التشفير بتقنية البلوك تشين ودوره في حماية المعاملات الإلكترونية

Blockchain encryption and its role in protecting electronic transactions

قادري نور الهدى*
مخبر المرافق العمومية والتنمية، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر
Inasse223@gmail.com

مكلكل بوزيان
مخبر المرافق العمومية والتنمية، جامعة جيلالي ليابس، سيدي بلعباس، الجزائر
mekelkelbouziane@yahoo.fr

- تاريخ الإرسال: 2022/09/28 - تاريخ القبول: 2022/12/22 - تاريخ النشر: 2022/12/27

الملخص: تعد تقنية البلوك تشين أحد أهم وأحدث ما توصلت إليه تكنولوجيات الإعلام والاتصال التي تلعب دورا بارزا في ضمان أمن وسلامة البيانات الخاصة بالمعاملات الإلكترونية من أي اختراق قد تطرأ عليها، وذلك بالنظر إلى اعتمادها على آلية التشفير الإلكتروني المعقد لها.

وعليه تهدف هذه الدراسة إلى تبيان دور التشفير بتقنية البلوك تشين في حماية المعاملات الإلكترونية من خلال توفير بنية تحتية آمنة لإبرام هذه الأخيرة، عن طريق تأمين البيانات والمعلومات في شكل كتل مشفرة يصعب اختراقها بما يضمن حمايتها وإثباتها أمام القضاء. وبالتالي فوجود التشفير يشكل مخرجا من كافة المشاكل الإلكترونية التي تعترض كافة التصرفات القانونية المبرمة بطريقة إلكترونية، مما يؤدي إلى توفير الأمن الإلكتروني لها.

الكلمات المفتاحية: التشفير الإلكتروني، البلوك تشين، حماية المعاملات الإلكترونية، الأمن المعلوماتي، الاختراق الإلكتروني.

Abstract: Blockchain technology is one of the most important and state-of-the-art media and communication technologies that play a prominent role in ensuring the security and integrity of data for electronic transactions from any breaches that may occur, given its reliance on the complex electronic encryption mechanism.

Accordingly, this study aims to demonstrate the role of encryption with blockchain technology in protecting electronic transactions by providing a secure infrastructure for the conclusion of the latter, by securing data and information in the form of encrypted blocks that are difficult to penetrate, ensuring their protection and proof before the judiciary. Electronic devices that interfere with all legal actions concluded ectronically, which leads to the provision of electronic security for them.

Keywords: Electronic encryption, blockchain, electronic transaction protection, information security; electronic hacking.

* المؤلف المرسل: قادري نور الهدى.

مقدمة:

يشهد العالم حاليا تطورات متلاحقة خاصة في مجال تبادل المعلومات عبر وسائل الاتصال الفوري، وظهور شبكة الأنترنت فتح أبوابا عالمية لتسهيل التبادلات التجارية، فقد ظهرت خلال السنوات الأخيرة تقنية جديدة في مجال إبرام المعاملات الإلكترونية تسمى بالبلوك تشين التي تعتبر أحد أهم التطورات التكنولوجية المعاصرة المرتبطة بالثورة الصناعية الرابعة في العالم الحديث.

تشكل تقنية البلوك تشين قفزة نوعية في مختلف الميادين التي ألقت بظلالها على مختلف المعاملات الإلكترونية، باعتبارها عبارة عن برنامج معلوماتي مشفر يتولى مهمة توثيق المعاملات والاحتفاظ بها جماعيا بدون تدخل جهات مركزية أو شخص أو هيئة محددة، بحيث تتيح هذه التقنية تتبع المعلومات عبر شبكة مغلقة وآمنة، باستخدام آلية التشفير الإلكتروني الذي يعد نتاج للمقتضيات الحفاظ والأمان للمعلومات الإلكترونية التي اقتضتها طبيعة التجارة الإلكترونية.

وتعد الإمارات أول دولة عربية تبادر باستخدام تكنولوجيا البلوك تشين، بحيث أطلقت إستراتيجية دبي للتعاملات الرقمية في أكتوبر 2016 عن استخدام تقنية البلوك تشين في تعاملات حكومة دبي المالية. وذلك بالنظر إلى الأمن المعلوماتي التي توفره هذه التقنية من كافة الاختراقات الإلكترونية بسبب اعتمادها على آلية التشفير الإلكتروني المعقد للمعاملات الإلكترونية.

وعليه تهدف هذه الدراسة إلى توضيح أهمية الدور التي يلعبه التشفير الإلكتروني عبر تقنية البلوك تشين في حماية المعاملات الإلكترونية، من خلال توفير بيئة آمنة يتم تسجيل التعاقدات في شكل سلسلة من الكتل يتم تشفيرها في سجل الإلكتروني على مستوى العالم، مما يؤدي إلى ضمان الأمن الإلكتروني للمعاملات المسجلة عبر منصة البلوك تشين.

وبالتالي تتمحور إشكالية الدراسة في أن النظام المعلوماتي لا يزال يكتنفه الغموض في نواح متعددة ولاسيما من الناحية القانونية بسبب تعدد استخدامات تقنيات الاتصال المستحدثة والمتنوعة خاصة من ناحية **إبراز مدى إسهام التشفير الإلكتروني عبر تقنية البلوك تشين في تجسيد الأمن المعلوماتي للمعاملات الإلكترونية.**

وللإجابة عن هاته الإشكالية المطروحة سيتم تقسيم الدراسة إلى المبحثين الآتين : **المبحث الأول** سنتناول كلا من مفهوم البلوك تشين والتشفير الإلكتروني، و**المبحث الثاني** فسيتم التطرق إلى دور التشفير الإلكتروني بتقنية البلوك تشين في حماية المعاملات الإلكترونية.

وسيتم إتباع المنهج التحليلي الوصفي من خلال تبيان مفهوم كلا من البلوك تشين والتشفير الإلكتروني وإبراز دورهما في حماية البيانات والمعلومات الخاصة بالمعاملات الإلكترونية.

المبحث الأول : ماهية تقنية البلوك تشين والتشفير الإلكتروني

تعد تقنية البلوك تشين (**Blockchain**) أو ما تسمى حديثا بالأنترنت التعاملات، من أحد أهم الحلول التكنولوجية المرتبطة بالثورة الصناعية الرابعة في العالم[1]، والتي تعتبر أسلوبا فريدا وآمنا لإجراء المعاملات الإلكترونية من خلال تسجيل البيانات في شكل سلسلة كتل يتم تشفيرها في سجل إلكتروني على مستوى العالم.

ونظرا لأهمية تقنية البلوك تشين التي تعد أساسا للتعاملات الإلكترونية المشفرة، فإنه كان لابد من التطرق إلى مفهوم هذه التقنية في (المطلب الأول) وإلى مفهوم التشفير الإلكتروني وذلك ضمن (المطلب الثاني).

المطلب الأول : مفهوم تقنية البلوك تشين (Blockchain)

لقد ظهرت التكنولوجيا الرقمية مع بداية إتفاقية البيتكوين عام 2009 وهي بروتوكول البيتكوين مفتوح المصدر[2]، وتعد تقنية البلوك تشين جيل جديد، وطريقة جديدة للحفاظ على البيانات والمعاملات الإلكترونية، نظرا لاعتمادها على آلية التشفير الإلكتروني المعقد لها.

لذلك كان لابد من التعرف على هذه التقنية. من خلال التطرق إل تعريفها في(الفرع الأول) وإلى أنواعها في(الفرع الثاني).

الفرع الأول : تعريف تقنية البلوك تشين وخصائصها

لقد تعددت التعريفات التي أعطيت لهذه التقنية، وذلك بالنظر للمميزات التي تتميز بها هذه التقنية وهو ما سوف نحاول التطرق إليه من خلال هذا الفرع :

[1] – مصطفى محمد الحسبان، النظام القانوني لتقنية البلوك تشين في ظل تشريعات التجارة الإلكترونية، مجلة الحقوق والعلوم الإنسانية، المجلد الثاني عشر، العدد 03، نوفمبر 2019، ص 134.

[2] – نجية معداوي ، العقود الذكية والبلوك تشين، مجلة المفكر للدراسات السياسية والقانونية، المجلد 04 ، العدد 02، جويلية، 2021 ص 60.

أولا : تعريف لتقنية البلوك تشين

عرفها البعض على أنها " قائمة رقمية من السجلات التي يتم فيها تسجيل المعاملات في كتل (Blocks) وترتبط بإستخدام التشفير وعندما تمتلئ الكتل بالبيانات، يتم ختمها زمنيا وإضافتها إلى سلسلة الكتل، بطريقة يمكن التحقق منها ولا يمكن تغييرها بدون توافق المشاركين."[3]

كما تعرف على أنه " برنامج معلوماتي مشفر يتولى مهمة سجل موحد للمعاملات على الشبكة فكل مجموعة من المعاملات مرتبطة بسلسلة ما، يمنح المشاركين صورة شاملة عن كل ما يحصل في المنظومة بأكملها . " [4]

وفي هذا الإطار عرف قانون ولاية واشنطن " **SB5638** " لعام 2019 " بأنها سجل مشفر آمن، متسلسل زمنيا ولا مركزي مبني على التوافق أو قاعدة بيانات توافقية محفوظة عبر الأنترنت أو شبكة الند للند أو أي وسيلة أخرى للتواصل مماثلة. " [5]

كما عرفها قانون ولاية إلينوي بشأن تقنية البلوك تشين الذي دخل حيز النفاذ في1 يناير 2020 " بأنها سجل إلكتروني تم إنشاؤه بواسطة استخدام طريقة لا مركزية من قبل أطراف متعددة، للتحقق من سجل رقمي للمعاملات وتخزينه، ويجرى تأمينه عن طريق استخدام الهاش الخاص بمعلومات المعاملة السابقة "[6].

ثانيا: خصائص تقنية البلوك تشين

ومن خلال التعاريف السابقة يستنتج أن تقنية البلوك تشين تتميز بمجموعة من الخصائص التي تتمثل فيما يلي :

- تتميز تقنية البلوك تشين بأنها دفتر للمعاملات لا مركزي[7]، لا تتحكم فيه جهة واحدة مركزية يتعين الرجوع إليها للوصول إلى محتوى الدفتر أو التفاعل معه، وإنما يتم حفظ نسخة من البيانات لدى

---

[3] -- هيثم السيد أحمد عيسى، نشأة العقود الذكية في عصر البلوك تشين، دار النهضة العربية للنشر والتوزيع، القاهرة، الطبعة الأولى، 2021، ص 15.

[4] – بيرغيت كلارك، سلسلة الكتل وقانون الملكية الفكرية، مجلة المنظمة العالمية للملكية الفكرية، فبراير 2018، المنشور على الرابط : http://www.wipo.into/wipo-magazine/ar/2018/01/article_0005.html.

تاريخ الإطلاع 2022/04/20 على الساعة 00:44

[5] – هيثم السيد أحمد عيسى، المرجع نفسه، ص 16.

[6] – مرجع نفسه، ص 16.

[7] – أنس محمد عبد الغفار سلامة، إثبات التعاقد عبر تقنية البلوك تشين، مجلة العلوم القانونية والإجتماعية، المجلد الخامس، العدد الثاني، جوان 2020، جامعة زيان عاشور الجلفة، ص 65.

المشتركين في شبكة البلوك تشين، وأي تعديل يحدث على هذه الأخيرة يضاف بشكل متزامن لدى الجميع، فليس هناك جهة واحدة تحتفظ بالبيانات[8].

- تقوم تقنية البلوك تشين على قاعدة الند للند أي يمكن لأعضاء الشبكة التفاعل فيما بينهم عن طريق إجراء المعاملات أو نقل القيم أو البيانات، بصورة مباشرة دون تدخل سلطة مركزية للقيام بذلك[9].

- تعد تقنية البلوك تشن على دفتر حسابات ثابت، بحيث إذا تم تسجيل البيانات داخل الكتلة وتم إضافتها فعلا إلى السلسلة بعد التحقق منها فإنه لا يمكن تغييرها، والسبب في ذلك هو اعتماد البلوك تشين على التشفير الذي هو عبارة عن خوارزميات تحول البيانات التي تم إدخالها في الكتلة، مهما كان حجمها، إلى مجموعة فريدة من الأرقام والحروف والرموز ذات طول ثابت يطلق عليها بالهاش. [10]

- إضافة إلى الخصائص السابقة، تتميز تقنية البلوك تشين في كون أنها عبارة عن مجموعة من الكتل المتسلسلة زمنيا، وهذا راجع إلى آلية التشفير الإلكتروني أو ما يطلق عليه بدالة التجزئة أو آلية الهاش Hash function التي تقوم عليها هذه الأخيرة، فهي عبارة عن خوارزميات تحول البيانات التي تم إدخالها في الكتلة مهما كان حجمها، إلى مجموعة فريدة من الأرقام والحروف والرموز ذات طول ثابت، بما يجعل الأمر اختراقها مستحيلا. [11]

الفرع الثاني : أنواع البلوك تشين

يعد البلوك تشين من أفضل الوسائل التقنية الآمنة لضمان سرية المعلومات والبيانات ومنع الغير من الإطلاع عليها في المعاملات الإلكترونية (كالعقود الإدارية الإلكترونية)، وفي الواقع هنالك العديد من النماذج المختلفة من البلوك تشين التي تختلف فيما بينها في درجة اللامركزية والوصول إليها:

أولا : البلوك تشين العامة والخاصة

تختلف تقنية البلوك تشين العامة عن تقنية البلوك تشين الخاصة من حيث أن هذه الأخيرة لا يستطيع أي شخص الوصول إليها بدون إذن من المسؤولين عنها[12]، إذ تعمل مع عدد من وكلاء محددين بوضوح ومعتمدين ومختارين مسبقا، وتجدر الإشارة أن سلسلة الكتل الخاصة تستخدم من طرف

---

[8] – هيثم السيد أحمد عيسى، المرجع السابق، ص 20.

[9] – هيثم السيد أحمد عيسى، المرجع السابق، ص 21.

[10] – مرجع نفسه، ص 23، 30.

[11] – https://tijaratuna.com/%D9%85%D9%8A%D8%B2%D8%A7%D8%AA تاريخ الإطلاع 2022/04/21، على الساعة 01:00.

[12] – هيثم السيد أحمد عيسى، المرجع السابق، ص 18.

الشركات والمؤسسات المصرفية لمشاركة قواعد البيانات داخليا من أجل تحسين سرعة التنفيذ وتقليل تكلفة معاملاتها، كما أنها تتميز عن البلوك تشين العامة أو ما تسمى بسلسلة الكتل العامة في أنها أكثر انسجاما مع مسائل المسؤولية القانونية والحوكمة نظرا لأنها تتم بطريقة مركزية وداخلية ومنظمة.[13]

عكس تقنية البلوك تشين العامة التي تمثل في كون أنها شبكة يمكن لأي شخص الوصول إليها والمشاركة فيها بدون إذن من أحد، فهي مفتوحة للجميع التي يمكنهم المشاركة في عملية التحقق والاعتماد أو المصادقة التي تجرى داخلها المعاملات أو البيانات الجديدة، إذ لا يتطلب الوصول إليها سوى الاتصال بالإنترنت، بالإضافة إلى تنزيل البرتوكول الكمبيوتر الذي يحدد قواعد التشغيل الشبكة المعنية[14]. ومن أمثلتها البتكوين بلوك تشين والإيثريوك بلوك تشين.

ثانيا : البلوك تشين الإتحادية

تعرف تقنية البلوك تشين الاتحادية على أنها شبكة تقوم بتشغيلها عدة جهات، كعدد من الشركات على سبيل المثال، وليست جهة واحدة تتضمن عدد من المشتركين في الشبكة كما هو الحال في البلوك تشين الخاصة، وتشارك كل جهة من تلك الجهات في عملية التحقق أو الاعتماد والمصادقة داخل الشبكة.[15]

وتجدر الإشارة أن الشبكة الاتحادية تتشابه مع الشبكة الخاصة في أنها أيضا ليست مفتوحة للجمهور وإنما الاشتراك فيها يحتاج إلى إذن من المسؤولين عنها. ومن أمثلتها شبكة " **EWF** " في مجال الطاقة وشبكة " **B3I** " في مجال التأمين. [16]

المطلب الثاني: مفهوم التشفير الإلكتروني بتقنية البلوك تشين

إن مفهوم التشفير بصفة عامة ليس حديثا فالكتابة المشفرة واستخدام الشيفرات في المراسلات موجودة منذ زمن طويل، إذ كانت تستعمل للأغراض العسكرية والإستخباراتية وغيرها من الأغراض التي كانت تقدرها الدول، بالنظر إلى أمن وسرية المعلومات المتبادلة.[17]

---

[13] – منصور داود، القيمة القانونية للبلوك تشين ودوره في نطاق التوثيق الرقمي للمعاملات الإلكترونية، مجلة الحقوق والعلوم الإنسانية، المجلد 14، العدد 02 . 2021، جامعة زيان عاشور، الجلفة، ص 285.

[14] – هيثم السيد احمد عيسى، المرجع السابق، ص 17.

[15] – مرجع نفسه، ص 18.

[16] – مرجع نفسه، ص 18.

[17] – موسى حسن فضالة، التنظيم القانوني للإثبات الإلكتروني – دراسة مقارنة – الطبعة الأولى، دار السنهوري، لبنان، 2016، ص 232.

و لتوضيح الدور الذي يلعبه التشفير الإلكتروني في ضمان الأمن المعلوماتي للمعاملات الإلكترونية خاصة في ظل انتشار الجرائم الماسة بسلامة وأمن هذه الأخيرة، فإنه سنتطرق إلى تعريفه في (الفرع الأول) وإلى أنواعه في (الفرع الثاني).

الفرع الأول: تعريف التشفير الإلكتروني

إن توثيق المعاملات الإلكترونية حفاظ على عدم تعرضها للتحريف أو التغيير، وحتى يكون لها درجات من الأمان والثقة في التعامل، ظهر التشفير كإجراء من إجراءات الأمان للحفاظ على المعلومات والبيانات الخاصة بمتعاملي البيئة الإلكتروني بصفة عامة. لذلك لقد اختلفت التعاريف التي أعطيت لهذا الأخير، سواء كان على مستوى الفقه القانوني أو على مستوى القانون. ونذكر أبرز هذه التعاريف ما يلي:

أولا: التعريف الفقهي للتشفير الإلكتروني

لقد اتجه الفقه إلى تعريف التشفير على أنه تحويل المعلومات إلى رموز وإشارات غير مفهومة لمنع الأشخاص غير المرخص لهم من الإطلاع عليها أو فهمها[18].

كما يعرفه البعض على أنه " عبارة عن تقنية تعتمد على المعادلات الرياضية التي تسمح لمن يمتلك مفتاحا سريا أن يحول الرسالة من رسالة مقروءة إلى رسالة غير مقروءة ". [19]

ويرى ليونال بوشرباغ LIONEL BOCHURNERG بأن التشفير الإلكتروني "مجموعة من التقنيات التي تهدف إلى حماية المعلومات، بفضل استعمال بروتوكولات سرية . تجعل البيانات مشفرة غير مفهومة لدى الغير، بواسطة البرامج المخصصة لذلك"[20].

ثانيا : التعريف القانوني للتشفير الإلكتروني

إن تشفير البيانات والمعلومات التي يتم التعامل بها من خلال وسائل الاتصال الحديثة خاصة في مجال المعاملات الإلكترونية التي تبرم وتنفذ عن بعد، تخضع إلى معايير قانونية نصت عليها بعض التشريعات المتعلقة بالمعاملات الإلكترونية.

---

[18] – آزد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني – دراسة مقارنة – الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2016، ص82.

[19] – موسى حسن فضالة، المرجع السابق ، ص 232.

[20] – يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، الطبعة الأولى، دار بلقيس للنشر، الجزائر، 2016، ص 186.

إذ عرف المشرع الفرنسي ضمن نص المادة 28 من القانون رقم 1170/90 المؤرخ في 1990/12/29 بشأن تنظيم الاتصالات عن بعد، أدوات التشفير بأنها " التقديمات التي تهدف إلى تحويل معلومات مقروءة إلى معلومات وإشارات غير قابلة للقراءة والفهم. " ولقد سمح هذا القانون للمشروعات الصغيرة، والأفراد باستخدام التشفير بعد أن كان قاصرا على المجالات العسكرية والحكومية فقط. [21]

و لقد أشار قانون الأونسترال بشأن التوقيعات الإلكترونية على أن التشفير الإلكتروني هو " فرع الرياضيات التطبيقية الذي يعني بتحويل الرسالة إلى أشكال تبدو غير مفهومة ثم إعادتها إلى أشكالها الأصلية. " [22]

كما عرف مشروع قانون التجارة الإلكتروني المصري التشفير الإلكتروني بأنه " تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من الإطلاع الغير عليها أو من تعديلها أو تغييرها ".[23]

ويتضح مما تقدم أن عملية التشفير تتألف من ثلاثة عناصر مترابطة مع بعضها البعض وهي :

- **المعلومات التي سيتم تشفيرها،** قد تكون رسالة نصية أو ملفات مهمة أو إشارات إلكترونية مشفرة ومنها في مجال التعاملات الإلكترونية، و التعاقد عن بعد، أو المفاوضات السرية التي تسبق التعاقد. [24]

- **خوارزمية التشفير** التي ستطبق على المعلومات وذلك لتحوليها إلى بيانات مهمة و**خوارزمية فك** التشفير التي تعيد هذه البيانات إلى حالتها الأصلية المفهومة. [25]

- **المفاتيح** وهي سلسلة أو أكثر من الرموز التي تستند إلى صيغ رياضية معقدة في شكل خوارزميات وتستخدم هذه المفاتيح في " تشفير " النصوص المرسلة وفك التشفير من قبل المرسل إليه المسموح له بتسليمها. [26]

---

[21] – محمد حسين عبد العليم، إثبات العقد الإداري الإلكتروني، دون طبعة، دار الجامعة للنشر، الإسكندرية، 2019 ص 249.

[22] – البند 32 من دليل الإشتراع قانون الأونسترال بشأن التوقيعات الإلكترونية، الصادر عن لحنة الأمم المتحدة للقانون التجاري الدولي لعام 2001.

[23] – المادة الأولى من مشروع قانون التجارة المصري لسنة 1999 .

[24] – محمد حسين عبد العليم، المرجع السابق، ص 253.

[25] – مرجع نفسه، ص 253

[26] – مرجع نفسه، ص 253

وعليه يمكن القول بأن عملية التشفير الإلكتروني ترتكز على عملية تحويل البيانات من حالتها الأصلية المقروءة إلى صيغة رقمية غير مفهومة للغير عن طريق الاستعانة ببرامج أو وسائل مخصصة لهذا الغرض، وذلك بهدف الحفاظ على سرية المعلومات وخصوصيتها.

الفرع الثاني: أنواع التشفير الإلكتروني

يسعى معظم الباحثين إلى الحصول لعدة طرق مختلفة للتشفير تتناسب مع حجم المعلومات حتى تكون أكثر فاعلية في حفظها، والوصول إليها بمستوى عالي من السرية والأمان، لذلك فإن طرق التشفير التي تستخدم في مجال تقنيات الإعلام والاتصال تنقسم إلى قسمين التشفير المتماثل (أولا) والتشفير غير المتماثل (ثانيا) وهناك من يضيف نوع جديدا من أنواع التشفير الذي يقوم على المزج بين النوعين السابقين وسيتم التطرق إليه في (ثالثا).

أولا: التشفير المتماثل

ويعرف أيضا بالمفتاح العام، و هو عبارة عن عملية رياضية يستعمل فيها مفتاح سري واحد يمتلكه كل من المرسل السند والمرسل إليه، والذي يتم بموجبه تشفير السندات وفك رموزها[27].

وتمر آلية إرسال السند في هذا النظام بتشفير السند والتوقيع عليه عبر الرموز التشفيرية المتفق عليها في المفتاح الخاص، ثم يرسل عبر وسيلة الاتصال الحديثة إلى المرسل إليه، إذ يقوم بتسليمه من حاسبه الآلي، الذي بدوره يقوم بفك الرموز التشفرية بالمفتاح الخاص المتماثل [28]. وغالبا ما تستعمل هذه الطريقة في البنوك لتشغيل آلات الصراف الآلي. وتجدر الإشارة أن هذا الأسلوب لا يخلو من مخاطر الاختراق والقرصنة، إذ تبدو عملية تبادل المفتاح السر بين شخصين عرضة للدخول غير المشروع من الغير.

ثانيا: التشفير غير المتماثل

إن هذه الطريقة من التشفير تختلف عن طريقة التشفير المتماثل في أنه لا يستخدم المفتاح أو الرمز السري في تشفير السند الإلكتروني، أو من أجل فك تشفيره، بل يستعمل مفتاحان سريان، الأول المفتاح الخاص ولا يعرفه سوى المستخدم السند الإلكتروني فقط ويبقى سريا[29]، والثاني فيعمم على المستخدمين الآخرين الذين يرغبون في التعامل برسائل مشفرة بحيث يستطيعون استخدام المفتاح العام في

[27] – حسن فضالة موسى، المرجع السابق، ص 234.

[28] – مرجع نفسه، ص 234.

[29] - مرجع نفسه، ص 235.

تشفير السندات وإرسالها إلى المستخدم الحائز على المفتاح الخاص. والذي يستطيع وحده دون غيره من فك تشفير السندات الواردة من المستخدمين. [30]

يعد التشفير غير المتماثل الطريقة المناسبة لحماية البيئة الافتراضية، إلا أن قوته وتقنياته مرهونة بمدى استخدام البرامج والأجهزة لتحقيق عملية حماية النظم المعلومات وسرية المعاملات والبيانات، وهوية المشاركين، والسرعة، ومستوى الخصوصية.

ثالثا : المزج بين التشفير المتماثل والتشفير غير المتماثل :

يتميز هذا النظام بتجاوزه لسلبيات الأنظمة السابقة، وذلك للتغلب على مشكلة إرسال المفتاح المتماثل بطرق آمنة لحل شفرة الرسالة، واقتصار الوقت باستخدام المفتاح العام من جهة أخرى[31]، إذ يمكن للمرسل والمرسل إليه أن يستخدما كلا من النظامين في التشفير البيانات، وهذا بتشفير الرسالة المرسلة بالمفتاح المتماثل (المفتاح السري) ثم بعدها يتم تشفير المفتاح المتماثل بالمفتاح غير المتماثل للشخص المرسل إليه الرسالة ويرسل المفتاح المشفر والرسالة المشفرة إلى المرسل إليه الذي يقوم بفك الشفرة بمفتاحه الخاص. [32]

فتشفير الرسالة بالمفتاحين يكون عبر عدة مراحل تتمثل فيما يلي :

-كتابة النص الأصلي وتشفيره بالمفتاح العام للمرسل إليه.

-تشفير ذات الرسالة مرة أخرى باستخدام المفتاح الخاص للمرسل وهذا بغرض التأكد من مرسلها وقابلية فكها باستخدام المفتاح العام للمرسل.

-إرسال الرسالة إلى المرسل إليه عبر الوسائل الإلكترونية.

-وصول الرسالة إلي المرسل إليه المشفرة بالفتاح المتماثل والمفتاح المتماثل المشفر. [33]

-يقوم المرسل إليه بفك تشفير المفتاح العام للمرسل فيتحصل على رسالة مشفرة بمفتاحه العام فيقوم بفكها باستخدام المفتاح السري الخاص به الذي يكون معلوما لديه.

---

[30] - مرجع نفسه، ص 235.

[31] – آزد دزه يي، المرجع السابق، ص 101.

[32] – سراح حليتم، خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية، مجلة الباحث للدراسات الأكاديمية، العدد 13، جويلية 2018 ، ص 743.

[33] – الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، دار الجامعة الجديدة، الإسكندرية، 2009، ص 20. 21.

وتعتبر هذه الطريقة أكثرها آمانا نظرا لدورها الفعال في تحقيق سرية البيانات الخاصة بالرسالة وإمكانية الحق من صاحبها.

المبحث الثاني : دور التشفير بتقنية البلوك تشين في حماية المعاملات الإلكترونية

إن الضرورات الحتمية التي فرضتها تكنولوجيا المعلومات خاصة في مجال المعاملات الإلكترونية أدت بالتشريعات الدولية منها والوطنية إلى تدارك ذلك في إطار إبرام العقود، من خلال فتح المجال للوسائل الإلكترونية في التعبير عن الإرادة، والتي أحيطت بخاصية حمائية تتجسد في حماية المعاملات الإلكترونية المبرمة عبر تقنية البلوك تشين باستعمال تقنيات التشفير الإلكتروني[34].

ونظرا لأهمية الدور التي تلعبه تقنية البلوك تشين بصفة عامة والتشفير الإلكتروني بصفة خاصة في حماية المعاملات الإلكترونية من أين إختراق قد تطرأ عليها، مما يؤدي إلى إضعاف من قوتها الثبوتية أمام القضاء. فإنه سنحاول من خلال هذا المبحث التعرف على الدور الذي يلعبه التشفير بتقنية البلوك تشين في حماية المعاملات الإلكترونية من خلال :

المطلب الأول : دور التشفير بتقنية البلوك تشين في توفير الأمن المعلوماتي للمعاملات الإلكترونية

تشكل تقنية البلوك تشين قفزة نوعية في مجال التعاملات الإلكترونية، التي تتميز بأنها تستطيع إدارة عدد غير نهائي من البيانات بطريقة شفافة وآمنة في شكل سجل إلكتروني مشفر عالمي تسجل فيه المعاملات[35]و الصفقات سواء قام بها الأفراد أو الإدارة العامة من خلال تحولها نحو إدارة إلكترونية. مما يضمن سلامتها من أي اختراق أو تعديل قد تطرأ عليها، وهو ما سوف نحاول التطرق إليه من خلال هذا المطلب.

الفرع الأول : مشاكل المساس بالأمن المعلوماتي للمعاملات الإلكترونية

إن دخول تكنولوجيا المعلومات إلى عالمنا وقيام الثورة العلمية العالمية في مجال نقل وتبادل المعلومات عبر الأنظمة الإلكترونية، وكذا في مجال إبرام المعاملات الإلكترونية، أدى إلى ظهور تحديات جديدة تعترض هذه الأخيرة، بما يضعف من قوتها الثبوتية أمام القضاء. والتي تتمثل أبرزها في :

[34] – سراح حليتيم، المرجع السابق، ص 737.

[35] – أنس محمد عبد الغفار سلامة، المرجع السابق، ص 63.

أولا : مشكلة اختراق الأنظمة الإلكترونية

على رغم ما قدمته التطورات الإلكترونية في مجال المعلومات من فوائد ومنافع، إلا أن الواقع يشير إلى قصور منها ما يتعلق بالحاسب الآلي، ومنها ما يتعلق بالحماية الفنية للمعلومات والمعاملات الإلكترونية بسبب بعض المشاكل منها الاختراق الإلكتروني للأنظمة الإلكترونية. الذي يتحقق بولوج شخص ما غير مخول له الدخول إلى نظام الكمبيوتر والقيام بالأنشطة غير المصرح له بها كالتعديل أو التغيير في البيانات والمعلومات الخاصة بالمعاملة الإلكترونية أو سرقتها أو إتلافها[36].

1 – تعريف الاختراق الإلكتروني:

لقد عرف المشرع الجزائري الاختراق بأنه " الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة على نظام معلوماتي أو حاسب آلي، أو شبكة معلوماتية أو ما في حكمها. " [37]

كما يعرف على أنه القدرة على الوصول لهدف معين بطريقة غير مشروعة، عن طريق وجود ثغرات في النظام الحماية الخاص بجهاز الحاسب الآلي المستهدف[38]، ويقوم بذلك ما يطلق عليهم بالقراصنة سواء كانوا قراصنة محترفين أم أشخاصا متدخلين عبر شبكة الأنترنت[39].

لذلك لقد فرضت التشريعات نصوصا عقابية للحماية من جرائم الاختراق التي تقع على المعاملات الإلكترونية بشكل عام، وذلك بهدف زرع الثقة والأمان لدى طرفي المعاملة الإلكترونية من جهة ومن جهة أخرى من أجل حماية هذه الأخيرة باعتبارها كدليل الإلكتروني يتمتع بالحجية الإثبات أمام القضاء في حالة النزاع.

2 – أنواع الاختراق للأنظمة المعلوماتية للمعاملات الإلكترونية

يأخذ الاختراق الإلكتروني ثلاثة أنواع تتمثل في :

أ – الدخول إلى النظام والبقاء غير المشروع فيه : تقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم ليست له علاقة بالحاسب الآلي وشبكاته، وسواء كانت لديه

[36] – محمد جمال زين العابدين، جرائم الاختراق النظم الإلكترونية بين التشريع المصري والمغربي، مجلة مستقبل العلوم الاجتماعية، العدد 01، أبريل 2020، ص 111.

[37] – المادة الأولى من القانون رقم 175، لسنة 2018، المتعلق بشأن مكافحة الجرائم المعلوماتية، الجريدة الرسمية، العدد 14، لسنة 2018/08/31 .

[38] – أشرف سعيد أحمد، القرصنة الإلكترونية، د ط، د د ن، د ب ن، 2013، ص 62، 63،

[39] – مرجع نفسه، ص 16.

المقدرة الفنية على الاستفادة من النظام أم لا، ومن الممكن التحقق من الدخول متى كان الدخول مخالفا لإرادة صاحب النظام وله الحق السيطرة عليه. [40]

ب – إعاقة أو تخريب تشغيل نظم معالجة البيانات : إن السلوك الإجرامي في هذه الجريمة ينصرف إلى كل عمل من شأنه تعطيل عمل نظام معالجة البيانات، ويستوي أن يكون النشاط الإجرامي إعاقة أو إفشاء نظام تشغيل في الإرسال، كما قد يؤدي إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة [41].

ج – التلاعب في البيانات نظم معالجة بيانات : والذي يتمثل في إدخال أو محو أو تعديل ولا يشترط اجتماعها وإنما يكتفي بتوافر إحداهما، فالجريمة هنا تقع على المعطيات أو البيانات المعالجة آليا دون المعلومة ذاتها. [42]

ثانيا : التزوير المعلوماتي للبيانات الخاصة بالمعاملات الإلكترونية

يعد التزوير المعلوماتي من أخطر صور الجرائم المعلوماتية التي تمس بالأنظمة المعلوماتية للمعاملات الإلكترونية، ويقصد به " تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في الورقة المكتوبة أو المسموعة عن طريق الرسم ويستوي في المحرر المعلوماتي أن يكون باللغة العربية أو بأي لغة أخرى لها دلالتها، وربما تمثل في صورة مخرجات غير ورقية بشرط أن تكون محفوظة على دعامة معلوماتية كبرنامج منسوخ على أسطوانة". [43]

و قد كان المشرع الفرنسي الأسبق عن معظم التشريعات في اتجاهه منحى متطورا في تعريفه للتزوير حيث عرفه ضمن نص المادة 01/441 من قانون العقوبات الفرنسي بأنه " تغيير الحقيقة المنطوي على غش ومن شأنه إحداث ضرر أذا أرتكب بأية وسيلة في سند أو في دعامة تعبر عن فكرة موضوعة أو يمكن أن يكون موضوعها إقامة الدليل على حق أو واقعة ذات آثار قانونية" [44].

[40] – محمد جمال زين العابدين، المرجع السابق، ص 118.

[41] – محمد جمال زين العابدين، المرجع السابق، ص 121.

[42] – مرجع نفسه، ص 121.

[43] – عبد الفتاح بيومي حجازي، نظام التجارة الإلكترونية وحمايتها مدنيا ، الكتاب الثاني، الإسكندرية دار الفكر الجامعي، 2004، ص206.

[44] – حسن فضالة موسى، المرجع السابق، ص 234.

الفرع الثاني : دور التشفير بتقنية البلوك تشين في التصدي لمشاكل الأمن المعلوماتي للمعاملات الإلكترونية

إن أخطر هاجس يهدد التعاقد الإلكتروني بصفة عامة، بالنظر إلى السرعة التي يمكن أن تتم بها العمليات التجارية بوقت قياسي هو إساءة استخدام الأنظمة المعلوماتية أو اختراقها والتمكن من بياناتها وما يترتب عليها من آثار وخيمة، الأمر الذي تطلب البحث عن آلية من شأنها التصدي لهذه الخروقات ومنعها قبل حدوثها وهو الهدف الذي يحققه التشفير[45]بتقنية البلوك تشين وذلك من خلال :

أولا : توفير بنية تحتية إلكترونية آمنة

تقوم هذه الميزة بدور كبير في ظل انتشار التعاقد الإلكتروني المبرم عبر الأنترنت بواسطة تقنية البلوك تشين في مجال التجارة، ذلك أن هذا النوع من التعاقد يرتبط بأمور فنية بالغة الدقة[46]عن طريق إعتمادها على آلية التشفير الإلكتروني، الذي يعتبر هذا الأخير نتاج لمقتضيات الحفاظ والأمان للبيانات والمعلومات الخاصة بالمعاملات الإلكترونية، التي اقتضتها طبيعة التجارة الإلكترونية[47]من جهة، ومن جهة آخرى بهدف توفير الثقة لدى متعاملي التجارة الإلكترونية على حدا سواء .

و هذا ما يتطلب بالضرورة وجود متخصصين في هذا المجال ملمين بالجانب القانوني والتقني المرتبطين بهذا النوع من التعاملات الإلكترونية التي تنفذ عبر منصات البلوك تشين، مما يؤدي إلى إبرام عقود تتسم بالثبات والصحة والوضوح والثقة بين جميع الأطراف فيها، نظرا لما يحققه التشفير الإلكتروني عبر تقنية البلوك تشين من بينة آمنة من أي تحريف او تغيير سواء كان بالحذف أو الزيادة أو الاستبدال في البيانات والمعلومات الخاصة بالمعاملات الإلكترونية، واعتمادهم لها مما يؤدي بالنتيجة إلى انتشار التعامل بها[48].

ثانيا : تأمين البيانات

إن اعتماد على تقنية البلوك تشين في مجال المعاملات الإلكترونية (العقود الإلكترونية) جعلها تتميز بطبيعة خاصة تميزها عن العقود التقليدية، بما في ذلك العقود التي تتم عبر الأنترنت من خلال أنظمة مركزية تملكها جهات معينة وتشرف عليها. إذ تقوم هذه التقنية بتأمين البيانات أو المعاملات دون

[45] – يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2007 ص، 135.

[46] – مصطفى محمد الحسبان، المرجع السابق، ص 141.

[47] – يوسف أحمد النوافلة، المرجع السابق، ص98.

[48] – مصطفى محمد الحسبان، المرجع السابق، ص 142.

وجود هيئة مركزية في سلسة الكتل، التي يفترض أن تقوم بالتأكد من صحتها قبل إدخالها في سلسة الكتل. [49]

إن أهم ما يميز تقنية البلوك تشن أنها تقوم بتخزين البيانات والمعلومات في شكل كتل مشفرة فإذ ما أدخلت تلك البيانات وتم إضافتها فعلا إلى سلسلة الكتل بعد التحقق منها من خلال " عقد الشبكة " فإنه لا يمكن تعديلها أو تغييرها، وهو ما يجعل البلوك تشين ثابت وغير قابل للتغيير[50]. والسبب في ذلك هو اعتماده على آلية التشفير عن طريق ما يطلق عليه بدالة التجزئة أو آلية الهاش وهي عبارة عن خوارزميات معينة للتشفير تحول البيانات التي تم إدخالها في الكتلة، مهما كان حجمها، إلى مجموعة فريدة من الأرقام والحروف والرموز ذات طول ثابت يطلق عليها بالهاش. فهو بمثابة بصمة مميزة للبيانات يتغير بتغير محتوى هذه الأخيرة [51].

و تجدر الإشارة أن كل كتلة تحتوي على تاريخ إنشاؤها والبيانات المراد تخزينها، وموضع الكتلة في السلسة، ورموز الهاش (البصمة الرقمية)، التي تم إنشاؤها من البيانات الموجودة في الكتلة إضافة إلى الهاش الخاص بالكتلة السابقة، وهذا يعني أن البلوك تشين عبارة عن سلسة من الكتل المترابطة عن طريق التشفير الإلكتروني، فإن أي إضافة أو سحب أو تعديل في الكتلة لا يؤدي فقط إلى إبطالها فحسب، وإنما يؤدي إلى إبطال جميع الكتل في السلسة بأكملها.[52]

و في هذا الإطار يمكن القول تقنية البلوك تشين تعتبر أحد أهم الحلول التكنولوجية الحديثة التي تلعب دورا كبير في ضمان أمن وسلامة بيانات المعاملات الإلكترونية من أي عطل أو قرصنة قد تطرأ عليها. وذلك بالنظر إلى اعتمادها على آلية التشفير الإلكتروني، وبالتالي فوجود التشفير يشكل مخرجا من كافة الاختراقات والاعتداءات على المعاملات الإلكترونية، مما يوفر الأمن الإلكتروني من خلال توفير قاعدة بيانات آمنة وذاتية الصيانة.

المطلب الثاني : دور التشفير بتقنية البلوك تشين في توثيق المعاملات الإلكترونية

أدى شيوع العقود الإلكترونية إلى مجموعة من الإشكاليات القانونية، لاسيما ما يتعلق بالإثبات بشان العلاقات الناجمة عن هذا النوع من العقود. ذلك أنها تقوم على وسيط غير مادي يتم من خلاله تحرير العقد وتدوين بنوده. وبما أن تقنية البلوك تشين تعتبر من أحدث المنصات الأكثر أمانا يتم من

[49] – مصطفى داود، المرجع السابق، ص 286.

[50] – هيثم السيد أحمد عيسى، المرجع السابق، ص 22.

[51] – مرجع نفسه، ص 22.

[52] – مصطفى داود، المرجع السابق، ص 286.

خلالها إبرام المعاملات الإلكترونية بطريقة مشفرة، مما تؤدي إلى حمايتها والاعتماد عليها كوسيلة وإثبات أمام القضاء في حالة النزاع، وهذا ما سنتعرف عليه من خلال هذا المطلب :

الفرع الأول : توثيق مضمون المعاملة الإلكترونية

إن المحرر الإلكتروني شأنه شان المحرر الكتابي في إثبات ما ورد فيه. إذ وبالرجوع إلى نص المادة **323** مكرر **01** من القانون المدني والتي جاء فيها " يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية صاحب الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها "[53].

أولا : من ناحية توثيق البيانات الواردة في المعاملة الإلكترونية

تتيح تقنية البلوك تشين قراءة البيانات المثبتة على المعاملة الإلكترونية، ولو بشكل غير مباشر في صورة رموز أو أرقام أو حروف إلى غير ذلك، كما أن ما يثبت عليها من بيانات يكون مخزنا تخزينا رقميا، ومن ثم تكون هذه البيانات بمثابة كتابة قابلة للإدراك هذا من جهة [54]، ومن جهة أخرى تقوم تقنية البلوك تشين بالحفظ الإلكتروني للبيانات باعتبارها سجلا مفتوحا يساعد في الوصول إلى هذه الأخيرة وتبادلها وإدارتها في أي وقت، وهذا ما يجعلها تتميز بصفة الدوام والاستمرارية.

وعليه تلعب تقنية البلوك تشين دور كبير في تحقيق درجة عالية من الأمن التقني تحول دون إحداث أي تغيير أو تحريف بالبيانات، كون أنها قاعدة لا مركزية يتم من خلالها تسجيل البيانات في شكل كتل مشفرة موزعة على كافة مستخدمي هذه التقنية[55]، مما يجعل من فرض إمكانية الإخلال بسلامة البيانات أمر صعب المنال.

ثانيا : من حيث تحديد علاقة بين التوقيع بالبيانات المرتبطة بها

تقوم تقنية البلوك تشين شأنها شأن التوقيع الإلكتروني، على خوارزميات التشفير غير المتماثل، حيث يتعين على المستخدم، لإجراء معاملاته على الشبكة، أن يقوم باستعمال البرنامج المزود لمفتاحي التوقيع غير المتماثل. [56]

[53] – المادة 323 مكرر 01 من القانون رقم 10/05، المؤرخ في 20 يونيو 2005، المتضمن القانون المدني.

[54] – جابر أشرف ، البلوك تشين والإثبات الرقمي في مجال حق المؤلف، المجلة الدولية للفقه والقضاء والتشريع مصر، العدد01، لسنة 2020، ص 45.

[55] – مصطفى داود، المرجع السابق، ص 293.

[56] – جابر أشرف، المرجع السابق، ص 47.

إذ تتيح تقنية البلوك تشين تحديد علاقة التوقيع بالبيانات المرتبطة به، بما يضمن سلامة هذه الأخيرة، حيث تعمل خوارزميات التشفير الإلكتروني على مفتاحين، الأول (وهو مفتاح المستخدم مرسل البيانات لا يعلمه غيره)، ويكون بمثابة توقيع له، والثاني عام، متاح للكافة وهو ما يقدمه المستخدم الآخر (متلقى البيانات) الذي يرغب في الدفع وإتمام المعاملة. وعن طريق هذا المفتاح الخاص يمكن فك تشفير المفتاح العام، فتحدد علاقة هذا الأخير بالبيانات المعاملة المسجلة على كتلة سواء من حيث تاريخ ووقت إجراءها وكذلك قيمتها. [57]

إلا أنه إذا كان بإمكان تقنية البلوك تشين تحديد علاقة التوقيع بالبيانات المرتبطة بها، بما يجعلها تتسم بالشفافية فيما يتعلق بالمعاملات التي تتم من خلالها، إلا أنها تتسم بالخفاء فيما يتعلق بهوية المتعاملين أو المستخدمين، حيث يكون بوسع أي منهم أن يلجأ إلى التعامل باسم مستعار، وبتالي يتم تبادل البيانات وأكواد التشفير للتحقق من المعاملات دون الوقوف على هوية المتعاملين. [58]

و تجدر الإشارة أن تقنية البلوك تشين لها دورا فعال في توثيق المعاملات الإلكترونية من خلال اعتمادها على أحد أهم الضوابط المنظومة الإلكترونية ألا وهو" الختم أو بصمة الوقت " وبمقتضاه يتم التأريخ الرقمي لأي عملية إنشاء بيانات تتم بواسطة أي مستخدمي شبكة البلوك تشين، وتحديد لحظة إجراءها داخل الكتلة.

الفرع الثاني : مدى اعتبار البلوك تشين جهة تصديق إلكتروني للمعاملات الإلكترونية

بما أن التوثيق، أو التصديق يتم عادة عن طريق وسيط محايد مرخص له قانونا بهدف إضفاء الثقة والأمان على المعاملة الإلكترونية، بينما تقوم تقنية البلوك تشين على نظام الند للند والتي يمكن من خلالها لأعضاء الشبكة، التفاعل بينهم عن طريق إجراء المعاملات أو نقل القيم أو البيانات بحسب الغرض من الشبكة، وبصورة مباشرة دون تدخل سلطة مركزية. [59] وهذا ما يخول لتقنية البلوك تشين أن تلعب مثل هذا الدور، كون أنه ليس مجرد " محول رقمي" بل أنه نظام مؤهل لأن يكون أيضا " موثقا رقميا " يضفي الصفة الرسمية على المحررات التي تنشأ وتحفظ من خلاله، فتتم عملية التوثيق تلقائيا بفضل " ختم الوقت " الذي يوثق الارتباط الزمني بين الكتل المشفرة. بما يضمن سلامة سلسلة الكتل ككل، فهو ليس مؤهل للقيام بهذا الدور فقط بالنسبة للبيانات بل ولكافة المعاملات أو التصرفات القانونية التي تتم من خلاله كالعقود الإدارية الإلكترونية[60].

---

[57] – مصطفى دواد، المرجع السابق، ص 294.

[58] – مصطفى دواد، المرجع السابق، ص 294.

[59] – أشرف جابر، المرجع السابق، ص 51.

[60] – مرجع نفسه، ص 51.

و عليه يمكن القول أن المحررات الإلكترونية التي تنشا وتحفظ عبر تقنية البلوك تشين تتمتع بالصفة الرسمية ، بحيث يكون لهذه المحررات ذات قوة المحرر الرسمي الذي يحرر عبر الدعامة إلكترونية بواسطة موظف عام مختص، ويعود ذلك بسبب آلية التشفير الإلكتروني المعقد التي تعتمد عليه تقنية البلوك تشين بما يضفي الثقة والأمان، مما يؤهلها ان تعتبر جهة تصديق إلكتروني. وهو ما اقترحه البعض في هذا الإطار ضمن نص المادة 1317 /02 من القانون المدني الفرنسي المعدلة بموجب المادة 13- 02/69 من ذات القانون وذلك في ماي 2016 والتي نصت " تعد محررات رسمية، بالمعنى الوارد بالفقرة الثانية من المادة 1317 القانون المدني ، المعاملات التي تتم من خلال نظام معد وفق سجل لا مركزي دائم لا يمكن العبث به في شكل سلسلة الكتل. " [61] إلا أنه قوبل بالرفض.

و بالتالي في ظل غياب نص تشريعي يعترف بحجية المحررات الإلكترونية التي تنشأ وتحفظ عبر تقنية البلوك تشين من خلال تشفيرها، فإنه يصعب التسليم قيام هذه الأخيرة بدور جهة التصديق. وذلك لعدم وجود الوسيط الثقة (وهو مقدم خدمات التصديق الإلكتروني)، الذي يتولى مهمة التحقق من هوية الموقع، وإصدار شهادة تصديق، تضمن ذلك. كما هو الحال بالنسبة للتوقيع الإلكتروني[62]الأمر الذي يجعل منه توقيعا محميا ومعززا يتمتع بالحجية في الإثبات أمام القضاء في حالة النزاع.

الخاتمة:

وخاتما يمكن القول أن من بين المميزات التكنولوجية أنها أفزت العديد من المسائل التي تتطلب دراسة ومعالجة قانونية، لذلك فإن دراسة موضوع التشفير الإلكتروني بتقنية البلوك تشين وإبراز دوره في ضمان أمن وسلامة البيانات والمعلومات الواردة في المعاملات الإلكترونية التي تبرم عبر هذه المنصة يعتبر من بين المواضيع الحديثة التي أثارت جدلا واسعا خاصة في مجال إنشاء دليل إلكتروني آمن قادر على إثبات مضمون المعاملات الإلكترونية وحمايتها من كل أشكال التلاعبات الإلكترونية.

ولقد توجت هذه الدراسة بمجموعة من **النتائج** يمكن إجمالها فيما يلي :

- إن مميزات التكنولوجيا المتقدمة أنها أفرزت العديد من الأدلة الإلكترونية التي أضحت تمثل نظاما قانونيا غريبا عن المعالجة القانونية بالنصوص التقليدية. وهو ما يؤدي إلى اتساع دائرة وسائل الإثبات الإلكتروني من بينها التشفير الإلكتروني.

[61] – أشرف جابر، المرجع السابق، ص 52.

[62] – مرجع نفسه، ص 52.

- وجود برنامج معلوماتي توثيقي مشفر مهمته إضفاء الثقة والطمأنينة بين أطراف العملية التعاقدية، ذلك بما توفره من سلامة وأمن للبيانات والمعلومات الواردة في المعاملات الإلكترونية.

- يعد التشفير الإلكتروني عبر تقنية البلوك تشين من أهم الحلول التكنولوجية التي تواجه مشاكل الإثبات الإلكتروني للمعاملات الإلكترونية، وذلك بالنظر إلى طبيعة التشفير المعقد لها، بما يضمن توفير الأمن السيبراني لهذه الأخيرة.

- يعتبر التشفير الإلكتروني بتقنية البلوك تشين من بين آليات التقنية والقانونية، التي لا تقتصر وظائفه فقط في توفير الأمن وسلامة البيانات الخاصة بالمعاملات الإلكترونية بل يمتد دوره إلى المساهمة في تدعيم وسيلة الإثبات الإلكتروني من خلال توثيق المعاملات الإلكترونية عن طريق تحديد مضمون هذه الأخيرة وتحديد العلاقة بين التوقيع بالبيانات المرتبطة بها.

- تلعب تقنية البلوك تشين دورا في التوثيق الرقمي للمعاملات الإلكترونية التي تنشأ وتحفظ عبر هذه المنصة، إلا أن غياب الاعتراف التشريعي لها، يمنع من أن تكون كجهة تصديق إلكتروني رسمية معترف بها قانونيا.

ومن التوصيات التي توصلنا إليها من خلال هذه الدراسة :

- ضرورة التدخل التشريعي في نطاق قوانين الإثبات بالنص صراحة على الأحكام الخاصة التي تنظم تقنية البلوك تشين ودورها في حماية وتوثيق المعاملات الإلكترونية.

- ضرورة الاعتراف القانوني للتقنية البلوك تشين بالقيام بدور جهة تصديق إلكتروني معتمد لها صلاحية التحقق من هوية الموقع، وإصدار شهادة تصديق تضمن ذلك.

- وضع نظام قانوني خاص ينظم أحكام التشفير الإلكتروني بصفة مباشرة باعتباره إجراء ضروري للتوثيق المعاملات الإلكترونية.

-تنظيم حملات وندوات علمية لنشر الثقافة الإلكترونية داخل المجتمع والإدارة على حد سواء للتعامل بتقنية البلوك تشين في مجال إبرام المعاملات الإلكترونية من أجل المساهمة في جذب الاستثمارات وتشجيع نقل التكنولوجيا ودفع الطاقات البشرية للإبداع والتطوير في هذا المجال.