بلاک‌چین (به دلیل ابهامات شرعی آن)، امکان انطباق بیشتر با ملاحظات شرعی و نهادی در ایران و سایر کشورهای اسلامی را فراهم می‌آورد.

بدین ترتیب، چارچوب نظری تحقیق در جهت طراحی معماری رمزنگاری هماهنگ با الزامات فقهی، تهدیدات نوظهور امنیتی و واقعیت‌های نهادی کشورهای اسلامی شکل می‌گیرد که در شکل ۱ به‌طور خلاصه نشان داده شده است:



شکل ۱: چارچوب نظری تحقیق

٤. تحلیل الزامات فقهی عقود اسلامی و تطبیق آن با ساختارهای رمزنگاری کوانتومی

خط فقه معاملات اسلامی بر مبنای اصولی چون امانت، صحت و شفافیت قرارداد، مالکیت مشروع، عدم غَرر و عدم ربا بنیان نهاده شده است. مبنای فقهی این تحلیل، بر پایه اصول فقه امامیه (شیعه جعفری) است که قواعدی چون اوفوا بالعقود، اصالهٔ الصحهٔ، قاعده سلطنت و لاضرر و لاضرار را محور صحت و مشروعیت قراردادها می‌داند. در عین حال، برای تعمیم و مقایسه تطبیقی، دیدگاه‌های فقهی مکاتب حنبلی و شافعی نیز در تحلیل غَرر، رضا و مالکیت مورد ارجاع قرار گرفته‌اند تا چارچوب ارائه‌شده قابلیت انطباق با نظام بانکداری اسلامی کشورهای مختلف را حفظ کند (موسوی بجنوردی، ۱۳۷۹؛ کمالی، ۲۰۱۹). این اصول نه‌تنها چارچوب شرعی برای تنظیم روابط مالی فراهم می‌کنند، بلکه بستری برای اعتماد متقابل میان طرفین معامله در غیاب نهادهای واسط سنتی به‌شمار می‌آیند. با ورود بانکداری اسلامی به مرحله دیجیتال و مواجهه آن با تهدیدات جدید محاسبات کوانتومی، تطبیق این اصول با زیرساخت‌های رمزنگاری نسل جدید، ضرورتی اجتناب‌ناپذیر یافته است. رمزنگاری پساکوانتومی و توزیع کلید کوانتومی ابزارهای فنی برای مقابله با تهدیدات محاسبات کوانتومی محسوب می‌شوند، و امکان ایجاد ساختارهایی قابل تطبیق با مقاصد شرعی در معاملات غیرربوی را فراهم می‌سازند. بررسی فقهی این فناوری‌ها از منظر سازگاری با اصول شریعت، شرط لازم برای ورود آن‌ها به نظام بانکداری اسلامی است.

٤-١. اصل صحت و شفافیت قرارداد در برابر تهدیدات جعل کوانتومی

در فقه اسلامی، صحت قرارداد بر پایه تحقق ارکان چهارگانه‌ای چون ایجاب و قبول، قصد و رضا، معلوم بودن عوضین، و اهلیت طرفین استوار است. از منظر فقه امامیه، صحت عقد منوط به تحقق واقعی ایجاب و قبول و قصد معتبر است و هرگونه جعل یا تحریف در ارکان آن موجب بطلان عقد می‌شود. در مقابل، فقه حنبلی صحت عقد را تا زمان اثبات فساد آن مفروض می‌داند. از این رو، طراحی فنی مبتنی بر رمزنگاری مقاوم به کوانتوم، که امکان جعل و تردید را از میان می‌برد، دقیقاً با مبنای فقه امامیه در «قطع به صحت عقد» هم‌خوان است و هم‌زمان قابلیت پذیرش تطبیقی در سایر مکاتب فقهی را نیز دارد (نجفی، ۱۴۲۵؛ ابن قدامه المقدسی، ۱۴۴۰). این ارکان نه‌تنها بیانگر توافق حقوقی،

بلکه ناظر بر مشروعیت اخلاقی و فقهی معاملات‌اند. ورود به عرصه دیجیتال، مستلزم بازتعریف این ارکان در قالب ابزارهای نوین، مانند امضای دیجیتال، احراز هویت غیرحضوری، و ثبت مطمئن داده‌ها است. اما این ابزارها، اگرچه در ظاهر کارآمدند، در برابر تهدیدات ناشی از رایانش کوانتومی، آسیب‌پذیری بنیادینی دارند. الگوریتم‌هایی نظیر شُر برای تجزیه اعداد اول، و گروور برای تسریع جستجو در پایگاه داده‌ها، نشان داده‌اند که رمزنگاری‌های متداول مانند امضای دیجیتال ریوست-شامیر-دلمن[۱] و الگوریتم امضای دیجیتال منحنی بیضوی[۲] در دوران پساکوانتوم قابلیت حفظ امنیت خود را از دست می‌دهند. این امر مستقیماً منجر به امکان جعل امضاهای دیجیتال، دستکاری اسناد رسمی، و مخدوش شدن احراز صحت و رضایت طرفین در عقود شرعی می‌شود. از منظر فقه معاملات، این وضع مصداق بارز تردید در تحقق ایجاب و قبول یا خدشه در قصد و رضاست و می‌تواند عقد را از حیث شرعی باطل یا غیرنافذ سازد (خمسه، ۱۳۹۴). در پاسخ به این تهدیدات، مجموعه‌ای از الگوریتم‌های رمزنگاری مقاوم به کوانتوم توسط مؤسسه جهانی استاندارد و فناوری توسعه یافته‌اند. الگوریتم‌هایی نظیر تبادل کلید[۳]، امضاهای دیجیتال[۴] به‌عنوان استانداردهای نهایی در سال ۲۰۲۲ معرفی شده‌اند (الاگیچ[۵]، ۲۰۲۲). این الگوریتم‌ها بر پایه ساختارهایی چون توابع هش مقاوم، شبکه‌های مشبک و چندجمله‌ای‌های ایزومتریک طراحی شده‌اند که در برابر الگوریتم‌های کوانتومی نیز ایمنی خود را حفظ می‌کنند. همچنین، در این چارچوب، مفهوم احراز صحت شرعی امضا (اصالة الصحة) با استفاده از امضاهای دیجیتال مقاوم به کوانتوم، به‌ویژه در بستر قراردادهای غیرربوی مانند مرابحه یا صکوک اجاره، قابل تضمین است. این امضاها نه‌تنها غیرقابل جعل و ردناپذیر هستند، بلکه امکان راستی‌آزمایی چندمرحله‌ای را نیز فراهم می‌آورند. بنابراین، اصل صحت قرارداد، از حیث فقهی (تحقق شروط عقد)، و از منظر فنی (امنیت اطلاعات)، با رویکرد رمزنگاری پساکوانتومی تقویت می‌شود. در نهایت، شفافیت و صحت اسناد مالی دیجیتال در عصر پساکوانتوم نه با اتکا به بلاک‌چین‌های ناسازگار، بلکه با استفاده از امضاهای مقاوم و

---

[۱] Rivest Shamir Adleman(RSA)
[۲] Elliptic Curve Digital Signature Algorithm (ECDSA)
[۳] CRYSTALS Kyber
[۴] Dilithium and Falcon
[۵] Alagic

توزیع کلید کوانتومی، امکان‌پذیر است، ساختاری که نه‌تنها با اصول فقهی انطباق دارد، بلکه پیش‌شرط اعتماد عمومی و مشروعیت نظام بانکداری اسلامی در آینده نیز خواهد بود.

٤-۲. اصل امانت و انتقال مالکیت در بستر رمزنگاری کوانتومی

در فقه معاملات اسلامی، اصل امانت‌داری جایگاهی کلیدی در اعتبار شرعی قراردادها دارد، به‌ویژه در عقودی نظیر مضاربه و مشارکه که یکی از طرفین (عامل یا شریک) موظف به حفظ و استفاده صحیح از سرمایه سپرده‌شده است. خدشه به امانت‌داری یا اختلال در انتقال شفاف مالکیت، از منظر فقهی می‌تواند موجب ضمان، فسخ یا بطلان عقد شود. در فقه امامیه، اصل «الامین لا یضمن الا بالتعدی» اقتضا می‌کند که هرگونه تخطی یا تقصیر در حفظ امانت حتی در فضای داده‌های دیجیتال، موجب ضمان است. فناوری توزیع کلید کوانتومی، با آشکارسازی هرگونه شنود یا دستکاری، مصداق عملی تحقق «امانت مطلقه» است (شهیدِ ثانی ، ۱۴۱۰). در فقه شافعی نیز، شرط صحت عقد مضاربه، تحقق «اطمینان به حفظ المال» است (النووی، ۱۴۲۵)، لذا سامانه‌های توزیع کلید کوانتومی به‌مثابه ابزارهای تحقق این شرط در فضای نوین مالی اسلامی قابل تلقی‌اند. بر همین مبنا، حفاظت از داده‌های مرتبط با مالکیت و مانع‌سازی در برابر تحریف یا دست‌کاری، به‌مثابه حفظ امانت مالی در بستر دیجیتال تلقی می‌گردد (ارزانی، ۱۴۰۳). در فضای سنتی رمزنگاری، انتقال کلیدهای رمزگذاری متکی بر بسترهای غیرقابل اعتماد اینترنتی، مستعد شنود، استراق سمع یا جعل بود؛ اما فناوری توزیع کلید کوانتومی انقلابی در این زمینه پدید آورده است. این فناوری با اتکا بر اصول بنیادی مکانیک کوانتومی، از جمله اصل عدم کپی‌پذیری کوانتومی و قابلیت تشخیص شنود از طریق تداخل حالات فوتونی، امکان انتقال کلید رمزنگاری را با امنیت نظری تضمین‌شده فراهم می‌کند (گیسن[1] ۲۰۰۲). در عمل، هرگونه تلاش برای استراق سمع در فرآیند توزیع کلید، منجر به تغییر وضعیت فوتون‌ها و ایجاد سیگنال هشدار خواهد شد. این ویژگی در بستر فقهی، مصداقی از تحقق امانت‌داری مطلق دیجیتال است؛ یعنی انتقال مالکیت یا اطلاعات، تنها در شرایط اطمینان از عدم دستکاری و بدون امکان جعل صورت می‌پذیرد. کاربرد این

[1] Gisin

فناوری به‌ویژه در قراردادهایی مانند مرابحه یا بیع مؤجل که در آن‌ها زمان و مالکیت به‌صورت مرحله‌ای منتقل می‌شود، اهمیت مضاعف دارد. اگر یکی از طرفین در مسیر اجرای قرارداد، داده‌ها را تحریف یا کلید رمزنگاری را به‌صورت نامشروع افشا کند، سامانه فوراً این تخلف را شناسایی می‌کند. از این منظر، توزیع کلید کوانتومی یک ابزار فنی و ابزاری برای تقویت وفای به عهد، شفافیت مالکیت و رفع شبهات غَرر و تدلیس در قراردادهای دیجیتال اسلامی است. در تحلیل فقهی مربوط به اصل صحت و امانت در قراردادهای دیجیتال، این پژوهش از رویکرد فقه امامیه بهره می‌گیرد که در آن، تحقق رضایت، قطعیت ایجاب و قبول، و حفظ امانت در داده‌های مالی از شرایط صحت عقد به شمار می‌رود. مطابق نظر فقهای امامیه از جمله شهید ثانی در «مسالک الأفهام»، هرگاه ابزار انتقال یا ثبت، موجب تردید در قصد یا رضایت طرفین شود، عقد فاقد اثر شرعی است. این مبنا با اصل «رفع ما استُرِیب فیه» (رفع حکم در موارد شک در تحقق عقد) سازگار است (شهیدِ ثانی ، ۱۴۱۰). در مقابل، در فقه حنبلی، حتی در صورت وجود احتمال ضعف در ابزارهای فنی، عقد تا زمان اثبات بطلان معتبر تلقی می‌شود (ابن قدامه المقدسی، ۱۴۴۰) . همین اختلاف در مبنا، نشان می‌دهد که چارچوب امنیتی پیشنهادی در این مقاله که بر پایه قطعیت رمزنگاری کوانتومی طراحی شده، بیشترین سازگاری را با مبنای فقه امامیه در تحقق «قطع به صحت عقد» دارد.

٤-۳. عدم‌غَرر، ربا و تضاد با بلاک‌چین‌های ناسازگار

یکی از اصول بنیادین در فقه معاملات اسلامی، پرهیز از غَرر است؛ یعنی منع هرگونه ابهام اساسی در ماهیت، مالکیت، ارزش یا نتیجه‌ی قرارداد. غَرر در متون فقهی، صرفاً به معنای جهل اطلاعاتی نیست، بلکه شامل هر نوع ابهام در نتیجه یا تحقق منفعت مشروع نیز می‌شود. بر اساس این مبنا، هرگونه قرارداد یا سازوکار مالی که با سطح بالایی از عدم‌قطعیت، نوسانات کنترل‌ناپذیر یا فرآیندهای غیرقابل‌راستی‌آزمایی همراه باشد، می‌تواند از منظر شریعت، مصداق غَرر یا حتی شبه‌ربا تلقی گردد. از منظر تطبیقی، در فقه امامیه، غَرر به معنای جهل در نتیجه عقد و تزلزل در تحقق مقصود معامله است، در حالی‌که در فقه شافعی، معیار «علم عرفی به نتیجه» و در فقه حنبلی، نوسانات شدید ارزش به‌عنوان

مصداق «غَرر فاحش» شناخته می‌شود (الرزقا[1] ۲۰۲۱). این تفاسیر به‌خوبی با وضعیت شبکه‌های عمومی بلاک‌چین انطباق دارند که در آن‌ها، نوسان قیمت و عدم شفافیت مالکیت موجب تزلزل در قصد و رضا می‌شود. این در حالی است که در سال‌های اخیر، بلاک‌چین به‌عنوان بستر غالب برای سامانه‌های مالی غیرمتمرکز معرفی شده است؛ با این حال، تحلیل‌های فقهی متعدد نشان داده‌اند که این فناوری، علیرغم مزایای فنی، در برخی ابعاد با اصول شرعی سازگاری کامل ندارد. از جمله می‌توان به غَرر در فرآیند تولید بلاک‌ها (الدهنی[2] ۲۰۲۳) به‌ویژه در مکانیزم‌های استخراج و اثبات کار[3] ابهام در مالکیت دارایی‌های رمزنگاری‌شده (توکن‌ها) و احتمال ربوی بودن پاداش‌های محاسباتی شبکه‌های عمومی اشاره کرد. افزون بر این، برخی صاحب‌نظران فقه تطبیقی، از جمله دکتر عبدالحمید ابوسلیمان تأکید کرده‌اند که در فقه اسلامی، «مالکیت باید بر پایه عین یا منفعت مشروع و معلوم» باشد و هر سامانه‌ای که این شفافیت را تضعیف کند، مشمول شائبه غَرر می‌شود. اصول فقه معاملات اسلامی بر ضرورت شفافیت، پیش‌بینی‌پذیری و حذف ابهام (غَرر) در قراردادها تأکید دارند (ابوسلیمان[4] ۱۹۹۸). از دیدگاه فقه شیعه و اهل‌سنت، هر معامله‌ای که در آن موضوع یا مالکیت نامعلوم باشد، یا یکی از طرفین دچار ابهام در منفعت گردد، باطل یا غیرنافذ است. از اینرو در نظام‌های مبتنی بر بلاک‌چین عمومی، این اصول با چالش‌هایی بنیادین روبه‌رو می‌شوند:

– غَرر در مالکیت و موضوع معامله: در شبکه‌های عمومی مانند بیت‌کوین یا اتریوم، مالکیت دارایی‌ها صرفاً به کلید خصوصی وابسته است و از منظر فقهی، چون هویت مالک حقیقی نامشخص است، تحقق شرط «معلومیّت مالک» در عقد بیع یا مشارکه محل اشکال است. پژوهش‌های الازهر و جدّه این وضعیت را مصداق «بیع ما لا یُملَک» دانسته‌اند.

– ربا در پاداش محاسباتی: نظام‌های اثبات کار به استخراج‌کنندگان پاداش مالی پرداخت می‌کنند بدون آنکه در قبال آن مال واقعی یا منفعت مشروع مبادله شود. فقیهان معاصر از جمله آیت‌الله

---

[1] Al-Zarqa
[2] Aldohni
[3] Proof of Work
[4] Abu Sulayman

اعرافی و شیخ عبدالکریم زیدان، این پدیده را مشابه «ربح بدون عوض» دانسته‌اند که در فقه، مصداق ربا یا اکل مال به باطل است.

– غَرر در قیمت‌گذاری و نو سان ارزش: نو سانات شدید ارزش رمزارزها و توکن‌های دیجیتال، سبب می شود که عقد بیع یا اجاره مبتنی بر آن‌ها فاقد پیش‌بینی‌پذیری لازم با شد. در عقود ا سلامی مانند صکوک اجاره یا سلم، این نوع نو سان موجب بطلان عقد به دلیل ابهام در عو ضین می شود. نمونه عملی این وضعیت را می‌توان در برخی طرح‌های توکن‌های غیرقابل‌تعویض[1]صکوک مشاهده کرد که به‌دلیل عدم تعیین ارزش عین، از سوی هیئت‌های شرعی در مالزی و بحرین رد شده‌اند.

علاوه بر این پژوهش‌های انجام شده در رابطه با بازارهای دیجیتال ا سلامی در مالزی (احمد[2] ۲۰۲۴) و مطالعه بازار توکنیزه‌شـــده صـــکوک (خان[3] ۲۰۲۲) نشـــان می‌دهند که معاملات مبتنی قراردادهای هو شمند و مبتنی بر توکن‌های غیرقابل‌تعویض، در صورتی که مالکیت دارایی پایه مشخص نبا شد یا پشتوانه‌حقوقی روشنی نداشته باشد، با چالش‌های جدی فقهی مواجه‌اند (رافاهه[4] ۲۰۲۴). این چالش‌ها شامل موارد زیر است:

- فقدان ارزش‌گذاری شفاف برای دارایی و وابستگی قیمت به نوسانات لحظه‌ای بازار ثانویه؛
- ابهام در احراز مالکیت واقعی به‌ویژه در شرایطی که دارایی دیجیتال فاقد سند حقوقی معتبر است؛
- نبود نهاد ناظر شرعی برای کنترل صدور، انتقال و ابطال توکن‌ها؛
- و عدم امکان فسخ یا تعدیل قرارداد در صورت بروز غَرر یا ضرر، به‌دلیل ساختار اجماع غیرقابل‌اصلاح شبکه‌های بلاک‌چین.

---

[1] Non-Fungible Token (NFT)
[2] Ahmad
[3] Khan
[4] Rafaheh

٤-٤. تطبیق میان ماهیت عقود و مکانیزم‌های رمزنگاری

در فقه معاملات اسلامی، دسته‌ای از عقود مانند سلم، اجاره، جعاله و استصناع نیازمند دقت بالا در ثبت جزئیات زمانی، محتوای تعهد، مبلغ و شرایط فسخ یا اجرا هستند. این عقود اغلب به‌صورت مؤجل یا تدریجی منعقد می‌شوند و صحت آن‌ها منوط به حفظ اصالت اسناد در طول زمان، امکان اثبات شرایط توافق‌شده، و قابلیت راستی‌آزمایی قرارداد بدون خدشه در مالکیت یا رضایت طرفین است (قادری، ۱۳۹۷). در فضای دیجیتال، یکی از چالش‌های اساسی برای صحت شرعی این عقود، نقض اصالت اسناد در گذر زمان یا جعل محتوا و امضای دیجیتال است. الگوریتم‌های سنتی امضای دیجیتال، مانند امضای دیجیتال ریوست–شامیر–دلمن و الگوریتم امضای دیجیتال منحنی بیضوی، در برابر تهدیدات رایانه‌های کوانتومی آسیب‌پذیر هستند. این امر به‌ویژه در عقود بلندمدت مانند استصناع در پروژه‌های زیرساختی یا اجاره بلندمدت املاک وقفی، می‌تواند اصالت قرارداد را زیر سؤال ببرد و از منظر فقهی موجب فسخ، بطلان یا ورود ضرر به یکی از طرفین گردد. در این راستا، رمزنگاری مقاوم به کوانتوم، با استفاده از الگوریتم‌هایی مانند امضای دیجیتال لیتون–مایکالی[۱] و امضای درخت مرکل[۲] بستری ایمن و آینده‌نگر برای ثبت اسناد دیجیتال فراهم می‌کند (فتح‌الله[۳] ۲۰۲۴؛ شالر[۴] ۲۰۲۳). این الگوریتم‌ها بر پایه توابع هش عمل می‌کنند و به دلیل ساختار تک‌جهتی و غیرقابل برگشت، حتی در برابر الگوریتم‌های کوانتومی مانند شُر نیز مقاوم‌اند. افزون بر این، استفاده از مهر زمانی[۵]مقاوم به کوانتوم، با بهره‌گیری از توزیع کلید کوانتومی، امکان ثبت دقیق لحظه انعقاد یا اصلاح قرارداد را فراهم کرده و احتمال دستکاری در سوابق را به صفر می‌رساند (لی[۶] ۲۰۲۴). این ویژگی‌ها با اصل فقهی الزام به وفای به عهد (أوفوا بالعقود)، شفافیت، و منع غَرر کاملاً هم‌راستا هستند. از منظر فقه امامیه، صحت عقود مؤجل مانند سلم و استصناع منوط به تعیین دقیق زمان، عوضین و شرایط اجرا است (شهیدِ ثانی

---

[۱] Leighton–Micali Signature Scheme (LMS)
[۲] eXtended Merkle Signature Scheme (XMSS)
[۳] Fathalla
[۴] Shaller
[۵] Timestamping
[۶] Li

، ۱۴۱۰). در فقه شافعی نیز، شرط «العلم بالمثمن و الاجل» برای صحت عقود لازم دانسته شده است (النووی، ۱۴۲۵). رمزنگاری مقاوم به کوانتوم، با ثبت غیرقابل‌تغییر مهر زمانی و جلوگیری از تحریف داده‌ها، به‌عنوان ابزار تحقق همین شرط فقهی در فضای دیجیتال عمل می‌کند. بنابراین، فناوری‌های نوین رمزنگاری نه‌تنها مانع فقهی ندارند، بلکه مصداق تحقق عملی قواعدی چون اوفوا بالعقود و لا ضرر و لا ضرار در بستر هوشمند محسوب می‌شوند. از اینرو اگر الزامات فقه معاملات اسلامی به‌درستی تفسیر و مدل‌سازی شوند نه‌تنها مانعی برای توسعه فناوری‌های امنیتی نیستند، بلکه می‌توانند به‌عنوان راهنمای طراحی زیرساخت‌های مقاوم و اخلاق‌محور مورد استفاده قرار گیرند. چارچوب ترکیبی فقهی و فناورانه پیشنهادی دقیقاً بر این مبنا توسعه یافته است: تلفیق الزامات شرعی و فقهی با پیشرفته‌ترین استانداردهای رمزنگاری مقاوم به کوانتوم، بدون اتکا به فناوری‌هایی که با اصول اسلامی در تعارض‌اند. در همین راستا این پژوهش تلاش می‌کند با جایگزینی ساختار نیمه‌متمرکز شرعی مبتنی بر «توزیع کلید کوانتومی» و «رمزنگاری مقاوم به کوانتوم»، امکان تحقق سه اصل بنیادین را فراهم می‌کند:

۱. شفافیت مالکیت و هویت مشروع طرفین معامله از طریق احراز رمزنگاری‌شده‌ی هویت‌ها؛

۲. امانت در انتقال و نگهداری داده‌ها به‌واسطه امنیت نظری توزیع کلید کوانتومی در برابر جعل و استراق؛

۳. قطعیت در اجرای تعهدات شرعی با استفاده از امضاهای غیرقابل‌انکار و قابل‌ردیابی.

این ساختار، به‌جای اتکا بر اجماع عمومی بلاک‌چین‌های باز، به مدل نیمه‌متمرکز با نظارت فقهی متکی است که امکان کنترل، فسخ، تعدیل یا ممیزی شرعی را فراهم می‌آورد. بدین‌ترتیب، چارچوب پیشنهادی نه‌تنها با اصول منع غَرر و ربا سازگار است، بلکه می‌تواند به‌عنوان الگوی فنی–فقهیِ قابل بومی‌سازی و از منظر امنیتی مقاوم‌تر برای بانکداری اسلامی در عصر پساکوانتوم به‌کار گرفته شود. این چارچوب در بخش بعدی مقاله، به‌صورت ساختاریافته و با ذکر اجزای عملیاتی ارائه خواهد شد.

۵. ارائه چارچوب ترکیبی پیشنهادی و تحلیل امکان‌سنجی آن در نظام بانکی اسلامی

در پاسخ به تهدیدات قریب‌الوقوع محاسبات کوانتومی علیه زیرساخت‌های رمزنگاری کلاسیک، این پژوهش چارچوبی تلفیقی میان فناوری توزیع کلید کوانتومی و الگوریتم‌های رمزنگاری پساکوانتومی

ارائه می‌دهد که با اصول فقه معاملات اسلامی سازگار بوده و امکان پیاده‌سازی گام‌به‌گام در نظام بانکداری اسلامی را داراست. در این چارچوب، فناوری توزیع کلید کوانتومی برای تأمین امنیت ارتباطی مطمئن و بدون قابلیت استراق سمع میان طرفین قرارداد شرعی به‌کار گرفته می‌شود. به‌ویژه در قراردادهایی نظیر مشارکت، مضاربه، مرابحه و اجاره به شرط تملیک که نیاز به انتقال محرمانه اطلاعات مالی، احراز هویت شرکای اقتصادی و تبادل مالکیت دارند، استفاده از توزیع کلید کوانتومی موجب تحقق اصل امانت در تبادل اطلاعات و حذف هرگونه غَرر اطلاعاتی خواهد شد. در گام بعد، برای ثبت دیجیتال قراردادها و اطمینان از صحت و تمامیت[۱]آن‌ها در برابر جعل یا تحریف، از الگوریتم‌های امضای دیجیتال مقاوم به کوانتوم مانند الگوریتم‌هایی برای تبادل کلید، امضاهای دیجیتال و امضای مبتنی بر هش استفاده می‌شود. این الگوریتم‌ها ضمن مقاومت در برابر حملات کوانتومی، از لحاظ ساختاری نیز فاقد ویژگی‌های نامطمئن همچون احتمال‌شناسی مخرّب‌اند و با اصول فقهی مانند صراحت در مالکیت، شفافیت مفاد قرارداد و ثبات شروط هم‌خوانی دارند.

۵-۱. چارچوب مفهومی روش پیشنهادی در بستر عقود شرعی

چارچوب پیشنهادی از سه لایه اصلی تشکیل شده است:

۱. لایه توزیع کلید کوانتومی[۲]: این لایه، بستر اصلی ارتباط امن میان مشتری و بانک است و با بهره‌گیری از پروتکل‌های شناخته‌شده‌ای چون BB84[۳]یا E91، امکان تبادل کلیدهای رمزنگاری بین طرفین را فراهم می‌سازد. داده‌ها در این مسیر از طریق فوتون‌های منفرد یا درهم‌تنیده‌شده، در

---

[۱] Integrity

[۲] QKD (Quantum Key Distribution) فناوری توزیع کلید رمزنگاری بر پایه مکانیک کوانتوم که شنود را به‌صورت فیزیکی قابل شناسایی می‌سازد.

[۳] پروتکل BB84، مخفف Bennett & Brassard 1984؛ نخستین پروتکل عملی توزیع کلید کوانتومی hsj که از قطبش فوتون برای تولید و تبادل کلید رمزگذاری استفاده می‌کند که در آن هرگونه اجرای شنود، موجب خطا در کلید خواهد شد. در مقابل، پروتکل Ekert 1991 (E91) بر پایه فوتون‌های درهم‌تنیده طراحی شده و امنیت آن از آزمون‌های عدم موضع‌گیری (Bell inequality violations) نتیجه می‌شود؛ هرچند اجرایی‌سازی آن پیچیده‌تر، و وابسته به حفظ همبستگی کوانتومی است اما سطح امنیت بالاتری نسبت به BB84 دارد.

کانال نوری امن[۱]منتقل می‌شوند، به‌گونه‌ای که هرگونه تلاش برای شنود، بنا بر اصل آشکارسازی تداخل در مکانیک کوانتوم، بلافاصله شناسایی می‌شود. نمونه‌های عملی این فناوری شامل دستگاه‌های Toshiba QKD Box و ID Quantique[۲] هستند که نرخ انتقال کلید امن تا ۳۰۰ کیلوبیت بر ثانیه در فاصله ۱۵۰ کیلومتر را با نرخ خطای کمتر از $۱۰^{-۱۰}$ ممکن می‌سازند (گروه محاسبات کوانتومی (آی‌آی‌تی)[۳] ۲۰۲۱؛ توشیبا[۴] ۲۰۲۵). در معماری‌های گسترده بانکی، این زیرساخت می‌تواند به‌صورت توزیع کوانتومی چندمسیره[۵]در شبکه‌های چند شعبه‌ای یا بین‌بانکی به‌کار رود. این سطح به‌طور بنیادین با اصل فقهی امانت‌داری مطلق در انتقال داده‌ها و شفافیت مالکیت، هم‌خوان است.

۲. لایه امنیت پساکوانتومی: در این لایه، تأکید اصلی بر احراز هویت شرعی، صحت امضا و جلوگیری از جعل دیجیتال است. بدین منظور، الگوریتم‌های استانداردشده توسط موسسه ملی جهانی استاندارد و فناوری مانند CRYSTALS-Dilithium، CRYSTALS-Kyber و Falcon به‌کار گرفته می‌شوند. این الگوریتم‌ها مقاومت ذاتی در برابر حملات کوانتومی نظیر الگوریتم شُر دارند و امکان تولید امضاهای دیجیتال با ویژگی‌های انتساب معتبر، عدم انکار و جلوگیری از جعل را فراهم می‌سازند. در حوزه فقه معاملات اسلامی، این ویژگی‌ها معادل با تحقق اصل صحت، وفای به عهد و عدم‌غَرر هستند. از این‌رو، امضای دیجیتال مقاوم به کوانتوم نه‌تنها از نظر فنی قابل اعتماد است، بلکه توسط بسیاری از نهادهای فقهی نیز به‌عنوان ابزار جایگزین امضای فیزیکی شرعی، پذیرفته شده است.

۳. لایه انطباق با شریعت: در این سطح، مدل داده‌پردازی مبتنی بر ساختار نیمه‌متمرکز طراحی شده است؛ بدین معنا که برخلاف بلاک‌چین‌های عمومی، که ذاتاً تمرکززدایی مطلق و فاقد مالک شفاف دارند، این مدل امکان نظارت فقهی و حقوقی توسط نهادهای معتبر همچون شورای فقهی بانک مرکزی و هیئت نظارت شرعی بانک‌ها را فراهم می‌سازد. این لایه، شامل مؤلفه‌هایی نظیر معتبرساز

---

[۱] Secure Optical Fiber Channel

[۲] نمونه سامانه‌های تجاری QKD هستند که در بانک‌های ژاپن و سوئیس به‌صورت پایلوت برای تبادلات مالی ایمن استفاده شده‌اند

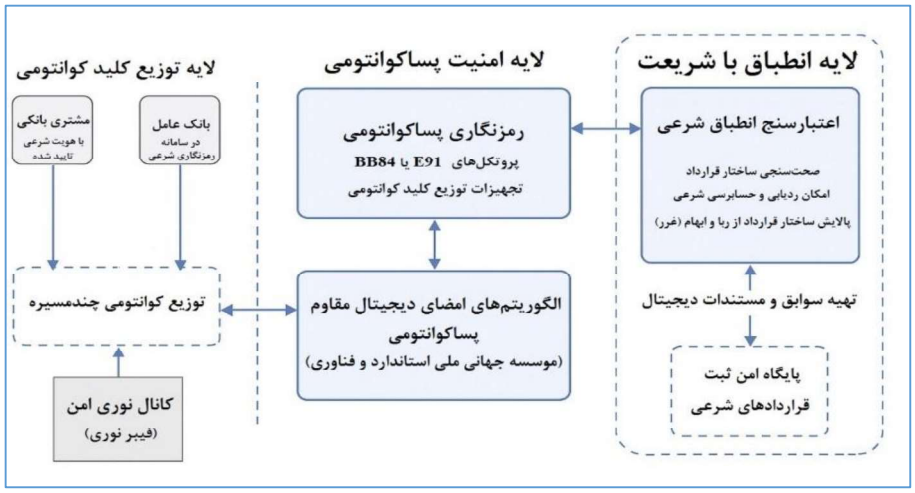
[۳] API

[۴] Toshiba

[۵] Quantum M-Distribution

شرعی قرارداد، مخزن امن و شفاف قراردادها، بررسی صحت شرعی و قابلیت حسابرسی، و ابزارهای حذف ربا و غَرر است که به‌صورت مستقیم، قرارداد را از منظر شرعی و حقوقی راستی‌آزمایی می‌کند. با این منطق، حاکمیت فقه بر ابزار رعایت شده و مسیر اعتمادپذیری حداکثری در نظام بانکی اسلامی فراهم می‌گردد.

ترکیب سه لایه فوق، چارچوبی را ایجاد می‌کند که امنیت رمزنگاری، مشروعیت فقهی، و شفافیت نهادی را به‌صورت هم‌زمان و قابل پیاده‌سازی در سطح ملی و منطقه‌ای تأمین می‌کند. در طراحی این چارچوب، به واقعیت‌های فناوری پساکوانتوم و به ریزبینی‌های فقه اسلامی توجه شده است. معماری چارچوب پیشنهادی در شکل ۲ نشان داده شده است:



شکل ۲: معماری ترکیبی (توزیع کلیدهای رمزگذاری کوانتومی–پساکوانتومی مقاوم) پیشنهادی

۵-۲. الزامات سخت‌افزاری پیشنهادی

برای پیاده‌سازی عملی این مدل، مجموعه‌ای از الزامات سخت‌افزاری وجود دارد که حداقل باید در نظر گرفته شوند که به صورت بسیار مختصر در حد اقتضائات این مقاله به آنها اشاره می‌شود. این الزامات عبارتند از:

– بستر انتقال فوتون: استفاده از فیبر نوری استاندارد تک‌مد یا سامانه‌های Free-Space برای مسافت‌های کوتاه، یا لینک‌های ماهواره‌ای توزیع کلید کوانتومی برای مسافت‌های دوربرد،

– رمزگذاران تک‌فوتون با حساسیت بالا: مانند سنسورهای نانوسیم‌نرم[۱] در سیستم‌های BB84 برای افزایش نرخ دستاورد کلید امن و کاهش خطر حملات جانبی (کرلین،[۲] ۲۰۲۴)،

– حفاظت ETSI / ISO منطبق با توزیع کلیدهای رمزگذاری کوانتومی: استفاده از پروفایل ETSI QKD016 که الزامات اجتناب از نشت اطلاعات و حملات عملیاتی را تعریف می‌کند (آی‌دی‌کیو،[۳] ۲۰۲۳).

۵-۳. امکان‌سنجی فنی و نهادی در بستر ایران و کشورهای اسلامی

اگرچه فناوری توزیع کلیدهای رمزگذاری کوانتومی نیازمند زیرساخت‌های نوری و مخابراتی پیشرفته است، اما اجرای تدریجی آن حتی در کشورهای دارای محدودیت‌های زیرساختی نیز امکان‌پذیر است. در ایران، با توجه به توسعه فیبرنوری توسط شرکت‌های ارتباطی و آزمایشگاه‌های کوانتومی در پژوهشگاه دانش‌های بنیادی، اجرای پایلوت در شبکه بین‌بانکی امکان‌پذیر است. الزامات امکان‌سنجی فنی عبارت‌اند از:

– بستر انتقال نوری ایمن: استفاده از فیبرهای نوری اختصاصی با نویز کنترل‌شده برای انتقال فوتون‌ها،

– مدیریت کلید و ذخیره‌سازی امن: بهره‌گیری از سخت‌افزارهای مقاوم در برابر دسترسی غیرمجاز (مثلاً حافظ امنیت سخت‌افزاری کوانتومی)[۴]،

– پروتکل‌های منطبق با نیازهای فقهی: توسعه رابط‌های برنامه‌نویسی[۵] برای تطبیق ساختار فناوری توزیع کلیدهای رمزگذاری کوانتومی و پساکوانتومی مقاوم با محتوای فقهی هر قرارداد.

در سطح نهادی، تحقق این چارچوب مستلزم همکاری میان نهادهای زیر است:

---

[۱] Superconducting Nanowire Single-Photon Detector (SNSPD)

[۲] Kyrlynn

[۳] IDQ

[۴] Quantum-resistant Hardware Security Module (HSM)

[۵] API

– شورای فقهی بانک مرکزی ایران: تدوین فتواها و دستورالعمل‌های شرعی مرتبط با امضای دیجیتال، تبادل کلید و صحت قرارداد،

– مرکز افتا (امنیت فضای تولید و تبادل اطلاعات): استانداردسازی الگوریتم‌های پساکوانتومی مقاوم،

– نظام بانکی و شرکت خدمات انفورماتیک: برای توسعه سامانه‌های اجرایی و زیرساخت نرم‌افزاری– سخت‌افزاری مورد نیاز.

مزایا و برتری‌ها نسبت به معماری‌های فعلی عبارت است از:

– عدم نیاز به بلاک‌چین: در حالی‌که بسیاری از راهکارهای پیشنهادی برای ثبت قراردادها متکی به بلاک‌چین‌اند که از منظر فقهی محل بحث است، چارچوب پیشنهادی با ساختار متمرکز یا نیمه‌متمرکز قابل اجراست،

– رعایت اصل امانت و شفافیت: با رمزنگاری مقاوم و تبادل امن کلید، احتمال خیانت یا دست‌کاری در قراردادها به‌صورت عملی صفر می‌شود،

– افزایش اعتماد عمومی به بانکداری اسلامی دیجیتال: با فراهم شدن زیرساخت‌های مقاوم در برابر آینده، پذیرش مردمی و اعتبار بین‌المللی بانکداری اسلامی افزایش می‌یابد.

می‌توان گفت چارچوب ترکیبی (توزیع کلیدهای رمزگذاری کوانتومی–پساکوانتومی مقاوم) پیشنهادی ارائه‌شده، پاسخی فنی–فقهی به دو چالش بنیادین عصر حاضر است:

– تهدیدات امنیتی محاسبات کوانتومی،

– ضرورت صیانت از اصول فقهی در بانکداری دیجیتال اسلامی.

از اینرو این چارچوب بر مبانی شرعی استوار است، و از آخرین دستاوردهای فنی و استانداردهای بین‌المللی نیز پیروی می‌کند و قابلیت اجرا در سطح پایلوت و سپس ملی را دارد.

٦. بررسی چالش‌ها، زیرساخت‌ها، و مسیر سیاست‌گذاری در ایران و کشورهای اسلامی

در مسیر پیاده‌سازی چارچوب ترکیبی (توزیع کلیدهای رمزگذاری کوانتومی–پساکوانتومی مقاوم) پیشنهادی در نظام بانکداری اسلامی، مجموعه‌ای از چالش‌های چندلایه ساختاری، زیرساختی، حقوقی

و فقهی قابل شناسایی است که بدون تدبیر نظام‌مند و سیاست‌گذاری گام‌به‌گام، تحقق عملی آن را دشوار می‌سازد. با این حال، باید توجه داشت که این دشواری‌ها نه به‌معنای غیرقابل‌اجرا بودن، بلکه بازتابی از فاصله‌ی سطح بلوغ فناورانه نظام بانکی ایران و سایر کشورهای اسلامی با الزامات عصر پساکوانتوم است. بر اساس گزارش «مرکز فناوری‌های نوین مالی بانک مرکزی ایران (۱۴۰۳)»، تنها تعداد محدودی از بانک‌های کشور به زیرساخت‌های رمزنگاری توزیع‌شده دسترسی دارند و حتی پروژه‌های پایلوت بلاک‌چین داخلی نیز در سطح مفهومی باقی مانده‌اند. ازاین‌رو، حرکت مستقیم از زیرساخت‌های فعلی به رمزنگاری کوانتومی، واقع‌بینانه نیست و باید از مسیرهای میانی و مرحله‌ای طی شود. چارچوب پیشنهادی این مقاله، با درک همین واقعیت، نه یک جهش فناورانه بلکه نقشه‌راهی تدریجی و شریعت‌محور برای گذار از رمزنگاری کلاسیک به رمزنگاری مقاوم به کوانتوم است. در این چارچوب، تحول فناورانه هم‌زمان با تحول فقهی و نهادی پیش می‌رود تا ثبات و مشروعیت نظام بانکی حفظ شود. کشورهای اسلامی، بسته به میزان بلوغ دیجیتال، زیرساخت فناوری اطلاعات، نهادهای مقررات‌گذار، و میزان اجتهاد فعال فقهی، با درجات متفاوتی از آمادگی برای پذیرش این فناوری نوین مواجه‌اند:

۱. چالش‌های زیرساختی: نخستین مانع، فقدان زیرساخت‌های مخابراتی و اپتیکی لازم برای پیاده‌سازی عملی توزیع کلیدهای رمزگذاری کوانتومی است. ایجاد خطوط فیبر نوری اختصاصی، توسعه گره‌های ارتباطی کوانتومی، و تأمین سخت‌افزارهای رمزنگاری کوانتومی، مستلزم سرمایه‌گذاری سنگین، انتقال فناوری، و تربیت نیروی انسانی تخصصی است. در حال حاضر، تنها تعداد انگشت‌شماری از کشورها از جمله چین، آلمان، کره جنوبی، و امارات، توانسته‌اند شبکه‌های آزمایشی یا تجاری توزیع کلیدهای رمزگذاری کوانتومی را مستقر کنند. ایران نیز در حوزه‌های اپتوالکترونیک، لیزر، و کوانتوم‌کامپیوتر، پیشرفت‌هایی پراکنده داشته، اما همچنان فاقد شبکه‌ای عملیاتی و پایدار برای رمزنگاری کوانتومی در نظام مالی است.

۲. ملاحظات حقوقی و رگولاتوری: فقدان چارچوب‌های قانونی مشخص برای پذیرش امضای دیجیتال مقاوم به کوانتوم، انتقال داده‌های رمزگذاری‌شده کوانتومی، و ثبت قراردادهای الکترونیکی غیرربوی، از دیگر موانع است. در بسیاری از کشورهای اسلامی، قوانین تجارت الکترونیک هنوز به‌روزرسانی لازم

برای تطبیق با فناوری‌های رمزنگاری نسل جدید را دریافت نکرده‌اند. همچنین، نهادهای مقررات‌گذار مالی و شرعی نیز از یک مدل تصمیم‌گیری همگرا برای اعتباربخشی به این فناوری‌ها برخوردار نیستند.

۳. چالش‌های فقهی و اجتهادی: یکی از جنبه‌های حیاتی، مشروعیت فقهی استفاده از سامانه‌های رمزنگاری جدید در قالب عقود شرعی است. پرسش‌هایی همچون: آیا ثبت دیجیتال قرارداد مضاربه با الگوریتم پساکوانتومی مقاوم موجب خدشه در اصل امانت‌داری یا شفافیت می‌شود؟ آیا انتقال کلید کوانتومی بین دو بانک اسلامی مطابق با قاعده عدم غَرر است؟ و آیا استفاده از الگوریتم‌های خارجی (مانند الگوریتم‌هایی برای تبادل کلید، امضاهای دیجیتال و امضای مبتنی بر هش) نیازمند تطهیر فقهی خاص است؟ همه از جمله مسائل اجتهادی نوپدیدی هستند که بدون اجماع علما، مشروعیت این فناوری‌ها در فضای بانکداری اسلامی محل تردید خواهد بود.

۴. چالش‌های فرهنگی و مدیریتی: فراتر از موانع فناورانه و فقهی، مسئله مقاومت نهادی در برابر نوآوری، عدم درک عمومی نسبت به تهدید کوانتوم، و نبود آموزش سیستماتیک در سطح بانک‌ها و نهادهای مالی، از دیگر موانع نرم محسوب می‌شوند. بانک‌ها اغلب نگاه محافظه‌کارانه‌ای به فناوری‌های نوظهور دارند، به‌ویژه اگر فرآیندهای اجرایی آن‌ها پیچیدگی تکنولوژیک و حساسیت شرعی داشته باشد.

در ادامه مجموعه‌ای از اقدامات سیاست‌گذاری برای تسهیل گذار ایمن و شرعی به دوران پساکوانتومی توصیه می‌شود این اقدامات نه به‌صورت جهشی بلکه در قالب برنامه‌ای تدریجی و مرحله‌به‌مرحله باید دنبال شوند تا امکان هم‌زمانی توسعه‌ی فقهی، فنی و نهادی فراهم گردد:

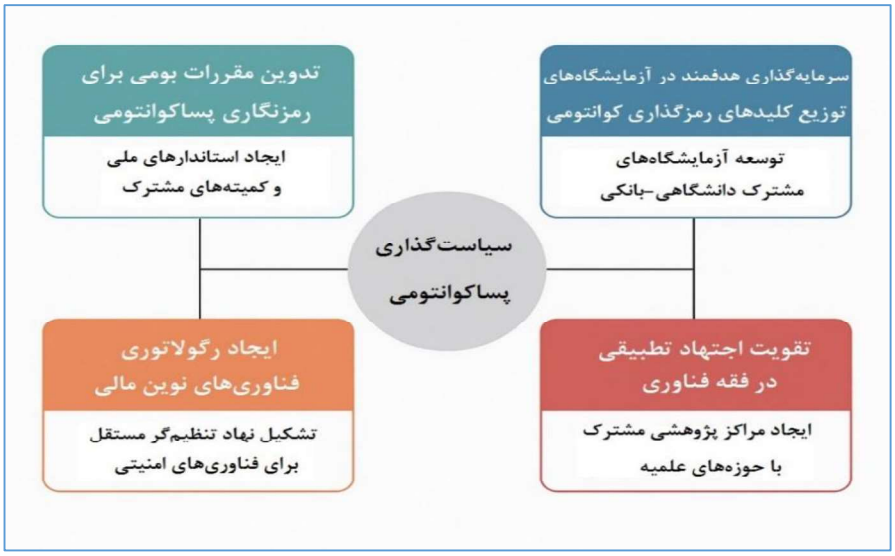
۱. تدوین مقررات بومی برای رمزنگاری پساکوانتومی: از جمله ایجاد استانداردهای ملی در تطابق با چارچوب مؤسسه جهانی استاندارد و فناوری و ایجاد کمیته‌های مشترک بین بانک مرکزی، سازمان فناوری اطلاعات، و شورای فقهی بانکداری اسلامی.

۲. سرمایه‌گذاری هدفمند در آزمایشگاه‌های توزیع کلیدهای رمزگذاری کوانتومی: توسعه آزمایشگاه‌های مشترک دانشگاهی–بانکی برای پیاده‌سازی شبکه‌های محدود توزیع کلیدهای رمزگذاری کوانتومی، ترجیحاً در بانک‌های توسعه‌ای یا بانک‌های اسلامی پیشرو.

۳. ایجاد رگولاتوری فناوری‌های نوین مالی: تشکیل نهاد تنظیم‌گر مستقل برای فناوری‌های امنیتی در نظام بانکی با اختیارات در تدوین سندهای سیاستی و تأیید پروژه‌های آزمایشی.

۴. تقویت اجتهاد تطبیقی در فقه فناوری: ایجاد مراکز پژوهشی مشترک بین حوزه علمیه و دانشگاه‌های فنی برای بررسی مشروعیت فناوری‌های نوین از منظر اصول معاملات اسلامی.

در این بین طراحی کارگاه‌های آموزشی برای مدیران و کارشناسان فناوری اطلاعات در بانک‌ها به‌منظور ارتقاء سواد کوانتومی و شناخت تهدیدات آینده از اهمیت بسزایی برخوردار است. سیاست‌گذاری منسجم و چندسطحی که ابعاد فناورانه، فقهی و نهادی را در کنار هم مورد توجه قرار دهد، تنها مسیر منطقی برای آماده‌سازی نظام بانکداری اسلامی در برابر چالش‌های قریب‌الوقوع امنیت اطلاعات در عصر پساکوانتوم است. نمودار سیاست‌گذاری طبقه‌بندی‌شده پساکوانتومی پیشنهادی در شکل ۳ نشان داده شده است.



شکل ۳: نمودار سیاست‌گذاری طبقه‌بندی‌شده پساکوانتومی پیشنهادی

٦-١. مسیر گام‌به‌گام مدیریت چالش‌ها و اجرای تدریجی چارچوب پیشنهادی

با وجود چالش‌های یادشـــده، گذار به بانکداری اســـلامی مقاوم به کوانتوم در صـــورت اتخاذ رویکرد مرحله‌ای و تدریجی، کاملاً قابل تحقق ا ست. م سیر مدیریت این د شواری‌ها را می‌توان در چهار گام اصلی تبیین کرد:

– گام نخست: توانمندسازی دانشی و فقهی: ایجاد «آزمایشگاه فقه و فناوری رمزنگاری» با مشارکت بانک مرکزی، پژوهشگاه ارتباطات و حوزه علمیه قم، برای شکل‌دهی به ادبیات مشترک میان فقها و متخ ص صان فناوری. در این مرحله، آموزش مفاهیم رمزنگاری کوانتومی برای اع ضای شورای فقهی بانک مرکزی و متخصصان بانکی ضروری است.

– گام دوم: تو سعه زیر ساخت فنی و آزماي شگاهی: اجرای پروژه‌های آزماي شی کوچک در بانک‌های اسلامی منتخب با استفاده از تجهیزات تجاری توزیع کلید کوانتومی (مانند Toshiba QKD Box) و الگوریتم‌های مقاوم بومی. این مرحله باید با همکاری دانشگاه‌های صنعتی کشور و شرکت‌های فیبر نوری انجام شود.

– گام سوم: تنظیم‌گری و تطبیق شرعی: تدوین «آیین‌نامه انطباق کوانتومی با شریعت» تحت نظارت شـــورای فقهی بانک مرکزی و مرکز ملی فضـــای مجازی. این آیین‌نامه چارچوب پذیرش قراردادها و امضاهای دیجیتال مقاوم به کوانتوم را تعیین می‌کند.

– گام چهارم: بومی‌ســـازی و اســـتقرار کامل: پس از اجرای آزمایشـــی و تأیید فقهی، الگوریتم‌ها و سامانه‌های بومی جایگزین رمزنگاری‌های کلاسیک می‌شوند. این مرحله باید با پایش مستمر از سوی «کمیته راهبری امنیت کوانتومی شرعی» انجام گیرد تا انطباق دائمی با ا صول فقه معاملات ا سلامی تضمین شود.

اجرای این فازها د شواری پیاده سازی چارچوب پی شنهادی را کاهش داده و م سیر گذار ایمن، تدریجی و بومی‌سازی‌شده به بانکداری کوانتومی اسلامی را فراهم می‌سازد. چنین رویکردی، هم‌زمان با حفظ

م شروعیت فقهی، موجب ارتقای اعتماد نهادی و ثبات ساختاری نظام مالی ا سلامی در آینده خواهد شد.

نتیجه‌گیری و پیشنهادهایی برای تحقیقات آینده

با ورود به عصر محاسبات کوانتومی، زیرساخت‌های رمزنگاری متعارف که بنیان امنیت اطلاعات در نظام‌های مالی بر آن استوار است، با تهدیدات بی‌سابقه‌ای مواجه شده‌اند. در این میان، نظام بانکداری اسلامی، با ویژگی‌هایی چون تأکید بر صحت قرارداد، شفافیت مالکیت، امانت‌داری، و اجتناب از ربا، بیش از سایر الگوهای بانکی نیازمند حفاظت از اصالت ساختارهای اطلاعاتی خود در برابر حملات کوانتومی است. پژوهش حاضر با تلفیق دانش فنی حوزه رمزنگاری توزیعی کوانتومی و رمزنگاری مقاوم به کوانتوم با الزامات فقه معاملات اسلامی، چارچوبی عملیاتی، تدریجی و سازگار با شریعت برای حفاظت از قراردادهای غیرربوی در نظام بانکی ارائه داد. از منظر فقه تطبیقی، چارچوب پیشنهادی مقاله با مبانی فقه امامیه همخوانی تام دارد و درعین‌حال قابلیت انطباق با اصول مشترک میان مکاتب فقهی اهل‌سنت، به‌ویژه در حوزه منع ربا و غَرر، را داراست. این ویژگی، امکان به‌کارگیری مدل ارائه‌شده در نظام‌های بانکی کشورهای مختلف اسلامی را فراهم می‌آورد. نتایج نشان داد که استفاده از پروتکل‌های توزیع کلید کوانتومی و الگوریتم‌های امضای دیجیتال مقاوم، نه‌تنها تهدیدات آینده را کاهش می‌دهد، بلکه می‌تواند اعتماد عمومی به صحت شرعی قراردادها را نیز تقویت کند. با توجه به تحلیل‌های امکان‌سنجی انجام‌شده، مهم‌ترین نتیجه پژوهش، امکان طراحی سامانه‌ای بومی، بدون نیاز به زیرساخت بلاک‌چین و ناسازگاری‌های فقهی آن، و متکی بر فناوری‌های قابل استقرار در کشورهایی چون ایران است. همچنین، نمودار سیاست‌گذاری ارائه‌شده در این مقاله، مسیر دقیقی را برای پیاده‌سازی تدریجی فناوری‌های کوانتومی در نظام بانکداری اسلامی ترسیم می‌کند. در ادامه پیشنهادهایی برای پژوهش‌های آینده تقدیم می‌گردد:

۱. تحلیل و توسعه رمزنگاری ترکیبی: با توجه به گذار تدریجی جهان از رمزنگاری کلاسیک به رمزنگاری مقاوم، پژوهش‌هایی پیرامون مدل‌های رمزنگاری ترکیبی که به‌طور هم‌زمان از الگوریتم‌های کلاسیک و مقاوم بهره می‌برند (مانند PQ-Hybrid TSL)، می‌تواند در محیط‌های بانکی اسلامی

مفید و کاربردی باشد. این رویکرد در سازمان ملی استاندارد ایالات متحده نیز به‌عنوان رویکرد انتقالی توصیه شده است.

۲. آموزش و توانمندسازی نخبگان حوزوی در حوزه امنیت رمزنگاری و فناوری اطلاعات: یکی از پیش‌نیازهای توسعه پایدار در زمینه امنیت دیجیتال اسلامی، تربیت نخبگان فقهی آشنا با مفاهیم فنی امنیت سایبری و رمزنگاری کوانتومی است. طراحی دوره‌های میان‌رشته‌ای در حوزه فقه فناوری[۱] برای مراجع ناظر بر بانک‌ها می‌تواند به مشروع‌سازی تخصصی فناوری‌های نو یاری رساند.

۳. تدوین مدل‌های ریاضی و صوری برای صحت‌سنجی قراردادهای اسلامی: به‌ویژه در حوزه صکوک و مشارکت، تدوین پروتکل‌هایی که به‌صورت صوری و اثبات‌پذیر بتوانند صحت و عدم جعل امضای شرعی را در الگوریتم‌های مقاوم تضمین کنند، می‌تواند مبنای طراحی سامانه‌های رسمی‌سازی قراردادها قرار گیرد.

۴. تحلیل فقهی-فنی در شرایط بحرانی امنیتی: سناریوهای بحرانی مانند نقض احتمالی پروتکل‌های توزیع کلید یا حملات جانبی به امضای دیجیتال، باید از منظر فقهی در قالب قواعد اضطرار، ضمان، و صحت عقود بررسی شوند تا ظرفیت انعطاف‌پذیری شرعی حفظ گردد.

۵. پژوهش در تعامل میان هویت دیجیتال اسلامی و امنیت پساکوانتومی: طراحی سازوکارهای احراز هویت مبتنی بر شناسه‌های اسلامی (مالکیت واضح، وفای به عهد، عدم تزویر) با استفاده از توزیع کلید کوانتومی و امضاهای مقاوم، می‌تواند زیرساختی امن و منطبق با فقه برای بانکداری غیرحضوری فراهم آورد.

۶. ارزیابی پایداری زیست‌محیطی و اقتصادی الگوریتم‌های کوانتومی در بانکداری اسلامی: با توجه به مصرف بالای انرژی در برخی الگوریتم‌های امنیتی، تحلیل این فناوری‌ها از منظر اخلاق محیط‌زیستی اسلامی (بر مبنای مفهوم خلافه و عدم اسراف) می‌تواند به توسعه اقتصاد سبز اسلامی در کنار امنیت کمک کند.

---

[۱] Fiqh of Emerging Technologies

در مجموع آینده بانکداری اسلامی بدون توجه به تحولات بنیادین در رمزنگاری و امنیت سایبری، هم منظر فنی، هم از حیث اعتماد عمومی و مشروعیت شرعی، در معرض آسیب قرار دارد. چارچوب پیشنهادی ارائه‌شده در این مقاله، پاسخی پیشرو و منطبق با اصول شریعت به این چالش است. اجرای تدریجی آن در کشورهایی مانند ایران، با وجود چالش‌های زیرساختی و نهادی، با تکیه بر ظرفیت‌های علمی و فقهی موجود، ممکن و ضروری است. این مسیر، آغازگر فصل تازه‌ای در تعامل هوشمندانه میان فناوری‌های نوین و ارزش‌های بنیادین بانکداری اسلامی خواهد بود.

منابع

ابن قدامه المقدسی، ع.ب.ا. (۱۴۴۰ق)، المغنی فی فقه الإمام احمد بن حنبل. دارالفکر. https://books.altafser.com/book/11564.

ارزانی، ن. (۱۴۰۳). چالش‌های معاملات الکترونیکی و راهکارهای مشروعیت‌بخشی به آن از منظر فقه امامیه. دوفصلنامه مطالعات فقه و حقوق فرهنگی، ۱(۱)، ۱۰۲–۱۲۷ . https://doi.org/10.22034/cjls.2025.2049684.1019.

خمسه، ا. (۱۳۹۴). اصل صحت از دیدگاه فقهی، حقوقی و کاربرد آن در قراردادهای منعقده، قوانین و آرای قضایی ایران. فصلنامه پژوهش‌های سلامت اداری، ۷(۳)، ۲۵- https://www.salamatedari-mag.ir/article_252698.html.

شهید ثانی، ز.ب.ع. (۱۴۱۰ق)، مسالک الأفهام إلی تنقیح شرائع الإسلام. دار احیاء التراث العربی. https://noorlib.ir/book/view/404.

قادری، ج.، و ایزدی، ب. (۱۳۹۷). بررسی آثار اقتصادی و مفاهیم فقهی عقود سه‌گانه جدید استصناع، خرید دین و مرابحه به عنوان ابزارهای نوین بانکداری اسلامی. فصلنامه اقتصاد بانکداری اسلامی، ۶(۲۰)، ۷۹–۹۷. http://mieaoi.ir/article-1-523-fa.html .

موسوی بجنوردی، م. (۱۳۷۹). قواعد فقهیه. مؤسسه تنظیم و نشر آثار امام خمینی (ره). مؤسسه چاپ و نشر عروج، https://noorlib.ir/book/info/551.

نجفی، م.ح. (۱۴۲۵ق). جواهر الکلام فی شرح شرایع الإسلام. جلد ۲۶. دار إحیاء التراث العربی. https://books.altafser.com/book/11564.

النووی، ی.ب.ش. (۱۴۲۵ق)، روضة الطالبین وعمدة المفتین. دارالکتب العلمیة. https://shamela.ws/book/499.

Abu Sulayman, A. H. (1998). The Theory of the Economics of Islam (II). IIUM Journal of Economics and Management, 6(2). https://doi.org/10.31436/ijema.v6i2.45.

Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. Ledger, 3. http://dx.doi.org/10.5195/LEDGER.2018.127.

Ahmad, A. A., & Mohd Sobri, N. A. (2024). Non-fungible tokens (NFTs) in Islamic perspective: Challenges and way forward. Journal of Contemporary Islamic Law, 9(1), 8–15. https://doi.org/10.26475/jcil.2024.9.1.02.

Ain, N. U., Waqar, M., Bilal, A., Kim, A., Ali, H., & Tariq, U. U. (2025). A novel approach based on quantum key distribution using BB84 and E91 protocol for resilient encryption and eavesdropper detection. IEEE Access, 13, 32819–32833. https://doi.org/10.1109/ACCESS.2025.3539178.

Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Silberg, H., Smith-Tone, D., & Waller, N. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process. NIST IR 8545. https://doi.org/10.6028/NIST.IR.8545.

Alagic, G., Cooper, D., Dang, Q., Dang, T., Kelsey, J. M., Lichtinger, J., Liu, Y.-K., Miller, C. A., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Apon, D. (2022). Status report on the third round

of the NIST post-quantum cryptography standardization process. NIST Interagency/Internal Report, 8413. https://doi.org/10.6028/NIST.IR.8413.

Aldohni, A.K. (2023). Understanding the inherent limitations of crypto finance in the Islamic finance context. Capital Markets Law Journal,18(4), pp. 573-588. https://doi.org/10.1093/cmlj/kmad017.

Al-Zarqa, M.A. (2021). Introduction to Islamic Jurisprudence Al-Madkhal Al-Fiqhi Al-'Âm. Damascus: Dar al-Qalam. https://www.iefpedia.com/english/?p=7742.

Aquina, N., Cimoli, B., Das, S., Hövelmanns, K., Weber, F. J., Okonkwo, C., Rommel, S., Škorić, B., Tafur Monroy, I., & Verschoor, S. (2025). A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. EPJ Quantum Technology, 12, 51. https://doi.org/10.1140/epjqt/s40507-025-00350-5.

Babu, P. R., Kumar, S. A. P., Reddy, A. G., & Das, A. K. (2024). Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. Computer Science Review, 54, 100676. https://doi.org/10.1016/j.cosrev.2024.100676.

BIS. (2023). Project Leap: Quantum-proofing the financial system. BIS Innovation Hub Reports. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA. https://doi.org/10.1109/SP.2015.14.

Dahdal, A. M., Truby, J., & Ismailov, O. (2022). The role and potential of blockchain technology in Islamic finance. European Business Law Review, 33(2), 175–192. http://dx.doi.org/10.54648/EULR2022005.

Daniels, T. P. (2017). Sharia dynamics: Islamic law and sociopolitical processes. Contemporary Anthropology of Religion. https://doi.org/10.1007/978-3-319-45692-8.

Elmisery, A. M., Sertovic, M., Zayin, A., & Watson, P. (2025). Cyber threats in financial transactions: Addressing the dual challenge of AI and quantum computing. Cryptography and Security. https://doi.org/10.48550/arXiv.2503.15678.

Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. IEEE Access, 12, 175969–175987. https://doi.org/10.1109/ACCESS.2024.3485602.

Fotova Čiković, K., & Keček, D. (2025). The application of blockchain technology in Islamic banking literature: A PRISMA-compliant literature review. In International Scientific Conference on Business and Economics (pp. 21–38). Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-031-73510-3_2.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74, 145. http://dx.doi.org/10.1103/RevModPhys.74.145.

HSBC. (2024). HSBC pilots quantum-safe technology for tokenised gold. HSBC Press Office. https://www.hsbc.com/news-and-views/news/media-releases/2024/hsbc-pilots-quantum-safe-technology-for-tokenised-gold.

ICBC. (2017). ICBC succeeds in applying thousand-km-level quantum communication technology. ICBC News. https://www.icbc-ltd.com/icbc/en/newsupdates/icbc%20news/ICBCSucceedsinApplyingThousandkmlevelQuantumCommunicationTechnology.htm.

ICBC. (2023). 2023 annual report (Stock Code: 1398). Industrial and Commercial Bank of China Limited.

https://v.icbc.com.cn/userfiles/Resources/ICBCLTD/download/2024/Announcement20240426_2.pdf.

IDQ. (2023). IDQ leads standardization efforts at ETSI to accelerate the adoption of QKD technology. https://www.idquantique.com/idq-leads-standardization-efforts-at-etsi-to-faster-the-adoption-of-qkd-technology.

Jahangir, H. A., Jamil, M. W., & Akhlaq, M. (2025). Islamic finance and digital currencies: Shariah perspectives on cryptocurrency and blockchain technology. AL-AASAR Journal Quarterly Research Journal, 2(2), 789–797. https://al-aasar.com/index.php/Journal/article/view/323.

JPMorgan. (2024). JPMorgan Chase establishes quantum-secured crypto-agile network. https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network.

Kamali, M.H. (2019). Principles of Islamic Jurisprudence. Islamic Texts Society, https://asimiqbal2nd.wordpress.com/wp-content/uploads/2009/06/islamic-law.pdf.

Khan, N., Kchouri, B., Yatoo, N.Y., Kräussl, Z., Anass Patel, A., State, S. (2022). Tokenization of sukuk: Ethereum case study. Global Finance Journal, 51, 100539, https://doi.org/10.1016/j.gfj.2020.100539.

Kwiatkowski, K. (2025). Guidance for migration to post-quantum cryptography. Internet-Draft. https://www.ietf.org/archive/id/draft-kwiatkowski-pquip-pqc-migration-00.html.

Kyrlynn, D. (2024). What is QKD or quantum key distribution, the quantum security protocol? Quantum Zeitgeist. https://quantumzeitgeist.com/what-is-qkd-or-quantum-key-distribution-the-quantum-security-protocol.

Li, M.-Y., Weng, C.-X., Liu, W.-B., Zhu, M., & Chen, Z.-B. (2025). Information-theoretically secure quantum timestamping with one-time

universal hashing. Science China Physics, Mechanics & Astronomy, 68, 100312. https://doi.org/10.1007/s11433-025-2709-x.

Mahmood, A., Khan, A., & Pasoon, H. (2025). Shari'ah and digital currencies: Analyzing cryptocurrency in the Islamic finance framework. Bulletin of Multidisciplinary Studies, 2(1), 135–145. http://dx.doi.org/10.5281/15294173.

Mansour, N., & Bujosa, L. (2024). Shari'ah law: An introduction. Contributions to Management Science. https://doi.org/10.1007/978-3-031-48770-5.

Matondang, D. M., Simanjuntak, W. W., Siregar, D. A., Siregar, B. G., & Rusydiana, A. S. (2024). Blockchain in Islamic finance: A review using bibliometric. Jurnal Ilmu Manajemen dan Bisnis Islam, 10, 70–103. https://jurnal.uinsyahada.ac.id/index.php/attijaroh/article/download/13266/pdf.

Menne, F., Hasiara, L. O., Setiawan, A., Palisuri, P., Tenrigau, A. M., Waspada, W., Juliana, J., & Nurhilalia, N. (2024). Sharia accounting model in the perspective of financial innovation. Journal of Open Innovation: Technology, Market, and Complexity, 10(1), 100176. https://doi.org/10.1016/j.joitmc.2023.100176.

Naz, A., Ali, M., & Ashfaq, M. (2025). Chapter 9: Governance and ecosystem in Islamic fintech: Frameworks, opportunities, and challenges. In Islamic finance and corporate governance: Synergies for sustainable growth. Emerald Insight. https://doi.org/10.1108/978-1-83662-346-520251020.

Nerem, R. R., & Gaur, D. R. (2023). Conditions for advantageous quantum Bitcoin mining. Blockchain: Research and Applications, 4(3), 100141. https://doi.org/10.1016/j.bcra.2023.100141.

Niederhagen, R., & Saarinen, M.-J. O. (2025). Post-quantum cryptography. In Lecture notes in computer science (Vol. 15577, Part I). 16th International Workshop, Taipei, Taiwan.https://doi.org/10.1007/978-3-031-86599-2.

Nielsen, M. A., & Chuang, I. L. (2011). Quantum computation and quantum information: 10th anniversary edition. Cambridge University Press. https://dl.acm.org/doi/10.5555/1972505.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79.

Quantum Computing Group, IIT Roorkee. (2021). Fundamentals of quantum key distribution — BB84, B92 & E91 protocols. Medium. https://medium.com/%40qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead.

Quantum Flagship. (2021). OpenQKD – Open European quantum key distribution testbed: Project description: Europe-wide quantum communication testing. https://qt.eu/projects/archive/communication/openqkd.

Quantum Zeitgeist. (2025). Korea Telecom & HEQA Security deploy quantum key distribution for enhanced cybersecurity. Quantum News. https://quantumzeitgeist.com/korea-telecom-heqa-security-deploy-quantum-key-distribution-for-enhanced-cybersecurity.

Rafaheh, N.R. (2024). Smart Contracts and the Possibility of Gharar. iECO Special Issue, 2(1), https://doi.org/10.59202/ieco.v2i1.787.

Salim, K., Abojeib, M., & Abdul Hamid, B. (2020). Islamic fintech in Malaysia: Reality & outlook. Kuala Lumpur: The International Centre for Education in Islamic Finance. https://capitalmarketsmalaysia.com/wp-content/uploads/2021/06/2020_21-Islamic-Fintech-in-Malaysia-Reality-Outlook.pdf.

Shaller, A., Zamir, L., & Nojoumian, M. (2023). Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures. Information and Computation, 295(2), 105112. http://dx.doi.org/10.1016/j.ic.2023.105112.

Singamaneni, K. K., & Muhammad, G. (2024). A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks. Ad Hoc Networks, 165, 103607. https://doi.org/10.1016/j.adhoc.2024.103607.

Toshiba. (2025). Quantum key distribution: The new age of secure communication, powered by quantum physics. https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html.

Zygelman, B. (2025). A first introduction to quantum computing and information. Undergraduate Topics in Computer Science. https://doi.org/10.1007/978-3-031-66425-0.