

**İTÜ**  
**LİSANSÜSTÜ DERS KATALOG FORMU**  
**(GRADUATE COURSE CATALOGUE FORM)**

Dersin Adı			Course Name	
Blokzincir Teknolojileri			Blockchain Technologies	
Kodu (Code)	Yarıyılı (Semester)	Kredisi (Local Credits)	AKTS Kredisi (ECTS Credits)	Ders Seviyesi (Course Level)
BGK 519E	Güz (Fall)	3	7,5	Y.L. (M.Sc.)
Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)			
Dersin Türü (Course Type)	Seçmeli (Elective)	Dersin Dili (Course Language)	İngilizce (English)	
Dersin İçeriği (Course Description)	Blokzincir, Kripto ve Kriptoparalara giriş. Sanal para mekaniği: Sanal para basma, Sanal para madenciliği ve Sanal para transfer yapısı. Blokzincirde kullanılan kriptografik yapıtaşları. Anonim Kriptoparalar. Konsensus Mekanizmaları. Akıllı Kontrat Teknolojisi. Blokzincirde diğer uygulamalar ve kullanım vakaları: Kimlik Yönetimi, Tedarik Zinciri, Loglama sistemleri, Sertifika Yönetimi. Güncel Blokzincir konuları ve yayınlar. <i>30-60 kelime arası</i>			
Dersin Amacı (Course Objectives)	1. Blokzincir teknolojilerini tanıtmak 2. Kriptoparaları sınıflandırmak ve genellikle bilinen ilk blokzincir uygulaması Sanal para analiz etmek 3. Blokzincirde kullanılan kriptografik yapıtaşlarını öğretmek 4. Blokzincir teknolojisi üzerindeki diğer uygulamaları tanımak <i>Maddeler halinde 2-5 adet</i>			
Dersin Öğrenme Çıktıları (Course Learning Outcomes)	Bu dersi başarıyla tamamlayan öğrenciler; 1. Öğrenciler Blokzincir Teknolojisinin neden gerektiğini kavrayacaklar. 2. Öğrenciler sık karşılaşılan Sanal para ve anonim kriptoparaları tanıyacaklar. 3. Öğrenciler blokzincirde kullanılan kripto yapıtaşları konusunda fikir sahibi olacaklar. 4. Öğrenciler blokzincir teknolojisinin kullanılabileceği alanlarla ilgili fikir edinecekler. <i>Maddeler halinde 4-9 adet</i>			
	Students who successfully completed this course; 1. Students will understand the necessity of Blockchain Technology 2. Understanding of the most well known cryptocurrency and related anonymous cryptocurrencies 3. Understanding of cryptographic methods used in Blockchain Technology. 4. Understanding the use-cases of Blockchain Technology.			

<b>Kaynaklar</b> (References) <i>En önemli 5 adedini belirtiniz</i>	<ul style="list-style-type: none"> <li>Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016</li> <li>CryptoSchool, Springer-Verlag Berlin Heidelberg, 2015</li> </ul>		
<b>Ödevler ve Projeler</b> (Homework & Projects)	---		
<b>Laboratuar Uygulamaları</b> (Laboratory Work)	--		
<b>Bilgisayar Kullanımı</b> (Computer Use)	--		
<b>Diğer Uygulamalar</b> (Other Activities)	--		
<b>Başarı Değerlendirme Sistemi</b> (Assessment Criteria)	<b>Faaliyetler</b> (Activities)	<b>Adedi*</b> (Quantity)	<b>Değerlendirmedeki Katkısı, %</b> (Effects on Grading, %)
	<b>Yıl İçi Sınavları</b> (Midterm Exams)	1	30
	<b>Kısa Sınavlar</b> (Quizzes)	-	-
	<b>Ödevler</b> (Homework)	-	-
	<b>Projeler</b> (Projects)	1	30
	<b>Dönem Ödevi/Projesi</b> (Term Paper/Project)	-	-
	<b>Laboratuar Uygulaması</b> (Laboratory Work)	-	-
	<b>Diğer Uygulamalar</b> (Other Activities)	-	-
	<b>Final Sınavı</b> (Final Exam)	1	40

\*Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

## DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Blokzincir, Kripto ve Kriptoparalar	1,2,3
2	Sanal para mekaniği: Sanal para basma. Sanal para transfer yapısı.	1,2,3
3	Sanal para madenciliği	1,2,3
4	Sanal para Konsensus Mekanizması.	1,2,3
5	Blokzincirde kullanılan kriptografik yapıtaşları	4
6	Blokzincirde kullanılan kriptografik yöntemler	1,2,3
7	Anonim Kriptoparalar	1,2,3
8	Alternatif Konsensus Algoritmaları	1,2,3
9	Etherium ve Akıllı Kontratlar	4
10	Blokzincirde diğer uygulamalar ve kullanım vakaları: Kimlik Yönetimi	1,2,3
11	Blokzincirde diğer uygulamalar ve kullanım vakaları: Tedarik Zinciri	1,2,3
12	Blokzincirde diğer uygulamalar ve kullanım vakaları: Loglama sistemleri	1,2,3
13	Blokzincirde diğer uygulamalar ve kullanım vakaları: Sertifika Yönetimi.	4
14	Güncel Blokzincir konuları ve yayınlar	4

## COURSE PLAN

Weeks	Topics	Course Outcomes
1	Blockchain, Crypto and Cryptocurrencies.	1,2,3
2	Mechanics of cryptocurrency: Cryptocurrency generation, structure of cryptocurrency transactions.	1,2,3
3	Cryptocurrency mining	1,2,3
4	Cryptocurrency Consensus Mechanism.	1,2,3
5	Cryptographic primitives in Blockchain	4
6	Cryptographic methods in Blockchain	1,2,3
7	Anonymous Cryptocurrencies.	1,2,3
8	Alternative Consensus Algorithms	1,2,3
9	Smart contract technology and Ethereum	4
10	Further applications and use-cases of blockchain such as Identity management	1,2,3
11	Further applications and use-cases of blockchain such as Supply Chain Management	1,2,3
12	Further applications and use-cases of blockchain such as Log systems.	1,2,3
13	Further applications and use-cases of blockchain such as Certification Management	4
14	Current Blockchain Topics and Publications.	4

## Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

	Programın mezuna kazandıracığı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirilme (yeterli bilgi birikimi) (bilgi).	X		
ii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).		X	
iii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).			
iv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).	X		
v.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümlenebilir (beceri).			
vi.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
vii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemez karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözülmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).			
x.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).	X		
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).	X		
xii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			
xiii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).		X	
xiv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümledikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).	X		
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).	X		

1: Az, 2. Kısmi, 3. Tam

**Relationship between the Course and Cybersecurity Engineering and Cryptography Graduate (MS) Curriculum**

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).	X		
ii.	Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge).		X	
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill).			
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill).	X		
v.	Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill).			
vi.	The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility).			
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).			
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Cybersecurity Engineering and Cryptography area (Competence to work independently and take responsibility)			
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).			
x.	Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).	X		
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).	X		
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency).			
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).		X	
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).	X		
xvi.	The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency).	X		

**1: Little, 2. Partial, 3. Full**

<b><u>Düzenleyen (Prepared by)</u></b>	<b><u>Tarih (Date)</u> 25.04.2019</b>	<b><u>İmza (Signature)</u></b>
--	---	--------------------------------