JUSTINDO
Jurnal Sistem dan Teknologi Informasi
http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO
E-ISSN: 25541-5735, P-ISSN: 2502-5724
Volume 6, No. 2, Agustus 2021

Implementasi *Multi Smart Contract* pada Bukti Digital dan *Chain of Custody* dalam Meningkatkan Keamanan dan Integritas Bukti Digital

Arif Surya Putra[1], Yudi Prayudi[2]

[1]Universitas Islam Indonesia
Email: [1]16917202@students.uii.ac.id, [2]prayudi@uii.ac.id)

(Naskah masuk: 18 Desember 2020, diterima; 1 Juli 2021, diterbitkan: 30 Agustus 2021)

ABSTRAK

Bukti digital yang disimpan dalam blok mengurangi kinerja blok, mengurangi kecepatan akses blok dan mengurangi kapasitas media penyimpanan data. Informasi-informasi metadata yang diambil dari bukti digital yang hanya berupa informasi dasar terkait bukti digital dapat mengurangi integritas bukti digital dan juga menyulitkan penyidik dalam mengidentifikasi bukti digital. Pengurangan integritas bukti digital menyebabkan bukti digital ditolak dalam persidangan. Penerapan multi smart contract dalam mengelola bukti digital dan chain of custody menjadi solusi untuk menyelesaikan permasalahan tersebut. Penerapan multi smart contract juga diharapkan mampu meningkatkan kinerja blok dan mengoptimalkan media penyimpanan bukti digital. Langkah-langkah untuk membuat sistem multi smart contract dimulai dengan melakukan identifikasi masalah, melakukan studi literatur, merancang dan membangun sebuah sistem multi-smart contract, pengujian terhadap implementasi, integritas, dan performa sistem multi smart contract , dan analisa terhadap implementasi multi-smart. Hasil dari penerapan multi smart contract ditemukan bahwa bukti digital memiliki karakteristik berbeda-beda dan detail informasi yang berbeda-beda antara satu jenis bukti digital gambar, audio, video, dan dokumen atau jenis bukti digital lainnya. Informasi yang detail mampu meningkatkan integritas bukti digital. Otomatisasi dalam membuat hash dan ekstraksi informasi dari suatu bukti digital dapat mengurangi waktu first responder dalam menginputkan form isian pada sistem multi smart contract. Penyimpanan bukti digital di luar blok dapat meningkatkan performa sistem multi smart contract. Penyimpanan bukti digital yang hanya berupa alat bukti persidangan mampu mengoptimalkan media penyimpanan bukti digital.

Kata kunci: *bukti digital, blockchain, multi smart contract, chain of custody*

ABSTRACT

Digital evidence stored in blocks reduces block performance, reduces block access speed and reduces the capacity of data storage media. Metadata information taken from digital evidence which is only basic information related to digital evidence can reduce the integrity of digital evidence and also make it difficult for investigators to identify digital evidence. This reduction in the integrity of digital evidence causes digital evidence to be rejected in court. The application of multi smart contracts in managing digital evidence and chain of custody is a solution to solve these problems. The implementation of multi smart contracts is also expected to improve block performance and optimize digital evidence storage media. The steps to create a multi smart contract system begin with identifying problems, conducting literature studies, designing and building a multi-smart contract system, testing the implementation, integrity and performance of the multi smart contract system, and analyzing the multi-smart implementation. The results of the application of multi smart contracts found that digital evidence has different characteristics and different details of information between one type of digital evidence, images, audio, video, and documents or other types of digital evidence. Detailed information can improve the integrity of digital evidence. Automation in creating hashes and extracting information from digital evidence can reduce the time for first responders to input form fields in a multi-

smart contract system. Storage of digital evidence outside the block can improve the performance of a multi smart contract system. Digital evidence storage, which only takes the form of evidence, is able to optimize digital evidence storage media..

Keywords: *digital evidence, blockchain, multi smart contract, chain of custody*

1. PENDAHULUAN

Peningkatan kejahatan di dunia maya memberi dampak pada meningkatnya volume bukti digital yang ditangani oleh para penyelidik. Ini juga dapat menyebabkan lebih banyak dokumentasi dan kompleksitas manajemen bukti digital. (Prayudi, Ashari, & K Priyambodo, 2014). Bukti digital yang tidak dikelola dengan baik maka integritasnya biasanya akan dipertanyakan dan bukti digital tersebut akan mengalami penolakan dalam persidangan (Bonomi, Casini, & Ciccotelli, 2018).

Permasalahan tersebut kemudian diselesaikan menggunakan teknologi blockchain oleh peneliti seperti Bonomi, Lone, dan Yunianto. Penelitan sebelumnya sebagian besar menggunakan satu smart contract dalam mengelola semua bukti digital. Namun integritas dan pengamanan bukti digital dirasa masih kurang, sehingga pada penelitian selanjutnya maka akan dikembangkan sebuah model blockchain yang bisa memisahkan chain of custody berdasarkan jenis atau tipe filenya dalam smart contract yang berbeda-beda. Dari hasil pemisahan tersebut kemudian akan disajikan informasi yang lebih detail mengenai bukti digital tersebut. Pengelompokkan dan penambahan detail informasi ini diharapkan bisa meningkatkan integritas dan keamanan bukti digital berserta *chain of custody* nya

2. LITERATUR REVIEW

Penelitan tentang penggunaan blockchain dalam mengelola bukti digital dan *chain of cusotdy* dimulai untuk mengatasi permasalahan tentang integritas bukti digital.

Lone, (2017) mengajukan sebuah model yang disebut *forensic chain* untuk menangani peningkatan pelanggaran integritas dan penolakan pada suatu bukti digital di persidangan, yang disebabkan oleh tidak jelasnya sumber, cara penanganan, dan cara mengamankan bukti digital. Model ini menggambarkan tentang cara *Blockchain* dengan *Smart Contract*-nya mampu mengelola dan mengamankan suatu rekaman aktivitas (*Chain of Custody*) dari suatu barang bukti digital dengan menyimpannya pada blok-blok yang terenkripsi.

Menurut Lone A. H., (2019) implementasi model ini sudah bisa digunakan untuk menjaga integritas, keaslian, keamanan, dan kemampuan mengaudit dokumen *Chain of Custody* dari suatu bukti digital. Selain itu dari hasil pengujian performa, sistem ini *overhead*-nya sudah bisa diterima dan bisa diimplementasikan di dunia nyata. Namun Lone masih menggunakan skema standar untuk mencatat aktivitas dari pengelolaan bukti digital. Tidak ada acuan penelitian lainnya dalam membuat instrumen *Chain of Custody* untuk *smart contract*-nya. *Smart contract* yang digunakan untuk menyimpan dokumen *Chain of Custody* masih menggunakan satu format untuk semua bukti digital.

Banyaknya investigator ataupun ahli yang ikut berpartisipasi dalam menganalisa bukti digital dan cara mempertanggungjawabkan bukti digital

 p-ISSN : 2502-5724; e-ISSN : 2541-5735

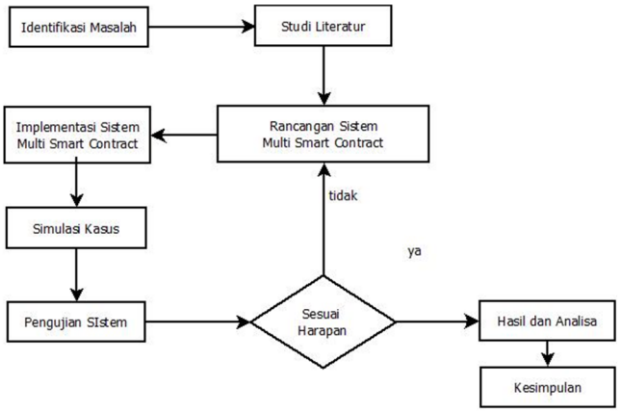
agar diterima di pengadilan yang melatarbelakangi penelitian tentang pemanfaatan *Blockchain Ethereum* dalam mengelola dokumen *Chain of Custody* (Bonomi, 2018). *Ethereum* digunakan sebagai *private* atau *permissioned Blockchain*, sehingga hanya pengguna dengan otoritas tertentu yang mampu mengakses dokumen *Chain of Custody*. Penggunaan *ethereum* dalam mengelola dokumen *Chain of Custody* dianggap sudah cukup efektif karena mampu mempertahankan beban kerja yang realistis dengan *overhead* yang dapat diterima. Akan tetapi dalam penelitian Bonomi, beberapa investigator belum bisa bekerja sama untuk menganalisa satu bukti digital. Tidak seperti pada penelitian Lone yang sudah mampu memberikan fasilitas beberapa investigator bisa menganalisa satu bukti digital yang sama.

Menurut Yunianto, 2019), barang bukti digital tidak bisa digunakan didalam persidangan karena masih digunakannya dokumen fisik untuk *Chain of Custody* bukti digital dan tidak kompetennya investigator. Pemanfaatan *framework Digital Evidence Cabinet* (DEC) dalam mengelola dan menyimpan dokumen *Chain of Custody* beserta bukti digitalnya (Prayudi et al., 2014) dikombinasikan dengan teknologi *Blockchain Ethereum*, diharapkan mampu memberikan integritas, keaslian, keutuhan terhadap barang bukti digital, sehingga mampu dipertanggungjawabkan dalam persidangan. Dari penelitian yang dilakukan Eko menghasilkan *framework* baru yaitu *Blockchain Digital Evidence Cabinet* (B-DEC) yang mampu mengelola dan menyimpan dokumen *Chain of Custody* dan bukti digital dalam blok yang terenkripsi. Penelitian ini sudah mampu memberikan hak akses kepada beberapa investigator terhadap suatu barang bukti seperti penelitian yang telah dilakukan oleh Lone.

Penelitian yang ada sudah mampu memanfaatkan suatu *Smart Contract* dalam mengelola dan menyimpan suatu *Chain of Custody* bukti digital pada blok-blok yang ternkripsi secara baik. Akan tetapi belum ada penelitian mengidentifikasi *Chain of Custody* bukti digital dalam format *Smart Contract* yang berbeda-beda dan bisa disesuaikan dengan kebutuhan. Oleh karena itu, pengembangan model *Multi Smart Contract* yang bisa mengelola bukti digital yang memiliki *tipe* dengan properti atau metadata yang berbeda-beda diperlukan.

3. METODOLOGI PENELITIAN

Kerangka penelitian yang sistematis digunakan untuk menjadi acuan langkah-langkah penelitian secara terstruktur agar mempermudah dalam melakukan proses penelitian yang dimulai dari identifikasi masalah hingga penyusunan laporan.



Gambar 1. Alur Penelitian.

.

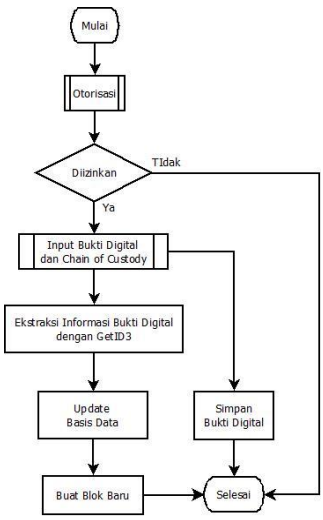
Gambar 1 menjelaskan tentang tahapan penelitian dalam membangun *Multi Smart Contract* dalam mengelola bukti digital. Pertama, Identifikasi masalah dilakukan dengan cara mengenali dan menandai masalah pengelolaan dokumen *Chain of Custody* pada suatu bukti digital yang dialami oleh aparatur penegak hukum khususnya kasus kejahatan siber. Selain itu peneliti juga mengidentifikasi masalah

yang ditemukan pada penelitian-penelitian sebelumnya. Dengan melakukan identifikasi masalah, peneliti berharap bisa mengetahui bahwa penelitian tentang implementasi model *Multi Smart Contract* dalam mengelola bukti digital dan *Chain of Custody* memang dibutuhkan.

Kedua, pengumpulan literatur yang berkaitan dengan pengguna terlibat dalam pengelolaan bukti digital, tema *Chain of Custody*, *Blockchain*, jenis-jenis bukti digital dan desain model *Multi Smart Contract* dalam mengelola bukti digital dan *Chain of Custody* diperlukan dalam membantu menyusun penelitian ini. Dari literatur yang diperoleh kemudian dipetakan menjadi beberapa bagian mencari poin penting dari masing-masing penelitian. Dari poin penting tersebut, maka akan diperoleh suatu kontribusi pada penelitian serupa. Kontribusi akan disajikan dalam sebuah aplikasi *Multi Smart Contract* untuk mengelola bukti digital dan *Chain of Custody*.

Ketiga, merancang sistem *Multi Smart Contract*. Dalam tahapan ini akan dilakukan analisa kebutuhan sistem, seperti: analisa kebutuhan otoritas sistem, analisa kebutuhan input sistem, analisa proses sistem, dan analisa output sistem. Selanjutnya merancang alur penyimpanan bukti digital dan *chain of custody* pada *naive chain*.

Gambar 2. *Alur Penyimpanan Bukti Digital dan Chain of Custody pada Naive Chain*



Gambar 2. Menjelakan alur penyimpanan yang dimulai dari pengguna sistem login berdasarkan akses yang telah diberikan, Kemudian pengguna dapat melakukan penambahan kasus, penambahan bukti digital, dan input form chain of custody. Kemudian ketika melakukan penyimpanan bukti digital, akan dilakukan eksraksi informasi tentang bukti digital tersebut dibantu dengan plugin GetID3. Data tentang kasus, chain of custody, dan informasi bukti digital akan disimpan ke dalam basis data. Kemudian rekaman data dari basis data akan disimpan ke dalam naive chain beserta log aktifitas yang dilakukan terhadap bukti digital. Sedangkan File bukti digital akan disimpan ke dalam server sistem naive chain.

Selanjutnya merancang *multi smart contract* untuk diimplementasikan pada naive chain. Tahapan tearkhir pada berikutnya yaitu merancang antar muka sistem yang akan menjadi penghubung antara pengguna dengan smart contract dan naive chain.

Keempat, tahapan implementasi sistem dimana prototipe akan dibangun dimulai dari membangun naive chain, membangun *multi smart contract*. Membangun penghubung antara *multi smart contract* dengan *naive chain (middleware)*, dan membangun antar muka (*front end*)

Kelima, langkah terakhir adalah melakukan pengujian sistem. Pengujian pertama adalah pengujian kerja sistem, yaitu dengan metode *black box* dan *white box*. Selanjutnya pengujian sistem kerja *smart contract* dengan cara memastikan *multi smart contract* berjalan sesuai rancangan. Tahapan berikutnya yaitu pengujian integritas bukti digital dan chain of cutody dengan cara memastikan bukti

p-ISSN : 2502-5724; e-ISSN : 2541-5735

digital yang masuk ke sistem sama dengan bukti digital yang asli. Pengujian terakhir yaitu pengujian performa multi smart contract dengan cara membandingkan kemampuan sistem dalam meningkatkan integritas bukti digital, kemampuan penyimpanan bukti digital, dan kecepatan akses multi smart contract dengan penelitian sebelumnya.

4. HASIL DAN ANALISA

A. Implementasi Multi Smart Contract

Langkah pertama dalam implementasi sistem yaitu dengan menjalankan *naive chain*. Sebelum naive chain digunakan untuk transaksi data,maka perlu dilakukuan inisiasi blok 0, yang biasa disebut file genesis. File genesis pada naive chain dibuat dengan kode berikut :

```
var getGenesisBlock = () => {
    return     new     Block(0,     "0",
1465154705,   "my   genesis   block!!",
"816534932c2b7154836da6afc367695e6337db
8a921823784c14378abed4f7d7");
    };
```

Langkah kedua, mengekstraksi informasi dari bukti digital dengan bantuan helper GetID3 . Hasil ekstraksi informasi akan disimpan dalam satu variabel array.

```
/*metadata */
 $metadata=[];$hash=[];
        if(count($listed_image)>0){

for($i=0;$i<count($listed_image);$i++){
              /* get metadata */

       $filelocation='uploads/bcoc/'.$l
isted_image[$i];

$metadata[]=json_encode(get_fileinfo($f
ilelocation));

$hash[]=get_hash($filelocation);

              /* get metadata */
          }

$save_data['hash']=json_encode($hash);

$save_data['file_properties']=json_enco
de($metadata);
        }
     /* end metadata*/
```

Ketiga, variabel array dari hasil ekstraksi informasi bukti digital digabungkan menjadi satu dengan variabel dari form isian chain of custody. Yaitu variabel $save_data. Keempat, variabel ini akan disimpan ke dalam naive chain dengan bantuan multi smart contract melalui pemanggilan fungsi new_block yang sudah didefinisikan di dalam helper smart contract.

```
$save_data['operation']='insert data';
/* save to blockchain */
      new_block($save_data);
    /* end save to blockchain*/
```

Fungsi new_blok ini dijabarkan dalam file contract_helper.php

```
if(!function_exists('new_block')){
   function new_block($dataarray){
      $data = ['data' => $dataarray];
      $headers = [
                    'Content-Type:
application/json'
                  ];
      $ch = curl_init();
      curl_setopt($ch,     CURLOPT_URL,
"http://localhost:3001/mineBlock");
      curl_setopt($ch,
CURLOPT_CUSTOMREQUEST, "POST");
      curl_setopt($ch,
CURLOPT_POSTFIELDS,
json_encode($data));
      curl_setopt($ch,
CURLOPT_HTTPHEADER, $headers);
      $results = curl_exec($ch);
      curl_close($ch);
      return $results;
   }
    }
```

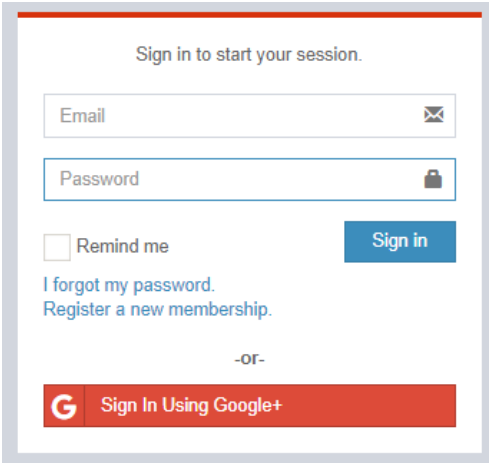
Fungsi untuk menampilkan isi blok adalah dengan memanggil fungsi get_block. Data yang ditampilkan dalam bentuk data json.

```
if(!function_exists('get_block')){
   function get_block(){
      $headers = [
            'Content-Type:
application/json'
      ];
      $ch = curl_init();
      curl_setopt($ch,
CURLOPT_CUSTOMREQUEST, "GET");
      curl_setopt($ch,
CURLOPT_RETURNTRANSFER, true);
      $results = curl_exec($ch);
      curl_close($ch);
      return $results;
   }
}
```

Keempat yaitu membangun *middleware* dengan cara menghubungkan *naive chain* ke multi smart contract mengunakan API dalam bentuk url yang diakses menggunakan fungsi curl pada multi smart contract. Sedangkan penghubung antara multi smart contract dengan antar muka atau frontend yaitu dengan menggunakan kode PHP. contract dibangun menggunakan kode PHP yang dijadikan sebagai fungsi *helper*. Smart contract ini akan menggabungkan data dari *form chain of custody*, hash, dan metadata untuk disimpan pada blockchian.

Gambar 3. Middleware Naive Chain, Multi Smart Contract dan Frontend.

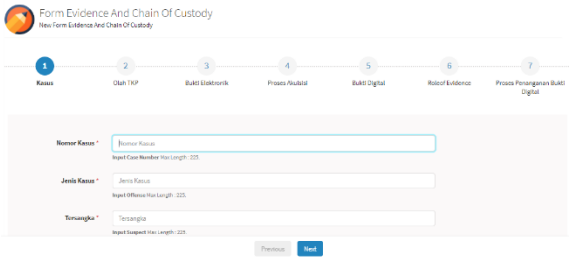
Kelima, implementasi sistem *multi smart contract* untuk mengelola bukti digital dan *chain of custody* dimulai dari mengaktifkan Service Apache, Mysql, Docker dan Composer. Setelah itu pengguna melakukan login



Gambar 4. Halaman Login

.

Setelah berhasil melakukan login untuk masuk ke aplikasi, penyidik bisa melakukan upload bukti digital dan mengisi *form Chain of Custody Pada* menu *Add Evidence*. Bukti digital bisa diinputkan lebih dari satu, karena bukti digital dari suatu kasus bisa saja terdiri dari beberapa buah.



Gambar 5. Halaman Menambahkan Bukti Digital

Bukti digital dan *form Chain of Custody* disimpan pada database dan juga pada Blockchain. Data yang ada pada Blockchain akan bertambah terus dan apabila ada penghapusan data, maka akan bisa terdeteksi dari urutan hash yang ada didalam block.

Gambar 6. Halaman Data pada Blockchain

Data yang ada pada Blockchain log-nya bisa dilihat pada Gambar 6. Semua proses penggunaan sistem *multi smart contract* untuk menyimpan bukti digital dan *chain of custody* dicatat pada log ini. Isi log berupa waktu proses, *previous* hash, hash baru, data, dan jenis aksi.

B. Pengujian *Multi Smart Contract*

. Pengujian sistem dimulai dari pengujian kerja sistem dilakukan dengan cara memastikan alur sistem dan hak akses sudah bisa berjalan sesuai rancangan multi smart contract pada naive chain untuk meningkatkan integritas bukti digital dan chain of custody.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Tabel 1. Pengujian Smart Contract

No	Skema Pengujian	Otoritas Pengguna			
		First Respon	Jaksa	Ahli	Lawyer
1	Input detail kasus	✓			
2	Lihat detail kasus	✓	✓		
3	Unggah Bukti Digital	✓			
4	Input *Chain of Custody*	✓			
5	Unduh Bukti Digital	✓		✓	
6	Lihat Chain of Custody	✓		✓	✓
7	Unduh form Chain of Custody	✓	✓		
8	Lihat Log akses data pada naive chain	✓			

Tabel 1 menunjukkan bahwa sistem sudah berjalan sesuai rancangan yang telah dibuat. Sistem sudah bisa menangani keperluan untuk menyimpan bukti digital dan chain of custody.Pengujian berikutnya yaitu pengujian implementasi sistem.

Tabel 2. Pengujian Implementasi sistem

No	Alur / Proses	BCOC	BDEC	Multi Smart Contract
1	Login sistem Blockchain	✓	✓	✓
2	Penyimpanan data user dan chain of custody ke database	✓	✓	✓
3	Penyimpanan Bukti digital ke dalam sistem	✓	✓	✓
4	Penyimpanan Hash bukti digital	✓	✓	✓
5	Penyimpanan Log aktivitas terhadap bukti digital dan *chain ofcustody*	✓	✓	✓
6	Ekstraksi informasi untuk meningkatkan integritas bukti digital	-	-	✓
7	Penggunaan multi smart contract secara otomatis okeh sistem.	-	-	✓

Tabel 2 menjelaskan bahwa beberapa fungsi dasar dari konsep blockchain digital chain of custody yang digunakan pada penelitian ini sudah sama dengan penelitian sebelumnya. Selain itu juga dari penerapan multi smart contract ini, informasi yang lebih detail diberikan untuk menjaga integritas bukti digital dan chain of custody. Pengujian integritas bukti digital dilakukan dengan ekstraksi informasi dari masing masing jenis bukti digital dengan bantuan plugin GetID3.

Tabel 3. Pengujian Integritas Multi Smart Contract

Komponen	**Image**	**Audio**	**Video**	**File**
Avdataend	✓	✓	✓	✓
Avdataoffset	✓	✓	✓	✓
Encoding	✓	✓	✓	✓
Fileformat	✓	✓	✓	✓
Filename	✓	✓	✓	✓
Filenamepath	✓	✓	✓	✓
Filepath	✓	✓	✓	✓
Filesize	✓	✓	✓	✓
mime type	✓	✓	✓	✓
bits per sample	✓	-	✓	-
compression ratio	✓	✓	-	-
Dataformat	✓	✓	✓	-
Lossless	✓	✓	-	-
pixel aspect ratio	✓	-	-	-
resolution x	✓	-	✓	-
resolution y	✓	-	✓	-
Bitrate	-	✓	✓	-
bitrate mode	-	✓	✓	-
channelmode	-	✓	✓	-
Channels	-	✓	✓	-
encoder setting	-	✓	✓	-
encoder options	-	✓	✓	-
sample rate	-	✓	✓	-
compatible brands	-	✓	✓	-
major brands	-	✓	✓	-
playtime seconds	-	-	✓	-
playtime string	-	-	✓	-
Controller	-	-	✓	-
display scale	-	-	✓	-
free hierarchy	-	-	✓	-
free name	-	-	✓	-
free offset	-	-	✓	-
free size	-	-	✓	-
ftyp fourcc	-	-	✓	-
ftype hierarchy	-	-	✓	-
ftype name	-	-	✓	-
ftype offset	-	-	✓	-

ftype signature	-	-	✓	-
ftype size	-	-	✓	-
ftype unknown	-	-	✓	-
hinting	-	-	✓	-
mdat hierarchy	-	-	✓	-
mdat name	-	-	✓	-
mdat offset	-	-	✓	-
mdat size	-	-	✓	-
Fourcc	-	-	✓	-
fourcc_lookup	-	-	✓	-
frame_rate	-	-	✓	-
Rotate	-	-	✓	-

Tabel 3 menyajikan bahwa masing masing bukti digital memiliki karakteristik sendiri dan memiliki jumlah karakter yang berbeda antara satu tipe bukti digital dengan tipe bukti digital lainnya. Hasil ekstarksi informasi secara otomatis yang dilakukan oleh GetID3 akan disimpan kedalam blo sehingga ketika ada perubahan yang dilakukan pada bukti digital, maka metadatanya akan ikut berubah dan history perubahan data bisa dilihat melalui data yang tercatat di dalam blok. Oleh karena itu penyajian informasi yang lebih detail akan meningkatkan integritas bukti digital.

Tabel 4. Pengujian Performa Multi Smart Contract

No	Skema Pengujian	Jumlah Komponen yang Disimpan	Ukuran File	Kecepatan Akses
1	Upload 1 Bukti Digital Gambar	1	1011 KB	2.18 detik
2	Upload 2 Bukti Digital Gambar	2	260 KB	1.99 detik
3	Upload 3 Bukti Digital Gambar	3	1271 KB	2.36 detik
4	Upload 1 Bukti Digital Audio	1	1106 KB	2.09 detik
5	Upload 2 Bukti Digital Audio	2	91 KB	1.91 detik
6	Upload 3 Bukti Digital Audio	3	1197 KB	2.16 detik
7	Upload 1 Bukti Video	1	1998 KB	2.08 detik
8	Upload 2 Bukti Video	2	2939 KB	2.02 detik
9	Upload 3 Bukti Video	3	4937 KB	2.06 detik
10	Upload 1 Dokumen	1	1777 KB	2.10 detik
11	Upload 2 Dokumen	2	859 KB	1.98 detik
12	Upload 3 Dokumen	3	2636 KB	2.09 detik
13	Upload 1 Gambar 2 Audio	3	1102 KB	2.58 detik
14	Upload 1 Gambar 2 Video	3	3950 KB	2.16 detik
15	Upload 1 Gambar 2 Dokumen	3	1870 KB	2.11 detik
16	Upload 2 Gambar 1 Audio	3	1366 KB	2.14 detik
17	Upload 2 Gambar 1 Video	3	2258 KB	2.15 detik
18	Upload 2 Gambar 1 Dokumen	3	2037 KB	2.22 detik
19	Upload 1 Audio 2 Video	3	4045 KB	2.51 detik
20	Upload 1 Audio 2 Dokumen	3	1965 KB	2.27 detik
21	Upload 2 Audio 1 Video	3	2089 KB	2.14 detik
22	Upload 2 Audio 1 Dokumen	3	1868 KB	1.99 detik
23	Upload 1 Video 2 Dokumen	3	2857 KB	1.97 detik
24	Upload 2 Video 1 Dokumen	3	3775 KB	1.88 detik
25	Upload 1 Gambar 1 Audio 1 Video dan 1 Dokumen	3	4786 KB	2.16 detik
26	Unduh Bukti Digital	1	1011 KB	0.5 detik
28	Hapus bukti digital	1	1011 KB	1.85 detik

Tabel 4 menjabarkan hasil pengujian performa bahwa jumlah file bukti digital , ukuran file belum mempengaruhi performa sistem multi smart contract. Namun perbandingan dengan hasil penelitian lain diperlukan agar bisa mengetahui performa dari sistem multi smart contract. Langkah pertama yaitu kita harus mengetahui nilai rata-rata dari ukuran file. Nilai rata rata ukuran file perhitungannya total ukuran dibagi dengan jumlah skema ujian, 56072 KB dibagi 27 mnejadi 2076.74 KB. Kemudian akan dihtiung juga rata-rata dari waktu . Nilai rata-rata waktu yang diperoleh dari perhitungan total waktu dibagi dengan jumlah jumlah skema ujian , 55.65 detik dibagi 27 adalah 2.06 detik. Selanjutnya perlu dicari nilai rasio antara rata-rata waktu dengan rata-rata ukuran file,Sehingga hasilnya akan menjadi, 2.06 : 2076.74 hasilnya rasionya adalah 0.000991939 .

p-ISSN : 2502-5724; e-ISSN : 2541-5735

C. Analisa Implementasi *Multi Smart Contract*

Hasil implementasi *Multi Smart Contract* dalam mengelola bukti digital dan *Chain of Custody* ditemukan adanya perbedaan dari hasil penelitian-penelitian yang sejenis

Penelitian sebelumnya seperti pada pengunaan metode *Block Chain Digital Evidence Cabinet* (BDEC), *Smart Contract* yang digunakan adalah model *Smart Contract* tunggal untuk mengelola semua jenis bukti digital karena bukti digital tidak dikelompokkan berdasarkan jenisnya. Sedangkan pada penelitian ini bukti digital dikelompokkan menjadi bukti digital tipe gambar, audio, video, dan *file* atau dokumen.Pengelompokkan ini disertai dengan penambahan komponen berupa informasi detail tentang bukti digital pada data yang akan disimpan pada *block* bersama dengan bukti digital dan *form Chain of Custody*.

Pengelompokkan bukti digital berdasarkan tipenya didasarkan pada UU ITE Nomor 11 tahun 2008 yang menyatakan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetakannya merupakan perluasan dari alat bukti hukum yang sah sesuai dengan hukum acara yang berlaku di Indonesia". Jadi gambar, audio, video, dan *file* atau dokumen dikelompokkan sebagai dokumen elektronik yang bisa menjadi alat bukti digital.

Adanya penambahan komponen informasi tentang detail bukti digital yang dikelola sesuai tipenya diharapkan bisa membantu menyajikan informasi yang lebih lengkap bagi investigator, ahli, dan pihak lain yang membutuhkan informasi tersebut. Penambahan komponen informasi ini bisa digunakan untuk mempermudah menentukan tindakan yang harus dilakukan dalam proses penyelidikan.

Hasil penerapan *Multi Smart Contract* pada pengelolaan bukti digital dan *Chain of Custody*, berupa sebuah model dengan tambahan informasi rinci tentang bukti digital ke dalam rantai *block* bersamaan dengan *form Chain of Custod.* Penambahan informasi rinci tentang bukti digital ini disajikan dalam bentuk *file properties* yang bisa diperoleh otomatis dari bantuan *plugin* getID3.

Penelitian sebelumnya yang menggunakan metode *Block Chain Digital Evidence Cabinet* (BDEC) penyajian informasi yang disimpan ke dalam *block* hanya berupa informasi dasar tentang bukti digital seperti ukuran *file*, nama *file*, lokasi penyimpanan bukti digital, dan *hash file*. Sedangkan pada penelitian ini, menggunakan metode Multi *Smart Contracts* dan dapat memberikan kontribusi berupa adanya temuan tambahan komponen informasi yang lebih detail terkait bukti digital. Penambahan informasi detail tentang bukti digital ini disertai dengan penyesuaian berupa penerapan *Multi Smart Contract* untuk mengelola bukti digital dengan tipe yang berbeda-beda.

Penambahan informasi yang lebih detail pada bukti digital dengan *Multi Smart Contract* maka dapat meningkatkan integritas dan akurasi bukti digital serta dapat membantu mempermudah dan mempercepat investigator atau ahli menentukan tindakan dalam memeriksa bukti digital yang dikelola. Berikut ini adalah detail komponen informasi dari masing-masing tipe *file* bukti digital yang diproses menggunakan metode *Multi Smart Contract*.

Selain itu berdasarlan hasil pengujian performa didapatkan bahwa nilai rasio dari penerapan multi smart contract dalam meningkatkan integritas bukti digital dan chain of custody menghasilkan nilai 0.000991939. Jika dilakukan perhitungan

rasio yang sama dengan penelitan Blockchain Digital Evidence Cabinet (BDEC) (Yunianto, E:2019) dengan menyamakan satuan dari ukuran file dan waktu maka rasionya 0.970812 : 5.261833333 dan jika dihitung maka akan menjadi 0.184500713. Dari perbandingan ini bisa kita lihat bahwa performa multi smart contract performanya hampir sama dengan penelitan sebelumnya.

5. KESIMPULAN

Hasil dari penerapan multi smart contract menjelaskan bahwa bukti digital memiliki karakteristik berbeda-beda dan detail informasi yang berbeda-beda antara satu jenis bukti digital gambar, audio, video, dan dokumen atau jenis bukti digital lainnya. Informasi yang detail mampu meningkatkan integritas bukti digital. Otomatisasi dalam membuat hash dan ekstraksi informasi dari suatu bukti digital dapat mengurangi waktu first responder dalam menginputkan form isian pada sistem multi smart contract. Penyimpanan bukti digital di luar blok dapat meningkatkan performa sistem multi smart contract. Penyimpanan bukti digital yang hanya berupa alat bukti persidangan mampu mengoptimalkan media penyimpanan bukti digital.

Saran untuk melengkapi kekurangan pada penelitian ini antara lain adalah perlu dilakukannya pengembangan dari rancangan *Multi Smart Contract* dengan menyesuaikan perkembangan dari pembaharuan jenis-jenis *file* yang kedepannya memiliki kemungkinan menjadi barang bukti digital serta perlu dilakukan peningkatan efisiensi akses terhadap *block* untuk mengatasi data yang terus bertambah jumlah dan ukurannya, karena data pada *block* tidak akan pernah dihapus untuk menjaga esensi dari *Blockchain*.

REFERENSI

Ahmad Liza, Khanji Salam, Iqbal Farkhund, Kamoun Fauzi. 2020. Blockchain-based Chain of Custody: Towards Real-time Tamper-proof Evidence Management. ARES '20: Article No.: 48 Pages 1–8. https://doi.org/10.1145/3407023.3409199

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. Retrieved from http://arxiv.org/abs/1807.10359

ChainLink. (2018). Blockchain ’ s Role in the Produce Supply Chain.

Chopade Mrunali. (2019). Digital Forensics : Maintaining Chain of Custody Using Blockchain. Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)

Cosic, J. (2017). Formal Acceptability of Digital Evidence. Springer International Publishing. http://doi.org/10.1007/978-3-319-44270-9

Hartikka Lauri. (2018). https://github.com/lhartikk/naivechain. Diakses tanggal 1 Desember 2020

Hegadekatti, K. (2017). Legal Systems and Blockchain Interactions, (66085).

Heinrich James. (2020). https://github.com/JamesHeinrich/getID3. DIakses tanggal 3 Desember 2020

Garcia-alfaro, J., Navarro-arribas, G., Eds, J. H., & Hutchison, D. (2017). Data Privacy Management, Cryptocurrencies and Blockchain Technology (Vol. 10436). https://doi.org/10.1007/978-3-319-67816-0

Gopalan. H. (2019). Digital Forensics Using Blockchain. IJRTE

Laurence, T. (2017). Blockchain for dummies. John Wiley & Sons, Inc. Hoboken.

Lone, A. H., & Mir, R. N. (2017). Forensic-Chain: Ethereum Blockchain Based Digital Forensics. Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):21-27, 1(2), 21–27.

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55. https://doi.org/10.1016/j.diin.2019.01.002

Nizamuddin, N., Salah, K., Ajmal Azad, M., Arshad, J., & Rehman, M. H. (2019). Decentralized document version control using ethereum blockchain and IPFS. Computers & Electrical Engineering, 76, 183–197. doi:10.1016/j.compeleceng.2019.03.014

Prayudi, Y., & SN, A. (2015). Digital Chain of Custody: State of The Art. International Journal of Computer Applications, 114(5), 1–9. https://doi.org/10.5120/19971-1856

Prayudi, Y., Ashari, A., & K Priyambodo, T. (2014). Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. International Journal of Computer Applications, 107(9), 30–36. https://doi.org/10.5120/18781-0106

Ratnasari, D., Prayudi, Y., & Sugiantoro, B. (2018). XML Approach for the Solution of Chain of Custody of Digital Evidence. International Journal of Computer Applications, 179(23), 20–25. https://doi.org/10.5120/ijca2018916445

Republik Indonesia. (2016). Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Shorish, J. (2018). Blockchain State Machine Representation. https://doi.org/10.17605/OSF.IO/EUSXG

Singhal, B., Dhameja, G., & Panda, P. S. (2018). Beginning Blockchain : A Beginner's Guide to Building Blockchain Solutions. Apress. https://doi.org/10.1007/978-1-4842-3444-0

Yunianto, E. (2019). Blockchain Digital Evidence Cabinet (B-DEC) : Manajemen Bukti Digital Berbasis Blockchain.