

National Institute of Technology Meghalaya

An Institute of National Importance

CURRICULUM

	Program		Bachelor of Technology in Computer Science and EngineeringAcademic Year of Regulation											0			
De	epartm	ent	Com	puter So	cience an	d Engine	ering						Seme	ster		VI	
Οοι					Co	urse Nam	1e				Credit S	Structure			Marks Dis	stribution	
Code									L	Т	Р	С	INT	MID	END	Total	
CS 417		Blockchain Technologies							3	0	0	3	50	50	100	200	
		This course explains the need and working principle of blockchain systems, cryptocurrency, cryptographic primitives.									CO1	Able to explain the need of Blockchain system and demonstrate the fundamentals of cryptocurrence cryptographic primitives.					
Course Objectives		This course describes the in-depth knowledge and concept of recent technologies, tools, and implementation strategies.								Course Outcomes	CO2	 Able to demonstrate the tools, Nakamoto consensus an demonstrate the working principals of payment verificatio protocol Able to describe and analyse the various consensus algorithr as per the application requirements. Able to design and develop the communication model for sending and receiving the messages in transaction. Able to design, develop and analyse the real time distribute 					
									CO3								
		This course provides the mechanism for the development of smart contract using solidity language for distributed applications.									CO4						
												eal time applications.			real time c	listribute	
No.	COs	Mapping with Program Outcomes (POs)										Мар	oing with PSOs				
۹U.	COS	P	D1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO
1	CO1	:	3	3	-	-	-	-	-	-	2	-	-	-	3	-	3
2	CO2	: :	3	3	3	1	2	-	-	-	1	-	-	-	2	3	2
3	CO3		1	2	3	3	2	2	-	-	-	-	-	-	2	3	3
4	CO4	. •	1	2	3	3	3	2	3	-	2	-	-	1	2	3	2
5	CO5		2	3	3	2	2	3	2	-	2	-	-	1	3	3	3
									SYLLAE	BUS							
No.	Content											ibutod	Hours COs		COs		
I	Blockchain Introduction and Overview: Background and evolution of technology, Distributed systems, Distributed Ledger: DLT concept, features, benefits and relevance in application, Security and Privacy: Cryptography, Hash, Permission										03 CO1		CO1				
		ssion			Cryptographic primitives: Symmetric cryptography, A Symmetric cryptography, DES, Hash functions, Patricia trees, Distributed hash tables (DHTs), Digital signatures, Sign then encrypt, Encrypt then sign Elliptic Curve Digital signature algorithm (ECDSA), How to generate a digital signature, ECDSA using OpenSSL Homomorphic												
11	Crypt trees,	ission ograph Distri	nic prir buted	hash ta	ables (DH	Ts), Digi	tal signa	tures, Sig	gn then	encrypt, E	ncrypt t	hen sign	Elliptic	Curve	04		CO1
	Crypt trees, Digita encry Bitcoi	ssion ograph Distri al signa ption, in, Bitc	nic prir buted ature a Signcr coin de	hash ta Igorithn yption, finition,	ables (DH n (ECDSA Zero knov , Keys an	Ts), Digi (), How to wledge p d addres	tal signa o generat roofs, Bli ses, Pub	tures, Sig e a digita nd signat	gn then I signati tures, Er	encrypt, E	ncrypt t A using (hemes	hen sign OpenSSL	Elliptic Homomo	Curve orphic	04		CO1 CO2 CO2
	Crypt trees, Digita encry Bitco units, Trans	ssion ograph Distri signa ption, in, Bito Base5 action	nic prir buted ature a Signcr coin de 68Chec s, The	hash ta Igorithn yption, finition, k encod transa	ables (DH n (ECDSA Zero knov , Keys an ding, Van action life	Ts), Digi), How to wledge p d addres ity addres e cycle,	tal signa o generat roofs, Bli sses, Pub sses The tran	tures, Sig e a digita nd signat lic keys i saction	gn then I signate tures, Er n bitcoir structure	encrypt, E ure, ECDSA ncoding sc n, Private k e, The scr	incrypt t A using (hemes keys in b	hen sign OpenSSL itcoin, Bi uage, Cc	Elliptic Homomo tcoin cur	Curve orphic rency			CO2
III IV V	Crypt trees, Digita encry Bitcoi units, Trans Opco Block	ssion ograph Distri al signa ption, in, Bitc Base5 actions des, Ty cchain,	nic prir buted ature a Signcr coin de 68Chec s, The ypes of ,The st	hash ta Igorithn yption, finition, k encoc transa f transa tructure	ables (DH n (ECDSA Zero kno , Keys an ding, Van ding, Van ding, Van ding, Tra ction, Tra of a bloc	Ts), Digi a), How to wledge p d addres ity addres cycle, nsaction k, The st	tal signa o generat roofs, Bli ses, Pub sses The tran fee, Con ructure o	tures, Sig e a digita nd signat lic keys i saction saction f a block	gn then Il signate tures, Er n bitcoin structure ansactio header,	encrypt, E ure, ECDSA ncoding sc n, Private k e, The scr on malleabi The genesi	incrypt t A using (hemes ceys in b ipt lang lity, Tran is block	hen sign OpenSSL itcoin, Bi uage, Co saction p Mining, T	Elliptic Homomo tcoin cur ommonly oools ask of mi	Curve orphic rency used	04		CO2 CO2
III IV V	Crypt trees, Digita encry Bitco units, Trans Opco Block Syncl	ission ograph Distri al signa ption, 3 in, Bito Base5 action des, Ty chain , hing up	nic prir buted ature a <u>Signcr</u> coin de <u>S8Chec</u> s, The s, The ypes of ,The st o with t	hash ta Igorithn yption, efinition, k encoc transa f transa f transa tructure the netw	ables (DH n (ECDSA <u>Zero know</u> , Keys an ding, Van ding, Van action life ction, Tra of a bloc vork,Proo	Ts), Digi), How to wledge p d addres ity addres cycle, nsaction k, The sti f of Work	tal signa o generat roofs, Bli ses, Pub sses The tran fee, Con ructure o	tures, Sig e a digita nd signat lic keys i saction saction f a block	gn then Il signate tures, Er n bitcoin structure ansactio header,	encrypt, E ure, ECDSA ncoding sc n, Private k e, The scr on malleabi	incrypt t A using (hemes ceys in b ipt lang lity, Tran is block	hen sign OpenSSL itcoin, Bi uage, Co saction p Mining, T	Elliptic Homomo tcoin cur ommonly oools ask of mi	Curve orphic rency used	04		CO2 CO2 CO3
III IV V VI	Crypt trees, Digita encry Bitcol units, Trans Opco Block Syncl CPU, The b	ission ograph Distril al signa ption, in, Bitc Base5 action des, Ty chain GPU, F itcoin	nic prir buted ature a Signcr coin de 88Chec s, The 7Pes of 7PGA, netwo	hash ta Igorithn yption, efinition, k encod transa transa f transa f transa tructure the netw ASICs, I rk: Wall	ables (DH n (ECDSA Zero know , Keys an ding, Van ding, Van ding, Van ding, Van ding, Van of a bloc vork,Proo Mining po ets, Payn	Ts), Digi a), How to <u>wledge p</u> d addres ity addres cycle, <u>nsaction</u> k, The sti f of Work ools nents: Bit	tal signa o generat roofs, Bli sses, Pub sses The tran fee, Con ructure o a, The min	tures, Sig e a digita nd signat lic keys i saction s tracts, Tra- f a block hing algon	gn then I signati tures, Er n bitcoir structure ansactic header, rithm, Th	encrypt, E ure, ECDSA ncoding scl n, Private k e, The scr on malleabi The genesi he hashing ng and sell	incrypt t A using (hemes ceys in b ipt lang lity, Tran is block rate, Mir	hen sign OpenSSL itcoin, Bi uage, Co saction p Mining, T ning syste	Elliptic Homomo tcoin cur ommonly oools ask of mi ems	Curve orphic rrency used ners	04		CO2 CO2 CO3 CO3 CO4 CO3
III IV V	Crypt trees, Digita encry Bitcoi units, Trans Opco Block Syncl CPU, The b Bitcoi	ission ograph Distri al signa <u>ption, s</u> in, Bitc Base5 actions des, Ty chain , hing up GPU, F oitcoin in prog	nic prir buted ature a <u>Signcr</u> coin de <u>8Chec</u> s, The <u>8Chec</u> s, The s (<u>7PGA</u> , netwoi grammi	hash ta Igorithn yption, finition, transa transa f transa tructure the netw ASICs, I rk: Wall ing and	ables (DH n (ECDSA Zero kno , Keys an ding, Van ding, Van ding, Van ding, Van ding, Van of a bloc vork,Proo Mining po ets, Payn the com	Ts), Digi a), How to <u>wledge p</u> d addres ity addres cycle, <u>nsaction</u> k, The str f of Work pols nents: Bit nand-line	tal signa o generat roofs, Bli ses, Pub sses The tran fee, Con ructure o c, The min coin inve	tures, Sig e a digita nd signat lic keys i saction s tracts, Tra- f a block hing algor estment a e, Bitcoin	gn then I signate tures, Er n bitcoin structure ansactio header, rithm, Th nd buyin improve	encrypt, E ure, ECDSA ncoding scl n, Private k e, The scr on malleabi The genesi he hashing ng and sell ement prop	incrypt t A using (hemes ceys in b ipt lang lity, Tran is block rate, Mir ing bitco osals (B	hen sign OpenSSL itcoin, Bi uage, Co saction p Mining, T ning syste Dins,Bitco IPs)	Elliptic Homomo tcoin cur ommonly oools ask of mi ems oin install	Curve orphic rency used ners lation,	04 04 05 04		CO2 CO2 CO3 CO3 CO4 CO3 CO4
V V VI	Crypt trees, Digita encry Bitco units, Trans Opco Block Synch CPU, The b Bitco Alterr adjus	ission ograph ograph I Distril I signa ption, 3 in, Bito Base5 action des, Ty chain, p des, Ty chain, p des, Ty chain, f des, f de	nic prir buted ature a <u>Signcr</u> coin de <u>8Chec</u> s, The <u>8Chec</u> s, The <u>8Chec</u> s, The <u>8Chec</u> s, The <u>8Chec</u> s, The <u>8Chec</u> s, The <u>7Chec</u> s, The <u>7Chec</u> s, The <u>7Chec</u> s, The st or s, s or s, s or s	hash ta Igorithn yption, efinition, ck encod transa transa f transa tructure the netw ASICs, I rk: Wall ing and Theoret targeting	ables (DH n (ECDSA Zero know , Keys an ding, Van action life ction, Tra of a bloc vork,Proo Mining po ets, Paym the comm the comm	Ts), Digi a), How to wledge p d addres ity addres cycle, nsaction k, The str f of Work ools nents: Bit nand-line dations, J	tal signa o generat roofs, Bli sses, Pub sses The tran fee, Con ructure o a, The min coin inve interface Alternativo oin limita	tures, Sig e a digita nd signat lic keys i saction s tracts, Tra- f a block ning algor estment a e, Bitcoin ves to Pro- tions, Ext	gn then I signati tures, Er n bitcoin structure ansactic header, rithm, Th ind buyi improve pof of We	encrypt, E ure, ECDSA ncoding scl n, Private k e, The scr on malleabi The genesi he hashing ng and sell	incrypt t A using (hemes ceys in b ipt lang lity, Tran is block rate, Mir ing bitco osals (B utsource	hen sign OpenSSL itcoin, Bi uage, Co saction p Mining, T hing syste Dins,Bitco IPs) able puzz	Elliptic Homomo tcoin cur ommonly oools ask of mi ems Din install	Curve orphic rency used ners lation, ulty	04 04 05		CO2 CO2 CO3 CO3 CO4 CO3
III IV VI VII	Crypt trees, Digita encry Bitcoi units, Trans Opco Block Synch CPU, The b Bitcoi Alterr adjus altcoi Smart Trans Ether	ission ograph ograph I signa <u>ption, s</u> in, Bitc Base5 actions des, Ty chain , hing up GPU, F bitcoin (in prog native (tment a ns, Con t Con sactions	nic prir buted ature a <u>Signcr</u> coin de <u>S8Chec</u> s, The <u>S8Chec</u> s, The <u>S8Chec</u> s, The <u>S8Chec</u> s, The <u>S8Chec</u> s, The tracts: s, Con	hash ta lgorithn yption, finition, ck encoce transa f transa transa f transa f transa transa f transa f transa f transa transa f transa f transa f transa f transa f transa transa f transa f tr	ables (DH n (ECDSA Zero know , Keys an ding, Van ding, Van ding, Van ding, Van ding, Van ding, Van of a bloc vork, Proo Mining po ets, Payn the com tical foun g algorith ithms, Co ition, Ri reation tra	Ts), Digi A), How to wledge p d addres a cycle, <u>nsaction</u> k, The st f of Work ools nents: Bit nand-line dations, J ams, Bitco oin, Minin cardian ansaction	tal signa o generat roofs, Bli ses, Pub sses The tran fee, Con ructure o a, The min coin inve interface Alternativ oin limita og guide, contract n, Messa	tures, Sig e a digita nd signat lic keys i saction s tracts, Tra- f a block ning algor estment a e, Bitcoin ves to Pro tions, Ext Zcash s, Ether ge call tr	gn then I signati tures, Er n bitcoin structure ansactic header, rithm, Th improve oof of We tended p reum 1 ansactic	encrypt, E ure, ECDSA ncoding scl n, Private k e, The scr on malleabi The genesi he hashing ng and sell ement prop ork, Non-ou	incrypt t A using (hemes ceys in b ipt lang lity, Tran is block rate, Mir ing bitco osals (B utsource n top of uction: ts of the	hen sign OpenSSL itcoin, Bi uage, Co saction p Mining, T ning syste Dins,Bitco IPs) able puzz bitcoin Do Ethereur e Ethereu	Elliptic Homomo tcoin cur ommonly oools ask of mi ems oin install les Diffic evelopme n block	Curve orphic rency used ners lation, ulty ent of chain, chain,	04 04 05 04		CO2 CO2 CO3 CO3 CO4 CO3 CO4
III IV V VI	Crypt trees, Digita encry Bitcoi units, Trans Opco Block Syncl CPU, The b Bitcoi Alterr adjus altcoi Smart Trans Ether mech	ission ograph ograph Distril al signa <u>ption, s</u> in, Bitc Base5 action des, Ty chain, b ing up GPU, F bitcoin in prog native (tment a ns, Con t Con saction anism	nic prir buted ature a <u>Signcr</u> coin de <u>S8Chec</u> s, The <u>S8Chec</u> s, Con s irtual r s	hash ta Igorithn yption, efinition, ck encod transa transa f transa tructure the netw ASICs, I rk: Wall ing and Theoret targeting us algor Defin tract cr machine	ables (DH n (ECDSA Zero know , Keys an ding, Van ding, Van ding, Van ding, Van ding, Van of a bloc vork,Proo Mining po ets, Payn the comm tical foun g algorith itian, Ri reation tra e (EVM),	Ts), Digi A), How to wledge p d addres ity addres cycle, nsaction k, The sti f of Work ools nents: Bit nand-line dations, f ims, Bitco oin, Minir cardian ansaction Precomp	tal signa o generat roofs, Bli ses, Pub sses The tran fee, Con ructure o a, The min coin inve interface Alternativo oin limita og guide, contract n, Messa iled cont	tures, Sig e a digita nd signat lic keys i saction s tracts, Tra- f a block ning algon estment a e, Bitcoin ves to Pro- tions, Ext Zcash s, Ether ge call tr racts, Ac	gn then I signati tures, Er n bitcoin structure ansactic header, rithm, Th improve of of We tended p reum 1 ansactic counts,	encrypt, E ure, ECDSA ncoding sci n, Private k e, The scr on malleabi The genesi he hashing ng and sell ement prop ork, Non-ou orotocols o 01 Introdu on, Elemen	incrypt t A using (hemes ceys in b ript lang lity, Tran is block rate, Mir ing bitco osals (B utsource n top of uction: ts of the ransactio	hen sign DpenSSL itcoin, Bi uage, Co saction p Mining, T ning syste Dins,Bitco IPs) able puzz bitcoin D Ethereur e Ethereu on and B	Elliptic Homomo tcoin cur ommonly oools ask of mi ask of mi ask of mi ems bin install les Diffic evelopme n block im block	Curve orphic rency used ners lation, ulty ent of chain, chain, dation	04 04 05 04 05		CO2 CO2 CO3 CO3 CO4 CO3 CO4 CO4

2. Melanie Swan, Blockchain: Blueprint for New Economy, 1/E, O'Reilly Media, 2015.

- 3. Sam Goundar, Blockchain Technologies, Applications And Cryptocurrencies: Current Practice And Future Trends, 1/E Word Scientific, 2020

Supplementary Readings

- 1. Alan T. Norman, Blockchain Technology Explained: The Ultimate Beginner's Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts, 1/E, [United States?] : Alan T. Norman, 2017
- 2. Jan Veuger, Blockchain Technology and Applications, 1/E, Nova Publisher, 2019
- 3. Andreas Bolfing, Cryptographic Primitives in Blockchain Technology : A Mathematical Introduction, 1/E, Oxford University Press, 2020.