REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SURAT PENCATATAN
CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202164435, 15 November 2021
Pencipta		
Nama	:	**Dr. Aslan Alwi, M.Cs., Dr. Julan Hernadi, M.Si. dkk**
Alamat	:	Gedongkuning KG1/192 RT. 010 RW 003 Rejowinangun Kec. Kotagede Kota Yogyakarta, Daerah Istimewa Yogyakarta 55171, Yogyakarta, DI YOGYAKARTA, 55171
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Universitas Muhammadiyah Ponorogo**
Alamat	:	Jalan Budi Utomo 10 Ronowijayan Siman Ponorogo Jawa Timur Gedung D Rektorat Lantai 3, Ponorogo, JAWA TIMUR, 63471
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Arsitektur**
Judul Ciptaan	:	**Arsitektur Pertama Desain Protokol Tanda Tangan Digital (Proses Verifikasi Yang Disandarkan Kepada Blockchain)**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	4 Oktober 2021, di Ponorogo
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000304647

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n Menteri Hukum dan Hak Asasi Manusia
Direktur Jenderal Kekayaan Intelektual
u.b.
Direktur Hak Cipta dan Desain Industri

Dr. Syarifuddin, S.T., M.H.
NIP.197112182002121001

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.

LAMPIRAN PENCIPTA

No	Nama	Alamat
1	Dr. Aslan Alwi, M.Cs.	Gedongkuning KG1/192 RT. 010 RW 003 Rejowinangun Kec. Kotagede Kota Yogyakarta, Daerah Istimewa Yogyakarta 55171
2	Dr. Julan Hernadi, M.Si.	Tempel Wirogunan UH 3/905 RT 046 RW 011 Tahunan Umbulharjo Yogyakarta
3	Munirah, S.Kom., M.T.	Gedongkuning KG1/192 RT. 010 RW 003 Rejowinangun Kec. Kotagede Kota Yogyakarta, Daerah Istimewa Yogyakarta 55171

DOKUMEN BUKTI HAK CIPTA

Protokol Tanda Tangan Cetak berbasis Blockchain
Proses penyimpanan dan verifikasi disandarkan pada blockchain

Pengusul Hak Cipta

Dr. Aslan Alwi, S.Si., M.Cs

Dr. Julan Hernandi, M.Si

Munirah, S.Kom., M.T

PONOROGO

2022

Protokol Tanda Tangan Cetak berbasis Blockchain
Proses penyimpanan dan verifikasi disandarkan pada blockchain

A. PENDAHULUAN

Tanda tangan cetak berupa penggunaan qrcode untuk menandatangani dokumen di dalam aktivitas administrasi perkantoran telah menjadi suatu bagian yang lazim kita temui di berbagai lembaga baik itu lembaga pemerintah atau swasta. Seperti misalnya pembubuhan qrcode pada kartu keluarga yang menyatakan tanda tangan Kepala Dinas Kependudukan dan Pencatatan Sipil, atau pada penerbitan sertifikat yang membubuhkan qrcode sebagai tanda tangan dari otoritas pemberi sertifikat.

Tanda tangan cetak seperti qrcode biasanya digunakan untuk penandatanganan dokumen yang tidak melibatkan transaksi atau transaksi yang bernilai besar, dikarenakan kekuatan hukumnya yang lebih lemah dari tanda tangan basah. Verifikasi dari tanda tangan cetak qrcode disandarkan pada sebuah situs yang memberi keterangan akan keabsahan tanda tangan cetak qrcode tersebut. Karena itu, biasanya sebuah qrcode mewakili sebuah link URL yang membawa kepada sebuah situs resmi yang menyatakan validitasnya. Akan tetapi tidak menutup kemungkinan bisa juga qrcode mewakili kode lain atau gambar tertentu yang dapat dipandang sebagai sebuah kekuatan yang cukup untuk memvalidasi tanda tangan tersebut.

Tanda tangan cetak termasuk ke dalam bagian dari tanda tangan elektronik. Jenis tanda tangan ini sangat berguna untuk menandatangani secara massal banyak dokumen tanpa harus melibatkan kehadiran di tempat si pembuat tanda tangan

B. KLAIM DESAIN PROTOKOL TANDA TANGAN CETAK BERBASIS BLOCKCHAIN

Berikut ini dikemukakan rancangan protokol tanda tangan cetak yang diharapkan dapat menjadi solusi bagi kelemahan tanda tangan cetak. Protokol ini dimulai dengan beberapa assumsi dasar. Dengan harapan, bahwa assumsi itu cukup menjamin kemanan mekanisme protokol. Protokol ini melibatkan blockchain sebagai tulang punggung yang menopang sifat keterjejakan dan anti tampering dari tanda tangan cetak. Protokol ini mestilah memiliki beberapa kelemahan, tetapi diharapkan dengan menginisiasi permulaan bagi pengembangannya, di masa depan protokol ini masih dapat terus bertumbuh dan diperbaiki.

Rancangan protokol untuk tanda tangan cetak yang diajukan di dalam makalah ini didasarkan pada beberapa asumsi sebagai berikut:

Assumsi dasar untuk user pembuat tanda tangan cetak:

1. User pembuat tanda tangan cetak adalah sebuah lembaga, baik lembaga pemerintah atau swasta. User pembuat selanjutnya disebut Lembaga.
2. Lembaga menetapkan menggunakan sebuah algoritma enkripsi yang asimetrik kemudian membuat public key dan private key baik secara permanen atau periodik.
3. Private key digunakan untuk melakukan enkripsi.
4. Publick key digunakan untuk dekripsi.
5. Public key dipublikasikan di situs resmi Lembaga.
6. Lembaga menetapkan algoritma hash untuk digunakan melakukan hashing di dalam mekanisme protokol tanda tangan cetak.
7. Metadata dokumen fisik atau digital adalah sebuah rincian catatan identitas dan point-point penting tentang dokumen yang hendak diberi tanda tangan cetak ditambahkan dengan bukti-bukti foto, video dan audio dari dokumen fisik jika diperlukan.
8. Blockchain penopang tanda tangan cetak dapat berupa blockchain private lembaga, atau konsorsium dengan lembaga lain atau menggunakan blockchain publik pihak ketiga.

Assumsi dasar untuk user pengguna dokumen yang ditanda tangani menggunakan tanda tangan cetak:

1. User pengguna dokumen adalah siapa saja baik perorangan atau berbentuk sebuah lembaga.
2. Dokumen yang digunakan boleh berbentuk fisik atau digital.

Assumsi dasar untuk user verifikator tanda tangan cetak:

1. Verifikator adalah siapa saja baik perorangan atau lembaga.
2. Verifikator memeriksa keabsahan tanda tangan cetak.

Protokol untuk pembuatan tanda tangan cetak (PTC)

Berikut ini berdasarkan sejumlah assumsi dasar yang dikemukakan sebelumnya. Sebuah algoritma protokol untuk pembuatan tanda tangan cetak dikemukakan. Protokol ini dilaksanakan oleh lembaga yang membuat kemudian mencetak tanda tangan cetak. Algoritma Protokol ini dinamakan protokol PTC dan dinyatakan dalam langkah-langkah sebagai berikut:

Protokol PTC

Step 0: Mulai.

Step 1: Lembaga membuat dokumen fisik atau digital untuk ditandatangani oleh lembaga dan membuat metadatanya.

Step 2: Lembaga melaksanakan protokol penyimpanan metadata ke blockchain menggunakan protokol PMB (protokol terpisah yang dinyatakan di dalam pasal C).

Step 3: Lembaga mengambil alamat blok dan nomor transaksi dari metadata yang telah disimpan di blockchain.

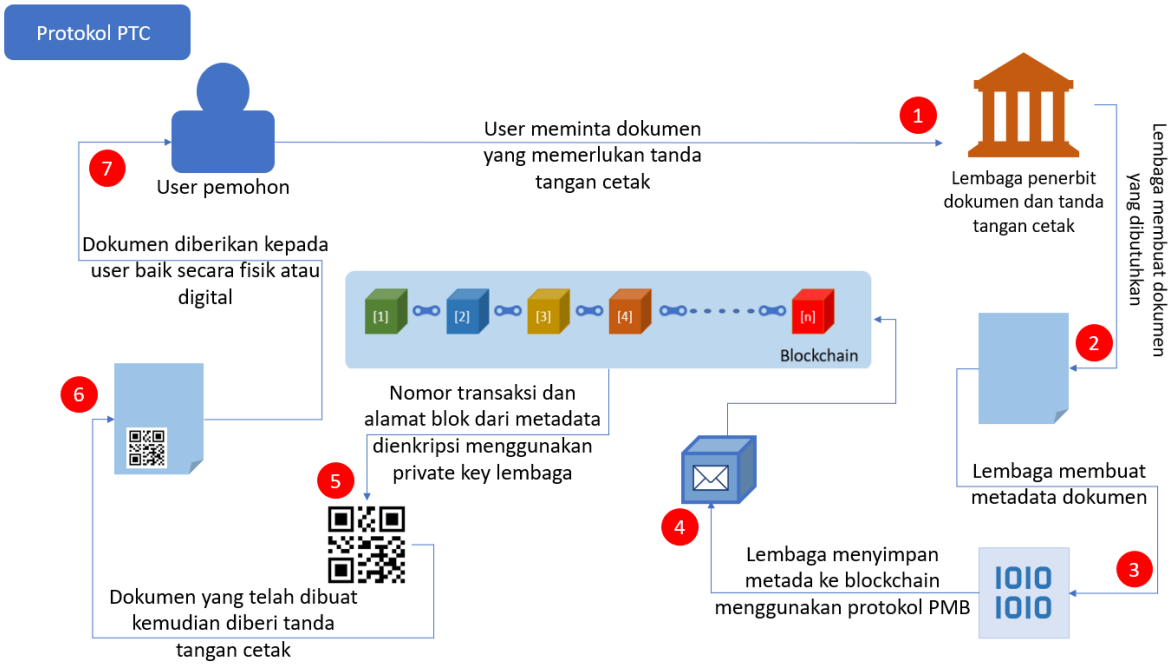
Step 4: Alamat blok dan nomor transaksi kemudian dienkripsi menggunakan private key Lembaga.

Step 5: Hasil enkripsi lalu dibuat Qr-Code.

Step 6: Qr-Code lalu dicetak sebagai tanda tangan digital pada dokumen fisik atau dilekatkan pada dokumen digital.

Step 7: Selesai.

Gambar 1. Memberikan ilustrasi lengkap dari jalannya protokol PTC.



Gambar 1. Protokol PTC

Protokol penyimpanan metadata di blockchain (PMB)

Berikut ini berdasarkan sejumlah assumsi dasar yang dikemukakan di awal dokumen hak cipta ini. Sebuah algoritma protokol untuk penyimpanan metadata di blockchain dikemukakan. Protokol ini dilaksanakan oleh lembaga ketika menyimpan metadata dokumen yang akan diberi tanda tangan cetak. Sebagaiman dinyatakan sebelumnya, metadata tanda tangan cetak berisi tentang identitas penerima tanda tangan cetak dan semua point penting yang merangkum dokumen yang akan ditandatangani. Tidak tertutup bahwa salinan digital lengkap dokumen dapat dilekatkan sebagai pelengkap bukti dari tanda tangan cetak. Protokol ini dinamakan protokol PMB (Penyimpanan metadat di Blockchain) dan dinyatakan sebagai berikut:

Protokol PMB

Step 0: Mulai.

Step 1: Lembaga telah membuat metadata dari dokumen yang hendak ditandatangani.

Step 2: Metadata kemudian dienkripsi menggunakan private key lembaga.

Step 3: Hasil enkripsi metadata kemudian dibuatkan kode hash.

Step 4: Metadata dan kode hash kemudian disimpan sebagai sebuah atau beberapa item transaksi kemudian disimpan di dalam sebuah blok kandidat.

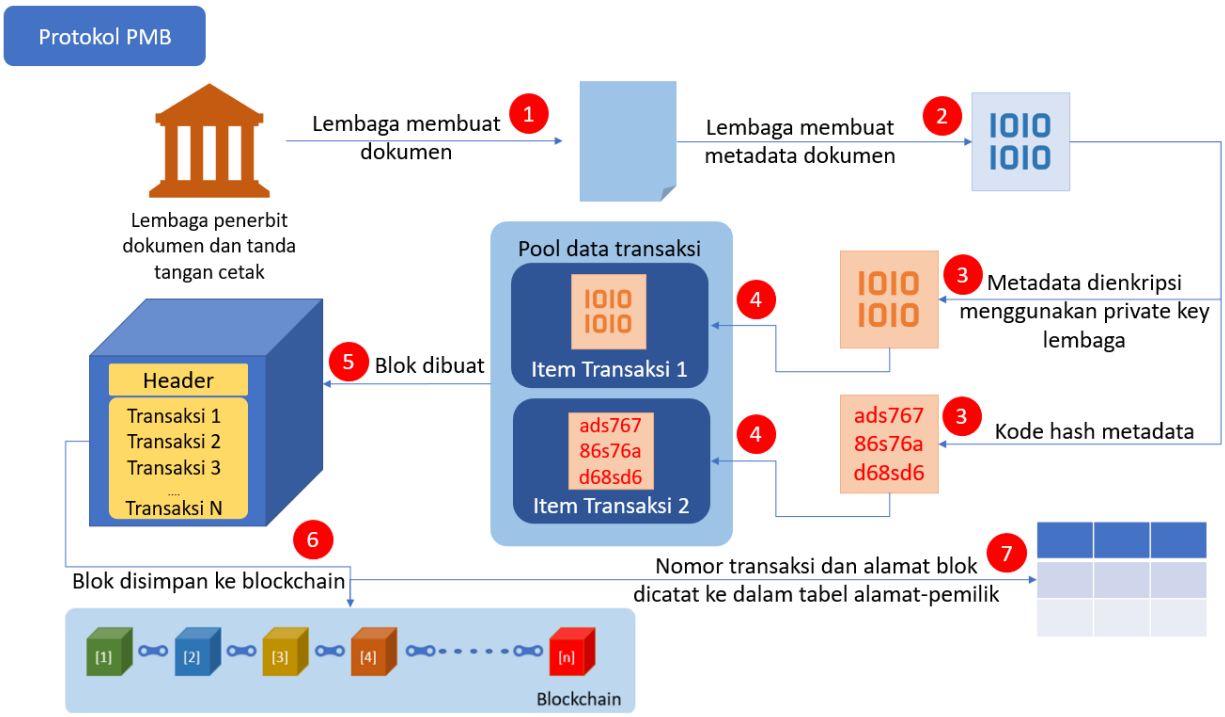
Step 5: Blok kandidat ditambahkan ke dalam blockchain menurut protokol blockchain yang dipilih lembaga. Protokol blockchain adalah menurut pilihan lembaga, apakah itu blockchain private, blockchain konsorsium atau blockchain publik.

Step 6: Lembaga kemudian mencatat alamat blok dan nomor transaksi pada sebuah tabel besar termasuk nilai hash dari dokumen bukti. Secara keseluruhan, tabel dalam satu rekord minimal menyatakan identitas orang yang diberi tanda tangan cetak, alamat blok dan nomor transaksi dan nilai hash dokumen bukti.

Step 7: Lembaga lalu menyimpan tabel besar di blok lain dari blockchain menurut tata cara atau protokol penyimpan blockchain yang dipilih lembaga.

Step 8: Selesai.

Gambar 2. Memberikan ilustrasi protokol PMB



Gambar 2. Protokol PMB

Protokol verifikasi tanda tangan cetak (VTC)

Berikut ini berdasarkan sejumlah assumsi dasar yang dikemukakan di awal dokumen hak cipta ini. Sebuah algoritma protokol untuk verifikasi tanda tangan cetak dikemukakan. Protokol ini menyatakan langkah-langkah untuk melakukan verifikasi tanda tangan cetak. Verifikasi dapat dilakukan oleh siapa saja. Verifikasi tidak tertutup kepada salah satu lembaga lain yang menerima dokumen atau siapa saja, akan tetapi bersifat terbuka kepada publik, baik kepada yang dituju oleh dokumen yang bertanda tangan cetak atau bukan yang dituju. Dengan harapan, di dalam protokol ini terpelihara sifat keterbukaan dan keterjejakan tanda tangan cetak (traceability).

Selanjutnya di dalam protokol ini, pihak yang melakukan verifikasi disebut sebagi verifikator. Protokol ini dinamakan sebagai protokol VTC (verifikasi tanda tangan cetak) dinyatakan sebagai berikut:

Protokol VTC

Step 0: Mulai.

Step 1: Verifikator mengekstrak tanda tangan cetak menjadi serangkain data.

Step 2: Verifikator mengakses publik key lembaga penerbit tanda tangan cetak pada dokumen. Publik key lembaga diakses pada situs rermi lembaga.

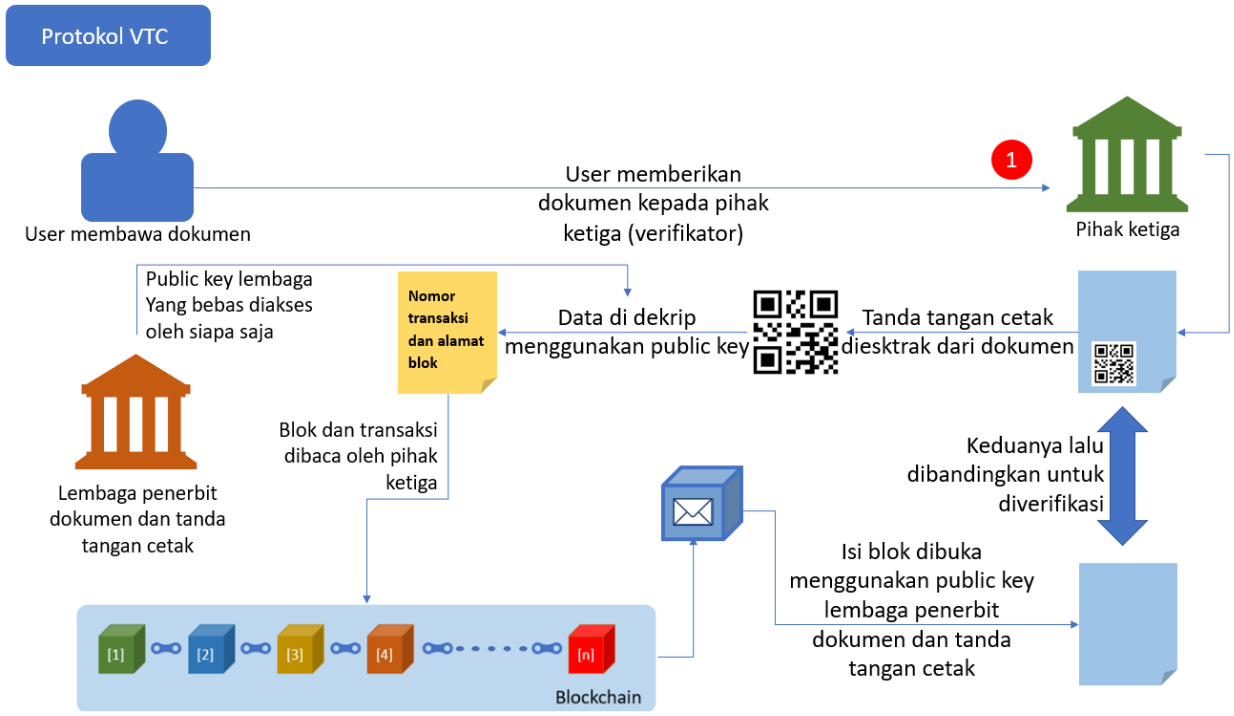
Step 3: Data hasil ekstrak kemudian didekripsi menggunakan publik key lembaga penerbit tanda tangan cetak.

Step 4: Alamat blok dan nomor transaksi yang diperoleh sebagai hasil dekripsi kemudian digunakan untuk mengakses blockchain.

Step 5: Isi blok pada nomor transaksi itu di blockchain kemudian didekripsi menggunakan publik key lembaga penerbit tanda tangan cetak.

Step 6: Verifikator kemudian memverifikasi dokumen yang telah ditandatangani menggunakan data transaksi yang telah didekrip tersebut.

Step 7: Selesai.



Gambar 3. Protokol VTC

C. PENUTUP

Pembuatan sistem tanda tangan cetak menggunakan Qr-Code atau barcode yang verifikasinya bertumpu pada sebuah server yang terpusat memilik kelemahan karena sifatnya yang terpusat itu, yaitu bahwa sekali seseorang dapat masuk mengintervensi komputer terpusat itu maka segala transaksi dan urusan yang melibatkan tanda tangan cetak menjadi mudah dimanipulasi dan menjadi tidak valid. Sehingga teknologi tanda tangan cetak yang ada hanya dapat digunakan untuk dokumen-dokumen yang tidak terlalu penting dan tidak kritis. Ini karena kekuatannya yang lemah di dalam menjamin dua pihak baik yang bertanda tangan atau yang menerima tanda tangan tersebut.

Akan tetapi, dengan menyandarkan protokol tanda tangan cetak kepada blockchain maka kekuatan tanda tangan diletakkkan pada penyimpanan yang terdistribusi-terdesentralisasi dan terenkripsi. Sehingga memberi jaminan yang lebih kuat akan keamanan dua pihak ketika terjadi tanda tangan cetak.