

## 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<br>Objectives   |   | This course describes the in-depth knowledge and concept of recent technologies, tools, and implementation strategies.   |   |  |  |  |  |   |   | Course<br>Outcomes  | CO2  | <ul> <li>Able to demonstrate the tools, Nakamoto consensus an demonstrate the working principals of payment verificatio protocol</li> <li>Able to describe and analyse the various consensus algorithr as per the application requirements.</li> <li>Able to design and develop the communication model for sending and receiving the messages in transaction.</li> <li>Able to design, develop and analyse the real time distribute</li> </ul> |   |   |                            |            |  |
|                        |   |  |   |  |  |  |  |   | 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<br>trees,   | ission<br>ograph<br>Distri   | nic prir<br>buted   | hash ta  | ables (DH  | Ts), Digi  | tal signa  | tures, Sig  | gn then   | encrypt, E  | ncrypt t   | hen sign  | Elliptic  | Curve   | 04                         |            | CO1  |
|                        | Crypt<br>trees,<br>Digita<br>encry<br>Bitcoi  | ssion<br>ograph<br>Distri<br>al signa<br>ption,<br>in, Bitc  | nic prir<br>buted<br>ature a<br>Signcr<br>coin de   | hash ta<br>Igorithn<br>yption,<br>finition,  | ables (DH<br>n (ECDSA<br>Zero knov<br>, Keys an  | Ts), Digi<br>(), How to<br>wledge p<br>d addres  | tal signa<br>o generat<br>roofs, Bli<br>ses, Pub   | tures, Sig<br>e a digita<br>nd signat   | gn then<br>I signati<br>tures, Er   | encrypt, E  | ncrypt t<br>A using (<br>hemes   | hen sign<br>OpenSSL   | Elliptic<br>Homomo  | Curve<br>orphic   | 04                         |            | CO1<br>CO2<br>CO2                                    |
|                        | Crypt<br>trees,<br>Digita<br>encry<br>Bitco<br>units,<br>Trans  | ssion<br>ograph<br>Distri<br>signa<br>ption,<br>in, Bito<br>Base5<br>action  | nic prir<br>buted<br>ature a<br>Signcr<br>coin de<br>68Chec<br>s, The   | hash ta<br>Igorithn<br>yption,<br>finition,<br>k encod<br>transa   | ables (DH<br>n (ECDSA<br>Zero knov<br>, Keys an<br>ding, Van<br>action life  | Ts), Digi<br>), How to<br>wledge p<br>d addres<br>ity addres<br>e cycle,   | tal signa<br>o generat<br>roofs, Bli<br>sses, Pub<br>sses<br>The tran  | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction  | gn then<br>I signate<br>tures, Er<br>n bitcoir<br>structure   | encrypt, E<br>ure, ECDSA<br>ncoding sc<br>n, Private k<br>e, The scr  | incrypt t<br>A using (<br>hemes<br>keys in b   | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Cc   | Elliptic<br>Homomo<br>tcoin cur   | Curve<br>orphic<br>rency  |                            |            | CO2  |
| III<br>IV<br>V         | Crypt<br>trees,<br>Digita<br>encry<br>Bitcoi<br>units,<br>Trans<br>Opco<br>Block  | ssion<br>ograph<br>Distri<br>al signa<br>ption,<br>in, Bitc<br>Base5<br>actions<br>des, Ty<br>cchain,  | nic prir<br>buted<br>ature a<br>Signcr<br>coin de<br>68Chec<br>s, The<br>ypes of<br>,The st   | hash ta<br>Igorithn<br>yption,<br>finition,<br>k encoc<br>transa<br>f transa<br>tructure   | ables (DH<br>n (ECDSA<br>Zero kno<br>, Keys an<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Tra<br>ction, Tra<br>of a bloc  | Ts), Digi<br>a), How to<br>wledge p<br>d addres<br>ity addres<br>cycle,<br>nsaction<br>k, The st   | tal signa<br>o generat<br>roofs, Bli<br>ses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o  | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction<br>saction<br>f a block  | gn then<br>Il signate<br>tures, Er<br>n bitcoin<br>structure<br>ansactio<br>header,   | encrypt, E<br>ure, ECDSA<br>ncoding sc<br>n, Private k<br>e, The scr<br>on malleabi<br>The genesi   | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ipt lang<br>lity, Tran<br>is block   | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T   | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi  | Curve<br>orphic<br>rency<br>used  | 04                         |            | CO2<br>CO2   |
| III<br>IV<br>V         | Crypt<br>trees,<br>Digita<br>encry<br>Bitco<br>units,<br>Trans<br>Opco<br>Block<br>Syncl  | ission<br>ograph<br>Distri<br>al signa<br>ption, 3<br>in, Bito<br>Base5<br>action<br>des, Ty<br>chain ,<br>hing up   | nic prir<br>buted<br>ature a<br><u>Signcr</u><br>coin de<br><u>S8Chec</u><br>s, The<br>s, The<br>ypes of<br>,The st<br>o with t   | hash ta<br>Igorithn<br>yption,<br>efinition,<br>k encoc<br>transa<br>f transa<br>f transa<br>tructure<br>the netw  | ables (DH<br>n (ECDSA<br><u>Zero know</u><br>, Keys an<br>ding, Van<br>ding, Van<br>action life<br>ction, Tra<br>of a bloc<br>vork,Proo  | Ts), Digi<br>), How to<br>wledge p<br>d addres<br>ity addres<br>cycle,<br>nsaction<br>k, The sti<br>f of Work  | tal signa<br>o generat<br>roofs, Bli<br>ses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o  | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction<br>saction<br>f a block  | gn then<br>Il signate<br>tures, Er<br>n bitcoin<br>structure<br>ansactio<br>header,   | encrypt, E<br>ure, ECDSA<br>ncoding sc<br>n, Private k<br>e, The scr<br>on malleabi   | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ipt lang<br>lity, Tran<br>is block   | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T   | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi  | Curve<br>orphic<br>rency<br>used  | 04                         |            | CO2<br>CO2<br>CO3                                    |
| III<br>IV<br>V<br>VI   | Crypt<br>trees,<br>Digita<br>encry<br>Bitcol<br>units,<br>Trans<br>Opco<br>Block<br>Syncl<br>CPU,<br>The b  | ission<br>ograph<br>Distril<br>al signa<br>ption,<br>in, Bitc<br>Base5<br>action<br>des, Ty<br>chain<br>GPU, F<br>itcoin   | nic prir<br>buted<br>ature a<br>Signcr<br>coin de<br>88Chec<br>s, The<br>7Pes of<br>7PGA,<br>netwo  | hash ta<br>Igorithn<br>yption,<br>efinition,<br>k encod<br>transa<br>transa<br>f transa<br>f transa<br>tructure<br>the netw<br>ASICs, I<br>rk: Wall  | ables (DH<br>n (ECDSA<br>Zero know<br>, Keys an<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>of a bloc<br>vork,Proo<br>Mining po<br>ets, Payn   | Ts), Digi<br>a), How to<br><u>wledge p</u><br>d addres<br>ity addres<br>cycle,<br><u>nsaction</u><br>k, The sti<br>f of Work<br>ools<br>nents: Bit   | tal signa<br>o generat<br>roofs, Bli<br>sses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o<br>a, The min   | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction s<br>tracts, Tra-<br>f a block<br>hing algon   | gn then<br>I signati<br>tures, Er<br>n bitcoir<br>structure<br>ansactic<br>header,<br>rithm, Th   | encrypt, E<br>ure, ECDSA<br>ncoding scl<br>n, Private k<br>e, The scr<br>on malleabi<br>The genesi<br>he hashing<br>ng and sell   | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ipt lang<br>lity, Tran<br>is block<br>rate, Mir  | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T<br>ning syste   | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi<br>ems   | Curve<br>orphic<br>rrency<br>used<br>ners   | 04                         |            | CO2<br>CO2<br>CO3<br>CO3<br>CO4<br>CO3               |
| III<br>IV<br>V         | Crypt<br>trees,<br>Digita<br>encry<br>Bitcoi<br>units,<br>Trans<br>Opco<br>Block<br>Syncl<br>CPU,<br>The b<br>Bitcoi  | ission<br>ograph<br>Distri<br>al signa<br><u>ption, s</u><br>in, Bitc<br>Base5<br>actions<br>des, Ty<br>chain ,<br>hing up<br>GPU, F<br>oitcoin<br>in prog   | nic prir<br>buted<br>ature a<br><u>Signcr</u><br>coin de<br><u>8Chec</u><br>s, The<br><u>8Chec</u><br>s, The<br>s<br>( <u>7PGA</u> ,<br>netwoi<br>grammi  | hash ta<br>Igorithn<br>yption,<br>finition,<br>transa<br>transa<br>f transa<br>tructure<br>the netw<br>ASICs, I<br>rk: Wall<br>ing and   | ables (DH<br>n (ECDSA<br>Zero kno<br>, Keys an<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>of a bloc<br>vork,Proo<br>Mining po<br>ets, Payn<br>the com   | Ts), Digi<br>a), How to<br><u>wledge p</u><br>d addres<br>ity addres<br>cycle,<br><u>nsaction</u><br>k, The str<br>f of Work<br>pols<br>nents: Bit<br>nand-line  | tal signa<br>o generat<br>roofs, Bli<br>ses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o<br>c, The min<br>coin inve   | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction s<br>tracts, Tra-<br>f a block<br>hing algor<br>estment a<br>e, Bitcoin  | gn then<br>I signate<br>tures, Er<br>n bitcoin<br>structure<br>ansactio<br>header,<br>rithm, Th<br>nd buyin<br>improve  | encrypt, E<br>ure, ECDSA<br>ncoding scl<br>n, Private k<br>e, The scr<br>on malleabi<br>The genesi<br>he hashing<br>ng and sell<br>ement prop   | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ipt lang<br>lity, Tran<br>is block<br>rate, Mir<br>ing bitco<br>osals (B   | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T<br>ning syste<br>Dins,Bitco<br>IPs)   | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi<br>ems<br>oin install  | Curve<br>orphic<br>rency<br>used<br>ners<br>lation,   | 04<br>04<br>05<br>04       |            | CO2<br>CO2<br>CO3<br>CO3<br>CO4<br>CO3<br>CO4        |
| V<br>V<br>VI           | Crypt<br>trees,<br>Digita<br>encry<br>Bitco<br>units,<br>Trans<br>Opco<br>Block<br>Synch<br>CPU,<br>The b<br>Bitco<br>Alterr<br>adjus   | ission<br>ograph<br>ograph<br>I Distril<br>I signa<br>ption, 3<br>in, Bito<br>Base5<br>action<br>des, Ty<br>chain, p<br>des, Ty<br>chain, p<br>des, Ty<br>chain, f<br>des, f<br>de | nic prir<br>buted<br>ature a<br><u>Signcr</u><br>coin de<br><u>8Chec</u><br>s, The<br><u>8Chec</u><br>s, The<br><u>8Chec</u><br>s, The<br><u>8Chec</u><br>s, The<br><u>8Chec</u><br>s, The<br><u>8Chec</u><br>s, The<br><u>7Chec</u><br>s, The<br><u>7Chec</u><br>s, The<br><u>7Chec</u><br>s, The<br>st<br>or<br>s, s<br>or s, s<br>or s | hash ta<br>Igorithn<br>yption,<br>efinition,<br>ck encod<br>transa<br>transa<br>f transa<br>tructure<br>the netw<br>ASICs, I<br>rk: Wall<br>ing and<br>Theoret<br>targeting  | ables (DH<br>n (ECDSA<br>Zero know<br>, Keys an<br>ding, Van<br>action life<br>ction, Tra<br>of a bloc<br>vork,Proo<br>Mining po<br>ets, Paym<br>the comm<br>the comm  | Ts), Digi<br>a), How to<br>wledge p<br>d addres<br>ity addres<br>cycle,<br>nsaction<br>k, The str<br>f of Work<br>ools<br>nents: Bit<br>nand-line<br>dations, J  | tal signa<br>o generat<br>roofs, Bli<br>sses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o<br>a, The min<br>coin inve<br>interface<br>Alternativo<br>oin limita  | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction s<br>tracts, Tra-<br>f a block<br>ning algor<br>estment a<br>e, Bitcoin<br>ves to Pro-<br>tions, Ext   | gn then<br>I signati<br>tures, Er<br>n bitcoin<br>structure<br>ansactic<br>header,<br>rithm, Th<br>ind buyi<br>improve<br>pof of We                                 | encrypt, E<br>ure, ECDSA<br>ncoding scl<br>n, Private k<br>e, The scr<br>on malleabi<br>The genesi<br>he hashing<br>ng and sell   | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ipt lang<br>lity, Tran<br>is block<br>rate, Mir<br>ing bitco<br>osals (B<br>utsource   | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T<br>hing syste<br>Dins,Bitco<br>IPs)<br>able puzz  | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi<br>ems<br>Din install  | Curve<br>orphic<br>rency<br>used<br>ners<br>lation,<br>ulty   | 04<br>04<br>05             |            | CO2<br>CO2<br>CO3<br>CO3<br>CO4<br>CO3               |
| III<br>IV<br>VI<br>VII | Crypt<br>trees,<br>Digita<br>encry<br>Bitcoi<br>units,<br>Trans<br>Opco<br>Block<br>Synch<br>CPU,<br>The b<br>Bitcoi<br>Alterr<br>adjus<br>altcoi<br>Smart<br>Trans<br>Ether  | ission<br>ograph<br>ograph<br>I signa<br><u>ption, s</u><br>in, Bitc<br>Base5<br>actions<br>des, Ty<br>chain ,<br>hing up<br>GPU, F<br>bitcoin (<br>in prog<br>native (<br>tment a<br>ns, Con<br>t Con<br>sactions   | nic prir<br>buted<br>ature a<br><u>Signcr</u><br>coin de<br><u>S8Chec</u><br>s, The<br><u>S8Chec</u><br>s, The<br><u>S8Chec</u><br>s, The<br><u>S8Chec</u><br>s, The<br><u>S8Chec</u><br>s, The<br>tracts:<br>s, Con  | hash ta<br>lgorithn<br>yption,<br>finition,<br>ck encoce<br>transa<br>f transa<br>transa<br>f transa<br>f transa<br>transa<br>f transa<br>f transa<br>f transa<br>transa<br>f transa<br>f transa<br>f transa<br>f transa<br>f transa<br>transa<br>f transa<br>f tr | ables (DH<br>n (ECDSA<br>Zero know<br>, Keys an<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>of a bloc<br>vork, Proo<br>Mining po<br>ets, Payn<br>the com<br>tical foun<br>g algorith<br>ithms, Co<br>ition, Ri<br>reation tra   | Ts), Digi<br>A), How to<br>wledge p<br>d addres<br>a cycle,<br><u>nsaction</u><br>k, The st<br>f of Work<br>ools<br>nents: Bit<br>nand-line<br>dations, J<br>ams, Bitco<br>oin, Minin<br>cardian<br>ansaction                  | tal signa<br>o generat<br>roofs, Bli<br>ses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o<br>a, The min<br>coin inve<br>interface<br>Alternativ<br>oin limita<br>og guide,<br>contract<br>n, Messa               | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction s<br>tracts, Tra-<br>f a block<br>ning algor<br>estment a<br>e, Bitcoin<br>ves to Pro<br>tions, Ext<br>Zcash<br>s, Ether<br>ge call tr               | gn then<br>I signati<br>tures, Er<br>n bitcoin<br>structure<br>ansactic<br>header,<br>rithm, Th<br>improve<br>oof of We<br>tended p<br>reum 1<br>ansactic           | encrypt, E<br>ure, ECDSA<br>ncoding scl<br>n, Private k<br>e, The scr<br>on malleabi<br>The genesi<br>he hashing<br>ng and sell<br>ement prop<br>ork, Non-ou  | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ipt lang<br>lity, Tran<br>is block<br>rate, Mir<br>ing bitco<br>osals (B<br>utsource<br>n top of<br>uction:<br>ts of the               | hen sign<br>OpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T<br>ning syste<br>Dins,Bitco<br>IPs)<br>able puzz<br>bitcoin Do<br>Ethereur<br>e Ethereu   | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi<br>ems<br>oin install<br>les Diffic<br>evelopme<br>n block                                       | Curve<br>orphic<br>rency<br>used<br>ners<br>lation,<br>ulty<br>ent of<br>chain,<br>chain,           | 04<br>04<br>05<br>04       |            | CO2<br>CO2<br>CO3<br>CO3<br>CO4<br>CO3<br>CO4        |
| III<br>IV<br>V<br>VI   | Crypt<br>trees,<br>Digita<br>encry<br>Bitcoi<br>units,<br>Trans<br>Opco<br>Block<br>Syncl<br>CPU,<br>The b<br>Bitcoi<br>Alterr<br>adjus<br>altcoi<br>Smart<br>Trans<br>Ether<br>mech  | ission<br>ograph<br>ograph<br>Distril<br>al signa<br><u>ption, s</u><br>in, Bitc<br>Base5<br>action<br>des, Ty<br>chain, b<br>ing up<br>GPU, F<br>bitcoin<br>in prog<br>native (<br>tment a<br>ns, Con<br>t Con<br>saction<br>anism  | nic prir<br>buted<br>ature a<br><u>Signcr</u><br>coin de<br><u>S8Chec</u><br>s, The<br><u>S8Chec</u><br>s, Con<br>s<br>irtual r<br>s  | hash ta<br>Igorithn<br>yption,<br>efinition,<br>ck encod<br>transa<br>transa<br>f transa<br>tructure<br>the netw<br>ASICs, I<br>rk: Wall<br>ing and<br>Theoret<br>targeting<br>us algor<br>Defin<br>tract cr<br>machine  | ables (DH<br>n (ECDSA<br>Zero know<br>, Keys an<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>ding, Van<br>of a bloc<br>vork,Proo<br>Mining po<br>ets, Payn<br>the comm<br>tical foun<br>g algorith<br>itian, Ri<br>reation tra<br>e (EVM),   | Ts), Digi<br>A), How to<br>wledge p<br>d addres<br>ity addres<br>cycle,<br>nsaction<br>k, The sti<br>f of Work<br>ools<br>nents: Bit<br>nand-line<br>dations, f<br>ims, Bitco<br>oin, Minir<br>cardian<br>ansaction<br>Precomp | tal signa<br>o generat<br>roofs, Bli<br>ses, Pub<br>sses<br>The tran<br>fee, Con<br>ructure o<br>a, The min<br>coin inve<br>interface<br>Alternativo<br>oin limita<br>og guide,<br>contract<br>n, Messa<br>iled cont | tures, Sig<br>e a digita<br>nd signat<br>lic keys i<br>saction s<br>tracts, Tra-<br>f a block<br>ning algon<br>estment a<br>e, Bitcoin<br>ves to Pro-<br>tions, Ext<br>Zcash<br>s, Ether<br>ge call tr<br>racts, Ac | gn then<br>I signati<br>tures, Er<br>n bitcoin<br>structure<br>ansactic<br>header,<br>rithm, Th<br>improve<br>of of We<br>tended p<br>reum 1<br>ansactic<br>counts, | encrypt, E<br>ure, ECDSA<br>ncoding sci<br>n, Private k<br>e, The scr<br>on malleabi<br>The genesi<br>he hashing<br>ng and sell<br>ement prop<br>ork, Non-ou<br>orotocols o<br>01 Introdu<br>on, Elemen | incrypt t<br>A using (<br>hemes<br>ceys in b<br>ript lang<br>lity, Tran<br>is block<br>rate, Mir<br>ing bitco<br>osals (B<br>utsource<br>n top of<br>uction:<br>ts of the<br>ransactio | hen sign<br>DpenSSL<br>itcoin, Bi<br>uage, Co<br>saction p<br>Mining, T<br>ning syste<br>Dins,Bitco<br>IPs)<br>able puzz<br>bitcoin D<br>Ethereur<br>e Ethereu<br>on and B  | Elliptic<br>Homomo<br>tcoin cur<br>ommonly<br>oools<br>ask of mi<br>ask of mi<br>ask of mi<br>ems<br>bin install<br>les Diffic<br>evelopme<br>n block<br>im block | Curve<br>orphic<br>rency<br>used<br>ners<br>lation,<br>ulty<br>ent of<br>chain,<br>chain,<br>dation | 04<br>04<br>05<br>04<br>05 |            | CO2<br>CO2<br>CO3<br>CO3<br>CO4<br>CO3<br>CO4<br>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.