ДОДАТОК А
ПРОГРАМНИЙ КОД

```
using Newtonsoft.Json;
using System;
using System.Collections.Generic;
using System.Diagnostics;
using System.IO;
using System.Linq;
using System.Net;
using System.Security.Cryptography;
using System.Text;

namespace BlockChainDemo
{
    public class BlockChain
    {
        private List<Transaction> _currentTransactions = new List<Transaction>();
        private List<Block> _chain = new List<Block>();
        private List<Node> _nodes = new List<Node>();
        private Block _lastBlock => _chain.Last();
        public string NodeId { get; private set; }
        //ctor
        public BlockChain()
        {
            NodeId = Guid.NewGuid().ToString().Replace("-", "");
            CreateNewBlock(proof: 100, previousHash: "1"); //genesis block
        }
        //private functionality
        private void RegisterNode(string address)
        {
            _nodes.Add(new Node { Address = new Uri(address) });
        }
        private bool IsValidChain(List<Block> chain)
        {
```

```
    Block block = null;
    Block lastBlock = chain.First();
    int currentIndex = 1;
    while (currentIndex < chain.Count)
    {
        block = chain.ElementAt(currentIndex);
        Debug.WriteLine($"{lastBlock}");
        Debug.WriteLine($"{block}");
        Debug.WriteLine("-----------------------------");
        //Check that the hash of the block is correct
        if (block.PreviousHash != GetHash(lastBlock))
            return false;
        //Check that the Proof of Work is correct
        if (!IsValidProof(lastBlock.Proof, block.Proof, lastBlock.PreviousHash))
            return false;
        lastBlock = block;
        currentIndex++;
    }
    return true;
}
private bool ResolveConflicts()
{
    List<Block> newChain = null;
    int maxLength = _chain.Count;
    foreach (Node node in _nodes)
    {
        var url = new Uri(node.Address, "/chain");
        var request = (HttpWebRequest)WebRequest.Create(url);
        var response = (HttpWebResponse)request.GetResponse();
        if (response.StatusCode == HttpStatusCode.OK)
        {
            var model = new
            {
                chain = new List<Block>(),
                length = 0
            };
            string json = new StreamReader(response.GetResponseStream()).ReadToEnd();
```

```
            var data = JsonConvert.DeserializeAnonymousType(json, model);
            if (data.chain.Count > _chain.Count && IsValidChain(data.chain))
            {
                maxLength = data.chain.Count;
                newChain = data.chain;
            }
        }
    }
    if (newChain != null)
    {
        _chain = newChain;
        return true;
    }
    return false;
}
private Block CreateNewBlock(int proof, string previousHash = null)
{
    var block = new Block
    {
        Index = _chain.Count,
        Timestamp = DateTime.UtcNow,
        Transactions = _currentTransactions.ToList(),
        Proof = proof,
        PreviousHash = previousHash ?? GetHash(_chain.Last())
    };
    _currentTransactions.Clear();
    _chain.Add(block);
    return block;
}
private int CreateProofOfWork(int lastProof, string previousHash)
{
    int proof = 0;
    while (!IsValidProof(lastProof, proof, previousHash))
        proof++;
    return proof;
}
private bool IsValidProof(int lastProof, int proof, string previousHash)
```

```
{
    string guess = $"{lastProof}{proof}{previousHash}";
    string result = GetSha256(guess);
    return result.StartsWith("0000");
}
private string GetHash(Block block)
{
    string blockText = JsonConvert.SerializeObject(block);
    return GetSha256(blockText);
}
private string GetSha256(string data)
{
    var sha256 = new SHA256Managed();
    var hashBuilder = new StringBuilder();
    byte[] bytes = Encoding.Unicode.GetBytes(data);
    byte[] hash = sha256.ComputeHash(bytes);
    foreach (byte x in hash)
        hashBuilder.Append($"{x:x2}");
    return hashBuilder.ToString();
}
//web server calls
internal string Mine()
{
    int proof = CreateProofOfWork(_lastBlock.Proof, _lastBlock.PreviousHash);
    CreateTransaction(sender: "0", recipient: NodeId, amount: 1);
    Block block = CreateNewBlock(proof /*, _lastBlock.PreviousHash*/);
    var response = new
    {
        Message = "New Block Forged",
        Index = block.Index,
        Transactions = block.Transactions.ToArray(),
        Proof = block.Proof,
        PreviousHash = block.PreviousHash
    };
    return JsonConvert.SerializeObject(response);
}
internal string GetFullChain()
```

```
{
    var response = new
    {
        chain = _chain.ToArray(),
        length = _chain.Count
    };
    return JsonConvert.SerializeObject(response);
}
internal string RegisterNodes(string[] nodes)
{
    var builder = new StringBuilder();
    foreach (string node in nodes)
    {
        string url = $"http://{node}";
        RegisterNode(url);
        builder.Append($"{url}, ");
    }
    builder.Insert(0, $"{nodes.Count()} new nodes have been added: ");
    string result = builder.ToString();
    return result.Substring(0, result.Length - 2);
}
internal string Consensus()
{
    bool replaced = ResolveConflicts();
    string message = replaced ? "was replaced" : "is authoritive";
    var response = new
    {
        Message = $"Our chain {message}",
        Chain = _chain
    };
    return JsonConvert.SerializeObject(response);
}
internal int CreateTransaction(string sender, string recipient, int amount)
{
    var transaction = new Transaction
    {
        Sender = sender,
```

```
            Recipient = recipient,
            Amount = amount
        };
        _currentTransactions.Add(transaction);
        return _lastBlock != null ? _lastBlock.Index + 1 : 0;
    }
  }
}
using Newtonsoft.Json;
using System.Configuration;
using System.IO;
using System.Net;
using System.Net.Http;

namespace BlockChainDemo
{
  public class WebServer
  {
    public WebServer(BlockChain chain)
    {
      var settings = ConfigurationManager.AppSettings;
      string host = settings["host"]?.Length > 1 ? settings["host"] : "localhost";
      string port = settings["port"]?.Length > 1 ? settings["port"] : "12345";
      var server = new TinyWebServer.WebServer(request =>
        {
          string path = request.Url.PathAndQuery.ToLower();
          string query = "";
          string json = "";
          if (path.Contains("?"))
          {
            string[] parts = path.Split('?');
            path = parts[0];
            query = parts[1];
          }

          switch (path)
          {
```

```
                //GET: http://localhost:12345/mine
                case "/mine":
                    return chain.Mine();
                //POST: http://localhost:12345/transactions/new
                //{ "Amount":123, "Recipient":"ebeabf5cc1d54abdbca5a8fe9493b479",
"Sender":"31de2e0ef1cb4937830fcfd5d2b3b24f" }
                case "/transactions/new":
                    if (request.HttpMethod != HttpMethod.Post.Method)
                        return $"{new HttpResponseMessage(HttpStatusCode.MethodNotAllowed)}";
                    json = new StreamReader(request.InputStream).ReadToEnd();
                    Transaction trx = JsonConvert.DeserializeObject<Transaction>(json);
                    int blockId = chain.CreateTransaction(trx.Sender, trx.Recipient, trx.Amount);
                    return $"Your transaction will be included in block {blockId}";
                //GET: http://localhost:12345/chain
                case "/chain":
                    return chain.GetFullChain();
                //POST: http://localhost:12345/nodes/register
                //{ "Urls": ["localhost:54321", "localhost:54345", "localhost:12321"] }
                case "/nodes/register":
                    if (request.HttpMethod != HttpMethod.Post.Method)
                        return $"{new HttpResponseMessage(HttpStatusCode.MethodNotAllowed)}";
                    json = new StreamReader(request.InputStream).ReadToEnd();
                    var urlList = new { Urls = new string[0] };
                    var obj = JsonConvert.DeserializeAnonymousType(json, urlList);
                    return chain.RegisterNodes(obj.Urls);
                //GET: http://localhost:12345/nodes/resolve
                case "/nodes/resolve":
                    return chain.Consensus();
            }

            return "";
        },
        $"http://{host}:{port}/mine/",
        $"http://{host}:{port}/transactions/new/",
        $"http://{host}:{port}/chain/",
        $"http://{host}:{port}/nodes/register/",
        $"http://{host}:{port}/nodes/resolve/"
```

```
            );
            server.Run();
        }
    }
}

using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Security.Cryptography;
using System.Text;
namespace Algorithm
{
    public class AES
    {
        public byte[] EncryptStringToBytes_Aes(string plainText, byte[] Key, byte[] IV)
        {
            // Check arguments.
            if (plainText == null || plainText.Length <= 0)
                throw new ArgumentNullException("plainText");
            if (Key == null || Key.Length <= 0)
                throw new ArgumentNullException("Key");
            if (IV == null || IV.Length <= 0)
                throw new ArgumentNullException("IV");
            byte[] encrypted;

            // Create an Aes object
            // with the specified key and IV.
            using (Aes aesAlg = Aes.Create())
            {
                aesAlg.Key = Key;
                aesAlg.IV = IV;

                // Create an encryptor to perform the stream transform.
                ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);
```

```
            // Create the streams used for encryption.
            using (MemoryStream msEncrypt = new MemoryStream())
            {
                using (CryptoStream csEncrypt = new CryptoStream(msEncrypt, encryptor, CryptoStreamMode.Write))
                {
                    using (StreamWriter swEncrypt = new StreamWriter(csEncrypt))
                    {
                        //Write all data to the stream.
                        swEncrypt.Write(plainText);
                    }
                    encrypted = msEncrypt.ToArray();
                }
            }
        }
        // Return the encrypted bytes from the memory stream.
        return encrypted;
    }
    public string DecryptStringFromBytes_Aes(byte[] cipherText, byte[] Key, byte[] IV)
    {
        // Check arguments.
        if (cipherText == null || cipherText.Length <= 0)
            throw new ArgumentNullException("cipherText");
        if (Key == null || Key.Length <= 0)
            throw new ArgumentNullException("Key");
        if (IV == null || IV.Length <= 0)
            throw new ArgumentNullException("IV");
        // Declare the string used to hold
        // the decrypted text.
        string plaintext = null;
        // Create an Aes object
        // with the specified key and IV.
        using (Aes aesAlg = Aes.Create())
        {
            aesAlg.Key = Key;
            aesAlg.IV = IV;
            // Create a decryptor to perform the stream transform.
```

```
            ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key, aesAlg.IV);
            // Create the streams used for decryption.
            using (MemoryStream msDecrypt = new MemoryStream(cipherText))
            {
              using (CryptoStream csDecrypt = new CryptoStream(msDecrypt, decryptor,
CryptoStreamMode.Read))
              {
                using (StreamReader srDecrypt = new StreamReader(csDecrypt))
                {
                  // Read the decrypted bytes from the decrypting stream
                  // and place them in a string.
                  plaintext = srDecrypt.ReadToEnd();
                }
              }
            }
          }
          return plaintext;
        }
    }
}
using System;
using System.Security.Cryptography;
using System.Text;

namespace Algorithm
{
    public class BlowFish
    {
        RNGCryptoServiceProvider randomSource;
        //SBLOCKS
        private uint[] bf_s0;
        private uint[] bf_s1;
        private uint[] bf_s2;
        private uint[] bf_s3;
        private uint[] bf_P;
        //KEY
        private byte[] key;
```

```
//HALF-BLOCKS
private uint xl_par;
private uint xr_par;
private byte[] InitVector;
private bool IVSet;
//COMPATIBILITY WITH javascript CRYPTO LIBRARY
private bool nonStandardMethod;
/// <summary>
/// Constructor for hex key
/// </summary>
/// <param name="hexKey">Cipher key as a hex string</param>
public BlowFish(string hexKey)
{
   randomSource = new RNGCryptoServiceProvider();
   SetupKey(HexToByte(hexKey));
}
/// <summary>
/// Constructor for byte key
/// </summary>
/// <param name="cipherKey">Cipher key as a byte array</param>
public BlowFish(byte[] cipherKey)
{
   randomSource = new RNGCryptoServiceProvider();
   SetupKey(cipherKey);
}
/// <summary>
/// Encrypts a string in CBC mode
/// </summary>
/// <param name="pt">Plaintext data to encrypt</param>
/// <returns>Ciphertext with IV appended to front</returns>
public string Encrypt_CBC(string pt)
{
   if (!IVSet)
      SetRandomIV();
   return ByteToHex(InitVector) + ByteToHex(Encrypt_CBC(Encoding.ASCII.GetBytes(pt)));
}
/// <summary>
```

```
/// Decrypts a string in CBC mode
/// </summary>
/// <param name="ct">Ciphertext with IV appended to front</param>
/// <returns>Plaintext</returns>
public string Decrypt_CBC(string ct)
{
   IV = HexToByte(ct.Substring(0, 16));
   return Encoding.ASCII.GetString(Decrypt_CBC(HexToByte(ct.Substring(16)))).Replace("\0", "");
}
/// <summary>
/// Decrypts a byte array in CBC mode.
/// IV must be created and saved manually.
/// </summary>
/// <param name="ct">Ciphertext data to decrypt</param>
/// <returns>Plaintext</returns>
public byte[] Decrypt_CBC(byte[] ct)
{
   return Crypt_CBC(ct, true);
}
/// <summary>
/// Encrypts a byte array in CBC mode.
/// IV must be created and saved manually.
/// </summary>
/// <param name="pt">Plaintext data to encrypt</param>
/// <returns>Ciphertext</returns>
public byte[] Encrypt_CBC(byte[] pt)
{
   return Crypt_CBC(pt, false);
}
/// <summary>
/// Encrypt a string in ECB mode
/// </summary>
/// <param name="pt">Plaintext to encrypt as ascii string</param>
/// <returns>hex value of encrypted data</returns>
public string Encrypt_ECB(string pt)
{
   return ByteToHex(Encrypt_ECB(Encoding.ASCII.GetBytes(pt)));
```

```
}
/// <summary>
/// Decrypts a string (ECB)
/// </summary>
/// <param name="ct">hHex string of the ciphertext</param>
/// <returns>Plaintext ascii string</returns>
public string Decrypt_ECB(string ct)
{
   return Encoding.ASCII.GetString(Decrypt_ECB(HexToByte(ct))).Replace("\0", "");
}
/// <summary>
/// Encrypts a byte array in ECB mode
/// </summary>
/// <param name="pt">Plaintext data</param>
/// <returns>Ciphertext bytes</returns>
public byte[] Encrypt_ECB(byte[] pt)
{
   return Crypt_ECB(pt, false);
}
/// <summary>
/// Decrypts a byte array (ECB)
/// </summary>
/// <param name="ct">Ciphertext byte array</param>
/// <returns>Plaintext</returns>
public byte[] Decrypt_ECB(byte[] ct)
{
   return Crypt_ECB(ct, true);
}
/// <summary>
/// Initialization vector for CBC mode.
/// </summary>
public byte[] IV
{
   get { return InitVector; }
   set
   {
      if (value.Length == 8)
```

```
        {
            InitVector = value;
            IVSet = true;
        }
        else
        {
            throw new Exception("Invalid IV size.");
        }
    }
}
public bool NonStandard
{
    get { return nonStandardMethod; }
    set { nonStandardMethod = value; }
}
/// <summary>
/// Creates and sets a random initialization vector.
/// </summary>
/// <returns>The random IV</returns>
public byte[] SetRandomIV()
{
    InitVector = new byte[8];
    randomSource.GetBytes(InitVector);
    IVSet = true;
    return InitVector;
}
#region Cryptography
/// <summary>
/// Sets up the S-blocks and the key
/// </summary>
/// <param name="cipherKey">Block cipher key (1-448 bits)</param>
private void SetupKey(byte[] cipherKey)
{
    bf_P = SetupP();
    //set up the S blocks
    bf_s0 = SetupS0();
    bf_s1 = SetupS1();
```

```
        bf_s2 = SetupS2();
        bf_s3 = SetupS3();
        key = new byte[cipherKey.Length]; // 448 bits
        if (cipherKey.Length > 56)
        {
           throw new Exception("Key too long. 56 bytes required.");
        }
        Buffer.BlockCopy(cipherKey, 0, key, 0, cipherKey.Length);
        int j = 0;
        for (int i = 0; i < 18; i++)
        {
           uint d = (uint)(((key[j % cipherKey.Length] * 256 + key[(j + 1) % cipherKey.Length]) * 256 + key[(j
+ 2) % cipherKey.Length]) * 256 + key[(j + 3) % cipherKey.Length]);
           bf_P[i] ^= d;
           j = (j + 4) % cipherKey.Length;
        }
        xl_par = 0;
        xr_par = 0;
        for (int i = 0; i < 18; i += 2)
        {
           encipher();
           bf_P[i] = xl_par;
           bf_P[i + 1] = xr_par;
        }
        for (int i = 0; i < 256; i += 2)
        {
           encipher();
           bf_s0[i] = xl_par;
           bf_s0[i + 1] = xr_par;
        }
        for (int i = 0; i < 256; i += 2)
        {
           encipher();
           bf_s1[i] = xl_par;
           bf_s1[i + 1] = xr_par;
        }
        for (int i = 0; i < 256; i += 2)
```

```
    {
        encipher();
        bf_s2[i] = xl_par;
        bf_s2[i + 1] = xr_par;
    }
    for (int i = 0; i < 256; i += 2)
    {
        encipher();
        bf_s3[i] = xl_par;
        bf_s3[i + 1] = xr_par;
    }
}
/// <summary>
/// Encrypts or decrypts data in ECB mode
/// </summary>
/// <param name="text">plain/ciphertext</param>
/// <param name="decrypt">true to decrypt, false to encrypt</param>
/// <returns>(En/De)crypted data</returns>
private byte[] Crypt_ECB(byte[] text, bool decrypt)
{
    int paddedLen = (text.Length % 8 == 0 ? text.Length : text.Length + 8 - (text.Length % 8));
    byte[] plainText = new byte[paddedLen];
    Buffer.BlockCopy(text, 0, plainText, 0, text.Length);
    byte[] block = new byte[8];
    for (int i = 0; i < plainText.Length; i += 8)
    {
        Buffer.BlockCopy(plainText, i, block, 0, 8);
        if (decrypt)
        {
            BlockDecrypt(ref block);
        }
        else
        {
            BlockEncrypt(ref block);
        }
        Buffer.BlockCopy(block, 0, plainText, i, 8);
    }
```

```
    return plainText;
}
/// <summary>
/// Encrypts or decrypts data in CBC mode
/// </summary>
/// <param name="text">plain/ciphertext</param>
/// <param name="decrypt">true to decrypt, false to encrypt</param>
/// <returns>(En/De)crypted data</returns>
private byte[] Crypt_CBC(byte[] text, bool decrypt)
{
    if (!IVSet)
    {
        throw new Exception("IV not set.");
    }
    int paddedLen = (text.Length % 8 == 0 ? text.Length : text.Length + 8 - (text.Length % 8));
    byte[] plainText = new byte[paddedLen];
    Buffer.BlockCopy(text, 0, plainText, 0, text.Length);
    byte[] block = new byte[8];
    byte[] preblock = new byte[8];
    byte[] iv = new byte[8];
    Buffer.BlockCopy(InitVector, 0, iv, 0, 8);
    if (!decrypt)
    {
        for (int i = 0; i < plainText.Length; i += 8)
        {
            Buffer.BlockCopy(plainText, i, block, 0, 8);
            XorBlock(ref block, iv);
            BlockEncrypt(ref block);
            Buffer.BlockCopy(block, 0, iv, 0, 8);
            Buffer.BlockCopy(block, 0, plainText, i, 8);
        }
    }
    else
    {
        for (int i = 0; i < plainText.Length; i += 8)
        {
            Buffer.BlockCopy(plainText, i, block, 0, 8);
```

```
            Buffer.BlockCopy(block, 0, preblock, 0, 8);
            BlockDecrypt(ref block);
            XorBlock(ref block, iv);
            Buffer.BlockCopy(preblock, 0, iv, 0, 8);

            Buffer.BlockCopy(block, 0, plainText, i, 8);
        }
    }
    return plainText;
}
/// <summary>
/// XoR encrypts two 8 bit blocks
/// </summary>
/// <param name="block">8 bit block 1</param>
/// <param name="iv">8 bit block 2</param>
private void XorBlock(ref byte[] block, byte[] iv)
{
    for (int i = 0; i < block.Length; i++)
    {
        block[i] ^= iv[i];
    }
}
/// <summary>
/// Encrypts a 64 bit block
/// </summary>
/// <param name="block">The 64 bit block to encrypt</param>
private void BlockEncrypt(ref byte[] block)
{
    SetBlock(block);
    encipher();
    GetBlock(ref block);
}
/// <summary>
/// Decrypts a 64 bit block
/// </summary>
/// <param name="block">The 64 bit block to decrypt</param>
private void BlockDecrypt(ref byte[] block)
```

```
{
    SetBlock(block);
    decipher();
    GetBlock(ref block);
}
/// <summary>
/// Splits the block into the two uint values
/// </summary>
/// <param name="block">the 64 bit block to setup</param>
private void SetBlock(byte[] block)
{
    byte[] block1 = new byte[4];
    byte[] block2 = new byte[4];
    Buffer.BlockCopy(block, 0, block1, 0, 4);
    Buffer.BlockCopy(block, 4, block2, 0, 4);
    //split the block
    if (nonStandardMethod)
    {
        xr_par = BitConverter.ToUInt32(block1, 0);
        xl_par = BitConverter.ToUInt32(block2, 0);
    }
    else
    {
        //ToUInt32 requires the bytes in reverse order
        Array.Reverse(block1);
        Array.Reverse(block2);
        xl_par = BitConverter.ToUInt32(block1, 0);
        xr_par = BitConverter.ToUInt32(block2, 0);
    }
}
/// <summary>
/// Converts the two uint values into a 64 bit block
/// </summary>
/// <param name="block">64 bit buffer to receive the block</param>
private void GetBlock(ref byte[] block)
{
    byte[] block1 = new byte[4];
```

```
    byte[] block2 = new byte[4];
    if (nonStandardMethod)
    {
        block1 = BitConverter.GetBytes(xr_par);
        block2 = BitConverter.GetBytes(xl_par);
    }
    else
    {
        block1 = BitConverter.GetBytes(xl_par);
        block2 = BitConverter.GetBytes(xr_par);
        //GetBytes returns the bytes in reverse order
        Array.Reverse(block1);
        Array.Reverse(block2);
    }
    //join the block
    Buffer.BlockCopy(block1, 0, block, 0, 4);
    Buffer.BlockCopy(block2, 0, block, 4, 4);
}
/// <summary>
/// Runs the blowfish algorithm (standard 16 rounds)
/// </summary>
private void encipher()
{
    xl_par ^= bf_P[0];
    for (uint i = 0; i < 16; i += 2)
    {
        xr_par = round(xr_par, xl_par, i + 1);
        xl_par = round(xl_par, xr_par, i + 2);
    }
    xr_par = xr_par ^ bf_P[17];
    //swap the blocks
    uint swap = xl_par;
    xl_par = xr_par;
    xr_par = swap;
}
/// <summary>
/// Runs the blowfish algorithm in reverse (standard 16 rounds)
```

```
        /// </summary>
        private void decipher()
        {
            xl_par ^= bf_P[17];
            for (uint i = 16; i > 0; i -= 2)
            {
                xr_par = round(xr_par, xl_par, i);
                xl_par = round(xl_par, xr_par, i - 1);
            }
            xr_par = xr_par ^ bf_P[0];
            //swap the blocks
            uint swap = xl_par;
            xl_par = xr_par;
            xr_par = swap;
        }
        /// <summary>
        /// one round of the blowfish algorithm
        /// </summary>
        /// <param name="a">See spec</param>
        /// <param name="b">See spec</param>
        /// <param name="n">See spec</param>
        /// <returns></returns>
        private uint round(uint a, uint b, uint n)
        {
            uint x1 = (bf_s0[wordByte0(b)] + bf_s1[wordByte1(b)]) ^ bf_s2[wordByte2(b)];
            uint x2 = x1 + bf_s3[this.wordByte3(b)];
            uint x3 = x2 ^ bf_P[n];
            return x3 ^ a;
        }
        #endregion
        #region SBLOCKS
        //SBLOCKS ARE THE HEX DIGITS OF PI.
        //The amount of hex digits can be increased if you want to experiment with more rounds and longer key lengths
        private uint[] SetupP()
        {
            return new uint[] {
```

```
        0x243f6a88,0x85a308d3,0x13198a2e,0x03707344,0xa4093822,0x299f31d0,
            0x082efa98,0xec4e6c89,0x452821e6,0x38d01377,0xbe5466cf,0x34e90c6c,
            0xc0ac29b7,0xc97c50dd,0x3f84d5b5,0xb5470917,0x9216d5d9,0x8979fb1b
    };
}
private uint[] SetupS0()
{
    return new uint[] {
            0xd1310ba6,0x98dfb5ac,0x2ffd72db,0xd01adfb7,0xb8e1afed,0x6a267e96,
            0xba7c9045,0xf12c7f99,0x24a19947,0xb3916cf7,0x0801f2e2,0x858efc16,
            0x636920d8,0x71574e69,0xa458fea3,0xf4933d7e,0x0d95748f,0x728eb658,
            0x718bcd58,0x82154aee,0x7b54a41d,0xc25a59b5,0x9c30d539,0x2af26013,
            0xc5d1b023,0x286085f0,0xca417918,0xb8db38ef,0x8e79dcb0,0x603a180e,
            0x6c9e0e8b,0xb01e8a3e,0xd71577c1,0xbd314b27,0x78af2fda,0x55605c60,
            0xe65525f3,0xaa55ab94,0x57489862,0x63e81440,0x55ca396a,0x2aab10b6,
            0xb4cc5c34,0x1141e8ce,0xa15486af,0x7c72e993,0xb3ee1411,0x636fbc2a,
            0x2ba9c55d,0x741831f6,0xce5c3e16,0x9b87931e,0xafd6ba33,0x6c24cf5c,
            0x7a325381,0x28958677,0x3b8f4898,0x6b4bb9af,0xc4bfe81b,0x66282193,
            0x61d809cc,0xfb21a991,0x487cac60,0x5dec8032,0xef845d5d,0xe98575b1,
            0xdc262302,0xeb651b88,0x23893e81,0xd396acc5,0x0f6d6ff3,0x83f44239,
            0x2e0b4482,0xa4842004,0x69c8f04a,0x9e1f9b5e,0x21c66842,0xf6e96c9a,
            0x670c9c61,0xabd388f0,0x6a51a0d2,0xd8542f68,0x960fa728,0xab5133a3,
            0x6eef0b6c,0x137a3be4,0xba3bf050,0x7efb2a98,0xa1f1651d,0x39af0176,
            0x66ca593e,0x82430e88,0x8cee8619,0x456f9fb4,0x7d84a5c3,0x3b8b5ebe,
            0xe06f75d8,0x85c12073,0x401a449f,0x56c16aa6,0x4ed3aa62,0x363f7706,
            0x1bfedf72,0x429b023d,0x37d0d724,0xd00a1248,0xdb0fead3,0x49f1c09b,
            0x075372c9,0x80991b7b,0x25d479d8,0xf6e8def7,0xe3fe501a,0xb6794c3b,
            0x976ce0bd,0x04c006ba,0xc1a94fb6,0x409f60c4,0x5e5c9ec2,0x196a2463,
            0x68fb6faf,0x3e6c53b5,0x1339b2eb,0x3b52ec6f,0x6dfc511f,0x9b30952c,
            0xcc814544,0xaf5ebd09,0xbee3d004,0xde334afd,0x660f2807,0x192e4bb3,
            0xc0cba857,0x45c8740f,0xd20b5f39,0xb9d3fbdb,0x5579c0bd,0x1a60320a,
            0xd6a100c6,0x402c7279,0x679f25fe,0xfb1fa3cc,0x8ea5e9f8,0xdb3222f8,
            0x3c7516df,0xfd616b15,0x2f501ec8,0xad0552ab,0x323db5fa,0xfd238760,
            0x53317b48,0x3e00df82,0x9e5c57bb,0xca6f8ca0,0x1a87562e,0xdf1769db,
            0xd542a8f6,0x287effc3,0xac6732c6,0x8c4f5573,0x695b27b0,0xbbca58c8,
            0xe1ffa35d,0xb8f011a0,0x10fa3d98,0xfd2183b8,0x4afcb56c,0x2dd1d35b,
            0x9a53e479,0xb6f84565,0xd28e49bc,0x4bfb9790,0xe1ddf2da,0xa4cb7e33,
```

```
            0x62fb1341,0xcee4c6e8,0xef20cada,0x36774c01,0xd07e9efe,0x2bf11fb4,
            0x95dbda4d,0xae909198,0xeaad8e71,0x6b93d5a0,0xd08ed1d0,0xafc725e0,
            0x8e3c5b2f,0x8e7594b7,0x8ff6e2fb,0xf2122b64,0x8888b812,0x900df01c,
            0x4fad5ea0,0x688fc31c,0xd1cff191,0xb3a8c1ad,0x2f2f2218,0xbe0e1777,
            0xea752dfe,0x8b021fa1,0xe5a0cc0f,0xb56f74e8,0x18acf3d6,0xce89e299,
            0xb4a84fe0,0xfd13e0b7,0x7cc43b81,0xd2ada8d9,0x165fa266,0x80957705,
            0x93cc7314,0x211a1477,0xe6ad2065,0x77b5fa86,0xc75442f5,0xfb9d35cf,
            0xebcdaf0c,0x7b3e89a0,0xd6411bd3,0xae1e7e49,0x00250e2d,0x2071b35e,
            0x226800bb,0x57b8e0af,0x2464369b,0xf009b91e,0x5563911d,0x59dfa6aa,
            0x78c14389,0xd95a537f,0x207d5ba2,0x02e5b9c5,0x83260376,0x6295cfa9,
            0x11c81968,0x4e734a41,0xb3472dca,0x7b14a94a,0x1b510052,0x9a532915,
            0xd60f573f,0xbc9bc6e4,0x2b60a476,0x81e67400,0x08ba6fb5,0x571be91f,
            0xf296ec6b,0x2a0dd915,0xb6636521,0xe7b9f9b6,0xff34052e,0xc5855664,
            0x53b02d5d,0xa99f8fa1,0x08ba4799,0x6e85076a
        };
    }
    private uint[] SetupS1()
    {
        return new uint[] {
            0x4b7a70e9,0xb5b32944,0xdb75092e,0xc4192623,0xad6ea6b0,0x49a7df7d,
            0x9cee60b8,0x8fedb266,0xecaa8c71,0x699a17ff,0x5664526c,0xc2b19ee1,
            0x193602a5,0x75094c29,0xa0591340,0xe4183a3e,0x3f54989a,0x5b429d65,
            0x6b8fe4d6,0x99f73fd6,0xa1d29c07,0xefe830f5,0x4d2d38e6,0xf0255dc1,
            0x4cdd2086,0x8470eb26,0x6382e9c6,0x021ecc5e,0x09686b3f,0x3ebaefc9,
            0x3c971814,0x6b6a70a1,0x687f3584,0x52a0e286,0xb79c5305,0xaa500737,
            0x3e07841c,0x7fdeae5c,0x8e7d44ec,0x5716f2b8,0xb03ada37,0xf0500c0d,
            0xf01c1f04,0x0200b3ff,0xae0cf51a,0x3cb574b2,0x25837a58,0xdc0921bd,
            0xd19113f9,0x7ca92ff6,0x94324773,0x22f54701,0x3ae5e581,0x37c2dadc,
            0xc8b57634,0x9af3dda7,0xa9446146,0x0fd0030e,0xecc8c73e,0xa4751e41,
            0xe238cd99,0x3bea0e2f,0x3280bba1,0x183eb331,0x4e548b38,0x4f6db908,
            0x6f420d03,0xf60a04bf,0x2cb81290,0x24977c79,0x5679b072,0xbcaf89af,
            0xde9a771f,0xd9930810,0xb38bae12,0xdccf3f2e,0x5512721f,0x2e6b7124,
            0x501adde6,0x9f84cd87,0x7a584718,0x7408da17,0xbc9f9abc,0xe94b7d8c,
            0xec7aec3a,0xdb851dfa,0x63094366,0xc464c3d2,0xef1c1847,0x3215d908,
            0xdd433b37,0x24c2ba16,0x12a14d43,0x2a65c451,0x50940002,0x133ae4dd,
            0x71dff89e,0x10314e55,0x81ac77d6,0x5f11199b,0x043556f1,0xd7a3c76b,
            0x3c11183b,0x5924a509,0xf28fe6ed,0x97f1fbfa,0x9ebabf2c,0x1e153c6e,
```

```
            0x86e34570,0xeae96fb1,0x860e5e0a,0x5a3e2ab3,0x771fe71c,0x4e3d06fa,
            0x2965dcb9,0x99e71d0f,0x803e89d6,0x5266c825,0x2e4cc978,0x9c10b36a,
            0xc6150eba,0x94e2ea78,0xa5fc3c53,0x1e0a2df4,0xf2f74ea7,0x361d2b3d,
            0x1939260f,0x19c27960,0x5223a708,0xf71312b6,0xebadfe6e,0xeac31f66,
            0xe3bc4595,0xa67bc883,0xb17f37d1,0x018cff28,0xc332ddef,0xbe6c5aa5,
            0x65582185,0x68ab9802,0xeecea50f,0xdb2f953b,0x2aef7dad,0x5b6e2f84,
            0x1521b628,0x29076170,0xecdd4775,0x619f1510,0x13cca830,0xeb61bd96,
            0x0334fe1e,0xaa0363cf,0xb5735c90,0x4c70a239,0xd59e9e0b,0xcbaade14,
            0xeecc86bc,0x60622ca7,0x9cab5cab,0xb2f3846e,0x648b1eaf,0x19bdf0ca,
            0xa02369b9,0x655abb50,0x40685a32,0x3c2ab4b3,0x319ee9d5,0xc021b8f7,
            0x9b540b19,0x875fa099,0x95f7997e,0x623d7da8,0xf837889a,0x97e32d77,
            0x11ed935f,0x16681281,0x0e358829,0xc7e61fd6,0x96dedfa1,0x7858ba99,
            0x57f584a5,0x1b227263,0x9b83c3ff,0x1ac24696,0xcdb30aeb,0x532e3054,
            0x8fd948e4,0x6dbc3128,0x58ebf2ef,0x34c6ffea,0xfe28ed61,0xee7c3c73,
            0x5d4a14d9,0xe864b7e3,0x42105d14,0x203e13e0,0x45eee2b6,0xa3aaabea,
            0xdb6c4f15,0xfacb4fd0,0xc742f442,0xef6abbb5,0x654f3b1d,0x41cd2105,
            0xd81e799e,0x86854dc7,0xe44b476a,0x3d816250,0xcf62a1f2,0x5b8d2646,
            0xfc8883a0,0xc1c7b6a3,0x7f1524c3,0x69cb7492,0x47848a0b,0x5692b285,
            0x095bbf00,0xad19489d,0x1462b174,0x23820e00,0x58428d2a,0x0c55f5ea,
            0x1dadf43e,0x233f7061,0x3372f092,0x8d937e41,0xd65fecf1,0x6c223bdb,
            0x7cde3759,0xcbee7460,0x4085f2a7,0xce77326e,0xa6078084,0x19f8509e,
            0xe8efd855,0x61d99735,0xa969a7aa,0xc50c06c2,0x5a04abfc,0x800bcadc,
            0x9e447a2e,0xc3453484,0xfdd56705,0x0e1e9ec9,0xdb73dbd3,0x105588cd,
            0x675fda79,0xe3674340,0xc5c43465,0x713e38d8,0x3d28f89e,0xf16dff20,
            0x153e21e7,0x8fb03d4a,0xe6e39f2b,0xdb83adf7
    };
}
private uint[] SetupS2()
{
    return new uint[] {
        0xe93d5a68,0x948140f7,0xf64c261c,0x94692934,0x411520f7,0x7602d4f7,
            0xbcf46b2e,0xd4a20068,0xd4082471,0x3320f46a,0x43b7d4b7,0x500061af,
            0x1e39f62e,0x97244546,0x14214f74,0xbf8b8840,0x4d95fc1d,0x96b591af,
            0x70f4ddd3,0x66a02f45,0xbfbc09ec,0x03bd9785,0x7fac6dd0,0x31cb8504,
            0x96eb27b3,0x55fd3941,0xda2547e6,0xabca0a9a,0x28507825,0x530429f4,
            0x0a2c86da,0xe9b66dfb,0x68dc1462,0xd7486900,0x680ec0a4,0x27a18dee,
            0x4f3ffea2,0xe887ad8c,0xb58ce006,0x7af4d6b6,0xaace1e7c,0xd3375fec,
```

```
    0xce78a399,0x406b2a42,0x20fe9e35,0xd9f385b9,0xee39d7ab,0x3b124e8b,
    0x1dc9faf7,0x4b6d1856,0x26a36631,0xeae397b2,0x3a6efa74,0xdd5b4332,
    0x6841e7f7,0xca7820fb,0xfb0af54e,0xd8feb397,0x454056ac,0xba489527,
    0x55533a3a,0x20838d87,0xfe6ba9b7,0xd096954b,0x55a867bc,0xa1159a58,
    0xcca92963,0x99e1db33,0xa62a4a56,0x3f3125f9,0x5ef47e1c,0x9029317c,
    0xfdf8e802,0x04272f70,0x80bb155c,0x05282ce3,0x95c11548,0xe4c66d22,
    0x48c1133f,0xc70f86dc,0x07f9c9ee,0x41041f0f,0x404779a4,0x5d886e17,
    0x325f51eb,0xd59bc0d1,0xf2bcc18f,0x41113564,0x257b7834,0x602a9c60,
    0xdff8e8a3,0x1f636c1b,0x0e12b4c2,0x02e1329e,0xaf664fd1,0xcad18115,
    0x6b2395e0,0x333e92e1,0x3b240b62,0xeebeb922,0x85b2a20e,0xe6ba0d99,
    0xde720c8c,0x2da2f728,0xd0127845,0x95b794fd,0x647d0862,0xe7ccf5f0,
    0x5449a36f,0x877d48fa,0xc39dfd27,0xf33e8d1e,0x0a476341,0x992eff74,
    0x3a6f6eab,0xf4f8fd37,0xa812dc60,0xa1ebddf8,0x991be14c,0xdb6e6b0d,
    0xc67b5510,0x6d672c37,0x2765d43b,0xdcd0e804,0xf1290dc7,0xcc00ffa3,
    0xb5390f92,0x690fed0b,0x667b9ffb,0xcedb7d9c,0xa091cf0b,0xd9155ea3,
    0xbb132f88,0x515bad24,0x7b9479bf,0x763bd6eb,0x37392eb3,0xcc115979,
    0x8026e297,0xf42e312d,0x6842ada7,0xc66a2b3b,0x12754ccc,0x782ef11c,
    0x6a124237,0xb79251e7,0x06a1bbe6,0x4bfb6350,0x1a6b1018,0x11caedfa,
    0x3d25bdd8,0xe2e1c3c9,0x44421659,0x0a121386,0xd90cec6e,0xd5abea2a,
    0x64af674e,0xda86a85f,0xbebfe988,0x64e4c3fe,0x9dbc8057,0xf0f7c086,
    0x60787bf8,0x6003604d,0xd1fd8346,0xf6381fb0,0x7745ae04,0xd736fccc,
    0x83426b33,0xf01eab71,0xb0804187,0x3c005e5f,0x77a057be,0xbde8ae24,
    0x55464299,0xbf582e61,0x4e58f48f,0xf2ddfda2,0xf474ef38,0x8789bdc2,
    0x5366f9c3,0xc8b38e74,0xb475f255,0x46fcd9b9,0x7aeb2661,0x8b1ddf84,
    0x846a0e79,0x915f95e2,0x466e598e,0x20b45770,0x8cd55591,0xc902de4c,
    0xb90bace1,0xbb8205d0,0x11a86248,0x7574a99e,0xb77f19b6,0xe0a9dc09,
    0x662d09a1,0xc4324633,0xe85a1f02,0x09f0be8c,0x4a99a025,0x1d6efe10,
    0x1ab93d1d,0x0ba5a4df,0xa186f20f,0x2868f169,0xdcb7da83,0x573906fe,
    0xa1e2ce9b,0x4fcd7f52,0x50115e01,0xa70683fa,0xa002b5c4,0x0de6d027,
    0x9af88c27,0x773f8641,0xc3604c06,0x61a806b5,0xf0177a28,0xc0f586e0,
    0x006058aa,0x30dc7d62,0x11e69ed7,0x2338ea63,0x53c2dd94,0xc2c21634,
    0xbbcbee56,0x90bcb6de,0xebfc7da1,0xce591d76,0x6f05e409,0x4b7c0188,
    0x39720a3d,0x7c927c24,0x86e3725f,0x724d9db9,0x1ac15bb4,0xd39eb8fc,
    0xed545578,0x08fca5b5,0xd83d7cd3,0x4dad0fc4,0x1e50ef5e,0xb161e6f8,
    0xa28514d9,0x6c51133c,0x6fd5c7e7,0x56e14ec4,0x362abfce,0xddc6c837,
    0xd79a3234,0x92638212,0x670efa8e,0x406000e0
};
```

```
}
private uint[] SetupS3()
{
   return new uint[] {
         0x3a39ce37,0xd3faf5cf,0xabc27737,0x5ac52d1b,0x5cb0679e,0x4fa33742,
         0xd3822740,0x99bc9bbe,0xd5118e9d,0xbf0f7315,0xd62d1c7e,0xc700c47b,
         0xb78c1b6b,0x21a19045,0xb26eb1be,0x6a366eb4,0x5748ab2f,0xbc946e79,
         0xc6a376d2,0x6549c2c8,0x530ff8ee,0x468dde7d,0xd5730a1d,0x4cd04dc6,
         0x2939bbdb,0xa9ba4650,0xac9526e8,0xbe5ee304,0xa1fad5f0,0x6a2d519a,
         0x63ef8ce2,0x9a86ee22,0xc089c2b8,0x43242ef6,0xa51e03aa,0x9cf2d0a4,
         0x83c061ba,0x9be96a4d,0x8fe51550,0xba645bd6,0x2826a2f9,0xa73a3ae1,
         0x4ba99586,0xef5562e9,0xc72fefd3,0xf752f7da,0x3f046f69,0x77fa0a59,
         0x80e4a915,0x87b08601,0x9b09e6ad,0x3b3ee593,0xe990fd5a,0x9e34d797,
         0x2cf0b7d9,0x022b8b51,0x96d5ac3a,0x017da67d,0xd1cf3ed6,0x7c7d2d28,
         0x1f9f25cf,0xadf2b89b,0x5ad6b472,0x5a88f54c,0xe029ac71,0xe019a5e6,
         0x47b0acfd,0xed93fa9b,0xe8d3c48d,0x283b57cc,0xf8d56629,0x79132e28,
         0x785f0191,0xed756055,0xf7960e44,0xe3d35e8c,0x15056dd4,0x88f46dba,
         0x03a16125,0x0564f0bd,0xc3eb9e15,0x3c9057a2,0x97271aec,0xa93a072a,
         0x1b3f6d9b,0x1e6321f5,0xf59c66fb,0x26dcf319,0x7533d928,0xb155fdf5,
         0x03563482,0x8aba3cbb,0x28517711,0xc20ad9f8,0xabcc5167,0xccad925f,
         0x4de81751,0x3830dc8e,0x379d5862,0x9320f991,0xea7a90c2,0xfb3e7bce,
         0x5121ce64,0x774fbe32,0xa8b6e37e,0xc3293d46,0x48de5369,0x6413e680,
         0xa2ae0810,0xdd6db224,0x69852dfd,0x09072166,0xb39a460a,0x6445c0dd,
         0x586cdecf,0x1c20c8ae,0x5bbef7dd,0x1b588d40,0xccd2017f,0x6bb4e3bb,
         0xdda26a7e,0x3a59ff45,0x3e350a44,0xbcb4cdd5,0x72eacea8,0xfa6484bb,
         0x8d6612ae,0xbf3c6f47,0xd29be463,0x542f5d9e,0xaec2771b,0xf64e6370,
         0x740e0d8d,0xe75b1357,0xf8721671,0xaf537d5d,0x4040cb08,0x4eb4e2cc,
         0x34d2466a,0x0115af84,0xe1b00428,0x95983a1d,0x06b89fb4,0xce6ea048,
         0x6f3f3b82,0x3520ab82,0x011a1d4b,0x277227f8,0x611560b1,0xe7933fdc,
         0xbb3a792b,0x344525bd,0xa08839e1,0x51ce794b,0x2f32c9b7,0xa01fbac9,
         0xe01cc87e,0xbcc7d1f6,0xcf0111c3,0xa1e8aac7,0x1a908749,0xd44fbd9a,
         0xd0dadecb,0xd50ada38,0x0339c32a,0xc6913667,0x8df9317c,0xe0b12b4f,
         0xf79e59b7,0x43f5bb3a,0xf2d519ff,0x27d9459c,0xbf97222c,0x15e6fc2a,
         0x0f91fc71,0x9b941525,0xfae59361,0xceb69ceb,0xc2a86459,0x12baa8d1,
         0xb6c1075e,0xe3056a0c,0x10d25065,0xcb03a442,0xe0ec6e0e,0x1698db3b,
         0x4c98a0be,0x3278e964,0x9f1f9532,0xe0d392df,0xd3a0342b,0x8971f21e,
         0x1b0a7441,0x4ba3348c,0xc5be7120,0xc37632d8,0xdf359f8d,0x9b992f2e,
```

```
            0xe60b6f47,0x0fe3f11d,0xe54cda54,0x1edad891,0xce6279cf,0xcd3e7e6f,
            0x1618b166,0xfd2c1d05,0x848fd2c5,0xf6fb2299,0xf523f357,0xa6327623,
            0x93a83531,0x56cccd02,0xacf08162,0x5a75ebb5,0x6e163697,0x88d273cc,
            0xde966292,0x81b949d0,0x4c50901b,0x71c65614,0xe6c6c7bd,0x327a140a,
            0x45e1d006,0xc3f27b9a,0xc9aa53fd,0x62a80f00,0xbb25bfe2,0x35bdd2f6,
            0x71126905,0xb2040222,0xb6cbcf7c,0xcd769c2b,0x53113ec0,0x1640e3d3,
            0x38abbd60,0x2547adf0,0xba38209c,0xf746ce76,0x77afa1c5,0x20756060,
            0x85cbfe4e,0x8ae88dd8,0x7aaaf9b0,0x4cf9aa7e,0x1948c25c,0x02fb8a8c,
            0x01c36ae4,0xd6ebe1f9,0x90d4f869,0xa65cdea0,0x3f09252d,0xc208e69f,
            0xb74e6132,0xce77e25b,0x578fdfe3,0x3ac372e6
    };
}
#endregion
#region Conversions
//gets the first byte in a uint
private byte wordByte0(uint w)
{
    return (byte)(w / 256 / 256 / 256 % 256);
}
//gets the second byte in a uint
private byte wordByte1(uint w)
{
    return (byte)(w / 256 / 256 % 256);
}
//gets the third byte in a uint
private byte wordByte2(uint w)
{
    return (byte)(w / 256 % 256);
}
//gets the fourth byte in a uint
private byte wordByte3(uint w)
{
    return (byte)(w % 256);
}
//converts a byte array to a hex string
private string ByteToHex(byte[] bytes)
{
```

```
            StringBuilder s = new StringBuilder();
            foreach (byte b in bytes)
                s.Append(b.ToString("x2"));
            return s.ToString();
        }
        //converts a hex string to a byte array
        private byte[] HexToByte(string hex)
        {
            byte[] r = new byte[hex.Length / 2];
            for (int i = 0; i < hex.Length - 1; i += 2)
            {
                byte a = GetHex(hex[i]);
                byte b = GetHex(hex[i + 1]);
                r[i / 2] = (byte)(a * 16 + b);
            }
            return r;
        }
        //converts a single hex character to it's decimal value
        private byte GetHex(char x)
        {
            if (x <= '9' && x >= '0')
            {
                return (byte)(x - '0');
            }
            else if (x <= 'z' && x >= 'a')
            {
                return (byte)(x - 'a' + 10);
            }
            else if (x <= 'Z' && x >= 'A')
            {
                return (byte)(x - 'A' + 10);
            }
            return 0;
        }
        #endregion
    }
}
```

ДОДАТОК Б

СЛАЙДИ ПРЕЗЕНТАЦІЇ

АТЕСТАЦІЙНА РОБОТА

Дослідження та оцінка ефективності алгоритмів шифрування, що використовуються в технології Блокчейн

1

- Метою роботи є вирішення науково-практичної задачі аналізу та оцінки ефективності алгоритмів шифрування при створенні смарт контрактів, що застосовуються у технології блокчейн, для попереджування неочікуваних наслідків від наявних вразливих місць та всіляких загроз.
- Об'єктом дослідження є оцінка ефективності алгоритмів шифрування, що використовуються в технології блокчейн.
- Предметом дослідження є алгоритми шифрування даних, які можуть бути використані у смарт контрактах.
- Методи досліджень. Теоретичною базою виконаних досліджень є фундаментальні положення теорії алгоритмів та теорії статистичного аналізу, методи математичного моделювання, порівняльний аналіз предмету досліджень, що застосовються і можуть бути запропоновані для майбутнього використання.

2

Завдання роботи

- проаналізувати і порівняти існуючі алгоритми і системи шифрування даних з точки зору предмета дослідження;
- дослідити смарт-контракти, що застосовуються у технології блокчейн;
- розробити власний блокчейн;
- визначити як працює блокчейн з алгоритмами шифрування та запропонувати ефективніший алгоритм, який дозволить підвищити надійність і рівень безпеки для блокчейну.

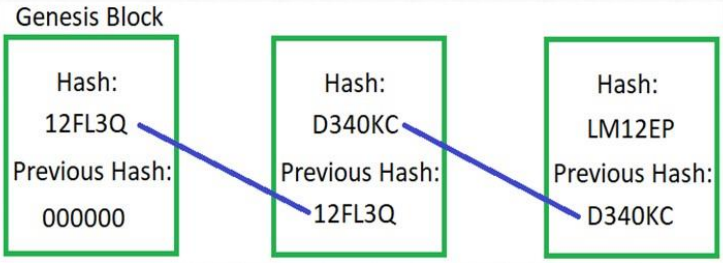
3

Дослідження в області

Проблемам вивчення ефективності алгоритмів шифрування присвячено чимало досліджень. Серед останніх робіт у цій галузі слід відмітити праці А. Єлізарова [5], дослідження Ю. Мінгальова [15], С. Кос [34], М. Лапіна [12], О. Г. Качко [6] та інших. Однак всі перелічені роботи розглядають алгоритми шифрування з огляду на криптостійкість та швидкодію у межах конкретних замкнених систем кожного з алгоритмів, а не у межах технології блокчейну, або смарт контрактах. Тому вважаємо актуальним питання дослідження та оцінки ефективності алгоритмів шифрування, що використовуються в технології блокчейн.

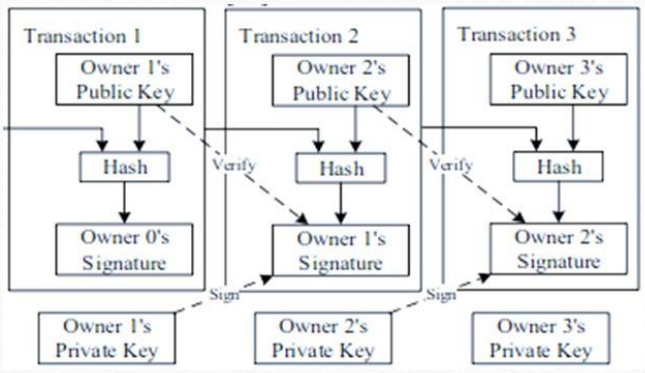
4

Блокчейн


Genesis Block
Hash:
12FL3Q
Previous Hash:
000000
Hash:
D340KC
Previous Hash:
12FL3Q
Hash:
LM12EP
Previous Hash:
D340KC

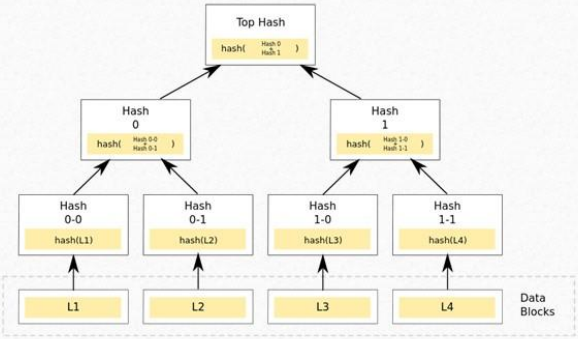
5


Блок
Заголовок блоку
...
Хеш транзакцій
Хеш 12
Хеш 34
Хеш 1
Хеш 2
Хеш 3
Хеш 4
Транзакція 1
Транзакція 2
Транзакція 3
Транзакція 4


Transaction 1
Owner 1's Public Key
Hash
Owner 0's Signature
Owner 1's Private Key
Transaction 2
Owner 2's Public Key
Hash
Owner 1's Signature
Owner 2's Private Key
Transaction 3
Owner 3's Public Key
Hash
Owner 2's Signature
Owner 3's Private Key
Verify
Verify
Sign
Sign

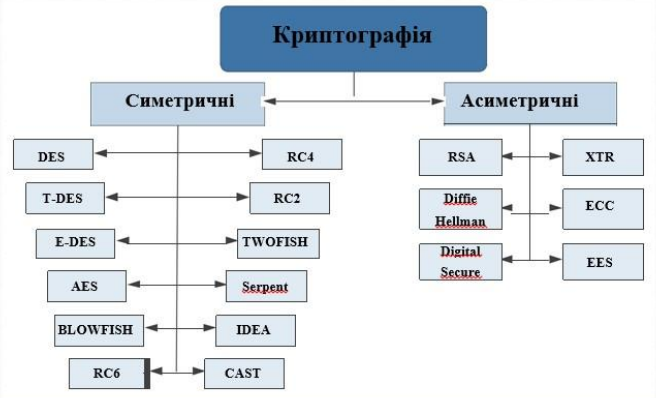
6

Дерево Меркле

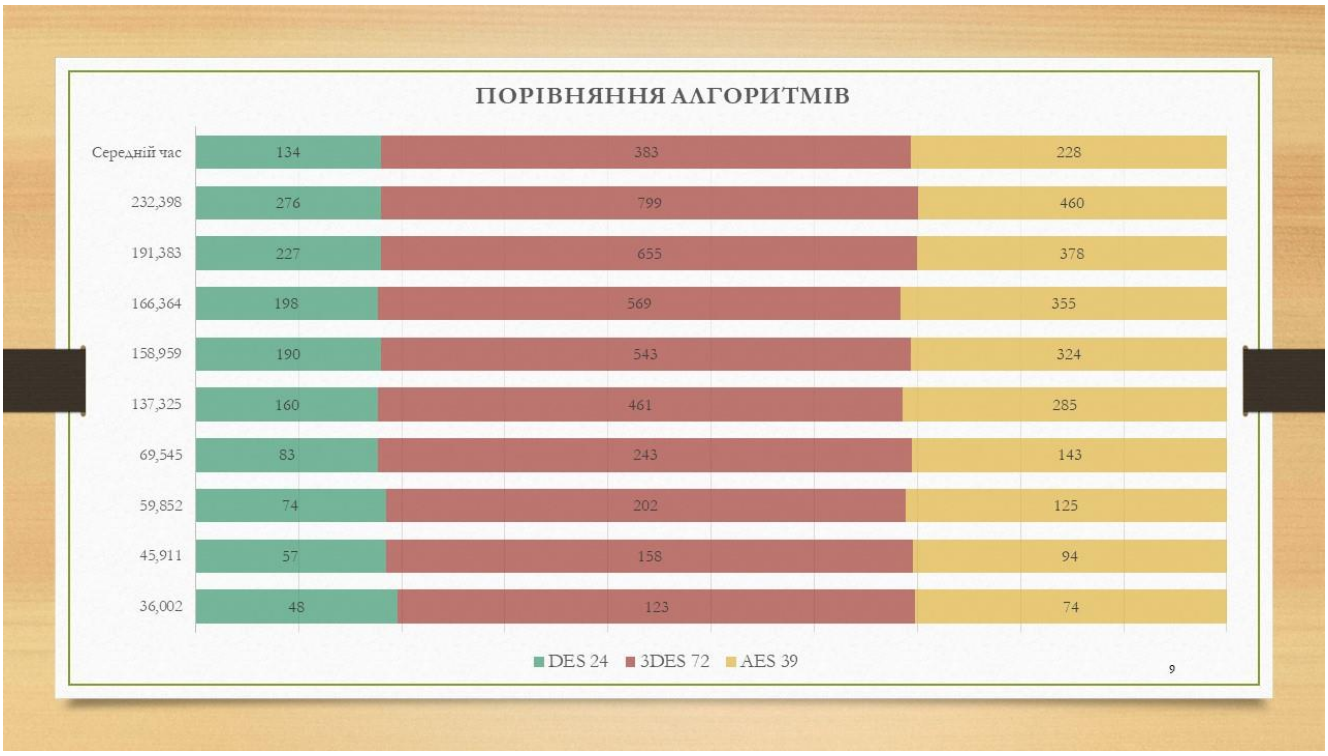


7

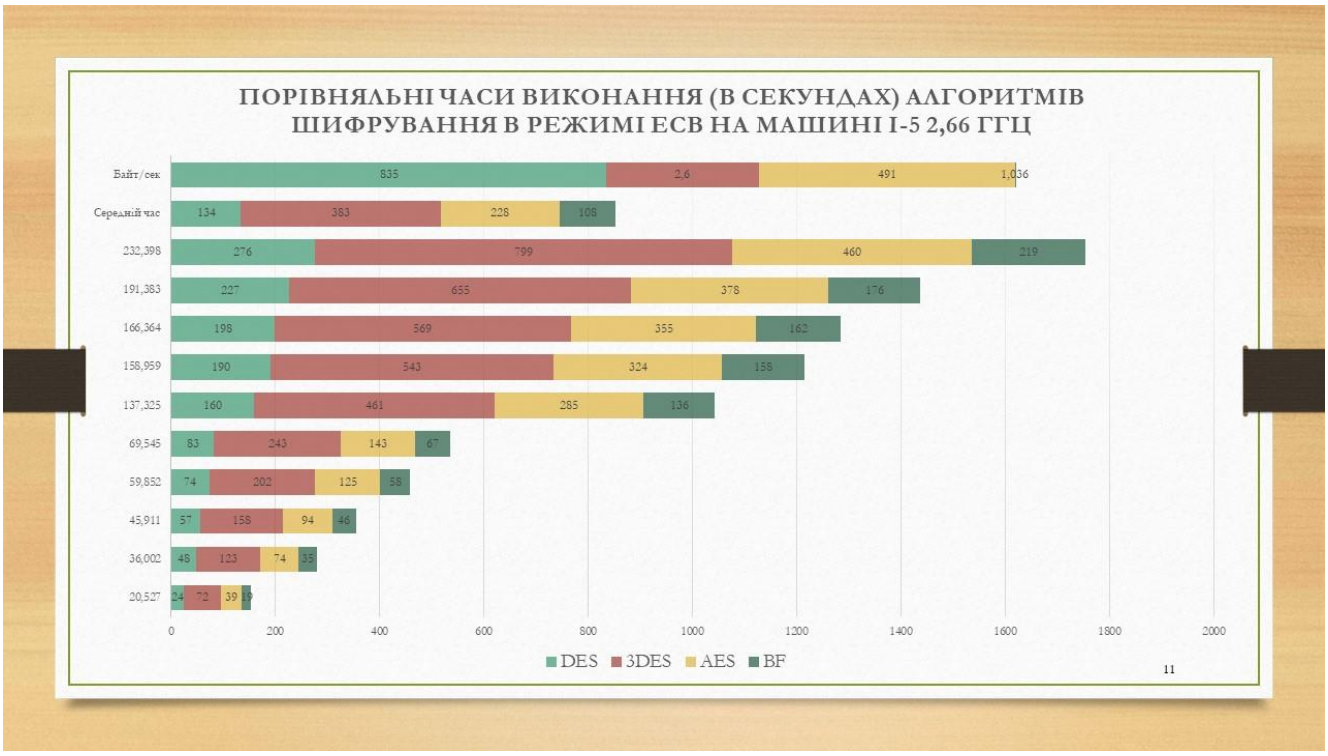
Класифікація алгоритмів шифрування

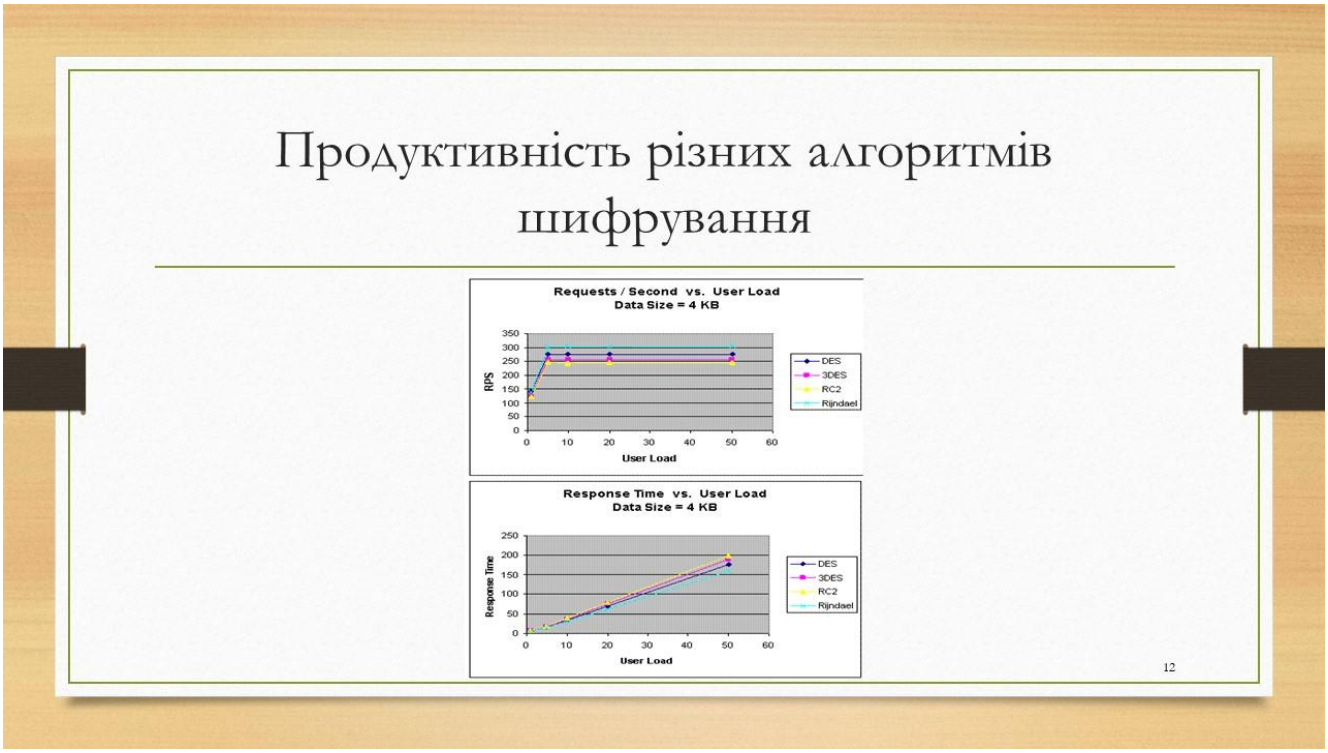


8

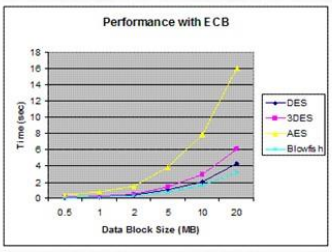

ПОРІВНЯННЯ АЛГОРИТМІВ
Середній час
232,398
191,383
166,364
158,959
137,325
69,545
59,852
45,911
36,002
134
383
228
276
799
460
227
655
378
198
569
355
190
543
324
160
461
285
83
243
143
74
202
125
57
158
94
48
123
74
DES 24
3DES 72
AES 39
9


ПОРІВНЯЛЬНИЙ ЧАС ВИКОНАННЯ (В СЕКУНДАХ) АЛГОРИТМІВ ШИФРУВАННЯ В РЕЖИМІ ECB НА МАШИНІ I-5 2,4 ГГЦ
Байт/сек
Середній час
232,398
191,383
166,364
158,959
137,325
69,545
59,852
45,911
36,002
20,527
5,32
10,167
7,9882
21
11
14
42
44
24
30
87
36
19
24
72
31
17
21
62
30
16
20
60
26
14
17
51
13
7
9
26
11
6
7
23
8
4
5
17
6
3
4
13
4
2
2
7
0
20
40
60
80
100
120
140
160
180
200
AES
BF
DES
3DES
10

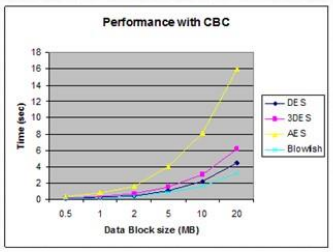

ПОРІВНЯЛЬНІ ЧАСИ ВИКОНАННЯ (В СЕКУНДАХ) АЛГОРИТМІВ ШИФРУВАННЯ В РЕЖИМІ ECB НА МАШИНІ I-5 2,66 ГГЦ
Байт/сек
Середній час
232,398
191,383
166,364
158,959
137,325
69,545
59,852
45,911
36,002
20,527
835
2,6
491
1,036
134
383
228
108
276
799
460
219
227
655
378
176
198
569
355
162
190
543
324
158
160
461
285
136
83
243
143
67
74
202
125
58
57
158
94
46
48
123
74
35
24
72
39
0
200
400
600
800
1000
1200
1400
1600
1800
2000
DES
3DES
AES
BF
11


Продуктивність різних алгоритмів шифрування
Requests / Second vs. User Load
Data Size = 4 KB
RPS
User Load
DES
3DES
RC2
Rijndael
Response Time vs. User Load
Data Size = 4 KB
Response Time
User Load
DES
3DES
RC2
Rijndael
12

Результати роботи в режимі ECB і в режимі CBC



Результати роботи в режимі ECB



Результати роботи в режимі CBC

13

Порівняння криптографійних алгоритмів

Алгоритм	Ким створений	Рік	Розмір ключа	Розмір блоку	Раунд	Структура	Складність	Функції
DES	IBM	1975	64 бітів	64 бітів	16	Фейстель	Ні	Не достатньо сильний
DH	Вітфілд Діфф і Мартін Гелман	1976	Змінна	-	-	Фейстель	-	Хороша безпека та швидкість
E-DES	IBM	1977	1024 бітів	128 бітів	16	Фейстель	-	Хороша безпека та швидкість
RSA	Рівест Шамір Адлеман	1977	1024 - 4096	128 бітів	1	Алгоритм відкритого ключа	Ні	Відмінна безпека та низька швидкість

14

Порівняння криптографійних алгоритмів

Алгоритм	Ким створений	Рік	Розмір ключа	Розмір блоку	Round	Структура	Складність	Функції
T-DES	IBM	1978	112 або 168	64 бітів	48	Фейстель	Так	Відмінна безпека та швидкість
ECC	Ніл Коблїц та Віктор Міллер	1985	Більше, ніж симетричні та змінні	Змінна	1	Алгоритм відкритого ключа	Так	Відмінна безпека та швидкість
EEE	Тахер Ельгамал	1985	1024 бітів	-	-	Алгоритм відкритого ключа	Так	Досить забезпечний і швидкісний
RC4	Рон Рівест	1987	Змінна	40-2048	256	Фейстель потік	Так	швидкий шифр
RC2	Рон Рівест	1987	8,128,64 за замовчуванням	64 бітів	16	Фейстель	-	Гарна та швидка безпека

15

Порівняння криптографійних алгоритмів

Алгоритм	Ким створений	Рік	Розмір ключа	Розмір блоку	Round	Структура	Складність	Функції
BLOWFISH	Брюс Шнайер	1993	32-448	64 бітів	16	Фейстель	Так	Швидкий шифр в SSL
SEAL	Філіп Рогавей та Дон Коппер-Сміт	1994	160 бітів	32 бітів	2	Алгоритм відкритого ключа	Так	Не сильна безпека і швидка швидкість
DSA	NIST	1997	Змінна	-	-	Алгоритм відкритого ключа	Так	Хороша безпека та швидкість
RC6	Рон Рівест та ін	1998	128 біт до 256 біт	128 бітів	20	Фейстель	Так	Хороша безпека
AES	Джоан Дейман та Інсент Ріджмен	1998	128,192,256 бітів	128 бітів	10,12,14	Перестановка заміни	Так	Безпека відмінна. Це найкраще в забезпеченні безпеки та шифрування

16

ВИСНОВКИ

В ході написання випускної кваліфікаційної роботи були вирішені всі поставлені завдання:

- По-перше, проаналівані і порівняні існуючі алгоритми і системи шифрування, а потім на підставі проведеного аналізу були відібрані чотири алгоритми для подальшого дослідження.
- По-друге, були досліджені смарт контракти та можливість поєднання смарт контрактів з обраними алгоритмами шифрування.
- По-третє, був розроблений власний блокчейн на прикладі онлайн гаманця для користувачів, в якому усі транзакції будуть проходити через блокчейн.
- По-четверте, було вивчено як алгоритми шифрування працюють з алгоритмами та вивчено криптостійкість, та швидкодія цих алгоритмів у блокчейні.
- По-п'яте, був обраний найкращий алгоритм для блокчейн – BlowFish, який виявився найбільш захищеним, швидким та показав найкращі результати на нагрузочне тестування.

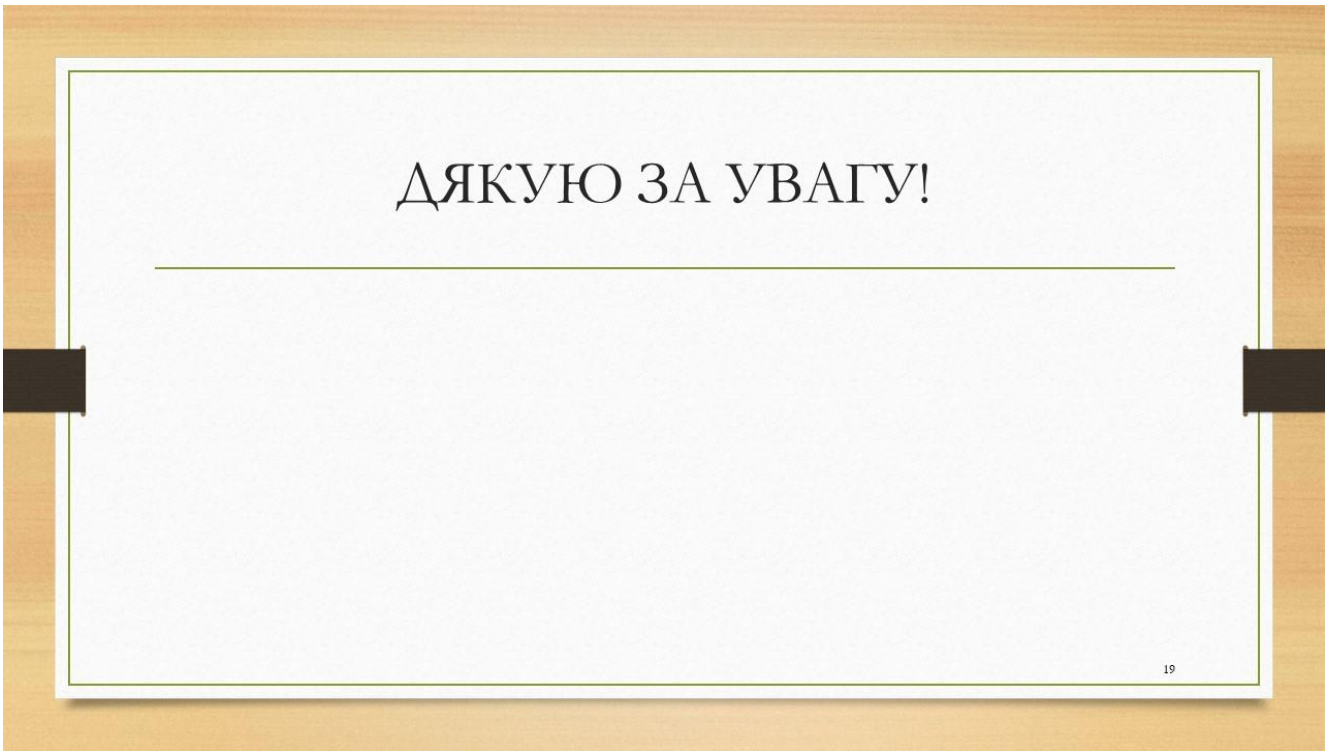
17

Апробація результатів дослідження

На тему дослідження було опубліковано сім статей та тез доповідей, зміст яких було викладено у періодичних фахових виданнях та на міжнародних науково-практичних конференціях, отримано свідоцтво про реєстрацію авторьского права на твір :

- konferencji medzynarodowej Naukowo-praktycznej «Rzwnój i praktyka. Inżynieria i technologia» (Zakopane (PL), 29.12.2017 р.);
- міжнародна Науково-технічна конференція «Інформаційні системи та технології» (ІСТ – 2017) (Коблево-Харків, 11-16 вересня, 2017 р.);
- 14-th International Scientific Conference «Intellectual Systems for Decision Making and Problems of Computational Intelligence» (ISDMCI'2018') (Kherson, 2018 р.);
- ІІ міжнародна Науково-практичнв конференція «Теорія і практика актуальних наукових досліджень» (м. Одеса, 28-29 квітня 2018 р.);
- 7-ма міжнародна науково-технічна конференція (Коблево - Харків, 2018 р.);
- міжнародна Науково-практична конференція «Інтелектуальні системи та інформаційні технології» (ISIT-2019) (Одеса, 19 – 24 серпня 2019 р.);
- 23-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті» (Харків, 2019 р.)

18


ДЯКУЮ ЗА УВАГУ!
19

ДОДАТОК В

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ

Міністерство економічного розвитку і торгівлі України

АВТОРСЬКЕ ПРАВО І СУМІЖНІ ПРАВА

Офіційний бюлетень № 49

Видається з 2002 року

Відомості, вміщені в даному бюлетені, вважаються опублікованими 27 липня 2018 р.

КНІВ – 2018

Авторське право і суміжні права. Офіційний бюлетень № 49, 2018

Номер свідоцтва про реєстрацію авторського права на твір	79820
Дата реєстрації авторського права	15.06.2018
Повне ім'я та/або псевдонім автора (авторів), чи позначення "Анонімно"	**Терещенко Глеб Юрійович**
Повне ім'я або повне офіційне найменування роботодавця	
Об'єкт авторського права, до якого належить твір	**Комп'ютерна програма**
Вид, повна та скорочена назва твору (творів)	**Комп'ютерна програма "Програмна система для перевірки достовірності якості товарів"**
Попередні дані для оприлюднення творів	
Анотація	**Даний програмний продукт є програмою для перевірки достовірності якості товарів. Метод реалізовано - платформа .NET, система розробки об'єктно-орієнтованих продуктів Microsoft Visual Studio 2017, мова програмування C#, а також система управління реляційною розподіленою базою даних.**

Номер свідоцтва про реєстрацію авторського права на твір	79821
Дата реєстрації авторського права	15.06.2018
Повне ім'я та/або псевдонім автора (авторів), чи позначення "Анонімно"	**Лисько Марина Миколаївна**
Повне ім'я або повне офіційне найменування роботодавця	
Об'єкт авторського права, до якого належить твір	**Твір образотворчого мистецтва**
Вид, повна та скорочена назва твору (творів)	**Графічне зображення "Зображення логотипу "Lamar"**
Попередні дані для оприлюднення творів	
Анотація	

Номер свідоцтва про реєстрацію авторського права на твір	79822
Дата реєстрації авторського права	15.06.2018
Повне ім'я та/або псевдонім автора (авторів), чи позначення "Анонімно"	**Жабєєв Володимир Павлович, Жабєєв Георгій Володимирович, Жабєєв Павло Володимирович, Жабєєва Ірина Анатоліївна**
Повне ім'я або повне офіційне найменування роботодавця	
Об'єкт авторського права, до якого належить твір	**Літературний письмовий твір науково характеру**
Вид, повна та скорочена назва твору (творів)	**Науково-літературний твір "Стаття "Знешкодження ратункового навантаження на земельні ресурси територіальних громад шляхом** 738

СОДЕРЖАНИЕ

ISSN 0555-2656

БИОНИКА ИНТЕЛЛЕКТА

ИНФОРМАЦИЯ, ЯЗЫК, ИНТЕЛЛЕКТ

№ 1 (92) 2019

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Основан в октябре 1967 г.

Учредитель и издатель
Харьковский национальный университет радиоэлектроники

Периодичность издания – *2 раза в год*

Харьков • ХНУРЭ • 2019

decentralized system for exchanging, storing and processing data. Or about the blockchain. The well-known advantages of the new technology are that it is possible to deposit authorship without the participation of a third party and without binding to geography. In the decentralized registry, you can store information about the output parameters of the author's object, as well as the object itself (or its digital imprint, if you need to save on the volume of the file blockchain). The authenticity of the object is confirmed by a cryptographic guarantee - a kind of digital seal. There are several startups that implement the certification of documents uploaded to a distributed database. Potentially, they will be able to solve, for example, the question of the authenticity of the authorship of photographs, which are purchased in stock shops. Such mechanisms can be used to write to the block and the right to own a licensed software (and check the license by the manufacturer or automatically when connected to the blockchain).

A revolution, or at least tectonic shifts, is called blockchain in the music industry. The fact is that everything related to royalties paid to the author of a musical work is a very complex and often opaque process. Blockchain and smart contracts solve this problem, as they eliminate the functions of organizations managing copyright and related rights - no more mediators, and hence distortions and additional costs. This is especially true for unknown performers who are just starting their career - these musicians simply do not have the money to enter into contracts with major labels.

However, entering into a certain state or non-state register can be useful for a number of purposes, including facilitating the receipt by users of information about the current rightholder. There may well be a prospect for using a detachment [3].

For example, downloading a movie (book, program) from the Internet, you along with it can get information about the current copyright holder and the terms of his public license (that is, how much you have to pay for downloading). If proper software is available, the download itself may be carried out upon payment in accordance with these conditions. Or, based on this technology, you can organize the exchange of electronic copies of movies (books, etc.), if, of course, this is the permission of the original copyright holder. Then users will be able to transfer files to each other (as the bitcoins are being transmitted right now), similar to how a paper book or a movie disc is transmitted. Including for money (real or virtual).

Each content unit has its own price. Actions in many content platforms on the blockchain, for example "Voice", are reduced to money. That is, each unit of text, each photo, a comment in the system is automatically assigned a certain amount. This amount can grow depending on how other users interact with this content: read it or create something new based on it. That is, each unit of text, each photo, a comment in the system is automatically assigned a certain amount

The author can choose the appropriate privacy policy for each content unit. When a user simply enters the block with the author's text, the author receives a reward. When the reader wants to use a fragment of the text for his own purposes, he chooses the appropriate item (if it is provided for by the privacy policy) and the author gets even more reward.

In addition, information about the source (author) of the text fragment will be in the chain with the new content created on its basis. But here is another thing.

Content-platforms on the blockchain themselves monitor the observance of your copyright. After the content unit is created and published in the system, it is assigned a code that is automatically "checked for uniqueness" for all units of the block system. You correctly understood: after adding each new element the whole system is updated.

It's as if Google were updating its search engine after the next page appeared. Only much, much faster. First of all, due to the fact that all data is not on any servers, like Google, but distributed among all participants of the block system. That is everywhere and nowhere at the same time.

Since your most evil critic is yourself in a year, many blockchain based content platforms open up opportunities for editing or deleting blocks with content without destroying the whole chain. Such developments are, for example, in Bandcamp and Accenture. That is where, the block will disappear, but if the deleted text fragment has already been used somewhere, information about you as an author will be preserved. This is what Americans call "legacy", a legacy. The bad news: no one will forget what you wrote that night. Good: you can manage content as a valuable asset, bequeathing it to heirs.

The principle of blockchain solves a very important issue in the world of information domination over the individual: how to preserve mercantilist benefits and leave a trace in history without investing in a PR brand, simply doing its own thing. In order to earn more, the author can assign any meta tags to the content units, improving their visibility in the system, but in the top of the tape there will still be texts with the greatest number of interactions from real users-backers. No cheat from the bots.

Blockchain can offer revolutionary changes for marketing, but this has never come into fashion among marketers and has not become a trend, like Snapchat and online video.

UDK 004.89

Bilous N.[1], Tereshchenko G.[2], Kyrychenko I.[3]

[1] Candidate of Technical Sciences, Professor of Software Engineering Department, Kharkov National University of Radio Electronics, nataliya.bilous@nure.ua, ORCID iD: 0000-0002-8850-9316

[2] Graduate students of the Department of Software Engineering, Kharkov National University of Radio Electronics, hlib.tereshchenko@nure.ua, ORCID iD: 0000-0001-8731-2135

[3] Candidate of Technical Sciences, Assistant of the Department of Software Engineering, Kharkov National University of Radio Electronics, iryna.kyrychenko@nure.ua, ORCID iD: 0000-0002-7686-6439

COPYRIGHT PROTECTION USING BLOCKCHAIN

This article examines the potential and limitations of blockchain technology and blockchain-based smart contracts in relation to copyright. Copyright has long been enforced through technological means, specifically Digital Rights Management. With the emergence of blockchains, many are now predicting a new era regarding the administration and enforcement of copyright through computer code. The article introduces the technology and related potential and limitations while stressing its capacity to act as a form of normative ordering that can express public or private objectives.

DIGITAL RIGHTS MANAGEMENT, COPYRIGHT, BLOCKCHAIN, SMART CONTRACTS, PRIVATE ORDERING, PERMITTED USES

Introduction

Current issue for today is who will regulate the author's and property issues in the 21st century. The matter concerns not only works of art and science, it concerns even your things, houses, motorcycles. Who or what will control the property and legal documents in the 21st century?

It is clear that this will not deal with the old market with offices and corporations dictating the conditions. Publishers, producers, promoters and PR people will be forced to look for new ways to earn on air and adapt to the growth of individualism, which is so often labeled "Western" and advised to get rid of many religions of the world. A system where the majority has to put up with the rules for the dissemination of information and goods, imposed by several large uncles, is a thing of the past.

And perhaps you ask: why so many people are deprive of work? After all, many will have a hard time, when it is impossible to earn on the fruits of someone else's work and creativity. Well, firstly, while the author receives "interest from sales" the media giant has superprofits, which it is sometimes so convenient to hide. This is not fair to the author. Secondly, if the authors themselves are not against the free circulation of everything being created, and some of them are even actively advocating, we must clearly understand and admit that we have the right to reform [1].

In addition, some products of creativity can impose cryptographic methods of protection. In the New World there will be no bloody revolution, the technology itself will make some ideas obsolete and others will be relevant, and since technology is inextricably linked with progress, if it is not weapon technology, it will only move it forward by overcoming artificial restrictions: superstitions, religion, ideology, dogma, titles, titles, legislative prohibitions, important pathos, and so on.

1. Blockchain

Blockchain — is a decentralized database, the storage devices of which are not connected to a shared server. Any member of the system can make records in it, which after verification are automatically displayed on all computers on the network. Thus, the main advantage of the blockchain is the safety of the information stored in it [2]. No one can forge or replace it, as unilateral changes on each of the network devices will require huge computing capabilities that are not available to the ordinary participant of the system. In the field of intellectual property (IP) protection, the technology will provide safe storage and prompt updating of information about any IP objects: from a patent for high-tech development to a musical work.

2. Copyright protection

The system for the protection of trademarks and patents is currently based on registers of rights to IP objects maintained by authorized state bodies. It is also important here that when entering the above-mentioned registers, non-trivial manual work should be performed to verify the IP object for protection. The system for the protection of trademarks and patents is currently based on registers of rights to IP objects maintained by authorized state bodies. It is also important here that when entering the above-mentioned registers, non-trivial manual work should be performed to verify the IP object for protection. Strange as it may seem, new technologies, some of which are called cryptoanarchic, came to the right holder to help. This is a

Taking into account the described potential of services, which are possible for implementation on the basis of evidence of existence, this principle may prove even more valuable than the cost of bitcoin, on which most investors are obsessed today.

Digital property can sometimes be viewed as intellectual, and blockchain technology can prove ownership of such property. For example, if you write an article or you have an idea suitable for a patent, in some cases you have to prove that you owned this idea or document earlier than someone else. A check is an example of the potential of a blockchain beyond simple monetary innovation.

Now you need someone to be a third party in proof of identity - like Facebook, Twitter or Google. You could very well do the same, using the architecture of the blockbuster.

4. Blockchain in economy

The technical side of the invention of Satoshi Nakamoto will allow you to develop business in different directions, this will not be exactly for your competitors, and this need not be reported to the authorities. When you build a business, people will buy everything that you invent and offer, if it is useful and interesting. But you need to prove that you are the author. Blokchain provides such a proof, and Bitkoyn is a method of anonymous international payments (anonymous means very fast). In addition, taking the crypto currency for payment today, you create a powerful foundation for your reputation and wealth tomorrow. Do you think that the pioneers of the Internet are rich? What can you read about the first directors, scientific innovators, cosmonauts? And what about the conquerors of America? Sometimes for success it is necessary not to run faster than everyone, but to run out early, and to do it as uniquely as possible.

It is important, however, to understand that the technology of blockchain (the system of keeping the register of rightholders) does not by itself protect against piracy. Since books and films must eventually be converted into a human-readable form, it seems that you can always make an unprotected copy from this form [5].

So in the final account for protection still have to go to the courts, and records in distributed registries can then be used as evidence. Well, that, of course, if the judge knows the word "blockchain".

5. Blockchain Technologies in the Copyright Domain

The potential of blockchain as a general-purpose technology is currently being experimented with in many domains, including copyright law. Over the past months and years variegated suggestions as to how the technology could be deployed for the management of copyrighted works and neighboring rights objects have been voiced by industry and in the academic literature. In this section, we provide a cursory overview of expected application of these technologies. We organize the following overview around three main drivers leveraging the main characteristics of blockchain technologies. The first driver revolves around the potential capacity of blockchain technology to precisely identify a digital asset and thereby counter the problem of digital "fluidity". The second driver is related to the ability of blockchain technologies to foster transparent and disintermediated transactions. The third axis focuses on the potential of blockchains to be developed as a DRM system. Finally, in the second sub-section we introduce some structural limits of blockchain technologies such as the so-called "garbage- in garbage- out" problem [6].

6. Prospects for Application

Firstly, it has been argued that DLT could be used to create artificial scarcity in the digital market. Indeed in the copyright domain tokens may represent various elements including a copy of a protected work. This may solve a number of issues related to the fluidity of digital objects and create new business models. This may lead to the commodification of digital works and thereby allowing the creation of new markets. Some projects have already been implemented, in particular in the field of artworks leveraging the fact that blockchain technologies make digital artworks more attractive for collectors. It has also been speculated that these developments create the necessary preconditions for flourishing, technologically-enabled secondary markets for digital content.

DLT may also enable the precise tracking of certain digital assets (through tokens) that could be used as evidence of authorship and provenance. In relation to attribution, hashing can create a unique fingerprint of copyrighted material that allows verification of authorship and that the creative work existed at a given time without revealing the actual contents. The hash allows monitoring of provenance in through recording ownership and usage. DLT has been presented as a "revolution in how to keep track of rights". Tokens can encode information including the terms of use of protected material (such information can be mentioned under the definition of RMI). For unregistered intellectual property (IP) rights such as copyright and neighboring rights, blockchain technologies offer the benefit of providing a time-stamped record of its conception, use and qualification requirements. For example, the hash may facilitate evidence in court cases concerning copyright authorship and violation of the terms of use [7].

Blockchains' characteristics provide an opportunity to conceive of a global registry for copyright and neighboring rights. Indeed only the existence of a global registry holding RMI would allow for the development

3. Future of blockchain

The chain of blocks or blockchain of bitcoin is well known due to its use as a kind of ledger for dealing with digital currencies. At the same time, this technology has the potential to be used to solve other, very radical, tasks. In particular, he gives us an idea of how bitcoin might one day affect the scope of intellectual property and intellectual rights.

And what about the disputes between the numerous "authors"? Constantly someone is suing someone for property or copyright, although the dispute can be resolved by a timely small entry in a block of several tens of kilobytes. Authors of works can prove authorship with the help of this system. It will no longer be necessary to resort to special complicated legal manipulations. It is enough to create in the locker, which is guaranteed never to be changed or erased, an encrypted entry with the first, seventeenth and last page of your book, for example. Leaving or receiving data, according to which you can be accurately acknowledged by the author of this record.

In the not too distant future, mankind will go on to write down not only pieces of its creativity at a certain time in the structure of the detachment, but also the management of the "logs" of life: incidents, data, discoveries, laws and rights will be written into the blockchain. It is not at all necessary to have an archive building or a state "office" servicing owners' catalogs. Governments in general pretend that they do not understand: maintaining secret documentation in an encrypted block system helps to avoid leakage.

Thus, it is possible to exclude the influence of centralized bodies - all-pervasive and senselessly harsh - on consumers and creators of content and products. The severity of corporations is caused by the desire for power, and the people always, at least subconsciously, strive for freedom. Imagine, by the way, how much money for the budget we will save! We do not need a building, furniture, light and water, computers and food in order to build archives and offices, hire staff there. Confirm the right to own creativity and inventions can be using a smartphone.

How do you model a step-by-step creation of a real hit, where do developers, actors or stunt people consult about all the details of the game, the movie or even the play with bitcoin investors? Already today, just adding a button "type" to our torrent distributions and receiving constructive comments, we partially step on this innovative path [4].

Your ideas can no longer be stolen! Everyone will be able to record unconditional priority and authorship of both artistic and scientific works. The world "Bit-net" will provide an opportunity to link real assets and assets to the blockchain. Truthfulness is assured, and a whole bunch of bureaucrats, lawyers and other air sellers are left without work. But the work will appear among millions of authors, inventors, artists around the world.

Some believe that their creativity is of no interest to anyone, but this is far from true! It is exclusive consumption that will become a characteristic feature of the first bitcoin users. Authors of news, scientific, entertainment and other content, rare goods and services have already learned to advertise themselves through the Internet and attract public attention, at the same time "burying" television and physical advertising.

Now it's time to start taking real money for your efforts. Your audience is not limited to the territory of your native city or home state. Why should its finances be limited to this territory?

While bitcoins will flow into your pockets, copyright will undergo some "moral" changes, so that suddenly it does not turn out that bitcoins flow into the pockets of some other company that stole your idea. To get acquainted with works of art and science will be completely free. As a consumer, you will be able to search, read, watch, listen and copy to yourself anything you like without restrictions and legitimately. In some corners of the Internet, similar services are already available even in the CIS, payment? Bitcoins, of course! If you think that only drugs are sold for crypto currency, you live in 2009.

As the author of music, books or games, you can make a profit and "tip" from people from all over the planet, in volumes that are still difficult to predict. Not only will you receive material support from the fan community, you will also multiply it. Since the rate is very variable, people's interest will only grow, and your current "state" of $ 5 tomorrow may turn into 25 ... or 50.

The Internet bit of the future will allow ordinary people with small and medium income to get a chance to enjoy the results of creative and intellectual work of all ages, at the same time offering the whole world their services. Not only classics, but modern works will be available anywhere in the world. The importance of a total rethinking of copyright in the 21st century is great, because now there is a huge amount of priceless information, which should be caught literally "on the fly". The first thing that comes to mind is that the proof of existence can be used to confirm the authenticity of the certificate of property without revealing its contents.

You put a hash next to the link to download the file and check the hash yourself. Even if someone breaks into your server, it will not be able to change it. Using this method, you can unambiguously prove that the document or part of the code was checked at a particular time, and the global database of transaction accounting in the Bitcoin network is ideally suited as a means of its implementation. These are just some of the directions for applying this service.

subject matter. Blockchains may offer right holders greater security and stronger protections against possible attackers including copyright infringers that seek to access the digital asset. User rights would be encoded on a blockchain. Connected systems would then verify these rights and decrypt the related copyrighted content where appropriate. A smart contract would then be used to allocate access to the digital asset via tokens (such as bitcoin, ether, etc.) that reside on the chain, the role of which consists in facilitating remuneration and payments.

Blockchains do not hold the copyrighted digital asset itself in light of the technology's limited processing capabilities but rather facilitate a smart contract that contains information regarding related rights and permissions. However, when users use a work through their device, they trigger communication with the distributed ledger. The DRM system can scan the record for the necessary permission and give the user access to the acquired work. For example, if the user has purchased a limited-duration license, the system can consult a trusted timeserver and compare the time with the contract terms coded on the blockchain and take away access once the user's license has expired. Blockchain technology could therefore control use-rights and just as is the case with current DRM systems, smart contracts do not necessarily encode legally permitted copyright uses. We will return to this point in the following section.

After having summarized the main themes revolving around copyright management by means of blockchain uses, it is worth stressing some structural limitations of blockchain technologies [9].

7. Smart Contracts

In essence, a smart contract is self-executing computer code that automatically processes its inputs when triggered. It is essentially a small computer program that is deployed on a blockchain. Thus while smart contracts are currently being avidly discussed in relation to blockchain, similar mechanisms have been used for a long time, also by DRM systems. As explained, DRM technology essentially embedded copyright law into digital files by limiting the user's ability to view, copy, play, print, or otherwise alter the works. For example, digital audio files encrypted with DRM technology were not subject to the double-spending problem because they contained a basic smart contract, which referenced a centralized network (that is, for example, Apple's server programmed to enforce the iTunes Store Terms and Conditions). Beyond this rather basic definition there is little consensus as to what this terminology really refers. It is worth noting that depending on the adopted definition, smart contracts are not necessarily linked to blockchain technology. Given that they are discussed in relation to distributed ledgers in the literature we introduce below, we will also examine them as such here.

To some, a smart contract is simply a piece of computer code with specific characteristics. Vitalik Buterin portrays smart contracts as "cryptographic 'boxes' that contain value and only unlock it if certain conditions are met". In the blockchain context, a smart contract is "programmed logic that runs on a ledger-like distributed system in response to transaction submission". From a technical perspective, smart contracts are thus simply computer programs that can be consistently executed by a network of computers without the need for an intermediary. Because of their distributed nature and thus guaranteed execution, smart contracts are resilient to tampering, which makes them appealing in many scenarios including the transfer of value.

Yet, because these technical tools can be relied upon to automate transactions typically governed by contract law (such as value transfers) smart contacts can be useful tools in a contractual setting. Nick Szabo indeed coined the term "smart contract" in 1994, to denote "a set of promises, specified in digital form, including protocols within which the parties perform on these promises". Szabo envisaged the creation of computer software resembling contractual clauses to connect parties in a fashion that would make it difficult for one party to unilaterally terminate an agreement. Seen from this perspective, a smart contract can be a Ricardian contract, the objective of which is to create contracts that can be read by humans and machines alike. Indeed to some, a smart contract is "a computer program that both expresses the contents of a contractual agreement and operates the implementation of that content, on the basis of triggers provided by the users or extracted from the environment".

The main value proposition of smart contracts is that of their automated execution. As second-layer applications, smart contracts benefit from the tamper-proof nature of the underlying blockchain infrastructure that anchors their automated execution. Given that many blockchain nodes run smart contract code, it "is not controlled by – and cannot be halted by – any single party". Smart contracts execute automatically and cannot be halted unless this option is specifically built into the code. This enables transactions in situations devoid of human or institutional trust, lowers transaction costs and reduces counterparty risk and interpretative uncertainty. Once an agreement has been translated into code, the intervention of a party or intermediary (other than the respective oracle) triggering contractual execution is replaced by the software's automated execution.

Where smart contracts are used to automate the execution of contractual obligations, performance is thus hard-wired into the code. For example, the software can be used for the automatic transfer of collateral in

of potential benefits into real benefits of blockchain and smart contracts as described in the following paragraph. In this regard it is worth mentioning the project currently implemented by PRS for Music, ASCAP and SACEM which aims at improving data accuracy for right holders. This point will be further developed in the next section.

Secondly, there is the prospect of transparency and cost savings related to smart contracts as once a user purchases the digital asset from a website, the smart contract can be triggered immediately so that all other actions – e.g. payment of royalties to right holders – are automated. Combined with digital currencies, this enables micropayments, which could change pricing models in relation to copyrighted materials. Micropayments – meaning the payment of a small sum, such as EUR 0002 – is currently not an economically viable solution as transaction fees exceed the price itself. The advantages of this method are manifold: "the smart contract facilitates microtransactions at little to no fee, and payment is divided nearly instantaneously – per the strict logic of the smart contract code – and is immediately disbursed to the musicians in amounts of less than $0.01". This innovation could also serve to enable an instantaneous, fairer and transparent remuneration of authors and artists. To illustrate, Ujo Music uses smart contracts to facilitate the sale of digital music files. The payment of a certain sum to download a song triggers the smart contract, which divides payment between the various contributors to the song. Notably, this transaction can theoretically occur without the need for a traditional intermediary such as a publisher, a music label or performance organization. Notwithstanding, these platforms still constitute a new form of for-profit intermediaries so that it is still to be determined what economic impact such solutions will eventually have. Thus blockchain promises allowing artists to independently determine prices and individually license their works in a "direct-to-fan" fashion. This appears to offer some remedies for the digital era's challenge of easy unauthorized access to and distribution of copyrighted works.

Some hope that smart contracts will generate disintermediation which would affect incumbents at different levels, including: (1) publishers and music labels, (2) collective management organizations (CMOs), and (3) online platforms. According to others, complete disintermediation is unlikely as blockchains may simply introduce new stakeholders. In the field of online music many blockchain projects promise disintermediation between artists and audience. Yet in reality such actors can be seen as new intermediaries. Indeed, while current discourse frequently envisages authors and artists themselves programming their smart contracts and thus directly defining terms of use, it appears that for numerous reasons of an economic, cultural and technological nature, this is an unrealistic prospect. Sometimes the role of intermediaries goes further than the mere management of legal tools being more related to marketing strategies. In any case, for the "direct-to-fan" model to take hold, solutions need to be devised that can provide a user-friendly form of smart contract management, which does not require the user to personally code the smart contract. It should be noted that some are already working on corresponding solutions [8].

Smart contracts may also play a role in standardizing licensing terms and conditions for copyright works across uses and jurisdictions. Standardized smart contracts, the terms of which can be described in comprehensible language, augment transparency and reduce barriers to using contracts for transactions. The technology could also be used to generate custom smart contracts with the terms of license payment and even its split between various beneficiaries.

Thirdly, some believe that DRM itself may be disrupted by blockchain technology. A number of projects are already underway in this domain. Sony recently applied for a patent for a DRM solution based on blockchain. Kodak launched a similar project, KodakOne, which is aimed specifically at photographers and agencies. Whereas over one trillion photos are uploaded to the web each year, most of them fall into the category of orphan works because it is burdensome for photographers to administer image licensing, infringement detection and reporting. KodakOne seeks to change this by creating an image rights management platform, combined with tokens (to manage instantaneous royalty payments) and smart contracts (to document licenses).

These early initiatives underline that blockchain can serve to create a hard-to-amend record of initial ownership with smart contracts being encoded to license the use of copyrighted works. Here, smart contracts are deployed to automate and standardize copyright-related transactions (such as use and exploitation of content as well as remuneration) in relation to blockchain-based tokenized elements. 144 Smart contracts would be modelled to hold, execute and monitor contractual code. The idea is that smart contracts would be used to establish and self-enforce copyright agreements such as licenses, and provide information about rights in copyrighted materials.

Highlighting that traditional DRM solutions rely on single points of failure, are expensive, can be overcome by a single hacker and interfere negatively with consumer expectations, blockchains' resilience-through-replication is appealing. It is important to note, however, that automated licensing through smart contracts is not to be confused with traditional DRM systems which always involve control of access and use of digital

the event of default. Automated execution of course not only provides benefits but also disadvantages. Where software executes automatically, unwanted transactions can no longer be rolled back. This can be problematic, such as when a party lacks legal capacity or a party decides to default on its obligations. Modifications, such as those mandated by law or court decisions also cannot easily be accommodated. Through these characteristics, smart contracts promise to trigger efficiency gains particularly attractive in commercial settings, including in relation to copyrighted materials [10].

References

[1] *Gates M.* Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. / Mark Gates., 2017. - 125 p.

[2] *Wright A.* Blockchain: Uncovering Blockchain Technology, Cryptocurrencies, Bitcoin and the Future of Money: Blockchain and Cryptocurrency Exposed (Blockchain and Cryptocurrency as the Future of Money / Alan Wright., 2017. - 130 p.

[3] *Buterin V.* The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology / V. Buterin, W. Mougayar., 2016. - 208 p.

[4] *Vigna P.* The Truth Machine: The Blockchain and the Future of Everything. P. Vigna, M. Casey., 2018. - 302 p.

[5] *Swan M.* Blockchain: Blueprint for a New Economy / Melanie Swan., 2015. - 152 p.

[6] *Williams S.* Blockchain: The Next Everything / Stephen Williams., 2019. – 208 p.

[7] *Antonopoulos A.* Mastering Bitcoin: Programming the Open Blockchain / Andreas Antonopoulos., 2017. – 416 p. – (2nd Edition).

[8] *Tapscott A.* Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World / A. Tapscott, D. Tapscott., 2018. – 432 p. – (Reprint edition).

[9] *Werbach K.* The Blockchain and the New Architecture of Trust (Information Policy) / Kevin Werbach., 2018. – 344 p.

[10] *Wright A.* Blockchain and the Law: The Rule of Code / A. Wright, P. De Filippi., 2018. – 312 p.

The article was delivered to your editory staff on the 17.04.2019

Міністерство освіти і науки України;
Одеська Міська Рада
Одеський державний екологічний університет
Одеський національний університет імені І.І. Мечникова,
Одеська державна академія технічного регулювання та якості
Харківський національний університет радіоелектроніки
Економічна академія "Д.А.Ценов", Болгарія
Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
AGH науково-технологічний університет ім. Ст. Сташіца, Польща;
Університет Бельсько-Біла, Польща;
Університет Північ, Республіка Хорватія;
Представництво "Польська академія наук" в Києві
Лодзький університет, Польща
Лодзький Технічний університет, Польща

«ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»

праці
міжнародної науково-практичної конференції
19 – 24 серпня 2019 року
Одеса, Україна

«INTELLECTUAL SYSTEMS
AND INFORMATION TECHNOLOGIES»

proceedings
of the International Scientific and Practical Conference
2019, August, 19th to 24th
Odesa, Ukraine

Одеса

ТЕС

2019

Проблеми і Перспективи Практичного Застосування Інформаційної Технології Blockchain в Smart-Контрактах

Н.В. Шаронова
кафедра інтелектуальних комп'ютерних систем
Національний технічний університет «Харківський політехнічний інститут»
Харків, Україна
nvsharonova@ukr.net
ORCID 0000-0002-8161-552X

І.В. Кириченко
кафедра програмної інженерії
Харківський національний університет радіоелектроніки
Харків, Україна
iryna.kyrychenko@nure.ua
ORCID 0000-0002-7686-6439

Г.Ю. Терещенко
кафедра програмної інженерії
Харківський національний університет радіоелектроніки
Харків, Україна
hlib.tereshchenko@nure.ua
ORCID 0000-0001-8731-2135

Problems and Prospects of Practical Application of Blockchain Information Technology in Smart-Contracts

N.V. Sharonova
Department of Intelligent Computer Systems
National Technical University "Kharkiv Polytechnic Institute"
Kharkiv, Ukraine
nvsharonova@ukr.net
ORCID 0000-0002-8161-552X

I.V. Kyrychenki
Department of software engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
iryna.kyrychenko@nure.ua
ORCID 0000-0002-7686-6439

G.Y. Tereshchenko
Department of software engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
hlib.tereshchenko@nure.ua
ORCID 0000-0001-8731-2135

***Анотація*—У світі сучасного бізнесу інформаційні технології займають важливе місце: практично кожен процес, як-то виробництво, логістика або ведення обліку, автоматизується. З появою технології Blockchain оптимізація процесів здійснення ділових угод стала можливою і привела до появи такого поняття як Smart-контракт. У статті розглядаються поняття Smart-контракту, його технологія і основні елементи, аналізується застосування у сфері логістики, а також виявляються головні переваги та недоліки. На основі цієї інформації робиться висновок про актуальність і подальші перспективи Smart-контрактів.**

***Abstract*—In the world of modern business information technologies occupy an important place: virtually every process, such as production, logistics or accounting, is automated. With the advent of Blockchain technology, the optimization of business transaction processes became possible and led to the emergence of such a concept as a Smart-contract. The article deals with the concept of Smart-contract, its technology and basic elements, analyzes the application in the field of logistics, as well as the main advantages and disadvantages. On the basis of this information, the conclusion is drawn on the relevance and future prospects of Smart-contracts.**

Ключові слова—децентралізована система; blockchain; Smart-контракт; логістика; інформаційна технологія.

Keywords—decentralized system; blockchain; Smart-contract; logistics; information technology

I. ВСТУП

Blockchain - це технологія для зберігання підтверджених записів, що може застосовуватися у державному або приватному доступі, при передачі фінансових операцій, документів, створенні Smart-контрактів, видачі власних токенів та видачах NODA регуляторам та третім особам.

Blockchain може застосовуватися в різних сферах, пропонуючи компаніям різні переваги та інноваційні бізнес-моделі. Одне з найбільш перспективних напрямків – технологія Smart-контрактів. Сьогодні можна передбачити технологічний прорив у логістичній галузі шляхом створення прозорої системи взаємодії між усіма учасниками ринку. Децентралізована логістична платформа може запропонувати інноваційні рішення, які засновані на впроваджені технології blockchain в управлінні ланцюжками поставок. Це децентралізована система, яка використовує blockchain і складається з декількох інтелектуальних контрактів всередині блочного ланцюга і його власних токенів (якщо необхідно) [1, с. 34].

II. SMART-КОНТРАКТИ ТА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Blockchain - це децентралізований цифровий регістр транзакцій, що обробляються розподілено або тимчасовою мережею. Щоб створити зашифрований запис, транзакція, яка називається "блоком", передається кожному вузлу в мережі. Використовуючи криптографію, кожен вузол підтверджує транзакцію як дійсну, а потім копує блок в "ланцюжок" з декількох транзакцій, які зберігає кожен вузол. Іншими словами, одна транзакція повинна бути перевірена, синхронізована і записана у всій мережі blockchain миттєво. Технологія Blockchain вперше потрапила в заголовки як основа для всіляких типів фінансових транзакцій, починаючи з біткойнів у 2009 році. Згідно з фінансовим консалтинговим Greenwich Associates, фінансові та технологічні компанії інвестували близько 1 мільярда доларів в технологію Blockchain в 2016 році. До 2020 року професійна Мережа сервісів PwC очікує, що системи, засновані на blockchain, замінять або усунуть багато проблем для різних бізнес-транзакцій; приватні особи та компанії зможуть обмінюватися широким спектром зашифрованих або представлених в цифровому вигляді активів та матеріальних цінностей з ким-небудь.

Наприклад, транзакції з підтримкою ланцюжка блоків можуть революціонізувати ланцюжки поставок (логістику), які на базовому рівні становлять собою серію транзакцій, необхідних для доставки товару з місця на місце. Оскільки система дозволяє користувачам безпечно і надійно документувати транзакції, можна використовувати blockchain для створення і документування кожної транзакції в рамках розширеного ланцюжка поставок, від виробництва продукту до його розподілу, транспортування і продажу, що скоротує тимчасові затримки, додаткові витрати та людські помилки, які завдають ланцюгам поставок сьогодні.

Творчим концепція Smart-контрактів виникло ще в 1994 році, завдяки Ніка Сабо, але втілення його ідеї стало можливим лише з появою технології blockchain. Зокрема, практична реалізація Smart-контрактів стала можливою завдяки використанню таких елементів, як протокол децентралізованого консенсусу, криптографічна безпека і загальнодоступний відкритий реєстр.

Термін Smart-контракт описує комп'ютерний код, який автоматично виконує всю угоду або її частини. Код зберігається на платформі, побудованій на основі blockchain. Код може бути єдиним оголошенням про угоду між сторонами, або доповнює традиційний текстовий контракт і виконує лише певні положення, такі як переказ грошей стороною А стороні Б. Сам код реплікується на кілька вузлів blockchain, таким чином, користується перевагами blockchain: по безпеці, збереженні і ненадійності. Реплікування також означає, що в міру додавання в blockchain кожного нового блоку код, по суті, може здійснитися. Якщо сторони ініціювали транзакцію і тим самим показали, що умови дотримані, це стало тригером, і код виконує якісь дії. Якщо ж транзакція не ініціювалася, то і код нічого не робить.

Поки що Smart-контракти найкраще підходять для автоматичного виконання транзакцій двох типів:

- оплата, що ініціюється певними подіями;
- викладання фінансових санкцій при невиконанні об'єктивних умов.

Коли розгорнутий контракт почав діяти, для виконання цих двох типів транзакцій не потрібно участі людей, в тому числі довірених власників умовного депонування або представників юридичної системи. Це дозволяє зекономити викладені витрати на виконання і правозастосування при укладанні договірних угод.

Варто відзначити, що розумні контракти реагують лише на транзакції. Коли актив або валюта переводяться в програму, вона починає стежити за виконанням умов контракту. Як тільки вони будуть виконані, продавець отримує гроші, а покупець товар (послугу).

Елементами Smart-контракту є такі об'єкти:

- Предмет угоди. Програма повинна мати доступ до товарів або послуг, з приводу яких полягає контракт, і мати можливість автоматично дати або закрити до них доступ.
- Цифрові підписи. Всі учасники ініціюють угоду, підписуючи договір своїми секретними ключами.
- Умови угоди. Умови Smart-контракту в формі точної послідовності операцій. Усі учасники повинні підписати ці умови.
- Децентралізована платформа. Smart-контракт емігрується в блок ланцюга та розподілено зберігається на її вузлах [2].

Smart-контракти, наприклад, можуть позбавити від так званих класових розривів. Як тільки товар прибув на склад і зареєстрований, Smart-контракт здатний миттєво відправити гонорари на підтвердження. Отримавши їх, він

- децентралізація, яка дозволить всім сторонам ланцюжка поставок брати участь в процесі в режимі реального часу: моніторинг руху товарів і транспорту, заповнення документів у вигляді розумних договорів (замінення ймовірності помилок і шахрайства), усунення незаконних ланок в ланцюжку поставок (контрафакція, контрабанда, використання рабської праці у виробництві).

Які існують проблеми впровадження blockchain в логістиці:

- усунення людей з роботи (скорочення робочих місць),
- правові засади (прийняття нормативних актів щодо впровадження Smart-контрактів);
- скептицизм щодо технологій;
- складність координації учасників і стандартизації бізнес-процесів.

Натомість одна з головних властивостей смарт-контрактів – їх здатність автоматично і неминуче виконувати транзакції без втручання людини. Однак автоматизація і той факт, що Smart-контракти можна змінити або перервати, тільки якщо сторони не передбачать такі можливості при створенні, – одні з головних складнощів, що заважають широкому розповсюдженню Smart-контрактів.

Наприклад, при найгіршій текстовій угоді одна зі сторін може пробачити порушення з іншого боку і не зауважувати її накласти штраф. Припустимо, цінний клієнт запізнився з оплатою на місяць, і вендор вирішив, що довгострокові комерційні відносини важливіше, ніж будь-яке право розірвати угоди або пені за прострочення. Але якщо в історії бере участь Smart-контракт, то вендор фізично не може ситуативно відмовитися від примусового виконання умов угоди. Затримка оплати призведе до автоматичного перерахунку пені з рахунку клієнта або до обмеження доступу до ПО або пристрою, якщо це передбачено в Smart-контракті. Автоматичне виконання не відповідає манері багатьох компаній вести бізнес.

Аналогічно при текстових договірних відносинах сторони можуть ситуативно домовитися, що часткове виконання угоди вважається повним виконанням. Наприклад, заради збереження все тих же довгострокових відносин – чи тому що сторони вирішили, що краще виконати угоду частково, чим не виконати зовсім. І об'єктивність, необхідна у випадку зі Smart-контрактом, може не відповідати реальним взаємодії сторін.

Smart-контракти додають додаткові ризики, яких немає в більшості зафіксованих в тексті угод такі як: злом контракту, внесення в програмні помилки в коді або протоколі. Якщо врахувати відносну бюнжку blockchain, ці компанії тісно взаємопов'язані. Тому сторонам, які уклали Smart-контракт, потрібно розуміти, який ризик і відповідальність за внесення в коді і їх використання зловмисниками розподіляються між сторонами й, можливо, третьою стороною – розробниками або страховиками Smart-контракту.

III. ВИСНОВКИ

Хоча Smart-контрактам ще потрібно розвиватися, перш ніж вони стануть широко використовуватися в складних комерційних відносинах, все ж вони вплинуть на революцію в структурі виконання та стимулювальні, яка визначить форму контрактів в майбутньому.

На основі розглянутого можна зробити висновок, що є досить переваг розумних контрактів. Основні з них полягають в наступному:

- Безпека. Smart-контракт зашифрований і зберігається на декількох пристроях, що гарантує захист від втрати або несанкціонованої зміни.
- Економія та швидкість. Більшість процесів автоматизовано, а більшість посередників усунуто з процесу.
- Стандартизація. Сьогодні існує безліч варіантів Smart-контрактів, і можна вибрати потрібний для конкретного завдання [2].

Таким чином, технологія розумних контрактів – це досить зручний, простий і швидкий інструмент, що дозволяє реалізувати угоди різних видів і призначень. Напрямок Smart-контрактів досить перспективний, до того ж він розвивається з величезною швидкістю. Про це заявляють як самі користувачі, так і співробітники великих компаній, що спеціалізуються на криптовалютах. Зокрема, Гевін Вуд, CTO (Chief Technology Officer) Ethereum, заявив, що Smart-контракти можуть бути застосовні в будь-якій галузі, починаючи від медицини й автопрому і закінчуючи нерухомістю і законотворчістю. «Smart--контракти можуть кардинально змінити нашe суспільство, ставши технічною базою для змін» [4].

Основна перевага впровадження технології blockchain у Smart-контрактах: забезпечення синхронізованого хаунту між партнерами та оптимізація процесів в режимі реального часу. Блокчейн підвищив рівень довіри у всьому ланцюжку і спростив процес прийняття рішень на кожному етапі, надаючи одноразовий доступ до інформації, яка дозволяє спільно прогнозувати процеси та дії [5, с. 42].

Впровадження технології blockchain для Smart-контрактів в логістиці забезпечить збереження даних, захистить сховища документів від злому, виключить можливість внесення змін в інформацію про хід перевезення. Така система, безумовно, може скоротити затримки при доставці та знизить ймовірність шахрайства, заощадивши мільярди доларів усім учасникам транспортного ланцюжка. За даними Світової організації торгівлі, усунення бар'єрів в ланцюжку міжнародних поставок товарів дозволить збільшити

відразу перевезе кошти від покупця продавцю. При цьому продавці отримають оплату миттєво, їм не доведеться нагадувати клієнтам про необхідність оплатити, а покупці заощадять на банківських операціях. Все це може зменшити вимоги до оборотного капіталу і спростити фінансові операції для обох сторін. Що стосується обов'язковості виконання, то Smart-контракт можна запрограмувати таким чином, щоб він закривав доступ до активів, що підключені через інтернет (наприклад, до контенту), поки не отримано оплату.

Корисним Smart-контракт буде в процесах логістики. Ланцюжок поставок зазвичай складається з багатьох ланок, проте кожна ланка має отримати підтвердження від попередньої, виконати свою частину контракту і передати інформацію далі. У традиційній практиці це забирає багато часу і знижує ефективність, а використання Smart-контрактів економить час і дозволяє відстежувати прогрес у реальному часі.

Одне з головних завдань Smart-контрактів - скоротити витрати на логістику, так щоб її частка в собівартості товару була мінімальна. Які існують питання? По-перше, проблема довіри. Контроль за перевезеними вантажів ідеальний, за винятком, до успішного завершення угоди. Всі дії фіксуються в blockchain, що виключає відсутність довіри між сторонами; Smart-контракт, який буде затверджений на початку відвантаження, автоматично виконає взаємний розрахунок відповідно до даних, що зберігаються в blockchain.

Токени будуть видаватися автоматично через Smart-контракт, а також підтвердження ризиків може бути сформовано шляхом інтеграції з банками та отримання Цінного папіру або отримання застави, страхування ризиків. Все це покликане замінити ряди недобросовісної ділової практики або людських контрактів на постачання, відсутності зобов'язань у реальному часі та:

- усуненню непотрібних посередників;
- формуванню відповідальних і автоматизованих операторів;
- керуванню процесом взаємних розрахунків онлайн;
- робота з документами, що супроводжують операції;
- онлайн відстеження місця розташування (GPS-відстеження) вантажів, транспортних засобів в режимі 24/7, що за допомогою технології blockchain;
- швидко знайти відповідний транспорт для доставки;
- знайти вантаж для перевізників;
- гарантований платіж усім учасникам платформи;
- гарантувати якість замовлення;
- не витрачати час на постійно дзвоні процеси та автоматизувати дзвінки з них;
- автоматизація та алгоритмізація основних постійних процесів;
- утворювати відкриті або закриті (конфіденційні) ланцюги поставок;
- зменшити юридичні витрати;
- зменшити транспортні витрати вантажовідправника;
- зменшити людський фактор і витрати для всіх учасників платформи;
- автоматизувати транспортних засобів і зменшення порожнього пробігу;
- контролювати стан водіїв і моменти відвантаження / прийомки вантажу;
- безумовне виконання Smart-контракту та зобов'язань;
- отримати аналіз і обмін пропозиціями вантажів і відвантажень, власників автотранспорту і професійних учасників ринку транспортних послуг;
- сформувати базу "довірених" постачальників і вантажовласників.

На даний момент комісія за посередницькі послуги при перевезеннях складає в середньому від 10 до 45% від загальної суми замовлення. Водночас формування цієї суми та її зміна не контролюються замовником жодним чином. Більшість ризиків у логістичній галузі пов'язані з фінансовими розрахунками та якістю виконання зобов'язань вантажними перевізниками, а також передачею інформації, яка може бути помилковою або викривленою. Упровадження роботи з централізованими службами та застосування технологій Smart-контрактів і blockchain забезпечить прозорість ринку логістики. Формування комісії стане прозорим, а ціни на послуги зменшаться через відкритту та прозору взаємодію всіх учасників ланцюгів поставок. IT-рішення дозволить значно скоротити час, фінансові та людські ресурси, залучені до процесу транспортування. Разом з тим, нові ринки відкриваються для перевізників, а платформа може стати доступною не тільки одному клієнту, але й бути стандартом якості транспортно-логістичних послуг, що надаються на ринку [3, с. 15].

При реалізації blockchain в ланцюжку поставок взяті в самій базовій версії технологія забезпечить:

- можливість відстежити товар від місця походження до кінцевого користувача, захистити покупця від підробки й обману. Це дозволить покупцеві прийняти зважене рішення про покупку;

MONOGRAFIA

POKONFERENCYJNA

ROZWÓJ I PRAKTYKA

INŻYNIERIA I TECHNOLOGIA

Zakopane (PL)

29.12.2017

світовий ВВП на 5%, а загальний обсяг перевищить на 15%.

Очікується, що до 2020-го року системи, засновані на blockchain, замінять або усунуть багато суперечностей для різних бізнес-трансакцій.

Литература References

[1] Reed J. Smart Contracts: The Essential Guide to Using Blockchain Smart Contracts for Cryptocurrency Exchange / Jeff Reed., 2016. – 54 p.

[2] Tar A., Smart Contracts, Explained [Електронний ресурс] // Cointelegraph: справ.-інформ. портал – Электрон. дан., 2017. – URL: https://cointelegraph.com/explained/smart-contracts-explained

[3] Parker T. Smart Contracts: The Ultimate Guide To Blockchain Smart Contracts - Learn How To Use Smart Contracts For Cryptocurrency Exchange! / Terry Parker., 2016. – 30 p.

[4] Rosic A., Smart Contracts: The Blockchain Technology That Will Replace Lawyers [Электронный ресурс] // Blockgeeks: инфорпс. портал. – Электрон. дан., 2017. – URL: https://blockgeeks.com/guides/smart-contracts/

[5] Bock S. Blockchain: Bitcoin, Ethereum, Smart Contracts, Cryptocurrencies and Everything about the Fintech Explained / Shane Bock., 2017. – 66 p.

SPIS/СОДЕРЖАНИЕ

WSPÓŁORGANIZATORZY:

The East European Scientific Group (Azerbaijan, Belarus, Poland, Serbia, Ukraine),
Virtual Training Centre «Pedagog of the 21st Century»,
Global Management Journal.

U.D.C. 004+62+54+66+082
B.B.C. 94
Z 40

Zbiór artykułów naukowych recenzowanych.

(1) Z 40 Zbiór artykułów naukowych z Konferencji Miedzynarodowej Naukowo-Praktycznej (on-line) zorganizowanej dla pracowników naukowych uczelni, jednostek naukowo-badawczych oraz badawczych z państw obszaru byłego Związku Radzieckiego oraz byłej Jugosławii.

(29.12.2017) - Warszawa, 2017. - 60 str.

ISBN: 978-83-65608-98-7

Wydawca: Sp. z o.o. «Diamond trading tour»
Adres wydawcy i redakcji: 00-728 Warszawa, ul. S. Kierbedzia, 4 lok.103
e-mail: info@conferenc.pl

Nakład: 100 egz.

In what areas of advertising can the blockchain develop?

1. Integration of big data with blockchain, which opens access to detailed information about consumers, their preferences, etc. at preservation of the personal data.

2. Improving the procurement of advertising, including programmatic. Blockchain will allow standardizing advertising contracts and making them more transparent, since even in programmatic purchases, the issue of traffic quality arises.

In the blockchain you can check the authenticity of the user and clicks. But here there is a downside: thus the advertiser and the platform can interact directly, and then the role of exchanges, advertising networks and agencies as focal points, guarantors and arbitrators may decrease.

3. Interaction between the client and the agency: storing data about the work done in the blockchain, transactions, confirming the results of the advertising campaigns, etc.

Solving problems of trust and control in digital marketing

It is smart contracts and a multifunctional block of people like Ethereum that allow you to make the relationships of the interested parties absolutely transparent – in any spheres of human activity where there are any agreements and obligations. To understand exactly what blockchain can be useful for the digital-advertising market, it is necessary to identify the most acute and pressing problems of digital marketing.

First one is Frod. A real scourge of digital advertising. Purchasing impressions on any sites, you can waste more than 50% of the advertising budget, since along with real users your ads will be viewed by bots. Disclosure of the botnet Methbot in late 2016 demonstrated the monstrous scale of click fraud. Together, the digital advertising industry is losing about $ 7 billion annually due to fake ad views. And while the approach to placing advertising in the digital environment will not change, this indicator will only grow. It is noteworthy that now there is almost no protection from bots automatically viewing ads. Whatever system of analytics you use, there are no guarantees that the displayed views were performed by real people.

Second one is Intermediaries. In circumstances where one can not trust the site directly, advertisers are forced to work with intermediaries who play the role of arbitrators. The problem is that the arbitrators are not always good at coping with their tasks – a huge amount of fraud proof of this.

In addition, intermediaries between the advertiser and the site take a substantial commission for their services. If we look at the largest intermediaries – such as Google or Facebook – we find that they account for a significant portion of all marketing costs. Huge power over the digital advertising market and ambiguous efficiency is what distinguishes these players.

Facebook, for example, has about 2 billion users around the world. This scale of the audience in combination with big data provides social networks with a significant impact on digital marketing in general. According to many marketers – even too significant. Companies like Facebook began to be "digital gardens of

USAGE OF BLOCKCHAIN TECHNOLOGY IN MARKETING

Tereshchenko G.U.
Student of the faculty of Computer Science
Kharkiv National University of Radio Electronics

Keywords: innovative technology, blockchain in marketing, problems of blockchain, new payment methods, fraud solution

Briefly about the blockchain.

Despite the actual complexity of the technology, it is quite enough for a general user to understand the general principles of the work of the blockchain in order to assess the significant advantages and possibilities of using this technology.

1. Decentralization

Blockchain is a distributed database. There is no single data center – the information is stored on the computers of each of the network participants. Moreover, it is stored entirely: the whole blockchain on each of the devices.

Thus, it is possible to disable 99% of the devices (which is almost impossible, if we are talking about millions of copies of blockchain around the world), but 1% of them will keep the entire database intact. And he will certainly transfer it to all new devices connected to the network.

2. Impossibility to enter inaccurate data or change already made records Unlike other databases, all information written to the blockchain is interrelated. The blockchain consists of a chain of blocks, arranged in chronological order. To the first block (the so-called genesis block) is attached the second, to the second – the third and so on. In this case, each new block added to the chain, contains information about the previous one.

Thus, all the blocks and ever committed transactions of network users are connected with each other using complex algorithms. An attempt to change anything in one of the blocks destroys the integrity of the chain and is rejected by the computers of the other participants. The authenticity of each new block is also checked by the participants, and when a general consensus is reached, it is added to the chain.

Each block stores information about user actions. If it is a block of bitcoin, then the block records data about the latest transactions made by users. However, theoretically it is possible to record any information in a locker, which must be made simultaneously publicly and protected from any editing or deletion.

3. The uniqueness and at the same time the anonymity of the participants All users of the network based on the blockchain have a unique identifier and a digital signature. At the same time, real personal data of a person can remain either confidential or publicly available – depending on the user's desire or requirements laid down in the algorithm of a particular blockchain [1].

thor will be preserved. This is what Americans call "legacy", a legacy. The bad news: no one will forget what you wrote that night. Good: you can manage content as a valuable asset, bequeathing it to heirs.

The principle of blockchain solves a very important issue in the world of information domination over the individual: how to preserve mercantilist benefits and leave a trace in history without investing in a PR brand, simply doing its own thing. In order to earn more, the author can assign any meta tags to the content units, improving their visibility in the system, but in the top of the tape there will still be texts with the greatest number of interactions from real users-backers. No cheat from the bots.

Blockchain can offer revolutionary changes for marketing, but this has never come into fashion among marketers and has not become a trend, like Snapchat and online video.

I believe that there are several problems here:

1. Hypacity. Few marketers have heard about the benefits of blockchain for marketing, and those who have heard do not know how to put everything into practice. Startups based on the blockchain, which will simplify marketing, today only appear, and the advertisers will only be able to evaluate them and understand the advantages over time.

2. A narrow circle of enthusiasts. In order for the blockchain system to function, you need to have enough clients in it. Only users who make transactions and other actions create a chain, without them there will be no blockchain. If your audience is not in the blockchain database, you will not be able to enjoy all the benefits.

3. Scalability. The most famous blockchain service today – Ethereum – processes up to 20 transactions per second. This is ten times less than auctions of advertisements (RTB). For marketing needs, such speeds are not enough, the blockchain needs to strengthen its technical positions [3].

However, blockchain may lead to such consequences:

1. Destruction of business model of advertising networks

The most successful of these certification centers were Google and Facebook. Google earns more than $ 4 billion on the Google Display Network. It is here that he acts as an intermediary between the site, which has an audience and an advertiser who needs to go to his site.

If they trust each other – the advertiser and the site, – Google will not be needed as an intermediary, which takes the share of profits. But this does not happen, therefore Google acts as a reliable certifying center. The advertiser can not trust the site when it comes to the use of questionable fraud tactics to increase revenue.

If it is possible to verify with the help of blockchain that each individual user is authentic with an accuracy of 100% and the site sells only genuine clicks, then the advertiser and the site itself do not need an intermediary and they can, by agreement with each other, exclude it from the business, while retaining their money.

So, now you can see what opportunities provides blockchain for the world of

data". Marketers believe that they have the right to claim some of this data. Meanwhile, the use of blockade in digital marketing can close the issue of fraud and intermediaries forever. And that's why.

As we have already said, the blockchain is able to ensure the uniqueness, the "reality" of the network participant and his anonymity at the same time. We can treat an ad as a bargain between the advertiser, the site owner and the user, while the third party (like Google, Facebook or Yandex) is the guarantor of the fulfillment of obligations, and the blockchain.

Digital identification without the transfer of personal information will prevent fraud of any type, protecting the user from the misuse of his personal data.

Blockchain is also able (in the long run) to deal a serious blow to intermediaries, giving the possibility of direct control over the placement of ads and the costs of advertising budgets. While the statistics on advertising campaigns can be relatively easy to manipulate, with the transfer of the same transactions on the block-base basis, falsification of statistics will become impossible [2].

Each content unit has its own price. Actions in many content platforms on the blockchain, for example "Voice", are reduced to money. That is, each unit of text, each photo, a comment in the system is automatically assigned a certain amount. This amount can grow depending on how other users interact with this content: read it or create something new based on it. That is, each unit of text, each photo, a comment in the system is automatically assigned a certain amount

The author can choose the appropriate privacy policy for each content unit. When a user simply enters the block with the author's text, the author receives a reward. When the reader wants to use a fragment of the text for his own purposes, he chooses the appropriate item (if it is provided for by the privacy policy) and the author gets even more reward.

In addition, information about the source (author) of the text fragment will be in the chain with the new content created on its basis. But here is another thing.

Content-platforms on the blockchain themselves monitor the observance of your copyright. After the content unit is created and published in the system, it is assigned a code that is automatically "checked for uniqueness" for all units of the block system. You correctly understood: after adding each new element the whole system is updated.

It's as if Google were updating its search engine after the next page appeared. Only much, much faster. First of all, due to the fact that all data is not on any servers, like Google, but distributed among all participants of the block system. That is everywhere and nowhere at the same time.

Since your most evil critic is yourself in a year, many blockchain based content platforms open up opportunities for editing or deleting blocks with content without destroying the whole chain. Such developments are, for example, in Bandcamp and Accenture. That is where, the block will disappear, but if the deleted text fragment has already been used somewhere, information about you as an au-

0.1 penny? Without blockchain, these micro-payments do not make sense, since the third party's transaction costs will be higher than the revenues from each transaction. But with instant and free transactions offered by blockchain such payments become real.

You can see with a small window in the corner of a popular site, which says something like: "Would you like to view our content without advertising? Just click here to pay 0.1 pence directly on this page. " Or the site may charge for access to its pages, but its size will be low enough not to scare off users, as it often happens now.

For sites, the transition to this kind of revenue model will mean a reduction in the number of materials that assume space for advertising (or their number will grow slower than it could), however, the demand for advertising will remain, so the cost per click will increase. This will mean that support for micro-transactions is more profitable for sites, because it will enable you to increase the cost of clicking on advertisements [4].

Conclusion

The wolf is not so terrible as it seems, and if one understands the intricacies of a blockchain, its advantages for marketing become obvious.

Blockchain will help:

- Get away from the monopoly of social networks and Google and reduce their impact on online advertising.
- Conduct safe transactions without guarantors.
- Pay for services, advertising and other services without intermediaries and interest.
- Place any data in the chain so that they can not be deleted or edited without the user's consent.

Projects that are now implementing blockchain in the advertising markets, have goals that differ from the purposes of the advertising agency. Often these projects are generally excluded by the agency, as they expect to create a platform in a bundle of client plus site.

This means that all the metrics and data collected by the project are transferred to the client for more accurate targeting, after which the sites are directly connected through a system where the site receives money directly from the client, since its money is already frozen on a smart contract and automatically transferred if it is complied with those or other conditions prescribed in this contract.

At the same time, the large potential for internal use within the agency is integrated with the blockichain and big date in digital advertising. This gives us fast, secure access to "immutable" data, which increases the quality and productivity of the work. Together, these two tools allow you to enter a new level of data processing, which will significantly increase the speed and accuracy of obtaining the right and right results.

Sources:

1. Akulich M. Blockchain and marketing / Margarita Akulich., 2017. – 110p.
2. Brinker S. The Blockchain Marketing Technology Landscape [Electronic resource] / Scott Brinker. – 2017. – Access to resource:

digital marketing. Probably there is no greater threat to Google's profits than blockchain. It poses no less threat to such IT giants than Bitcoin, for large banks. We agree, however, that this is good news for advertisers and sites. They will be able to save more revenue for themselves and do not have to pay to a third party.

2. Click-fired strike

A distributed transaction register, which is a blockchain, can provide not only a "non-hacking" transaction record, but also a digital signature of people for their unambiguous identification. This means that the user gets the opportunity to prove that he is a real person, but not to disclose his personal data, which can be used for criminal purposes. Such a technology has already been developed and its wide distribution is only a matter of time. Microsoft is already working on building its own digital identification system based on the blockchain. Probably other technological giants will also see the potential of these technologies, and integrate them into their own systems to prevent multiple types of click fraud.

This will allow you to check with much greater certainty who clicks on ads and who sees them.

Fraud with click fraud is an extremely common problem. It will cost advertisers more than $ 7 billion in 2017. Solving this problem would increase the combined effectiveness of advertisements on the Internet by $ 7 billion. Advertisers will get higher profits and return on investment after eliminating fraud and working without intermediaries like Google. This will mean, in turn, large budgets, which is good news for internet marketers. Provided that they play by the rules and do not wind the clicks with the help of bots, of course.

3. Changing profit-making models for sites

Currently, all online transactions must be processed by a third party, such as Paypal, Stripe or Worldpay. These businesses must compensate their costs (for example, server infrastructure, employees and marketing) and lay some profit. The intermediary takes the commission for each transaction. For the most part, these commissions are quite reasonable. If you buy a watch, dress or refrigerator on the Internet, the amount of compensation paid to a third party for the "purity of the transaction" will be a very small part of the total value of the purchased goods.

But with the help of blockchain you can transfer any amount of money (in digital currency), regardless of its size, completely free of charge (in popular currencies, for example, Emercoin, there are rewards for miners that are known to everyone and do not constitute a share of the purchase, but a fixed, (See the trans.). The third party does not exist and there is no need to pay for servers, personnel and marketing. All transactions are stored in the blockchain, which is distributed to all members of the Network.

This means no fees at all, which opens up the possibility of micro-transactions that could create a completely new profit model for different sites.

How much would you pay for viewing a web page without advertising? 1 pound? 1 penny? 0.5 penny, maybe? How about a

http://chiefmartec.com/2017/09/blockchain-marketing-technology-landscape-2017/.
3. Schebesta F. How Blockchain Is Disrupting Digital Marketing [Electronic resource] / Fred Schebesta – Mode of access to the resource: https://www.singlegrain.com/digital-marketing/how-blockchain-is-disrupting-digital-marketing/.
4. Epstein J. Blockchain marketing: How the technology behind Bitcoin could change marketing forever [Electronic resource] / Jeremy Epstein. – 2017. – Access to resource mode: https://www.clickz.com/blockchain-marketing-how-the-technology-behind-bitcoin-could-change-marketing-forever/114114/.

Матеріали міжнародної наукової конференції
Материалы международной научной конференции
Conference proceedings

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ ТА ПРОБЛЕМИ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ И ПРОБЛЕМЫ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА

INTELLECTUAL SYSTEMS FOR DECISION MAKING AND PROBLEMS OF COMPUTATIONAL INTELLIGENCE

INTELLECTUAL SYSTEMS FOR DECISION MAKING AND PROBLEMS OF COMPUTATIONAL INTELLIGENCE

May 21-27 2018
Zaliznyi Port, Ukraine

21-27 мая 2018
Железный Порт, Украина

21-27 травня 2018
Залізний Порт, Україна

THE CONFERENCE ORGANIZERS:

Kherson National Technical University
IT Step University
Lublin University of Technology
Black Sea Scientific Research Society
State Ecological Academy of Postgraduate Education and Natural Resources Management of Ukraine
Vinnytsia National Technical University

CO-ORGANIZERS OF THE CONFERENCE:

Ministry of Education and Science of Ukraine
Southern Scientific Center of NAS of Ukraine and the MES of Ukraine
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
Kharkiv National University of Radio Electronics
National Metallurgical Academy of Ukraine (Dnepropetrovsk)
Lviv Polytechnic National University
Uzhhorod National University
University of Zilina (Slovakia)
National Aviation University (Kyiv)
Public Academy of Sciences (Lodz, Poland)
Lodz University of Technology (Poland)
Igor Sikorsky Kyiv Polytechnic Institute
International Research and Training Center for Information Technologies and Systems of the NAS of Ukraine and MES of Ukraine (Kyiv)
Petro Mohyla Black Sea State University (Mykolaiv)
Lviv State University of Life Safety
Odesa National Polytechnic University
2018 IEEE Second International Conference on Data Stream Mining & Processing
Game & Design club
It Beans: student community

INTELLECTUAL SYSTEMS FOR DECISION MAKING AND PROBLEMS OF COMPUTATIONAL INTELLIGENCE

ISDMCI'2018

International Conference

Intellectual Systems for Decision Making and Problems of Computational Intelligence: Conference Proceedings.– Kherson: PP Vyshemirsky V. S., 2018. – 322 pp.

ISBN 978-617-7573-17-2

International Conference

INTELLECTUAL SYSTEMS FOR DECISION MAKING AND PROBLEMS OF COMPUTATIONAL INTELLIGENCE

ISDMCI'2018

Conference proceedings

Analysis and modeling of complex systems and processes
Theoretical and applied aspects of decision-making systems
Computational intelligence and inductive modeling

Zaliznyj Port – 2018

3. For ISP operated at the ground vehicles the important and necessary performance is the rigidity by the moment. This parameter can be determined in the following way. The increased disturbing moment is given to the system input in an immovable state. After some time delay (10…20) s the disturbing moment decreases to the nominal value. So, the law of change of the disturbing moment applied to the plant may be represented in the following form

$$M(t) = M_1[1(t)] - M_2[1(t)]. \quad (1)$$

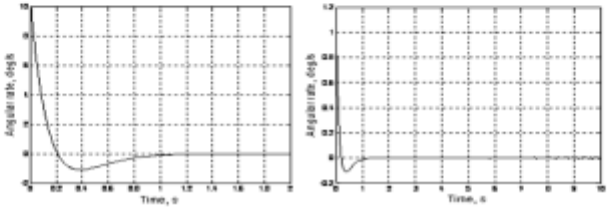
Further, the difference of the platform deviations under action of disturbing moments is determined

$$\Delta\varphi = \varphi_1 - \varphi_2. \quad (2)$$

Based on expressions (1), (2) the rigidity by the moment can be determined as a ratio of the difference of disturbing moments to the difference of values defining the platform angular stabilised position

$$c = (M_1 - M_2)/\Delta\varphi.$$

Depending on the solved problem and requirements to the given system modeling has been carried out by one channel only. Results of designed system simulation are given in Fig. 2.



a b

Fig. 2. Results modeling: (a) is the step signal without disturbances; (b) is the step signal taking into consideration irregularities of the relief (presence of hummocks

Conclusions. Features of ISP and its basic sensor (rate gyro) modelling are analysed. Simulation results of the designed system are given.

REFERENCES

1. J. Hilkert J.M. Inertially Stabilized Platform Technology // IEEE Control Systems Magazine. – No 1. – Vol. 28. – 2008. – P. 26 – 46.
3. Sushchenko O.A., Belinvtsev Y.V. Modeling of Inertial Sensors in UAV Systems // Proceedings 2017 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD) (October 17-19, 2017, Kyiv, Ukraine). 2017 – P. 130-133.
3. GG5200 two axis MEMS gyro. Access mode: http://wikis.controltheorypro.com/index.php?title=MEMS_Gyros.
4. Sushchenko O.A., Korostalev O.P. Mathematical Modeling of Inertially Stabilized Platforms Applied at Ground Vehicles // Electronics and Control Systems. – 2015. – no. 4(46). – P. 100–108.

BLOCKCHAIN IN EDUCATION

Tereshchenko G.U.

student of Kharkiv National University of Radio Electronics
pereulok Nikitenko, h.1, Kharkiv, 61075, Ukraine, gtereschenko3@gmail.com

Nowadays, the distributed database of the blockchain is increasingly being integrated into the document storage and control systems. The advantage of this technology lies in the lack of practical ability to manipulate the data recorded in the system, due to the fact that the information in the database can only be added, but not overwritten. At the same time, the truth of the document is easily traced, since everyone sees who has written it into the blockchain. Along with the identity card and the banking sector, "Cryptorevolution" did not ignore the education system.

ЗМІСТ

СЕКЦІЯ „АНАЛІЗ ТА МОДЕЛЮВАННЯ СКЛАДНИХ СИСТЕМ І ПРОЦЕСІВ”

The problem of control can become relevant for the education market. Up to now, the transfer of knowledge has gone largely through well-known institutions - schools and universities. Through them today the main financial flows of the education market also follow.

However, the blockchain threatens to shake this system. Technology allows students and teachers to contact faster, easier and more efficiently. More importantly, the blockchain will allow students to pay less for education, and teachers to earn more.

Anyone can announce a tender, for example, a student wants to attend a basic course in atomic physics, which will result in a number of proposals from teachers. Intermediaries of the educational institution will not be required.

Prospects for using blockchain technology are not limited to a distributed database. Its dynamism and transparency also has the potential to revolutionize the education system as a whole (by developing and legitimizing online learning). The popularity of Mass Open Online Courses (MOOC) is constantly growing, as they provide an opportunity to gain practical knowledge from anywhere in the world, and also have a lower cost of training. Based on the ability to combine individual courses into course blocks, you can offer different learning strategies for narrowly focused specialties.

Blockchain technology can be easily used for something else, except the hyper-fashionable in our days of the crypto-currency market. Here are four ways to change the education system:

1. Blockchain is able to let go of paper. Yes, these endless blocks can save trees from destruction. The block chain can safely and permanently store all records, issue reliable certificates and rewards, transfer funds and monitor progress in learning throughout the life of each person.

2. There is no need for a central authority to verify certificates. The Ministry of Information will no longer need to. Educational organizations will no longer have to send copies of alumni documents at the request of various organizations and companies in order to confirm the fact of getting an education. There will be no more "phony" doctors, as all diplomas will be kept freely available and easily subject to verification. Intellectual property management will also be simplified. Blokchain will track the sources of publications and quotations, eliminating the need for supervisory authorities. He can also help the author of the quoted work get automatic payment for the use of his works.

3. Educational institutions will save money and get very important information. Since people participating in the use of the blockchain have the right of ownership and control over their personal data, educational institutions will significantly reduce the cost of data management. Also, costs for legal costs related to claims in this sphere will be reduced. Currently, some professions that are in high demand by society, suggest a relatively small salary (for example, teachers). At the same time, representatives of other professions receive significantly more income, but for society their work is not so significant. With the help of distributed registry technology, the government will be able to obtain information about which professions are most in demand, just by looking at the blockchain. This will allow the authorities, for example, to approve scholarships and benefits for those professionals in which society at the moment most in need.

4. Crypto-currencies based on block-system will simplify the payment systems of educational institutions. All payments to students, such as scholarships and grants will be transferred almost instantly after the submission of relevant documents. In addition, you can create custom digital currencies to fund grants and projects.Certificates and diplomas confirm the presence of certain skills and knowledge of the candidate. Storing data in one system allows them to be distributed among companies, creating a system of dynamic personal search by a set of specialist skills for specific enterprises. In turn, this will create demand for certain skills, which, in turn, sets the trend for learning certain courses in real time. The candidate will see what exactly is required to study to obtain the desired position. Educational organizations, adjusting to the new trends of the labor market, will offer "dynamic blockchain courses," where the student chooses only what he needs for further professional growth.

Such vector of the development of the education system also fundamentally solves the problem of the rapid deactuation of curricula, formed during the acceleration of the development of Information Technologies.

Every year, the labor market trends are becoming ever more volatile. The speed of technology development is growing exponentially, and with it, the requirements for professionals in all areas of work. The relevance of educational programs that offer classical educational systems is sometimes reduced even at the beginning of the academic year and requires adjustment. The presence of dynamic monitoring of the requirements of companies for candidates, as well as the growing popularity of Massive Open Online Courses and online education in general, will allow educational organizations to painlessly adjust to the development trends in education, and establish relationships without intermediaries between them (specific universities, educational organizations, students and enterprises, working as a single system due to the blockchain register.

The cryptonomy grows, and the scope of technology based on the blockbuster is constantly expanding. A wide range of people continues to show a strong interest in crypto-currencies and progressive digital technologies.

Blockchain becomes the basis not only for financial instruments, but also for technologies that will soon surround us in everyday life. All this will contribute to the growth of the market of educational services in the field of digital technologies.

USED SOURCES:

1. Hoberman S. Blockchainopoly: How Blockchain Changes the Rules of the Game / Steve Hoberman., 2018. – 250 p.
2. White A. Blockchain: Discover the Technology behind Smart Contracts, Wallets, Mining and Cryptocurrency (including Bitcoin, Ethereum, Ripple, Digibyte and Others) / Abraham White., 2018. – 321 p.
3. Tapscott D. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World / D. Tapscott, A. Tapscot., 2016. – 368 p.

INFORMATION TECHNOLOGY FOR USING LIGHTS IN A VOLUME-ORIENTED RENDERING

Sergey I. Vyatkin[1], Olexander N. Romanyuk[2], Sergii V. Pavlov[2], Waldemar Wójcik[3]

[1]Institute of Automation and Electrometry SB RAS, Novosibirsk, 630090 Russia,
[2]Vinnytsia National Technical University
[3]Lublin Politechnica

INTRODUCTION. Voxel based volume graphics support a high degree of realism for simulation and visualization applications because they can contain both the surface and internal characteristics of a real object [1].Voxels are the basic unit of 3D volume graphic objects.Voxels (or volume elements) are simply pixels with a third coordinate (Z, in addition to X and Y coordinates). Voxels are typically placed on a regular grid so that every location for a voxel is the same size and same distance from the one beside, above, and below it.

Use the Light class to create one or more directional lights. A light has intensity and a direction that are specified in world space. Once lights have been created using Light class, they can be added to a rendering context using methods in the Context class. The Light class performs the following functions: creates a light object and returns a pointer to it; specifies a light's direction and intensity; returns current attributes of a light The Light object is a shareable object, and therefore inherits the methods and data of the Shareable class: Add Ref, Release, and others. The application is responsible for tracking the number of pointers to an object, using the Shareable Add Ref and Release methods, as appropriate.

PHONG MODEL. It describes the way a surface reflects light as a combination of the diffuse reflection of rough surfaces with the specular reflection of shiny surfaces [2]. It is based on Phong's informal observation that shiny surfaces have small intense specular highlights, while dull surfaces have large highlights that fall off more gradually. The model also includes an ambient term to account for the small amount of light that is scattered about the entire scene [3].

$$I_{res} = M_{re} \times LS_{ra}; I_{red} = M_{rd} \times LS_{rd}; I_{res} = M_{re} \times LS_{ra};$$

$$I_{rge} = M_{ge} \times LS_{ga}; I_{rgd} = M_{gd} \times LS_{gd}; I_{rge} = M_{ge} \times LS_{ga};$$

$$I_{rbe} = M_{be} \times LS_{ba}; I_{rbd} = M_{bd} \times LS_{bd}; I_{rbe} = M_{be} \times LS_{ba};$$

$$I_r = \begin{vmatrix} I_{re} & I_{rd} & I_{re} \\ I_{rge} & I_{rgd} & I_{rge} \\ I_{rbe} & I_{rbd} & I_{rbe} \end{vmatrix}, I = \begin{vmatrix} I_r \\ I_g \\ I_b \end{vmatrix} = \begin{vmatrix} \sum_i [I_{ra} + I_{rd}(\vec{l} \cdot \vec{n}) + I_{re}(\vec{H} \cdot \vec{n})^{shin}] \\ \sum_i [I_{ra} + I_{rd}(\vec{l} \cdot \vec{n}) + I_{re}(\vec{H} \cdot \vec{n})^{shin}] \\ \sum_i [I_{ra} + I_{rd}(\vec{l} \cdot \vec{n}) + I_{re}(\vec{H} \cdot \vec{n})^{shin}] \end{vmatrix}$$

Calculation of all color components of a pixel is performed in the same manner by the following formula:

$$C = (Q_{ambi}C_{ambi} + Q_{diff}C_{diff} + Q_{spec}C_{spec}) / (Q_{ambi} + Q_{diff} + Q_{spec});$$

where "ambi" refers to characteristics of ambient light, whereas "diff" and "spec" refer to the diffused and specular components of reflected light, respectively; C are the color components; Q are the weight coefficients. Color components are calculated by a vector light model. Four vectors are involved in the calculation: normal to the surface (n), vector to the light source (l), reflected light direction (r) and vector to the viewer (v):

$$C_{diff} = (n, l)\, C_{lm}\, C_{surf};$$

C_{lm} - is the light source color; C_{surf} - is the surface color;

УДК 001.8(063)
Т 33

Теорія і практика актуальних наукових досліджень. Матеріали
Т 33 II Міжнародної науково-практичної конференції (м. Одеса, 28-29 квітня 2018 року). – Херсон : Видавництво «Молодий вчений», 2018. – 184 с.

ISBN 978-617-7640-12-6

МАТЕРІАЛИ II МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ТЕОРІЯ І ПРАКТИКА АКТУАЛЬНИХ НАУКОВИХ ДОСЛІДЖЕНЬ»

(28-29 квітня 2018 року)

Одеса
2018

можливо лише в тому випадку, якщо до цього провести навчання по певній кількості оцінок меж коефіцієнтів k та y, які відповідають різним дефектам в підшипниках.

По результатам експериментальної перевірки та встановлення кількісних оцінок діагностичних ознак, які відповідають різноманітних технічним станам підшипників які досліджуються, можливо перейти до формування навчальних правил по діагностиці та класифікації конкретних видів пошкоджень підшипників [5].

В даній статті був розглянутий принцип діагностування підшипників кочення за допомогою вібраційних сигналів. На цьому принципі будуються системи вібродіагностування, які використовуються сьогодні. Ця тема є дуже актуальною. Бо в процесі використання певної машини чи пристрою, має велике значення прогнозувати термін роботи таких складових, як підшипників кочення. Це важливо і з економічної точки зору, тому для сучасних фабрик, цехів та підприємств є необхідністю завестись певними системами моніторингу та прогнозування стану машини, задля не втрати конкурентоспроможності.

Список використаних джерел:

1. Марченко Б.Г., Мыслович М.В. Вибродиагностика подшипниковых узлов. – К.: Наук. Думка, 1992. – 196 с.
2. Неразрушающий контроль: Справочник: В 7 т. Под общ. Ред. В.В. Клюева. Т. 7: В 2 кн. Кн. 1: В.И. Иванов, И.Э. Власов. Метод акустической эмиссии / Кн.2: Ф.Я. Балицкий, А.В. Барков, Н.А. Баркова и др. Вибродиагностика. – М.: Машиностроение, 2005. – 829 с.: ил.
3. Гузенков П.Г. Детали машин: Учеб. Для вузов. – 4-е изд, испр. М.: Высш. шк., 1986. – 359 с.: ил.
4. Костюков В.Н., Наумченко А.П. Учебное пособие. – Омск: Научно-производственный центр «Диагностика, надежность машин и комплексная автоматизация», 2007. – 286 с.
5. Бабак С.В., Мыслович М.В., Сысак Р.М. Статистическая диагностика электротехнического оборудования – К.: Ин-т электродинамики НАН Украины, 2015. – 456 с.

Tereshchenko G.U.
Student,
Kharkiv National University of Radio Electronics

BLOCKCHAIN AND SMART CONTRACTS IN CARGO TRANSPORTATION

Blockchain is a technology for storing confirmed records in public or private access, transferring financial transactions, documents, creating smart contracts, issuing their own tokens and providing NODA to regulators and third parties. We can provide a solution with the integration of existing IT solutions and implement AI, VoIP, BPM, CRM, ERP.

Today it is possible to propose a technological breakthrough in the logistics industry by creating a transparent system of interaction between all market participants. The decentralized logistics platform offers innovative solutions based on the implementation of blockchain technology in supply chain management. It is a decentralized system that uses a blockchain and consists of several smart-contracts inside a blockchain and its own tokens (if necessary) [1, p. 34].

The main task is to reduce the cost of logistics, so that its share in the cost of goods is minimal. The problem of trust. The control of cargo transportation is carried out, upon request, until the transaction is successfully closed. All actions are recorded in the blockchain, which excludes non-trusting relationships between the parties; Smart-contract, which will be approved at the beginning of the shipment, will automatically perform a mutual settlement in accordance with the data stored in the blockchain.

ТЕХНІЧНІ НАУКИ

– Danger of hidden damage. During transportation, the cargo may be damaged, while the carrier may not be aware of this. If the owner of the goods (or the last link in the supply chain) receives defective goods, sometimes it is not possible to demand compensation in court, since it is not known who is responsible for the damage.

– The problem of idle runs. The pendulum principle means up to 50% loss of efficiency in the logistics sector.

The problem is that the balance of exports and imports is skewed in the subregions, that is, the truck driver delivers the drink from point A to point B and returns blank because there is nothing to transport from point B. Thus, the charterers tend to double their bets. – The problem of information barriers and high prices. The costs of finding information on tariffs and transactional costs of the carrier are critically high due to fragmentation of the market and the lack of standardization of payment algorithms, document flows, availability of additional services and taxation. This leads the market to less competitiveness and makes it a managed seller. Thus, the cargo owner faces the need to know in advance and compare the prices for transportation and to make an expensive check. This problem affects both cargo owners and cargo carriers. For example, the lack of a common information space leads to loss of efficiency and delays due to the lack of data on empty containers. The main advantage of implementing blockchain: providing synchronized audit between partners and optimizing processes in real time. Blockchain will increase the level of trust within the entire chain and simplify the decision making process at each stage, by providing a one-time access to information that allows you to jointly forecast processes and actions [3, p. 42].

When implementing blockchain in the supply chain even in the most basic version, the technology will provide:

– the ability to track the product from the place of origin to the end user, protect the buyer from forgery and deception. What will allow the buyer to make a measured decision about the purchase;

– decentralization, which will allow all parties to the supply chain to participate in the process in real time: monitoring the movement of goods and transport, filling out documents in the form of smart contracts (reducing the likelihood of errors and fraud), eliminating illegal links in the supply chain (counterfeiting, smuggling, use slave labor in production).

Problems for implementing blockchain in logistics:

– elimination of people from work (reduction of jobs);

– skepticism about technology;

– complexity of coordination of participants and standardization of business processes.

The implementation of Blockchain in logistics will ensure the safety of data, protection of the repository of documents from hacking, eliminate the possibility of making changes in information about the progress of transportation. Such a system can definitely reduce delivery delays and reduce the likelihood of fraud, saving billions of dollars by all participants in the transportation chain. According to the World Trade Organization, removing barriers in the chain of international supply of goods will increase world GDP by 5% and the total volume of transport by 15%.

References:

1. Reed J. Smart Contracts: The Essential Guide to Using Blockchain Smart Contracts for Cryptocurrency Exchange / Jeff Reed., 2016. – 54 p.
2. Parker T. Smart Contracts: The Ultimate Guide To Blockchain Smart Contracts – Learn How To Use Smart Contracts For Cryptocurrency Exchange! / Terry Parker., 2016. – 30 p.
3. Bock S. Blockchain: Bitcoin, Ethereum, Smart Contracts, Cryptocurrencies and Everything about the Fintech Explained / Shane Bock., 2017. – 66 p.

Tokens will be issued automatically through a smart contract, as well as the provision of risks can be formed through integration with banks and the receipt of a Security or receipt of collateral, risk insurance. All of this is designed to reduce the risk of unfair business practices or invalid delivery contracts, lack of real-time obligations, and:

– eliminate unnecessary intermediaries;

– to form responsible and automated operators;

– manage the process of mutual payments online;

– work with documents accompanying transactions;

– track location Online GPS tracking of cargo, vehicles in 24/7 mode is carried out using blockchain technology;

– quickly find suitable transport for delivery;

– to find cargo for the carrier;

– guarantee payment to all participants of the platform;

– guarantee the quality of the order;

– do not waste time on permanent business processes and automate some of them; – automate and algorithmize the main permanent processes;

– to form open or closed (confidential) supply chains; – Reduce legal costs;

– Reduce transportation costs for the shipper;

– Reduce the human factor and costs for all participants in the platform;

– load vehicles and reduce empty mileage;

– monitor the condition of drivers and the moments of shipment / acceptance of cargo

– unconditional execution of a smart contract and commitments

– to receive the analysis and the exchange of offers of freight and cargoes, owners of motor transport and professional participants of the market of transport services;

– to form the base of «trusted» suppliers and cargo owners;

At the moment, the commission for intermediary services during the carriage of an average of 10 to 45% of the total amount of the order. At the same time, the formation of this amount and its change are not controlled by the customer in any way. Most of the risks in the logistics industry are related to financial calculations and the quality of performance of obligations by freight carriers, as well as the transfer of information that may be false or incomplete. Avoiding work with centralized services and applying Smart-contract and blockchain technologies will ensure transparency in the logistics market. The formation of the commission will become transparent, and the prices for services will decrease due to open and transparent interaction of all participants in the supply chains. IT solution will significantly reduce the amount of time, financial and human resources involved in the transportation process. At the same time, new markets will open up for carriers, and the platform can become available not only to one customer and return the invested funds, but also be a standard of quality of transport and logistics services provided in the market [2, p. 15].

The final payment is usually made after the moment when the owner of the cargo receives it from the carrier. This forces freight carriers to conduct due diligence of cargo owners and to charge a premium for the risk of a possible default on their obligations. Logistic companies change their fees in the range of up to 30% and even deviate from the transaction depending on the reputation of the counterparty:

– Insufficient insurance. Most forwarding companies practice insurance only for transport losses, but not for cargo loss and compensation for damage.

– Currency risk. Carriers and forwarders can set prices in a currency that is different from the current currency. In this case, the logistics company is forced to supplement the contract with the payment of fees in order to exclude the risk of currency devaluation. This makes logistical services more expensive.

– The risk of tax evasion. If there is a suspicion of the tax regulator, in relation to at least one of the parties to the supply chain in evading taxes, the goods will be recalled or frozen.

УДК: 004.9

Наукові редактори: А.Д. Тевяшев - доктор технічних наук, професор (Харківський національний університет радіоелектроніки);
Л.Б. Петришин - доктор технічних наук, професор (Прикарпатський національний університет ім. В. Стефаника, Науково-технологічний університет "Гірничо-металургійна академія" імені Станіслава Сташіца в Кракові);
В.Г. Кобзєв – кандидат технічних наук, старший науковий співробітник (Харківський національний університет радіоелектроніки)

Рецензенти:

Секція 1. В.О. Філатов - доктор технічних наук, професор (Харківський національний університет радіоелектроніки);
Секція 2. В.В. Безкоровайний - доктор технічних наук, професор (Харківський національний університет радіоелектроніки);
Секція 3. О.Є. Федорович - доктор технічних наук, професор (Національний аерокосмічний університет «ХАІ»);
Секція 4. В.П. Машталір - доктор технічних наук, професор (Харківський національний університет радіоелектроніки);
Секція 5. О.О. Шумейко - доктор технічних наук, професор (Дніпровський державний технічний університет);
Секція 6. Н.В. Шаронова - доктор технічних наук, професор (Національний технічний університет «ХПІ»);
Секція 7. І.С. Шостко - доктор технічних наук, професор (Харківський національний університет радіоелектроніки);
Секція 8. В.А. Лужецький - доктор технічних наук, професор (Вінницький національний технічний університет);
Секція 9. Є.В. Бодянський - доктор технічних наук, професор (Харківський національний університет радіоелектроніки)

Матеріали статей рецензовано та опубліковано в авторській редакції.

Інформаційні системи та технології: матеріали статей 7-ї Міжнародної науково-технічної конференції, Коблеве - Харків, 10-15 вересня 2018 року / наук. ред. А.Д. Тевяшев, Л.Б. Петришин, В.Г. Кобзєв. – Х.: ХНУРЕ, 2018. – 478 с.

ISBN 978-617-7683-63-5

Збірник містить матеріали статей Мiжнародної науково-технічної конференції з проблем сучасних інформаційних систем та технологій.

Матеріали представляють інтерес для фахівців, науковців і аспірантів, діяльність яких пов'язана з розробкою та впровадженням сучасних інформаційних систем і технологій.

Міністерство освіти та науки України
Національна академія наук України
Люблінський відділ Польської Академії Наук
Представництво „Польська академія наук" у Києві
Харківський національний університет радіоелектроніки
Харківський національний університет міського господарства ім. А.М. Бекетова
AGH науково-технологічний університет в Кракові
Миколаївський кораблебудівний університет ім. адмірала Макарова
Одеський національний політехнічний університет
Прикарпатський національний університет ім. В. Стефаника
Українська нафтогазова академія
Українська Федерація Інформатики
Академія Наук Прикладної Радіоелектроніки
Білоруський державний університет інформатики та радіоелектроніки
Білоруський національний технічний університет
Національний університет цивільного захисту України
Запорізький національний технічний університет

«Інформаційні системи та технології» ІСТ-2018

МАТЕРІАЛИ

7-ї Міжнародної науково-технічної конференції,

присвяченої 55-річчю кафедри Прикладної математики ХНУРЕ, 55-річчю кафедри Програмної інженерії ХНУРЕ та 40-річчю кафедри Прикладної математики та інформаційних технологій ХНУМГ імені О.М. Бекетова

10-15 вересня 2018
Коблеве-Харків, Україна

«INFORMATION SYSTEMS AND TECHNOLOGIES» IST-2018

Proceedings
of the 7-th International Scientific and Technical Conference

September 10-15, 2018
Kobleve-Kharkiv, Ukraine

Харків 2018

Blockchain in Public Administration

Glib Tereshchenko
Department of Software Engineering
Kharkiv National University
of Radio Electronics
Kharkiv, Ukraine
hlib.tereshchenko@nure.ua

Oleksii Nazarov
Associate Professor of Program Engineering Department
Kharkiv National University
of Radio Electronics
Kharkiv, Ukraine
oleksii.nazarov1@nure.ua

Блокчейн у Державному Управлінні

Гліб Терещенко
Кафедра Програмної інженерії
Харківський національнийуніверситет
радіоелектроніки
Харків, Україна
hlib.tereshchenko@nure.ua

Олексій Назаров
Доцент Кафедри Програмної інженерії
Харківський національнийуніверситет
радіоелектроніки
Харків, Україна
oleksii.nazarov1@nure.ua

***Abstract*—The article describes the possibilities of using blockchain technology in public administration. Cautions against possible negative consequences of its use, the authors pay attention to the advantages of the technology in question.**

Keywords—blockchain; bureaucracy; public administration.

Анотація—The article describes the possibilities of using blockchain technology in public administration. Cautions against possible negative consequences of its use, the authors pay attention to the advantages of the technology in question.

Ключові слова—блокчейн; public administration; державне управління.

I. BLOCKCHAIN

Blockchain is a database in which you can store records about objects and events in real life. At the same time, the blockchain is significantly different from other similar technologies due to its openness and reliability. Entries in the blockchain is almost impossible to fake, replace or delete. At the same time, everything recorded in the blockchain is easy to check and make sure that the entries are correct.

Currently, this technology is used most often in cryptocurrencies, such as the well-known Bitcoin. Developers usually try to create their own Bitcoin counterpart, in which they try to take into account the mistakes of the founder and introduce something of their own. That is why, studying the technology of a distributed database, you can see a lot of cryptocurrency technologies similar to each other. [1]

The concept of blockchain originated a long time ago and is now used mainly in combination with a cryptocurrency bitcoin. The essence of technology in the distributed storage of information relating to any vital issues. Simply put, this is the database, the registry, which allows us to constantly record the event.

Blockchain is needed wherever there is a question of potential mistrust between participants. For example, when buying and selling, there are always at least two questions: whether the seller will receive the money and whether the buyer will receive the service / product. Similarly, when obtaining important documents, it is also necessary to make sure that the documents are not forged and relevant. In addition, in many situations it is necessary to find out the reliable history of a product, service, company or person. For these tasks, the blockchain will be very useful and appropriate. One of the applications of blockchain technology is "smart contracts" that are used in various sectors of the economy, in particular insurance, loans and notarial services.

II. PUBLIC ADMINISTRATION

The public sector is a complex and inert mechanism, while remaining a centralized system. From the development of this system depends the effectiveness of public administration as such, the uniform coverage of public services by the needs of the population and entrepreneurs (for example, company registration, marriage, receipt of certificates and extracts). Sometimes on the complexities in the interaction of a person and the state apparatus, its non-transparency, whole industries of intermediaries grow up (help in registering LLC, filling in certificates of traffic police, etc.). The more intermediaries - the more expensive and more difficult the service. The organizational structures of the state apparatus are often fragmented and almost always scattered, which makes it difficult to exchange information between departments and departments. Often, intermediaries in the chain of receiving state services are invisible to the recipient (agencies communicate with each other in the "back-end").

Many countries are aware of the demands of a new generation, people who are accustomed to fast and convenient products, conduct research and solve the aforementioned problems - are actively reforming the delivery system of public services. Some mobilize the separated IT departments into unified systems - the so-called "agencies"; others start

Национальная академия наук Украины
Люблинский отдел Польской Академии Наук
Представительство „Польская академия наук" в Киеве
Харьковский национальный университет радиоэлектроники
Одесский национальный политехнический университет
Прикарпатский национальный университет
им. В. Стефаника
Университет таможенного дела и финансов
Национальный горный университет
Академия Наук Прикладной Радиоэлектроники
Украины, России и Беларуси
Украинская нефтегазовая академия
Украинская Федерация Информатики
Харьковский национальный университет городского хозяйства им.
А.Н. Бекетова
Белорусский государственный университет информатики и
радиоэлектроники
Белорусский государственный экономический университет
Люблинская Политехника

МАТЕРИАЛЫ

6-й Международной научно-технической конференции

Информационные системы и технологии ИСТ-2017,

посвященной 80-летию В.В. Свиридова

11-16 сентября 2017
Коблево, Украина

Харьков 2017

using alternative deep data and "dark analytics" for a quick analysis of correspondence and requests from the public; others develop new architectures of interaction between state units; Well, the last, the most advanced, of course, apply the technology of the distributed registry (blockchain), on which we will stop [2].

The speed with which various state departments of the countries of the world today are beginning to use blockchain technologies is not proportional to the real development and the level of practical implementation of this technology - which is quite logical and understandable. The public administration system must be stable, it is an extremely static, slow-moving mechanism, and any implementation must prove its effectiveness. In addition, not all blockchain-based solutions are able to scale and correspond to the load.

III. Health care.

Despite the fact that electronic medical cards, online access to patient data and their modification can be realized without the use of blockchain systems, the problem of reliability and reliability of data remains unresolved. With the use of blockchain-technology, unauthorized modification / access / use of citizens data becomes impossible, since any information about such actions is recorded in the system [3].

Blockchain is ideal for creating a single patient registry. In fact, there will be a single electronic database with a high level of security, stable operation and access from anywhere. Having such an infrastructure, the patient does not have to worry about the synchronization and security of personal data.

IV. Keeping the land cadaster

It is interesting that this direction of the implementation of blockchain is popular both in developed and developing countries. In developing countries, the ownership of land is still poorly documented, as a result of which owners can not sell it, take loans on bail and conduct other operations with land. People suffer from abuse of employees of relevant departments. Developed countries improve operational processes, decreasing the time of the transaction, which often takes several months, reduce the risk of fraud and errors in documents and transactions (transfer of rights, for example), making the process and system more reliable. This leads to an increase in the attractiveness of the country for doing business and investments [4].

In addition to legal certainty, the technology also guarantees the physical preservation of data - even if the server is destroyed, it is stored on the computers participating in the chain.

But, in addition to a few abstract concepts of trust and reputation, developers rely on and quite tangible practical effects from the implementation of the blockade. True, they are all in perspective.

V. Company registration, voting

These areas are most closely connected with the exchange of information between government agencies, and thus, existing projects are aimed at reducing the costs associated with the exchange of information and unification in a single information storage system.

Elections using blockchain are similar to the usual deal in the crypto currency. Citizens receive special colored coins from the election commission, which are then transferred to one of the special accounts associated with one or another candidate. To determine the winner, it is enough to check the accounts after the election is over. Since a public blockchain can be analyzed by anyone, each user can track the fate of his voice. And in order for the members of the electoral committee not to demonize the voters, scientists suggest distributing colored coins with the help of technology of blind signatures.

VI. Reforms in Education

If educational institutions register registered education diplomas or certificates of training in a detachment, it is not difficult for a potential employer to make sure that you did study at a given institution or course, and did not acquire a "lime" diploma.

Certificates and diplomas confirm the presence of certain skills and knowledge of the candidate. Storing data in one system allows them to be distributed among companies, creating a system of dynamic personnel search by a set of specialist skills for specific enterprises. In turn, this will create demand for certain skills, which, in turn, sets the trend for learning certain courses in real time. The candidate will see what exactly is required to study to obtain the desired position. Educational organizations, adjusting to the new trends of the labor market, will offer "dynamic blocks of courses," where the student chooses only what he needs for further professional growth.

VII. Conclusion

According to a survey of participants of one of the last World Economic Forum, by 2023 the technology of blockchain will be actively used in the sphere of public services by the leading world powers. Moreover, about 10% of world GDP (according to the OECD forecasts) will be created with the direct use of blockchain technology. The main benefits from the introduction of technology are expected in the reduction of operating expenses, reduction of settlement time, risk reduction, an increase in the possibility of receiving additional income. This technology will allow each of us, as a time machine, to jerk, and in another way we do not know how to move from an ineffective bureaucratic state system of cohabitation to a home state, to a modern, easy, convenient, trust system "the state is me" [5].

References

[1] Jun M. Blockchain Government: A next form of infrastructure for the twenty-first century / Myungsan Jun., 2018. – 241 p.

[2] Vigna P. The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order / P. Vigna, M. Casey., 2016. – 384 p. – (Reprint edition).

[3] Nichol P. The Power of Blockchain for Healthcare: How Blockchain Will Ignite The Future of Healthcare / Peter Nichol., 2017. – 222 p. – (1 edition).

[4] IPRA-CINDER International Review: Blockchain and Land Registries / [B. Arrufada, B. Rodriguez-Rosado, P. O'Connor та ін.]., 2017. – 137 p. – (Kindle Edition). – (ICIR Book 1).

[5] Gates M. Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. / Mark Gates., 2017. – 125 p.

УДК: 004.9

Информационные системы и технологии: материалы 6-й Международ. науч.-техн. конф., посвященной 80-летию В.В. Свиридова, Коблево-Харьков, 11-16 сентября 2017 г.: тезисы докладов / [редкол.: А.Д. Тевяшев (отв. ред.) и др.]. – Х.: ХНУРЭ, 2017. – 330 с. В предзаг.: Министерство образования и науки Украины, Харьковский национальный университет радиоэлектроники.

В сборник включены тезисы докладов, посвященных современным информационным системам и технологиям: опыту создания, моделям, инструментам и проблемам.

Материалы конференции представляют интерес для специалистов и аспирантов, связанных с разработкой и внедрением современных информационных систем и технологий.

APLICATION OF TECHNOLOGY BLOCKCHAIN IN ECONOMY

Tereshchenko G.Y.
Kharkiv National University of Radio Electronics

Blockchain is a database in which you can store records about objects and real-life events. At the same time, blockade is significantly different from other similar technologies due to its openness and reliability. Records in the blockade are almost impossible to forge, replace or delete. At the same time, everything fixed in the block is easy to check and make sure the records are correct.

Currently, this technology is used most often in crypto-currencies, such as the well-known bitcoin. Developers usually try to create their analog bitcoin, in which they try to take into account the errors of the founder and bring something of their own. That is why, when studying the technology of a distributed database, one can see a lot of technologies that are similar to each other [1].

The concept of blockchain arose long ago and is now used primarily in conjunction with the crypto currency bitcoin. The essence of technology in the distributed storage of information relating to any vital issues. Simply put, it's a database, a registry, which allows us to permanently fix an event.

The railway changed our notion of distance: the world became closer, we began to move faster on it. Aircraft helped us to reduce the distance between the continents. Telecommunications allowed to communicate freely and influenced the ways of information transfer. But the issue of fixing property rights remains unresolved. The institution of the state and the notary himself has been discredited: it is easy to forge any documents that prove your ownership of one or another object of the physical world.

Blockchain is needed everywhere, is there a question of potential mistrust between the participants. For example, when buying and selling, there are always at least two questions: will the seller receive money and will the customer receive the service / goods. Similarly, when you receive important documents, you also need to make sure that the documents are not forged and relevant. In addition, in many situations it may be necessary to find out the true history of a product, service, company or person. For these tasks, blockchain will be very useful and relevant. One of the areas of application of block technology is "smart contracts", which are applied in various sectors of the economy, in particular - insurance, lending and notarial services [2].

Blockchain is designed, among other things, to solve the problem of fixing property rights once and for all. That is why it is so important for business, because ownership is one of the cornerstones of business. And if now this way of storing information is a novelty, then remember that the word "google" 20 years ago looked like a set of letters. I believe that after 20 years the blockchain will also not be exotic, but will become a habitual way of storing any important information - financial transactions, property data, and ideally a single passport containing data on DNA, funds and property rights.

And having lost the documents of the physical world, you can by a drop of blood prove that you are you, and get back all the objects that belong to you by right [3].

It is known about the recent change in Ray Kurtzweil's prediction, Google's technical director, who reduced the timing of the onset of the singularity by almost half. We must now understand that the speed of change, including the emergence of new technologies, is growing catastrophically. And the technology of blockchain will play a significant role in this.

Many are not yet ready to tolerate such changes, but after all, a wired phone was once also a frightening curiosity. Blocking is a serious change that simply changes our attitude to the right of ownership and the way of fixing certain events.

Companies will have the opportunity to conduct any financial, insurance and other transactions in an environment where everything is fully automated, since the transaction will be considered perfect if there are signatures from both parties and all the terms of the contract are fulfilled. All this is fixed within the system, and there is no possibility of interference in the process of execution or signing of the contract, that is, it is impossible to change its conditions at any time, until all the participants in the contract agree to this. This excludes any fraud, which in turn will be very interesting to users of the system and also helps to exclude undesirable intermediaries. In addition, the block can be used in the sphere of notarial services.[4]

Also worth noting is the usefulness of using blockade in the media sphere. In the last two decades, digital technologies have greatly influenced the entertainment industry and the media sphere. Still, the problems have not disappeared, especially when it comes to free copying of content and issues of compensation to authors for the fact that their works are used or sold through legal channels of distribution. With the help of the blockbuster, it is possible to solve this problem both by directly communicating musicians, writers and videographers with their clients, and by restructuring the processes within the main players of the media market. The technology of blocking can also be used to create technologies to automate most business processes. In particular, AIRA technology allows managing a decentralized autonomous organization, adding agents, creating contracts and values, in other words - automating the company's business processes.

1. Antonopoulos A. Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Andreas Antonopoulos. – Sebastopol: O'Reilly Media, 2014. – 298 p.

2. Vigna P. The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order / P. Vigna, M. Casey. – US: Picador, 2016. – 384 p.

3. Tapscott D. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World / D. Tapscott, A. Tapscott. – NY: Portfolio, 2016. – 368 p.

4. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction / [A. Narayanan, J. Bonneau, E. Felten and others] // Princeton University Press, 2016. – 336 p.

АЛФАВІТНИЙ ПОКАЖЧИК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ XXIII МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

16 -- 18 квітня 2019 р.

Том 6

КОНФЕРЕНЦІЯ «ІНФОРМАЦІЙНІ ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ»

Харків 2019

DECENTRALIZED SYSTEM IN IT INDUSTRY

Tereshchenko G.U.
Scientific adviser - candidate of technical sciences, Associate Professor at the Department of Software Engineering, Nazarov A.S.
Kharkiv National University of Radio Electronics
(61166, Kharkiv, 14, Nauky ave., Department of Software Engineering, phone: (057) 702-14-46)
e-mail: hlib.tereshchenko@nure.ua, phone: +380661574986

The Blockchain technology is able to transform established business processes and radically change the work with regulators. However, the blockchain remains an experimental technology - many problems of its use have not yet been resolved. The technology is really able to protect the data with which we have to work, while making them more accessible and transparent. In addition, the blockchain can significantly reduce costs and minimize the time required to solve problems and eliminate errors.

The introduction of the blockchain is by definition a complicated process, but the basic idea of the technology is simple: a distributed registry or database running simultaneously on many (sometimes millions of) nodes distributed around the world between different users and organizations. The uniqueness of the blockchain lies in its immutability or irreversibility, which is guaranteed by a cryptographic system of protection. For example, when transactions from the registry are grouped into blocks and written to the database, the entry is preceded by cryptographic verification, as a result of which it is almost impossible to change the state of the registry by any frauds. The fact that any changes in the data in the block chain are possible only if the participants in the network confirm the legitimacy of the transaction in accordance with the general rules and protocols also speaks in favor of trusting the blockchain [1].

The capabilities of Distributed Registry Technologies (DLT) are attractive not only for the IT industry. Their potential allows you to combine many concepts and functions in one solution. They provide an opportunity to take a different look at the established processes, simplify them, add transparency and reduce costs, making the business more flexible [2].

We are talking about immutable transactions, preventing data loss, the ability to track digital assets, cryptographic security, consensus algorithms, joint verification of transactions by untrusted participants. All processes are carried out in the cloud and meet the principles of distribution and sharing.

We will see an increase in the number of projects in which the blockchain technology will find application in processes that are not directly related to payments or cryptocurrencies. For example, one should expect a rapid growth in the share of research and development aimed at studying exclusive blockchains and the use of smart contracts to solve problems of low efficiency and delays in business processes related to inspections, coordination and control [3].

The combination of blockchain technology with machine learning capabilities will automate the development of complex solutions (for example, in working with insurance companies). Examples of the use of this blockchain-innovation include placement of contracts, evaluation of claims, and invoicing based on triggers.

We expect to see new financial services solutions where smart contracting principles are used for data management and sharing, especially in those areas where the data was originally recorded in PDF files (for example, financial statements or loan agreements) [4].

In the near future, we should expect solutions from larger companies and communities, such as the B3i insurance group (The Blockchain Insurance Industry Initiative). Their initiatives can seriously affect industry standards and business practices in the future.

Open source companies will increasingly help companies create new technical components and solutions for entire industries (for example, smart contracts libraries and data sharing).

The use of the blockchain in various industries has enormous potential, and in 2019 that promises to be a turning point in development. The blockchain has ceased to seem a mysterious technology available to the units. Now, with its help, leaders seek to transform entire industries, going beyond the narrow confines of the blockchain's original purpose [5].

Blockchain is a new paradigm of the information world. She knocked on the door in 2008, when someone named Satoshi Nakamoto described an electronic payment protocol for a peer-to-peer network. This was the basis for the blockchain technology. This is a mathematical algorithm that allows you to safely and privately share values through peer-to-peer networks. The first practical implementation of the blockchain was the Bitcoin network.

List of sources

1. Hoberman S. Blockchainopoly: How Blockchain Changes the Rules of the Game / Steve Hoberman., 2018. – 250 p.
2. White A. Blockchain: Discover the Technology behind Smart Contracts, Wallets, Mining and Cryptocurrency (including Bitcoin, Ethereum, Ripple, Litecoin and Others) / Abraham White., 2018. – 321 p.
3. Tapscott D. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World / D. Tapscott, A. Tapscott., 2016. – 368 p.
4. Chris Skinner Value Web / Chris Skinner -- K. Information technologies, 2016. – С. 150 – 175.
5. Roger Wattenhofer The Science of the Blockchain / Roger Wattenhofer – Information technologies, 2016 – С. 94 – 120.