ورقة تحليلية

الأمن الاقتصادي الرقمي والحروب السيبرانية

اختراق منصة Binance: حين تتحول سرقة الأصول الرقمية إلى مسألة أمن اقتصادي

إعداد: د. عامر أبو هنية

ما الذي يتغير في الأمن الاقتصادي حين يستطيع فاعل يملك قدرات دولة، ويحتفظ بإنكار معقول، أن يضرب وسيطاً مالياً رقمياً لا يخضع لسيادة دولة بعينها، فيما تبقى أدوات التجميد والتتبع بيد شركات خاصة خارج المنطقة؟

مقدمة

خرجت من المحافظ الساخنة لأكبر منصة تداول عملات مشفرة أصول تقارب 6.36مليار دولار بحسب LabsTRM، و6.43 مليار بحسب Elliptic، عبر عشر شبكات ومعظمها في نحو 20دقيقة، أي أكثر من أربعة أضعاف اختراق Bybitفي فبراير 2025[1,2].وقد نسبت FBIالعملية إلى جهات «TraderTraitor»المرتبطة بكوريا الشمالية، وسبقتها TRMو Chainalysis [3,4] ، فالفاعل مرتبط بدولة وليس جهة غير حكومية، وإن نفت بيونغ يانغ ذلك رسمياً .[5]

وتشير الوقائع إلى أن الاختراق وقع على الأرجح في منظومة التوقيع لا في التشفير، إذ بدأت الرواية بحاسوب مهندس مخترَق، ولم تجد Binanceدليلاً على تسرّب مفتاح خاص [1,4,6].أما المجمَّد، وهو نحو 2.85مليار دولار أي 44% من المسروق، فعملات مستقرة في معظمه جمدتها جهات إصدارها، بينما بقي بيد المهاجم نحو 3.25مليار دولار من ETHو BTC وأصول أخرى لا يملك أحد تجميدها .[2]وقد احتُوي الأثر المباشر على المستخدمين بتعهد المنصة بالتغطية؛ أما الأثر الاستراتيجي، فيكمن في اعتماد المنطقة على منصات وجهات إصدار خارجية تملك وحدها قدرة التجميد والتتبع. وتعيد الورقة بناء الوقائع وتفصل بين أرقامها، ثم تختبر وصف «الحرب الاقتصادية» بمعايير معلنة، ثم تنقل النتائج إلى أدوات سياسة محددة لفلسطين والأردن والخليج.

1. مشكلة الورقة ومنهجيتها

كشف الحادث مفارقة. وقعت السرقة على منصة مركزية، ونجح التجميد لأن جزءاً كبيراً من الأموال كان في عملات مستقرة تصدرها شركات مركزية أيضاً. فقد جمد نحو 44% من المسروق، مقابل نحو 3% فقط في اختراق Bybit [7]. غير أن هذه القدرة لا تملكها دول المنطقة ولا جهاتها الرقابية؛ يملكها مصدرون خاصون يقررون متى يجمدون، وبطلب ممن. وفي المقابل بقي ما يزيد على 3 مليارات دولار من ETH وBTC خارج أي قدرة على التجميد.

لا تتعلق مشكلة الورقة إذن بتقدير الخسارة، فقد غطتها المنصة. تتعلق بما يعيد الحادث توزيعه: من يتحمل الخطر، ومن يملك أداة الرد، ومن يستفيد. فدولة معاقبة حصلت في ليلة واحدة على ما يعادل نحو سدس ناتجها المحلي [5]، ومصدرو العملات المستقرة مارسوا سلطة تشبه السلطة السيادية، والمنطقة العربية، ومنها فلسطين، تستخدم هذه البنية دون أن تملك مفاتيحها. وتتفرع عن السؤال المركزي ثلاثة أسئلة: ما الذي يمكن الجزم به من وقائع الحادث وأرقامه بعد خمسة أيام من وقوعه؟ وهل يصح وصفه بالحرب الاقتصادية، وبأي معيار؟ وما الذي يعنيه لفلسطين ومحيطها، وما الأدوات المتاحة لها؟

تعتمد الورقة تتبع العملية (process tracing) في حادث واحد، مع مثلثة المصادر. تقارن أرقام ثلاث شركات تحليل blockchain، هي TRM وElliptic وChainalysis، فيما بينها، ثم مع بيانات Binance وFBI والجهات الرقابية، ثم مع التغطية الصحفية الدولية. وحين تختلف الأرقام تعرضها الورقة كما هي مع مصدرها ووقت رصدها، ولا تختار بينها إلا لسبب معلن. والأوقات الواردة بتوقيت UTC، وتاريخ إغلاق البيانات 3 نوفمبر 2026.

ولتقييم وصف «الحرب الاقتصادية» تبني الورقة مصفوفة من خمسة معايير (القسم 6)، يقاس كل منها على سلم ثلاثي معرف مسبقاً، منخفض ومتوسط ومرتفع، لكل درجة مؤشر قابل للتحقق، حتى يمكن تطبيقها على حوادث لاحقة ومقارنة النتائج. أما السيناريوهات فتقديرات نوعية مشروطة بمؤشرات إنذار مبكر، وليست احتمالات إحصائية.

2. الإطار المفاهيمي

المدخل الأول هو فن الحكم الاقتصادي (economic statecraft). يعرف Baldwin الأدوات الاقتصادية بأنها وسائل تستعملها الدولة للتأثير في سلوك غيرها، ويميز بين غاية الأداة وأثرها [8]. وبهذا المعيار تكون الحرب الاقتصادية بالمعنى الصارم فعلاً مقصوداً لإضعاف قدرة خصم محدد. أما حين تكون الغاية جمع الإيراد ويأتي الضرر عابراً للحدود يصيب أطرافاً خارج النزاع، فالورقة تسميه «حرباً اقتصادية بالتبعية»: نشاط مالي لدولة معاقبة يعمل في الواقع على تقويض نظام العقوبات المفروض عليها.

المدخل الثاني يخص الفاعل. يصف Maurer علاقة الدول بالقراصنة بطيف يمتد من التفويض إلى التوجيه إلى الرعاية، ويجعل الإنكار المعقول جزءاً من وظيفة هذه العلاقة .[9] ويبين Buchanan كيف حولت كوريا الشمالية العمليات السيبرانية إلى مصدر دخل للدولة، من سرقة المصرف المركزي في بنغلادش عام 2016 إلى منصات العملات المشفرة .[10] وقال فريق خبراء الأمم المتحدة في تقريره الختامي إنه حقق في 58 هجوماً سيبرانياً مشتبهاً به بين 2017 و2023 بقيمة نحو 3 مليارات دولار .[11] فالفاعل هنا وحدة تابعة لدولة، تعمل بمنطق الإيراد وتحتفظ بالإنكار، وهي بذلك أبعد من الجهة غير الحكومية المستقلة وأقرب من الجيش النظامي.

المدخل الثالث هو الترابط المسلح (weaponized interdependence). يرى Farrell و Newman أن الشبكات المالية العالمية تتمركز حول عقد قليلة، وأن من يملك سلطة على هذه العقد يستطيع استخدامها بطريقتين: أثر المرصد (panopticon)، أي رؤية ما يمر عبر الشبكة، وأثر نقطة الاختناق (chokepoint)، أي منع المرور .[12] ويقدم الحادث تطبيقاً مباشراً للمفهوم في سوق الأصول الرقمية؛ فشركات التحليل أدت دور المرصد، ومصدرو العملات المستقرة أدوا دور نقطة الاختناق. والفارق عن الإطار الأصلي أن العقدة هنا شركة خاصة، تقرر التجميد بتقديرها وتحت ضغط سلطات إنفاذ القانون الأمريكية.

يجمع الإطار هذه المداخل في ثلاثة أطراف: فاعل بقدرات دولة يسعى إلى الإيراد، ووسيط مالي لا يخضع لسيادة دولة بعينها، وحراس بوابات خاصون يملكون الرؤية والمنع. ومن موقع هذه الأطراف تشتق الورقة سؤالها عمن يملك أداة الرد ومن يقع تحت أثرها. ولهذا السؤال وزن خاص في الحالة الفلسطينية، لأن أداة التجميد ذاتها استخدمت ضد فلسطينيين بطلب إسرائيلي القسم 8.

3. ما الذي حدث؟

في مساء 29 أكتوبر 2026 بدأت أصول تخرج من محافظ Binance، فعلّقت المنصة السحب وقدرت الأثر لاحقاً بنحو 6.3 مليار دولار. وأكد رئيسها التنفيذي المشارك ريتشارد تينغ أن المحفظة الساخنة للمنصة هي المتضررة، وأن معظم أصول المستخدمين في محافظ باردة .[6] وقد جاء التسلسل الزمني لعملية الاختراق والاستجابة الأمنية، بتوقيت UTC، على المراحل التالية:

مرحلة التحضير: وفقاً لتحليل شركة LabsTRM، سبقت عملية الاختراق مرحلة تحضيرية استمرت 36 ساعة على الأقل، استخدم خلالها المهاجمون مبالغ صغيرة من العملات الرقمية المحوّلة عبر خدمة Tornado Cash لتمويل المحفظة التي نُفذت منها العملية. كما أجروا اختبارات تقنية للشيفرة المستخدمة على محفظتين، قبل اختبارها على

محفظة ثالثة، للتأكد من فاعلية آلية الاختراق قبل بدء التنفيذ الفعلي .[1]ونشر المهاجم عقد «sweeper»عند الساعة 15:59من يوم الهجوم، أي قبل نحو أربع ساعات من التنفيذ .[2]

بداية الهجوم واستنزاف الأموال: بين الساعة 20:05و20:20، بدأت عمليات سحب غير مصرح بها من محافظ المنصة على عدد من شبكات البلوك تشين، شملت XRP Ledgerو Solana و Optimism. وتزامن ذلك مع تحويل نحو 18,270وحدة من عملة Bitcoin، جرى تقسيمها مباشرة على 19 عنواناً يحمل معظمها 1,000 وحدة، في محاولة لتشتيت حركة الأموال وتعقيد تتبع مساراتها [1، .[2

الضربة الرئيسية على شبكة :Ethereumعند الساعة 20:20، نفّذ المهاجمون معاملة تضمنت 50تفويضاً باستخدام آلية EIP-7702، نجح أحدها في تفعيل صلاحية استُخدمت للاستيلاء على أصول المحفظة الساخنة للمنصة على شبكة .Ethereumوخلال ثلاث دقائق و24 ثانية فقط، جرى سحب كامل رصيد المحفظة، الذي شمل 167,464 وحدة من Ethereum، و63 رمزاً رقمياً مختلفاً، إضافة إلى نحو 1.615مليار وحدة من العملة المستقرة USDT، وكانت أكبر تحويلة منفردة، عند 20:24، بقيمة 2.53مليار دولار .[2]ولم يتوقف الهجوم عند هذه المرحلة؛ إذ بقي التفويض الأمني المستغل فعالاً، ما أتاح للمهاجمين استنزاف الأموال الجديدة التي وصلت إلى المحفظة في عمليات إضافية امتدت من الساعة 20:41حتى 23:56، عددها ست بحسب TRMوأربع بحسب Elliptic [1,2].

الاستجابة واحتواء الأضرار: بدأت جهود احتواء الهجوم وتجميد الأصول الرقمية نحو الساعة 21:04؛ جمدت Tether محفظة فيها 1.18مليار USDTبعد 37دقيقة من وصول الأموال إليها، وتبعتها Circleبعد ثلاث دقائق بتجميد 823 مليون USDC[2]، ثم انضمت إليهما Rippleعند الساعة 22:01، وشركة World Liberty Financialعند الساعة 22:10. وفي اليوم التالي أعلنت Binance تخصيص أكثر من 6.34مليار دولار لتغطية الأضرار وحماية مصالح المستخدمين .[6] ونسبت شركة TRM Labsالهجوم، بدرجة ثقة عالية وفق تقييمها، إلى مجموعة .TraderTraitor وفي 31أكتوبر أعلن مكتب التحقيقات الفيدرالي الأمريكي (FBI)مسؤوليّة جهات مرتبطة بمجموعة TraderTraitor، التي تربطها السلطات الأمريكية بكوريا الشمالية، ونشر قائمة بالعناوين التي تحتفظ بالأموال المسروقة .[3]وفي 1 نوفمبر بدأت المنصة إعادة فتح عمليات السحب بصورة تدريجية بدءاً بالبيتكوين، ثم العملات التقليدية في 2 نوفمبر[3,13]، وفي 3نوفمبر نفت كوريا الشمالية، على لسان كيم يو جونغ، أي صلة بالعملية ووصفت الاتهام الأمريكي باستفزاز سياسي [5].

4. القراءة التقنية

- **المسار الأرجح.** قالت Binanceإن التحقيق الأولي يشير إلى حاسوب مهندس DevOpsمخترَق، ثم أعلنت عن «نقاط اختراق إضافية»، ونفت وجود دليل على تسرّب مفتاح خاص لأي محفظة [4، .[6ووصف تينغ الهجوم بأنه معقّد ويتضمن برمجية خبيثة صُممت لإتلاف الأدلة، ولم ينفذه شخص واحد .[6]وفي تحديث لاحق قال إن التفويض عبر EIP-7702منح المهاجم صلاحية التنفيذ على المحفظة الساخنة دون أن يمر بضوابط الموافقة المعتادة، وإن المنصة تعيد بناء بنية السحب بالكامل وتراجع أمن الأجهزة والسحابة وإدارة المفاتيح وأنظمة التوقيع [6].
- **ما لا تفسّره .EIP-7702**هذه الآلية، التي دخلت Ethereumمع ترقية Pectraفي مايو 2025، تتيح لمحفظة أن تفوّض عقداً ذكياً بالتصرف باسمها؛ وقد حوّل بها المهاجم محفظة Binance 14إلى «sweeper»لا يقبل إلا أوامره .[1]غير أنها تفسّر Ethereumوحدها؛ ففي بقية الشبكات (XRP Ledgerو Arbitrumو Avalancheو Optimismو Baseو Bitcoinو Tronو Solana) خرجت الأموال بتحويلات موقّعة عادية دون تفويض. لذلك ترجّح TRMأن المهاجم تحكّم بمنظومة التوقيع في Binanceنفسها، فوقّعت ما اختاره عبر الشبكات .[1] ويتسق ذلك مع قول رئيس Blockaidإن المهاجمين وصلوا غالباً عبر حاسوب مطوّر إلى بنية التوقيع، وإن الموقِّع «وقّع معاملة ما كان ينبغي أن يوقّعها»، وإن EIP-7702ربما سرّعت الاستنزاف دون أن تكون سببه .[14]ولم تنشر Binanceسبباً جذرياً بعد. ويعني ذلك أن نفي تسرّب المفتاح لا يناقض الاختراق: يكفي أن تُخترق الجهة التي تستخدم المفاتيح ليُوقَّع ما لا ينبغي توقيعه. ويبقى بين الروايتين فرق يستحق المتابعة: تصف Binanceثغرة في مسار الموافقات، وتصف TRMسيطرة على منظومة التوقيع نفسها، والتقرير الفني الموعود هو ما يحسم ذلك.
- **الغسل والتتبع.** تختلف العملية عن Bybitفي أن الغسل لا يعتمد على الجسور بقدر اعتماده على صنّاع السوق وعقود مبنية على النوايا ومنصات الإقراض (Aaveو JustLend)، وتتوقع TRMانتقالاً لاحقاً إلى الجسور وخدمات المبادلة ووسطاء .[1] OTCوتتوقع FBIتحويل الأصول إلى ETHثم غسلها عبر التمويل اللامركزي وخدمات المبادلة الفورية، وقد دعت القطاع الخاص إلى حظر المعاملات المرتبطة بعناوين الغسل .[3]وقالت Chainalysisإنها ترصد أنماط غسل «لم تُشاهد من قبل»، تتسم بالسرعة والتكرار الآلي .[15]وبحسب Elliptic، حوّل المهاجم نحو 786مليون دولار من العملات المستقرة إلى ETHو TRXقبل التجميد، منها 434مليون USDT مقابل 160,451 ETHبأسعار أسوأ من السوق بنسبة تتراوح بين 12%و26% .[2]وخلال أقل من أربعة أيام توزعت الأموال على نحو 12ألف محفظة في 11شبكة عبر أكثر من 40ألف معاملة، أي محفظة جديدة كل

25ثانية تقريباً، واختلط جزء منها، نحو 16مليون دولار، بعائدات اختراق Bitgetفي سبتمبر؛ ولم يرصد حتى 2 نوفمبر تسييل يذكر[7] .

- **نقاط الفشل المرشحة بتقديري.** تركّز سيولة ضخمة في محافظ ساخنة قليلة؛ منظومة توقيع مركزية واحدة تخدم عشر شبكات؛ غياب سقوف ومهلات تلقائية للسحب الكبير؛ بقاء التفويض فعّالاً في عدة عمليات بعد الاستنزاف الأول، ما يعني أن كشفه وإبطاله لم يكونا فوريين.

5. المسروق والمجمَّد والمتبقي

يخلط التناول الإعلامي بين هذه المفاهيم؛ والفصل بينها جوهري لأي تقدير للأثر:

المسروق. تتراوح التقديرات بين نحو 6.3مليار دولار عند Binance، و6.36 مليار عند TRM، و6.43 مليار عند Elliptic، وأكثر من 6مليارات عند FBI[4، 1، 2، .[3ويعود الفرق إلى ما يدخل في الحساب، إذ استبعدت Elliptic نحو 169مليون دولار خرجت بعد تعليق السحب وتبدو أموالاً تخص Binanceنفسها، وإلى أن القيمة تُحسب بسعر كل أصل وقت سحبه، وتبلغ نحو 6.23مليار بأسعار 30أكتوبر بحسب [1,2] TRM .

المجمَّد. نحو 2.85مليار دولار، أي 44%من المسروق، بحسب ما تحققت منه Ellipticحتى 1نوفمبر، 94%منه عملات مستقرة؛ وتقدره Binanceبنحو 3مليارات . وكانت TRMقد رصدت في الساعات الأولى نحو 2.7مليار دولار، منها نحو 1.77مليار عند Tetherونحو 825مليوناً عند Circleو40.5 مليون RLUSDعند Rippleو27.8 مليون USD1عند WLFIونحو 30مليوناً على .[1] Arbitrumوالتجميد منع المهاجم من التصرف بالأموال، وهو لا يعني استردادها؛ فإعادتها تتطلب إتلاف الرموز المجمدة وإعادة إصدارها لصاحبها بعد إثبات الملكية، وقد تحتاج أوامر قضائية في أكثر من ولاية قضائية [16].

ما بقي بيد المهاجم. نحو 3.25مليار دولار موزعة على أكثر من 800عنوان، منها نحو 584ألف ETHو18,327 BTCو233 مليون XRP، بحسب Ellipticفي 1نوفمبر .[2]وكان تقدير TRMالأول، في 30أكتوبر الساعة 00:30، نحو 2.4مليار دولار .[1]ويعكس ارتفاع الرقم تحويل المهاجم ما بيده من رموز إلى ETH، كما أفادت FBI[3]، فالرقم متغيّر.

ما بيع قبل التجميد. باع المهاجم في الساعات الأولى نحو 325مليون USDTلصنّاع سوق مقابل نحو 122,300 ETHبخصم يتجاوز 10%[1]، وارتفع الرقم في حصر Ellipticاللاحق إلى 434مليون USDTمقابل 160,451

ETH، واقترض 19,762 ETHمن Aaveمقابل 59.9مليون .[2] USDTأي أنه سابق قرارات التجميد، وقبل خسارة تصل إلى ربع القيمة، ليحوّل جزءاً من الأموال إلى أصول لا تُجمَّد.

ما تغطيه .Binanceحجزت المنصة أكثر من 6.34مليار دولار، كان نحو 5مليارات منها محفوظاً أصلاً في الرموز المتضررة USDT)وUSDC وBTC وETH وBNB)، واشترت الباقي عبر السوق ووسطاء .[6] OTCوقالت في 31 أكتوبر إنها استبدلت نحو 90%من المبلغ والباقي في رموز أقل سيولة، ثم ارتفعت النسبة إلى نحو 95%[17، 13]، بتمويل من جزء من صندوق SAFU(نحو مليار دولار بالبيتكوين) وجزء من صندوق تأمين العقود الآجلة وخزينة الشركة .[17]وهذه التزام من المنصة تجاه مستخدميها وليست استرداداً للأموال المسروقة.

الفجوة المالية. التزام Binanceتجاه مستخدميها هو كامل المبلغ، أياً كان حجم ما جُمد. فالتجميد لا يخفض الكلفة على المنصة إلا إذا أعاد المصدرون إصدار الرموز المجمدة لصالحها، وهو مسار قانوني قد يطول. لذلك تقارب الكلفة الفورية على خزينة Binanceكامل المبلغ، وتنخفض لاحقاً بقدر ما يعاد إصداره من 2.85مليار مجمدة، ولا ينتظر استرداد يذكر من 3.25مليار بقيت بيد المهاجم. والمقياس الأدق لقدرة المنصة هو اختبار السحب: بلغ صافي السحب 4.72مليار دولار حتى 2نوفمبر، أي نحو 3%من أصول المنصة، وسُحب في أول 9.5ساعة بعد الاستئناف 4.65مليار مقابل إيداع 1.01مليار [5]، .[13وهو ضغط ملموس، لكنه لم يبلغ حد الهلع.

السوق. انزلق Bitcoinإلى نحو 77,400 دولار بعد أن اقترب من 76ألفاً، في أدنى مستوى منذ نحو خمسة أسابيع، وخسر BNBنحو 5%، وصُفّيت مراكز شراء بما بين 1.3 و1.5 مليار دولار خلال 24ساعة [18]، .[19وامتد الأثر إلى أسهم القطاع، فهبط سهم Coinbaseنحو 11%وسهم Circleنحو .[20] 9%لكن ذلك تزامن مع هبوط عقود Nasdaq 100بنسبة 2.4%وانتهاء خيارات بنحو 11مليار دولار على Deribit، فلا يُعزى التراجع إلى الحادث وحده .[18]ويرى Geoff Kendrickمن Standard Charteredأن الهبوط لم يكتمل، وأن الحادث قد يسرع انتقال التداول من المنصات المركزية إلى المنصات اللامركزية .[19]ولم ترد في المصادر المراجعة إشارة إلى تعثّر منصات أخرى حتى 3نوفمبر.

6. هل هي حرب اقتصادية؟

تقترح الورقة خمسة معايير قابلة لإعادة الاستخدام على حوادث مقبلة، ويعرض الجدول 1تعريف كل درجة ونتيجة الحادث:

الجدول :1مصفوفة تقييم الحادث بمعايير الحرب الاقتصادية

المعيار	منخفض	متوسط	مرتفع	نتيجة الحادث
الدافع	انتهازي أو فردي	مالي لجهة منظمة	مالي أو سياسي يخدم دولة أو برنامجها	مرتفع: تمويل دولة معاقبة
الارتباط بدولة	لا توجد نسبة	نسبة من شركات تحليل	نسبة رسمية من جهة حكومية	مرتفع، مع نفي رسمي وتحفظ سياسي
العبور للحدود	شبكة وجهة إصدار واحدة	عدة شبكات	عدة شبكات وجهات إصدار وولايات قضائية	مرتفع: عشر شبكات وخمس جهات إصدار
الوظائف الحرجة	لا انقطاع في الخدمة	تعليق مؤقت لخدمة كبرى	توقف نظامي أو عدوى	متوسط: تعليق السحب أكثر من يومين
قابلية التكرار	حادث منفرد	تشابه جزئي مع سوابق	نمط موثق ومتكرر	مرتفع: Bybitو KelpDAO وBitget

الدافع. يرى خبراء أن كوريا الشمالية تلجأ إلى سرقة العملات الرقمية لتمويل اقتصادها وبرنامجها النووي في ظل العقوبات .[4]ويعطي الحجم هذا الدافع وزناً جديداً: تقدر Ellipticما سرقته كوريا الشمالية من العملات المشفرة في 2026بنحو 7.6مليار دولار، وهو الأعلى على الإطلاق، ويعادل اختراق Binanceوحده نحو سدس ناتجها المحلي لعام 2025الذي قدره بنك كوريا بنحو 35مليار دولار .[5]فالدافع مالي لا إضعاف Binanceبحد ذاتها، لكنه دافع دولة.

الارتباط بدولة. نسبت FBIالعملية إلى جهات مرتبطة بكوريا الشمالية، وسبقتها TRMبثقة عالية [1، .[3والارتباط هنا مرتفع، لكنه نسبة أمنية رسمية وليس حكماً قضائياً، وكانت Binanceقد امتنعت عن تأكيدها .[4]ونفت بيونغ يانغ المسؤولية [5]، وقال الرئيس الأمريكي إن التحقيق لم يصل إلى يقين نهائي .[21]فالدرجة مرتفعة تقنياً، ومحل تجاذب سياسي.

العبور للحدود. شملت العملية عشر شبكات وعدة جهات إصدار Tetherو Circleو Rippleو WLFIو First Digital[1، 19]، فالمعيار متحقق بدرجة مرتفعة.

الوظائف الحرجة. علّقت أكبر منصة تداول السحب أكثر من يومين ثم استأنفته على مراحل، وبلغ صافي السحب نحو 3%من أصولها .[5]فالأثر متوسط، ولم يُوثَّق توقف نظامي في النظام المالي.

قابلية التكرار. يتشابه الهجوم مع Bybitوهجوم KelpDAO(أبريل (2026في التمويل بسحوبات صغيرة من Tornado Cashوالتجهيز المسبق وتنفيذ تواقيع محضّرة دفعة واحدة [1]، وغسلت أمواله إلى جانب عائدات اختراق Bitgetفي سبتمبر .[2] 2026وتقدر Chainalysisأن كوريا الشمالية ارتبطت بنحو 89%من خسائر الاختراقات في 2026، مقابل 15%في 2021[5]، فاحتمال التكرار مرتفع.

يخلص الحادث، بمعايير الإطار المفاهيمي، إلى أنه أقرب إلى حرب اقتصادية بالتبعية، لم يُصمَّم لإضعاف خصم بعينه، لكنه يؤدي عملياً وظيفة التهرب من العقوبات وتمويل دولة معاقَبة، بآثار عابرة للحدود على أطراف خارج النزاع. أما وصفه بحرب اقتصادية بالمعنى الصارم فيحتاج دليلاً على قصد الإضرار بالنظام المالي للجهة المستهدفة، وهو غير متوفر. والقدرة على إحداث صدمة عابرة للحدود تخص هنا فاعلاً بقدرات دولة وإنكار معقول، لا جهة غير حكومية مستقلة؛ وعلى ذلك بنيت صياغة سؤال الورقة.

7. النتائج

أولاً: التجميد غيّر حصيلة السرقة. جمد نحو 44%من المسروق في هذا الحادث، مقابل نحو 3%في .[7] Bybit ويعود الفارق إلى تركيبة الأصول المسروقة أكثر مما يعود إلى تحسن الأمن، فقد شكلت العملات المستقرة 54%منها .[7]وكلما زادت حصة العملات المستقرة في الأصول المعرضة للخطر، زادت قدرة حراس البوابات على الحد من الخسارة.

ثانياً: سلطة التجميد تقديرية، ويحكمها حجم الحادث. قالت Circleفي أبريل إنها لا تجمد USDCإلا بأمر من جهة إنفاذ أو محكمة، ولم تجمد الأموال المسروقة في اختراق Driftالبالغ نحو 290مليون دولار، ثم جمدت 823مليون USDCفي هذا الحادث خلال دقائق [16، .[2ويقرأ بعض المختصين ذلك قراراً تجارياً فرضه حجم السرقة، ويطالب آخرون بمعايير قانونية موحدة تمنح الضحايا الصغار الاستجابة نفسها .[16]وهذا هو أثر نقطة الاختناق في إطار Farrellو Newman، وصاحب القرار فيه شركة .[12]

ثالثاً: يقبل المهاجم دفع ثمن الإفلات من التجميد. حوّل قبل التجميد نحو 786مليون دولار بخسارة بين 12%و26%، ثم وزع الأموال آلياً على آلاف المحافظ [2، .[7فالتجميد يرفع كلفة السرقة ولا يمنعها، والميزة لمن يتحرك في الدقائق الأولى. وقد جاء أول تجميد بعد 37دقيقة من وصول الأموال [2]، وكانت هذه المهلة كافية لتسرب ما يقارب 800 مليون دولار.

رابعاً: اجتازت المنصة اختبار السيولة، والخطر في التركز. غطت Binanceالخسارة من مواردها، واستوعبت صافي سحب بنحو 4.7مليار دولار دون تعثر [5]، ولم يظهر أثر نظامي. لكن قدرة منصة واحدة على امتصاص صدمة بحجم 6مليارات دولار دليل على حجم التركز نفسه؛ فالمنصة التي تحتمل الصدمة هي المنصة التي يعني تعثرها أكبر الضرر. ويرى Daniel Tunkelمن Edwin Coeأن على الجهات الرقابية أن تختبر قدرة المنصات على امتصاص اختراق كبير، إلى جانب الوقاية منه .[22]

خامساً: نقطة الضعف تشغيلية. لم يتسرب مفتاح خاص، واستغل المهاجم مسار الموافقات وبنية التوقيع عبر جهاز مهندس [6، .[14والعلاج المقترح، من فصل صلاحيات التوقيع وسلاسل الموافقة وسقوف السحب، أدوات تستخدمها المصارف منذ عقود .[22]فالحادث مسألة حوكمة تشغيلية قابلة للتنظيم، وهذا ما يجعل التوصيات أدناه ممكنة التطبيق.

8. الانعكاسات على المنطقة العربية وفلسطين

هناك بيان واحد موثق في المنطقة العربية حتى 3نوفمبر؛ إذ أعلنت هيئة تنظيم الخدمات المالية (FSRA)في سوق أبوظبي العالمي، في 30أكتوبر، أنها على علم بالحادث وتتواصل بشكل وثيق مع Binanceوتتابعه .[23]ولهذا البيان سياق: فالهيئة هي المرخص الرئيسي للمنصة منذ حصولها على ترخيص عالمي من سوق أبوظبي العالمي في ديسمبر 2025[24]، وصندوق MGXفي أبوظبي يملك حصة في Binanceمنذ استثماره ملياري دولار فيها عام 2025، دُفعت بعملة USD1التي تصدرها WLFI[25]، وهي إحدى الجهات التي جمدت أموالاً في هذا الحادث. ولم أجد في المصادر المراجعة مواقف منشورة لجهات رقابية في بقية الدول. وما يلي تحليل مخاطر فقط:

- **السيادة المالية:** العملات المستقرة قناة التحويل العابر للحدود، ويملك قرار تجميدها مُصدِرون خاصون خارج الإقليم يقررون بتقديرهم، كما بينت النتيجة الثانية. والوجه الآخر أن نحو 3.25مليار دولار من ETHوBTC وغيرها بقيت خارج أي قدرة على التجميد.
- **الغسل:** قد تمر أموال مسروقة عبر وسطاء OTCوأسواق تداول مباشر (peer-to-peer)في مصر والعراق ولبنان وغيرها، حيث الإنفاذ التنظيمي أضعف. ويرجح Tom Robinsonمن Ellipticأن جزءاً من الأموال بلغ شبكات غسل صينية استخدمتها كوريا الشمالية سابقاً [3]، وهي شبكات تنشط في أسواق المنطقة. ولم يوثق حتى الآن مرور أموال هذا الحادث تحديداً عبر المنطقة.

- **دول الخليج:** مراكز مالية ترخص المنصات العابرة للحدود وتستثمر فيها في آن، فأبوظبي مرخص Binance الرئيسي وأحد مساهميها. والخطر المشترك هو التركّز على منصات قليلة، وغياب قنوات إنذار مشتركة، واحتمال تعارض دور الرقيب ودور المستثمر عند وقوع حادث.

- **الأردن:** دخل قانون تنظيم التعامل بالأصول الافتراضية رقم 14لسنة 2025حيز النفاذ في 14سبتمبر 2025، وهو يلزم المزودين بفصل أموال العملاء ويحميها من دائني المزود، ويفرض مدققاً تقنياً خارجياً لأنظمة الحفظ [26، .[27ولم تصدر تعليماته التنفيذية بصيغتها النهائية بعد، وهي المكان المناسب لإدخال دروس الحادث: سقوف المحافظ الساخنة، وفصل صلاحيات التوقيع، ومهل الإبلاغ عن الحوادث.

- **فلسطين:** القيود المصرفية ومحدودية الوصول إلى الأدوات التقليدية تزيد الاعتماد على وسائط رقمية عابرة للحدود، فيتعرض الأفراد والمؤسسات الصغيرة لخسارة أو تجميد بلا سبل انتصاف. والتجميد هنا سابقة موثقة. فقد صادرت السلطات الإسرائيلية منذ 2021نحو 189حساباً على Binance، بينها 80حساباً لثلاث شركات صرافة في غزة بأمر من المكتب الوطني لمكافحة تمويل الإرهاب (NBCTF)في 2023[28]، وأمرت في العام نفسه بمصادرة 26 محفظة على شبكة Tronبقيمة نحو 93.7مليون دولار معظمها عملات مستقرة .[29]وفي 2024نفى تينغ ادعاءات بتجميد أموال كل المستخدمين الفلسطينيين، وقال إن الحظر طال عدداً محدوداً من الحسابات .[30] فأداة التجميد التي حدت من خسارة Binanceهي ذاتها الأداة التي استخدمت في الضغط على قنوات المال الفلسطينية، وقرارها في الحالتين خارج يد المؤسسات الفلسطينية. ولم أتحقق من موقف رسمي فلسطيني تجاه الحادث؛ ويقتضي الأمر جرداً وطنياً لمدى استخدام الأصول الرقمية قبل صياغة سياسة.

9. السيناريوهات

الاحتمالات هي تقديرات نوعية مبنية على السوابق المذكورة، وليست حسابات إحصائية.

السيناريو الاحتوائي. تنجح Binanceفي استعادة الثقة. المؤشر المبكر نشر إثبات احتياطيات كامل واستقرار صافي السحب، وهو الأرجح لأن السحب استؤنف والتغطية تجاوزت 90%، وتوقف صافي السحب عند نحو 3%من الأصول [17، .[5والاستجابة المناسبة شروط ترخيص أشد وإبلاغ إلزامي عن الحوادث.

السيناريو التصعيدي. تتكرر اختراقات كبرى في منصات أخرى، المؤشر اختراق منصة كبرى جديدة بالأسلوب نفسه، واحتماله متوسط إلى مرتفع لأن TRMترى النمط متكرراً [1]، ولأن Bitgetتعرضت لهجوم مشابه قبل شهر [2]،

وبلغت خسائر الاختراقات في الربع الثالث من 2026نحو 1.28مليار دولار، بزيادة نحو 56%عن الربع السابق بحسب CertiK [22].والاستجابة تبادل مؤشرات التهديد إقليمياً ومراقبة تفويضات الحسابات.

السيناريو النظامي. تنتقل المخاطر إلى مؤسسات وأسواق أخرى. المؤشر سحب مؤسسي وضغط سيولة على منصات أخرى، واحتماله منخفض إذ لا مؤشر عليه حالياً، وقد استوعبت Binanceصافي السحب دون تعثر. والاستجابة اختبارات إجهاد وسقوف انكشاف عبر العملات المستقرة.

السيناريو الجيوسياسي. يتواصل غسل الأموال وتخفيف أثر التجميد بوصفه مصدر تمويل لدولة معاقَبة. المؤشر استمرار الغسل الآلي، واحتماله مرتفع لأن الدافع موثق والغسل مستمر، وما زال نحو 3.25مليار دولار بيد المهاجم [2، 7].وقد يتحول الحادث إلى ورقة في أي مسار تفاوضي بين واشنطن وبيونغ يانغ، بعد نفي الثانية وتحفظ الرئيس الأمريكي العلني [5، 21].والاستجابة رقابة على نقاط الدخول والخروج وتنسيق دولي.

10. التوصيات

- **لسلطة النقد الفلسطينية وهيئة سوق رأس المال:** مسح وطني خلال ستة أشهر، بالتعاون مع الجهاز المركزي للإحصاء، يقيس حيازات الأصول الرقمية لدى الأفراد وشركات الصرافة والتحويل، والمنصات المستخدمة، وقنوات الدخول والخروج؛ ثم تعليمات تلزم شركات الصرافة المرخصة بالإفصاح عن تعاملها بالعملات المستقرة، حتى يقوم أي تنظيم لاحق على أرقام لا على افتراضات.
- **للجهات الرقابية في الأردن والإمارات:** أن تتضمن التعليمات التنفيذية الأردنية، قبل إقرارها، سقفاً لنسبة الأصول في المحافظ الساخنة، وتوقيعاً متعدد الأطراف بفصل فعلي للصلاحيات، ومهلة إلزامية للإبلاغ عن الحوادث تقاس بالساعات؛ وأن تنشر FSRA، بصفتها المرخص الرئيسي لـBinance، تقييماً علنياً للحادث ولنتائج إثبات الاحتياطيات، وأن تفصل حوكمياً بين دور الرقيب ودور المستثمر في المنصات التي تملك فيها أبوظبي حصصاً.
- **لوحدة المتابعة المالية الفلسطينية ومراكز الأمن السيبراني:** قدرة تتبع blockchainعبر شراكة مع شركة تحليل أو عبر مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (MENAFATF)، وإدراج العناوين التي نشرتها FBIفي قوائم الفحص لدى شركات الصرافة فوراً، وقناة اتصال مسبقة مع Tetherو Circle لطلبات التجميد، حتى لا تبقى هذه القناة حكراً على جهات خارجية تستخدمها ضد الفلسطينيين.

- **للمصارف وشركات الصرافة والتكنولوجيا المالية في فلسطين والأردن:** فحص المعاملات الواردة من العناوين المرتبطة بالحادث، ووضع حدود لانكشاف العملاء على منصة واحدة، وتوعيتهم بأن العملة المستقرة قابلة للتجميد من مصدرها، وأن الحيازة على منصة لا تعني ملكية مباشرة، وخطط استمرارية لانقطاع السحب.
- **على المستوى العربي:** أن يتبنى مجلس محافظي المصارف المركزية العربية، عبر أمانته في صندوق النقد العربي، قناة إنذار مبكر مشتركة لحوادث الأصول الرقمية، وتصنيفاً إقليمياً موحداً للمنصات الكبرى بوصفها بنية تحتية حرجة، ومعايير موحدة لطلبات التجميد ترفع الموقف التفاوضي العربي أمام المصدرين الخاصين.
- **للمستثمرين:** عدم ترك مبالغ كبيرة على المنصات، والحفظ المستقل بتوقيع متعدد، وتوزيع العملات المستقرة على أكثر من جهة، والحذر من رسائل «استرداد الأموال» الاحتيالية التي تعقب الحوادث الكبرى.

11. حدود الورقة وما يُنتظر

تقوم الورقة على تقارير شركات التحليل وتغطيات صحفية دولية وبيانات جهات رسمية، وهي لا تدّعي كشفاً جنائياً. لم تنشر Binance تقريرها الفني النهائي حتى الآن، وأرقام شركات التحليل تعود إلى الفترة بين 30 أكتوبر و2 نوفمبر وهي قابلة للتعديل. والإطار المفاهيمي مستمد من أدبيات سابقة للحادث، أما ما كتب بعده فتحليلات مهنية وصحفية لا دراسات محكمة، بحكم قصر المدة. تُحدَّث الورقة عند صدور التقرير الفني، ونتائج إثبات الاحتياطيات، وحجم ما يعاد إصداره من الأموال المجمدة، ومواقف الجهات الرقابية العربية.

المراجع

[1] TRM Team. (2026, October 29). North Korea steals USD 6.36 billion from Binance in the largest hack in history. TRM Labs. https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history

[2] Elliptic. (2026, November 1). The largest theft in history: North Korea likely behind the $6.4 billion Binance hack. https://www.elliptic.co/insights/binance-largest-hack-in-history/

[3] Nextgov/FCW. (2026, October 30). FBI is involved in response to $6.3 billion Binance hack linked to North Korea. https://www.nextgov.com/cybersecurity/2026/10/fbi-involved-response-63-billion-binance-hack-linked-north-korea/416946/

[4] Associated Press. (2026, October 30). North Korea linked to $6.3 billion hack on Binance, blockchain intelligence firms say. Hawaii News Now. https://www.hawaiinewsnow.com/2026/10/30/north-korea-linked-63-billion-hack-binance-blockchain-intelligence-firms-say/

[5] Reuters. (2026, November 3). North Korea rejects US allegation over Binance crypto heist. Investing.com. https://www.investing.com/news/economy-news/north-korea-rejects-us-allegation-overbinance-crypto-heist-4993595

[6] Bitcoin.com News. (2026, October 30). New breach points: Binance CEO reveals fresh findings in $6.3B hack. https://news.bitcoin.com/security/new-breach-points-binance-ceo-reveals-fresh-findings-6-3b-hack/

[7] Yahoo Finance. (2026, November 2). North Korea is laundering Binance hack loot at one new wallet every 25 seconds. https://finance.yahoo.com/markets/crypto/articles/north-korea-laundering-binance-hack-184603378.html

[8] Baldwin, D. A. (1985). Economic statecraft. Princeton University Press.

[9] Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.

[10] Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.

[11] United Nations Security Council. (2024). Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023) (S/2024/215).

[12] Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79.

[13] Ynetnews. (2026, November 3). Binance users withdraw $5B after North Korean hackers steal $6.3B in record crypto heist. https://www.ynetnews.com/business/article/rjljuu8pzl

[14] Cointelegraph. (2026, October 30). EIP-7702 didn’t cause Binance hack, but may have amplified losses. https://cointelegraph.com/news/binance-hack-security-ethereum-eip-7702-role

[15] CryptoSlate. (2026, October 30). Binance hackers deploy never-seen-before laundering tactics to conceal $6.3 billion theft. https://cryptoslate.com/binance-hackers-deploy-never-seen-before-laundering-tactics-to-conceal-6-3-billion-theft/

[16] CoinDesk. (2026, October 30). Crypto experts question double standard after issuers freeze billions in Binance hack. https://www.coindesk.com/business/2026/10/30/experts-divided-over-binance-hack-asset-freezes-warn-recovery-is-another-matter

[17] Guardian staff. (2026, November 1). Binance says 90% of losses from $6.3bn hack covered as FBI says North Korea behind attack. The Irish Times. https://www.irishtimes.com/world/2026/11/01/binance-says-90-of-losses-from-63bn-hack-covered-as-fbi-says-north-korea-behind-attack/

[18] Nairametrics. (2026, October 30). Bitcoin drops below $77,000 as $6 billion Binance hack rattles crypto market. https://nairametrics.com/2026/10/30/bitcoin-drops-below-77000-as-6-billion-binance-hack-rattles-crypto-market/

[19] CoinDesk. (2026, October 30). $6B Binance hack sends bitcoin, ether tumbling; Standard Chartered sees more losses ahead. https://www.coindesk.com/markets/2026/10/30/usd6-billion-binance-hack-sends-bitcoin-ether-tumbling-standard-chartered-sees-more-losses-ahead

[20] 24/7 Wall St. (2026, October 30). Coinbase tumbles 11% as record Binance hack hits crypto and trading revenue slides. https://247wallst.com/investing/2026/10/30/coinbase-tumbles-11-as-record-binance-hack-hits-crypto-and-trading-revenue-slides-strategy-sinks-12-robinhood-plunges-10-circle-drops-9/

[21] نوفمبر). ترامب يشكك باتهام كوريا الشمالية في اختراق بينانس. https://mustaqila.com/ترامب-يشكك-باتهام-كوريا-الشمالية-في-اخ/ (2026، 1مستقلة.

[22] CoinDesk. (2026, November 2). Crypto vs. traditional banks: What Binance’s $6.3B hack reveals about vulnerability. https://www.coindesk.com/business/2026/11/02/why-crypto-exchange-hacks-can-be-harder-to-contain-versus-global-banks

[23] Maniyeri, P. (2026, October 30). UAE's FSRA issues statement after Binance reports $6.3-billion security breach. Khaleej Times. https://www.khaleejtimes.com/business/uae-fsra-statement-binance-63-billion-security-breach

[24] Gulf News. (2025, December 7). Binance secures global exchange licence from Abu Dhabi financial regulator. https://gulfnews.com/your-money/cryptocurrency/binance-secures-global-exchange-licence-from-abu-dhabi-financial-regulator-1.500372508

[25] Bloomberg. (2025, May 1). Trump-tied stablecoin used for MGX's $2 billion Binance deal. https://www.bloomberg.com/news/articles/2025-05-01/trump-linked-stablecoin-used-for-mgx-s-2-billion-binance-deal

[26] المملكة الأردنية الهاشمية. (2025). قانون تنظيم التعامل بالأصول الافتراضية رقم 14 لسنة 2025. الجريدة الرسمية، 16 يونيو 2025. هيئة الأوراق المالية: https://www.jsc.gov.jo

[27] Al Tamimi & Company. (2026). القانون رقم 14 لسنة 2025: تدخل الأردن في العملات المشفرة. Eyes on 2026. https://www.tamimi.com/our-knowledge/publications/eyes-on-2026/

[28] Finance Magnates. (2023, May 5). Israel seized 189 Binance accounts linked to terror groups [citing Reuters]. https://www.financemagnates.com/cryptocurrency/israel-seized-189-binance-accounts-linked-to-terror-groups/

[29] Elliptic. (2023, August 2). Israel orders seizure of crypto wallets worth $94 million linked to Palestinian Islamic Jihad. https://www.elliptic.co/insights/israel-orders-seizure-of-crypto-wallets-worth-94-million-linked-to-palestinian-islamic-jihad/

[30] Bitcoinist. (2024, August 28). Binance CEO denies mass freezing Palestinian crypto assets. https://bitcoinist.com/binance-ceo-denies-allegations-of-mass-freezing-palestinian-crypto-assets/