TEMARIO CURSO DE BITCOIN

Módulos de aprendizaje	Temáticas
Introducción	Libro Blanco (White Paper)
	Si hubiéramos sabido lo que estábamos empezando en 2017.
	Pedigree académico de Bitcoin
	Introducción a la cadena de Bloques
	Límites económicos de Blockchain Y Bitcoin
	Prueba de Trabajo (PoW)
	Ajuste de dificultad
	Problema de los generales Bizantinos
	Ejecutar un NODO completo
Historia y Filosofía Bitcoin	Historia del desarrollo de Bitcoin
	¿Qué es el consenso?
Soft Forks y descripción general del protocolo	Categorización de los forks (Soft, Hard, evil, etc)
	Actualizacion del dia de la bandera
	Señalización IsSuperMajority
	Señalización BIP9
	BIP148 Y BIP149
	BIP91
Modelos de Seguridad	Visión de Conjunto
	Puntos de control, supuestos Válidos, mínimos de trabajo en cadena.
	Definición de SVP y clientes ligeros
	BIP 37 (filtros de Floración)
	Neutrino
	Filtros de Floración comprometidos
	Pruebas de Fraude
	Hashes UTXOS Comprometidos
	Asumir UTXO
	Utreexo
	Propuestas alternativas de conjuntos UTXO
Minería	Distribución de Poisson/libre de progreso
	Llegadas en Bloques en la Blockchain de Bitcoin
	Tasa de Fee
	Mineria Egoista
	Ataques de 51%
	MejorHash
	Descripción General de la minería sin recompensa
	Descripción general del Pool
	Salto al Pool

	PPs como una solución empresarial del mundo real.
	Pagos del Canal de Pago
	Impulso de ASIC
	Minería BCH/Ajuste de dificultad
	Tumblebit
Ataques	**Ataques de povo**
Enfoques de consenso	**Visión de Conjunto**
	Fantasma
	Tolerancia a fallas bizantinas
	Trenza
	Bitcoin-NG/PoW+BFT
	Prueba de participación
	Cadenas Laterales
Cambios de consenso y bifurcaciones duras (HARD FORK)	**Historia**
	Bloques de extensión
	Bifurcaciones duras: Peligros potenciales
	Protección de reproducción
	Protección contra borrado
	Investigación Actual (spoonet, etc.)
Criptografía	**Los 3 eventos seminales en criptografía**
	Una descripción general de la criptografía de clave pública
	Campos finitos, curvas elípticas, ECDSA, schnoor.
	Bitcoin, azar y aleatoriedad
	Sobre la seguridad de Bitcoin en presencia de primitivos criptográficos rotos.
	Firmas y pruebas de conocimiento cero
	pruebas de conocimiento cero
	a prueba de balas
	esquemas de compromiso; compromisos pedersen
	Deffie-Hellman
	Firmas de anillo
	RSA
Actas	**Comprender una transacción Bitcoin sin procesar**
	Comprender una transacción Bitcoin sin procesar de manera difícil.
	Trabajar con transacciones
	Formato de transacción
	Texto
	Firma de transacciones
	Normalidad
	Transacciones 0-conf
	Transacciones de Bitcoin parcialmente firmadas
	SIGHASH-NOINPUT
	Transacciones compactadas
	Mempool
Bloques	**árboles de Merkle**
	Estructura de datos en Validación.
	Reorganizaciones
	Poda
Segwit	**Antecedentes e Historia de Segwith**
	Segwith Avanzado
	Segwith y escalabilidad
	Maleabilidad tx

	Segwith y tamaño de Bloque
	Bech32
Billeteras	**Desarrollo de Billetera**
	Desarrollo de Billetera en Bitcoin Core
	Billetera HD
	Carteras de descriptores nativos
	Monedero BerkeleyDB almacén de valor clave, archivo de datos, entorno, registros y vaciado.
	Tipos de clave de billetera, normal, solo reloj, HD.
	Gestión de claves de billetera: conjuntos de claves, metadatos de clave, metadatos de direcciones.
	Volver a escanear la billetera
	Tarifa
	Estimación de tarifas
	Reemplazar por tarifa
	Selección de monedas
	Cartera de hardware con Bitcoin Core.
Scripts y Contracts	**Secuencias de comandos y transacciones.**
	Secuencias de comandos P2PKH, P2SH, P2WPKH, P2WSH, BECH32
	Descriptores de Script
	P2EP
	Contratos inteligentes en una cadena tonta, Mimble Wimble
	Contratos Inteligentes en una cadena tonta: Scriptless scripts.
	Cadenas de Pago
	MÁSTIL
	SNARKS ZK
	ZK STARS
	Contratos y registros discretos
	Mini Script
	Estado del script
Fungibilidad y escalabilidad	**Visión de conjunto**
	Sobre la escalabilidad de las blockchain descentralizadas
	Porque es importante la fungibilidad
	Privacidad
	Análisis de cadena
	Huella digital de billetera
	Análisis del origen de la Transacción
	CoinJoin
	Transacciones Confidenciales
	Tumblebit
	Mezcla de Monedas
	Schnoor
	Bellare Neven
	Esquemas de Umbral
	Agregación de Firmas
	Taproot
	Injertroot
Red P2P	**Resumen de la red P2P**
	Propagación de Transacciones
	Sincronización de Headers First
	Avances de la propagación de bloques
	Bloques compactos
	Des-anonimización de la red P2P de Bitcoin

	Dandelion
	Descubrimiento de pares
	Descubrimiento de topología
	Conectividad entre pares
	Secuestro BGP
	Partición de red y ataques de privacidad a nivel de red
	Investigación de ataques de privacidad P2P
	Ataques de eclipse de red punto a punto de Bitcoin 2015
	Conceptos de denegación de servicio
	Prevención de denegación de servicio
	Nodos SPV
	MiniSketch
FORKS Y FALLAS	**BIP66 Bifurcación y minería espía**
Arquitectura BTC	**Descripción general de la arquitectura**
BITCOIN	**Aprendiendo Bitcoin desde la línea de comandos**
Contribución básica de BITCOIN CORE	**Contribuir a Bitcoin Core**
	Depuración de Bitcoin Core