

DAFTAR ISI

HALAMAN PENGESAHAN.....	ii
BUKTI BEBAS PLAGIASI.....	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vii
DAFTAR TABEL	viii
DAFTAR ISTILAH	ix
DAFTAR KODE.....	x
CATATAN REVISI DOKUMEN	xi
INTISARI.....	xii
ABSTRACT	xiii
RINGKASAN EKSEKUTIF.....	xiv
BAB 1 PENGANTAR	1
1.1 Rumusan Masalah	2
1.2 Tujuan Penelitian.....	2
BAB 2 DASAR TEORI PENDUKUNG	3
2.1 Keamanan Jaringan Komputer	3
2.1.1 Trias CIA (Confidentiality, Integrity, Availability)	3
2.1.2 Autentikasi.....	3
2.1.3 Otorisasi.....	4
2.1.4 Akuntansi.....	4
2.1.5 Serangan Siber.....	4
2.2 Kriptografi.....	4
2.2.1 Algoritma Hash.....	5
2.2.2 Kunci Kriptografi	5
2.3 <i>Internet of Things</i>	7
2.4 <i>Blockchain</i>	7
2.4.1 <i>Public Blockchain</i>	8
2.4.2 <i>Private Blockchain</i>	8
2.5 Ethereum	8
2.5.1 Ethereum Virtual Machine	9
2.5.2 Application Binary Interface	10
2.5.3 Solidity.....	10

2.5.4	<i>Address</i>	10
2.5.5	Kontrak Pintar (Smart Contract).....	11
2.5.6	Keccak-256	11
2.5.7	Consensus Mechanism	12
2.6	Public Key Infrastructure (PKI)	13
2.6.1	Sertifikat Digital	13
2.6.2	Certificate Authority (CA).....	13
2.6.3	Registration Authority (RA).....	14
2.6.4	Metode Verifikasi Sertifikat	14
BAB 3	ANALISIS STUDI PUSTAKA KUNCI DAN PEMILIHAN METODE	15
3.1	Pendekatan Keamanan Berbasis Kepercayaan.....	15
3.1.1	Kepercayaan Berorientasi Data	15
3.1.2	Kepercayaan Berorientasi Entitas.....	15
3.1.3	Kepercayaan Berbasis Hibrid	16
3.1.4	Perbandingan Pendekatan Kepercayaan	16
3.2	Implementasi Layanan Keamanan	17
3.2.1	Layanan Tersentralisasi	17
3.2.2	Layanan Terdesentralisasi	18
3.2.3	Komparasi Implementasi Layanan	18
3.3	Pemilihan Metode	19
BAB 4	DETAIL IMPLEMENTASI	21
4.1	Luaran <i>Capstone Project</i> beserta Spesifikasinya	21
4.2	Batasan Masalah.....	23
4.3	Detail Rancangan	24
4.3.1	Gambaran Umum Ekosistem.....	24
4.3.2	Sisi Pengguna	27
4.3.3	Sisi Otoritas	29
4.3.4	Sisi Penyedia Layanan.....	29
4.3.5	Implementasi Nilai Kepercayaan.....	30
4.3.6	Simulasi dan Ilustrasi Kerja.....	34
BAB 5	PENGUJIAN DAN PEMBAHASAN	40
5.1	Pengujian dan Pembahasan	40
5.1.1	Basis Serangan Token dan Analisis.....	40
5.1.2	Basis Serangan <i>Feedback</i> dan Analisis	45

5.1.3	Basis Serangan <i>Entity Registration</i> dan Analisis	48
5.1.4	Basis Serangan <i>Policy</i> dan Analisis.....	54
5.1.5	Basis Serangan <i>Trust</i> dan Analisis	59
5.2	Pengembangan Lebih Lanjut.....	61
5.2.1	Sisi Perangkat Lunak	61
5.2.2	Faktor Keamanan.....	62
BAB 6	ANALISIS MENGENAI PENGARUH SOLUSI <i>ENGINEERING DESIGN</i>	64
6.1	Konteks Keamanan	64
6.2	Konteks Ekonomis	64
6.3	Konteks Global.....	64
BAB 7	KESIMPULAN DAN SARAN	65
7.1	Kesimpulan.....	65
7.2	Saran.....	66
REFERENSI.....		67