Cluster-Based Classification of Blockchain Consensus Algorithms

Fredy Aponte, Luz Gutierrez, Magda Pineda, Ines Meriño, Augusto Salazar , and Pedro Wightman, *Senior Member, IEEE,*

***Abstract*—In recent years, Blockchain has become a disruptive technology to protect the integrity of information, especially in open and collaborative information systems. Its main advantage is the possibility to reach consensus on the new data blocks to be added to the chain, even with anonymous actors. The most common consensus mechanism is Proof of Work, but it has been proven to be very inefficient in terms of energy spent by the members of the blockchain. In the literature there are many other techniques that pretend to become the new popular mechanism. However, the number of this techniques is growing too fast to really be able to differentiate among all the options. In this work, a new characterization of consensus algorithm is proposed, that can be used to find families of mechanism using cluster-based classification. Using the Ward Method and Spearman's Rank Correlation analysis, new clusters of consensus mechanisms were identified. The results describe the behavioral patterns not seen before in the literature. In addition, some open problems of current consensus algorithms are discussed.**

***Index Terms*—Blockchain, Cluster-based classification, Consensus algorithms, Proof of Work, Spearman Rank Correlation, Ward Method.**

I. Introducción

La tecnología Blockchain es una oportunidad para crear diferentes soluciones a los problemas de la sociedad, "... Al igual que Internet reinventó la comunicación, blockchain puede redefinir de manera similar las transacciones, los contratos y la confianza, los cimientos de los negocios, el gobierno y la sociedad". [1]

Olson y Wessel [2] explican el blockchain como, "es un registro de transacciones perpetuamente actualizado que los usuarios guardan de forma independiente en Internet", en otras palabras, pueden decir que es un libro mayor distribuido inmutable. La operación básica de blockchain consiste en la administración segura del libro mayor compartido, donde las transacciones se verifican y almacenan en una red que no tiene una autoridad central. Una blockchain puede ser pública o privada en la que puede configurar los permisos de lectura o escritura. Los algoritmos, los cálculos en conjunto con las matemáticas (como funciones hash criptográficas) permiten que blockchain funcione, no solo permiten la realización de transacciones, sino que también permiten proteger la integridad y el anonimato de blockchain. Blockchain al igual que otras tecnologías, ofrece solución a varios problemas, sin embargo presenta aspectos que son susceptibles de mejorar. Adicionalmente, tiene múltiples beneficios. No obstante, se debe tener presente el problema de los requisitos computacionales para ejecutar los algoritmos de consenso de blockchain por ejemplo, la capacidad computacional, porque algunos de estos algoritmos consumen mucho tiempo y recursos computacionales como es el caso de los algoritmos basados en Prueba de Trabajo , *Proof of Work (PoW)*, de forma diferente los algoritmos basados en pruebas de participación *Proof of Stake (PoS)* no requieren gran poder computacional [1].

Por su parte Du y colaboradores [3] presentan los principios básicos y las características de los algoritmos de consenso: *Proof of Work, Proof of Stake, Delegated Proof of Stake, Practical Byzantine Fault Tolerance y Raft*. Las características que comparan son: *byzantine fault tolerance, crash fault tolerance, verification speed, throughput, y scalability*. Adicionalmente, describen las limitaciones de estos algoritmos. Los autores sugieren cuál algoritmo debe ser usado de acuerdo con el tipo de blockchain, para el caso de Blockchain públicas: PoW, PoS, y DPoS. En Blockchain privadas: PBFT y RAFT y en Blockchain autorizadas: PBFT. Los autores no presentan una propuesta de clasificación, se apoyan en la literatura existente acerca de los tipos de Blockchain.

Por otro lado Bach y colaboradores [4] describen las alternativas para resolver el problema de consenso en los sistemas distribuidos. Abordan el problema de los generales bizantinos, BFT, y dBFT. Los autores presentan las 10 criptomonedas más rentables hasta el año 2018, ocupando el primer puesto Bitcoin. Además Realizan una descripción de los algoritmos *PoW, Ripple, PoS, Stellar, dPOS, y Proof of Importance*. Los criterios de comparación que usan son: *energy saving, tolerated power of adversary, y scalability*. Afirman que los algoritmos PoW y PoS son los más utilizados, sin embargo, mencionan que se pueden utilizar híbridos de PoW y PoS. Adicionalmente, introducen dos nuevos algoritmos que en el año 2018 no eran de dominio público: *Proof of Luck (PoL)*

Este trabajo fue realizado con apoyo de los programas "Convocatoria 779 de 2017 - Doctorado Nacional Convocatoria para la Formación de Capital Humano de Alto Nivel para el Departamento de Boyacá – 2017", "Convocatoria 785 de 2017 - Convocatoria de Doctorados Nacionales 2017" y la Universidad del Norte.

F. Aponte, Universidad Santo Tomás, Tunja - Universidad del Norte, Barranquilla, Atlántico Colombia e-mail: fredy.aponte@usantoto.edu.co , faponte@uninorte.edu.co

L. Gutiérrez, Universidad del Norte, Barranquilla, Atlántico, Colombia email: egluz@uninorte.edu.co

M. Pineda, Universidad del Norte, Barranquilla, Atlántico, Colombia, email: magdap@uninorte.edu.co

I. Meriño, Universidad del Magdalena, Santa Marta, Colombia email: imerino@uninorte.edu.co

A. Salazar, Universidad del Norte, Barranquilla, Atlántico, Colombia email: augustosalazar@uninorte.edu.co

P. Wightman, Universidad del Norte, Barranquilla, Atlántico, Colombia email: pwightman@uninorte.edu.co

Manuscript received April 19, 2005; revised August 26, 2015.

y *Proof of eXercice (PoX)*. Este trabajo está orientado hacia la valoración de los algoritmos más populares de acuerdo con los criterios *energy saving, tolerated power of adversary y scalability*. Los autores no presentan una categorización de los algoritmos.

Nguyen y Kim en [5] describen el concepto, arquitectura y características de Blockchain. Además clasifican los algoritmos de consenso en dos grupos: basados en prueba y por votación, estos últimos los subdividen en *Byzantine fault tolerance-based consensus y Crash fault tolerance-based consensus*. Los algoritmos del primer grupo que presentan son: original y variantes de *Proof of Work, Proof of Stake*, híbrido de PoW y PoS, *Proof of burn, Proof of Space, Proof of Elapsed Time, Proof of Luck y Multichain*. Nguyen y Kim comparan PoW, PoS, y el híbrido de PoS y PoW con base en los criterios: *energy efficiency, modern hardware, forking, double spending attack, block creating speed, y pool mining*. Los algoritmos del segundo grupo que describen son: *Hyperledger with practical Byzantine fault tolerance, Ripple, Stellar y Chain*.

Del mismo modo que Nguyen y Kim en [5], Zheng y colaboradores [6] describen el concepto, arquitectura y características de Blockchain. Presentan tres tipos de Blockchain: públicas, consorcio y privadas. Los criterios de comparación usados para los tipos de Blockchain son: *Consensus determination, Read permission, Immutability, Efficiency, Centralized y Consensus process*. En este estudio abordan los algoritmos de consenso: *Proof of Work, Proof of stake, Practical byzantine fault tolerance, Delegated proof of stake, Ripple y Tendermint*. Comparan los algoritmos de consenso con base en los siguientes criterios: *Node identity management, Energy saving y Tolerated power of adversary*. También enumeran cuales son los retos que enfrenta esta tecnología. El objetivo del trabajo no es presentar una categorización de los algoritmos de consenso sino compararlos de acuerdo con tres criterios.

El trabajo de Sankar y Sindhu [7] presenta los 3 tipos de Blockchain: pública, consorcio y privada. El objetivo de los autores es presentar el protocolo de consenso *Stellar* y compararlo con las plataformas *Corda e Hyperledger Fabric*. Los criterios de comparación que mencionan son *view transactions y latency*. SCP utiliza el concepto de segmentos de quórum que garantiza más libertad a los usuarios para decidir cuáles son los participantes de confianza. Corda mantiene registros de varios contratos comerciales y financieros. El proyecto Hyperledger permite que varias tecnologías blockchain se interconecten y garantiza un entorno seguro de *plug and play* para ellos. El hiperledger no proporciona a los usuarios tanta libertad como el SCP. El enfoque de [7] es presentar cómo funciona el protocolo de consenso *Stellar* y cómo interactúa con *Hyperledger Fabric*. No está orientado a clasificar algoritmos de consenso.

Por su parte Chaudhry y Yousaf [8] presentan una arquitectura genérica y la categorización de los mecanismos de consenso en sistemas distribuidos. Basada en criterios como: *scalability, communication model, category y failure models*. Adicionalmente, expresan que la categorización específica de Blockchain se divide en dos grupos: *proof-based consensus y vote-based consensus*. El trabajo describe una propuesta para evaluar los algoritmos de consenso teniendo en cuenta los parámetros de: Blockchain *type, transaction rate, scalability, adversary tolerance model, experimental setup, latency, throughput, bandwidth, communication model, communication complexity, attacks, energy consumption, mining, consensus category y consensus finality*. Con base en los criterios anteriores evalúan los algoritmos: *ELASTICO, Leader- free Byzantine Consensus, Implicit Consensus, Proof of trust (PoT), DBFT Consensus Algorithm, PoPF, Ripple, Proof of Vote (PoV), y Proof of Work (PoW)*.

Hao y colaboradores [9] proponen un método para evaluar los algoritmos PBFT y PoW en las plataformas *Ethereum e Hyperledger Fabric*. La arquitectura de evaluación está compuesta por 3 módulos integrados en *Yahoo Cloud System Benchmark (YCSB)*. Las dos métricas de evaluación de rendimiento utilizadas son: *Latency y Throughput*. Hao y colaboradores concluyen que PBFT adaptado para *Hyperledger* tiene mejor comportamiento que PoW para *Ethereum* en función de rendimiento y retraso promedios. El enfoque de este trabajo es la evaluación de dos algoritmos de consenso en plataformas privadas no la categorización de los algoritmos.

El objetivo de Arjun y Suprabha en [10] es presentar los resultados de una revisión sistemática de literatura enfocada a 3 frentes: el primero, identificación de soluciones para la industria bancaria. Como modelos teóricos o marcos empíricos con potencial de cambio estratégico, ventajas operativas o funciones del mercado de valores. El segundo enfoque era encontrar documentos que resaltaran el alcance práctico o los desafíos en plataformas, dimensiones legales, técnicas y organizativas y el tercer frente, seleccionar documentos orientados a aplicaciones específicas que utilizaran entornos conceptuales experimentales. Los repositorios que revisaron fueron: *Scopus, Web of Science, ACM, IEEE, AIS*. La ventana de observación de los trabajos revisados fue del año 2008 a año 2019. Entre los hallazgos más relevantes se encuentran estudios de: banca, sistemas de información, innovación, derecho, finanzas, sostenibilidad, emprendimiento e infraestructura digital.

Este artículo busca analizar los algoritmos de consenso de blockchain basados en mecanismos de trabajo. Comienza con una descripción de los algoritmos base de consenso; luego se realiza una categorización teórica basada en los mecanismos de trabajo. Después de eso, una explicación detallada sobre cómo se etiquetó y organizó la información para el análisis posterior. Se realizaron análisis estadísticos como correlaciones, análisis de ordenación y de agrupamiento, para entender no solo cómo los atributos describen cada algoritmo de consenso; sino también para proponer una nueva categorización basada en los resultados obtenidos.

II. Descripción Algoritmos de Consenso

A continuación, se describe de forma general los algoritmos de consenso empleados en Blockchain, como son los algoritmos de prueba de trabajo *Proof of Work* [3]–[6], los algoritmos de prueba de participación *Proof of Stake* [3]–[6], los algoritmos de soluciones híbridas PoW y PoS [3]–[6] y otros tipos de algoritmos [3]–[7].

A. Proof of Work Original

En Blockchain cuando se agrega un nuevo bloque, se requiere un acuerdo entre los nodos, para esto, el algoritmo

Proof of Work requiere que cada uno de los nodos solucione un reto (rompecabezas) al cual se le pueda ajustar la dificultad, de modo que el primer nodo que resuelva el reto, obtendrá el derecho de adicionar un nuevo bloque a la cadena actual. El esfuerzo realizado por el nodo para la solución del reto o puzzle, se denomina PoW y es pago al nodo que acertó, a este nodo se denomina minero y a la acción de solucionar el reto se denomina minería [5]. El funcionamiento de PoW se basa en la búsqueda de un valor (solución al reto) que al aplicarle una codificación hash se obtenga un resultado con un número definido de bits 0's a la izquierda de este. El trabajo promedio que se requiere es exponencial con relación a la cantidad de bits ceros necesarios y se puede validar ejecutando una única operación de *hash*. [11]. En PoW la dificultad del reto se ajusta cada vez que se adicionan 2016 bloques, de modo que en la red Bitcoin el tiempo promedio para adicionar un nuevo bloque en la cadena es de diez minutos [5], [11], [12]. Cuando se crea un nuevo bloque la información del encabezado se combina y es enviada como parámetro de entrada a la función *hash (SHA-256)* [11]. Si la salida de esta función se encuentra por debajo de un umbral T (el cual depende de la dificultad), entonces el valor buscado es aceptado. En caso contrario el nodo debe continuar calculando el valor secreto hasta que la salida de la función *SHA-256* sea aceptada. El valor T se hace menor a medida que aumenta la dificultad del reto [5].

B. Soluciones Basadas en PoS

El algoritmo *Proof of Work* no es equitativo para todos los mineros, debido a que no todos tienen el mismo hardware. Algunos poseen equipos modernos y otros equipos muy básicos en procesamiento, a los primeros se les facilita encontrar solución al reto y a los otros les es muy difícil realizar esta tarea. Los algoritmos basados en pruebas de participación (PoS) buscan tratar con esta desigualdad. El principio básico de los algoritmos PoS es usar la apuesta o la magnitud de participación, para definir que nodo tendrá la oportunidad de minar el siguiente bloque de la cadena. Al emplear participación como prueba se tiene una ventaja: cualquier nodo que tenga mucha participación es más confiable, este nodo no realiza ninguna acción fraudulenta para atacar a la cadena que contiene gran parte de sus ganancias, asimismo el uso de PoS implica que al menos el 51% de todas las apuestas en la red para realizar un ataque de doble gasto el cual permite el uso de las mismas monedas múltiples veces, lo cual es poco probable que suceda. Existen actualmente dos tipos populares de consenso que emplean PoS, los que usan la participación pura para obtener consenso y lo híbridos que combinan PoS y PoW [5].

C. Soluciones Híbridas PoW y PoS

King y Nadal propusieron un nuevo concepto denominado edad de la moneda (*coin age*) de cada minero, la cual se calcula por su apuesta multiplicada por el tiempo que el minero la posee [13]. Para que un nodo consiga el derecho de adicionar un nuevo bloque a la cadena, este crea un bloque especial llamado *coin stake*, el cual contiene muchas transacciones, pero además incluye una especial de ese minero para sí mismo. El monto de dinero gastado en la transacción le proporciona al minero más posibilidades de minar un nuevo bloque, después realiza el reto, tal como en PoW. Entre más dinero se gaste en la transacción, más fácil es resolver el reto. Cuando se resuelve el reto, el nodo minero obtiene 1% de la cantidad de monedas que han gastado en la transacción, sin embargo, la edad de la moneda acumulada por estas monedas se reinicia a cero [5].

Diferente a la propuesta de King y Nadal [14], Vasin no utiliza el *coin age* en su Blackcoin, pues se supone que al hacer uso del *coin age* se puede dar posibilidad al atacante de acumular suficiente valor para engañar a la red [15]. Otro problema, es la posible existencia de algunos mineros que mantengan su apuesta hasta que tengan una gran cantidad de monedas, mientras se mantienen fuera del sistema de verificación, por lo tanto, lo propuesto por Vasin en [15], consiste en utilizar la participación pura en cambio de la edad de la moneda para ofrecer a los mineros la posibilidad de minar un nuevo bloque, esto puede animar a más nodos a estar en línea para obtener las ganancias. Al ser desatacada la existencia de mineros fuera de línea, Ren [16] propone emplear una función de decadencia exponencial con la edad de la moneda, en la cual, cuando más espera el minero por el aumento de la edad de la moneda, menor es la velocidad de aumento. El ataque de doble gasto (*double spending attack*) considera un alto riesgo para la seguridad de Blockchain, ya que cuando los mineros poseen más del 51% de la potencia minera, se puede presentar un ataque de fuerza bruta de gran efectividad en el que se los mineros atacantes pueden generar bloques más rápido que el resto de la red. Para mitigar este problema, Duong et al [17] propusieron un método combinando PoW y PoS. El objetivo de este método es cerciorar que, si un minero posee más del 51% del poder de minería, este todavía no tiene muchas posibilidades de realizar una acción fraudulenta. Para lograr esto, los autores proponen usar primero un PoW para elegir un nodo ganador, el cual es el primero en resolver el reto. A continuación, este nodo además de adicionar un bloque llamado *PoW Block* a la cadena, suministra una base para elegir a otro minero que tenga una apuesta. Si el valor de retorno de la función *hash* que tiene parámetros de entrada del bloque PoW recién agregados y la clave privada del propietario de la apuesta, está por debajo de un umbral, el minero elegido tendrá la posibilidad de agregar el bloque PoS a la cadena.

D. Otros Tipos de Algoritmos

Uno de los principales problemas de PoW es que demanda demasiada energía para encontrar el *nonce*, además que no tiene significado en la vida cotidiana, esto fue presentado por Blocki y Zhou en [18] al igual que King en [19]. Por otro lado, PoW no es justo con los mineros que no cuentan con hardware moderno, puesto que tienen poca oportunidad de minar nuevos bloques. Para dar solución a esta situación, los autores en [18] propusieron el uso de algunos tipos de reto para la educación y actividades sociales, los cuales fueran fáciles de resolver para los computadores pero difíciles de resolver por las personas, así el esfuerzo para resolver el reto para minar un nuevo bloque corresponde a las personas y no en usar hardware. Esto es más

justo para todos pues no todos los mineros pueden invertir en hardware modernos [5]. Diferentes autores han propuesto otros algoritmos de consenso basados en prueba (*proof-based*) que no utilizan la idea de PoW y de PoS, ejemplo de estos son *Proof of Burn* [20] y *Proof of Space* [21]. En *Proof of Burn*, los mineros envían sus monedas a una dirección para ser quemadas, de esta manera estas monedas no pueden ser utilizadas por otros, así el minero que más queme monedas gana el derecho de minar un nuevo bloque. Por otra parte, los mineros de *Proof of Space* deben invertir en disco duro para sus computadores, que en comparación con el hardware requerido en PoW es mucho más económico. El algoritmo de *Proof of Space* genera grandes conjuntos de datos llamados *plots on the hard dish*; entonces cuantos más gráficos tiene un nodo, existe mayor probabilidad de que este pueda minar un nuevo bloque. Teniendo en cuenta la información dada previamente, en la Fig. 1 se presenta una organización básica de los algoritmos de consenso según su mecanismo de trabajo. Dicha organización responde a las categorizaciones que se han dado de los mismos teniendo en cuenta la bibliografía y no considera las variaciones que algunos derivados tienen de los algoritmos base de los cuales descendieron.

III. CATEGORIZACIÓN TEÓRICA BASADA EN LOS MECANISMOS DE TRABAJO

A. Organización de la Información

Las características de los algoritmos de consenso evaluadas, son variables cualitativas propuestas y descritas por varios autores en estudios previos [3]–[7].Teniendo como referencia esta información, se definió una valoración en categorías numéricas, con el fin de poder aplicar mecanismos estadísticos. El mecanismo consistió en etiquetar cada una de las características de los algoritmos de consenso, dando una valoración menor a la condición deseada en función de la eficiencia de cada atributo; e incrementando dicho valor cuando se obtiene la condición menos favorable Tabla (I).

TABLA I
VALORACIÓN DE ATRIBUTOS

Característica	Escala	Valores asignados
Energy efficiency	Yes	0
	No	1
Modern hardware	No need	0
	Low need	1
	Need	2
	High need	3
Forking	Never	0
	Very difficult	1
	Difficult	2
	Probably	3
	Very probably	4
Double spending attack	Never	0
	Difficult	1
	More or less	2
	Easy	3
Block creating speed	Very fast	0
	Fast	1
	Low	2
	Very low	3
Pool mining	Never	0
	Very difficult	1
	Can be prevented	2
	Difficult to prevent	3
	It occurs	4
Agreement making basement	From majority of the node decisions	0
	Following nodes performing enough proof (PoW, PoS, etc.)	1
Nodes can join freely	No	0
	Mostly	1
Number of nodes executing	Mostly unlimited	0
	Limited	1
Decentralization	Mostly high	0
	Low	1
Trust	More trustful	0
	Less trustful	1
Nodes identities are managed	No	0
	Yes	1
Security threat	More serious	0
	Less serious	1
Award	Yes	0
	Mostly no	1

B. Análisis de Correlación entre las Características Evaluadas

Los análisis estadísticos se generaron utilizando el programa Past [22]. Primero se realizó un análisis de correlación de rangos de Spearman el cual es un método no paramétrico, que cuantifica la relación entre dos descriptores; definiendo una correlación perfecta de estos cuando los rangos de todos los objetos son los mismos en ambos elementos [23], [24]. Adicionalmente se aplicó la corrección de Bonferroni [25] para evitar el tipo de error I (encontrar diferencias significativas cuando no existen). Los resultados se muestran en la Fig. 2, donde todas las elipses azules significan una correlación significativa y positiva entre las variables ($p < 0{,}05$), mientras que las rojas indican correlaciones negativas significativas entre las variables.

La mayoría de las variables muestran correlaciones significativas. Específicamente, los parámetros *number of nodes executing, decentralization, trust, nodes identities are managed, security threat*, y *award*, muestran una correlación significativa entre ellas (recuadro verde en 2), correspondiendo a las características que tienen las condiciones de eficiencia ideales (valores de cero en el material suplementario 1), de los algortimos de prueba de trabajo.

Por su parte, los parámetros *energy efficiency, modern hardware, forking, double spending attack, pool mining, agreement making basement*, y *nodes can join freely*, muestran también una correlación significativa entre ellas (recuadro amarillo en

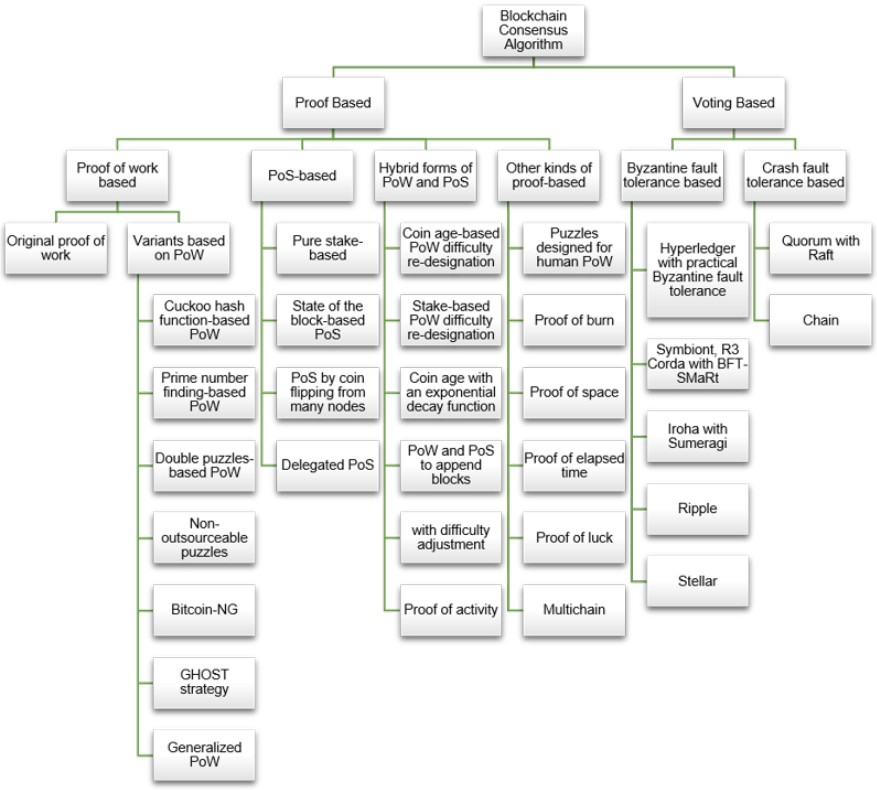

Fig. 1. Organización algoritmos de consenso basada en [5]

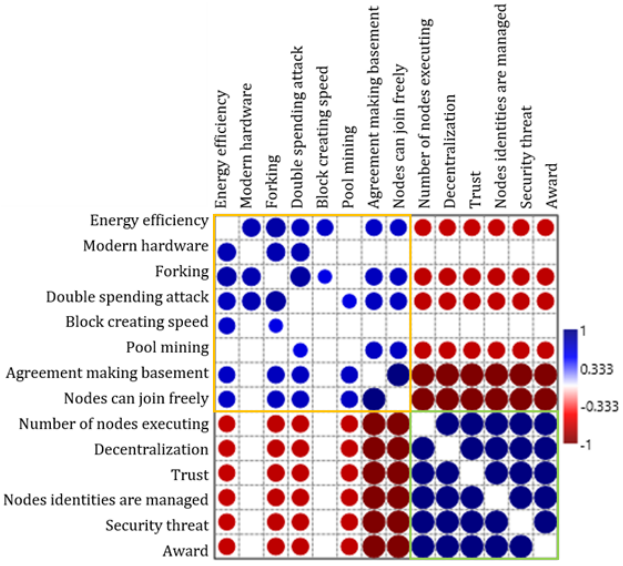

Fig. 2. Resultados del análisis de correlación de rangos de Spearman, las elipses azules que indican correlaciones significativas positivas, y las elipses rojas indican correlaciones significativas negativas (p <0,05). Los espacios en blanco indican que no hay correlaciones significativas (p >0,05).

la Fig. 2), correspondiendo a las características que tienen las condiciones de eficiencia ideales (valores de cero en la tabla del material complementario), de los algortimos basados en votos.

Se evidencian también dos parámetros con pocas correlaciones. El primero es *block creating speed*, que solo presenta una correlación significativa con los parámetros *energy efficiency* y *forking*, dado que a pesar de que la velocidad de creación de bloques no tiene valores ideales en casi ningún algoritmo (excepto en el de *proof of luck*), muestran tendencias similares de modo que cuando un valor es mayor en uno de ellos, en el otro también es mayor. *Modern hardware*, a pesar de también presentar sus condiciones ideales (valores basados en cero) en los algoritmos basados en votos; presenta una variabilidad de su eficiencia en los algoritmos basados en pruebas. En algunos de ellos (*Pure PoS (Nextcoin), State of the block-based PoS, PoS by coin flipping from many nodes, Delegated PoS, Puzzles designed for human PoW, Proof of burn*), incluso tiene también los valores ideales. Por esta razón presenta pocas correlaciones significativas con los otros parámetros.

A manera de resumen, las características con valores ideales de los algoritmos basados en pruebas están relacionadas directamente entre ellas, pero presentan una correlación inversa con las variables de mayor eficiencia de los algoritmos basados en votación (Tabla del material complementario). Además, se puede observar que la característica *block creating speed* es una variable que solo se correlaciona significativamente con las características *energy efficiency* y *forking*. Así mismo, el *modern hardware* solo se correlaciona con *energy efficiency*, el *forking* y *double spending attack*; mientras que *pool mining* no se correlaciona con *energy efficiency*, *modern hardware*, *forking*, y *block creating speed* (Fig. 2).

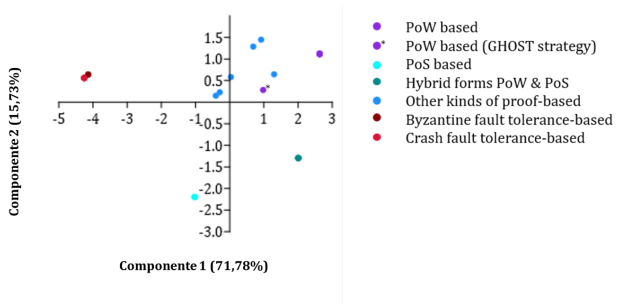

Fig. 3. Análisis de componentes principales de los algoritmos de consenso analizados.

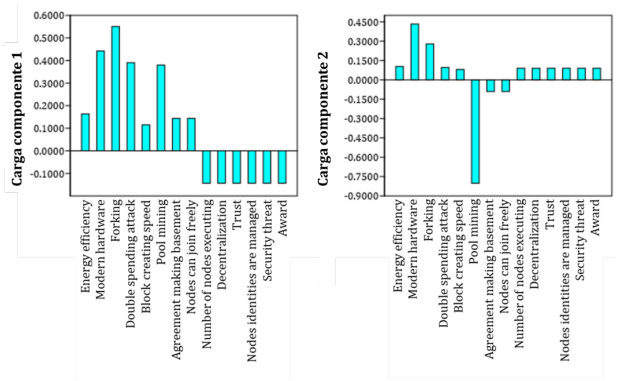

Fig. 4. Carga de atributos para el primero (PC1, izquierda) y segundo (PC2, derecha) componente del PCA.

C. Variabilidad de las Características de los Mecanismos de Trabajo de los Algoritmos de Consenso en Blockchain

Posteriormente se realizó un Análisis de Componentes Principales (PCA) principales el cual es una técnica de ordenación multivariada que busca reducir la dimensionalidad de los datos, a partir de las correlaciones, para encontrar los factores que pueden explicar el conjunto de la información. La ordenación se define a través de factores a los cuales se les denominan "componentes principales". Estos componentes definen los ejes de la rotación original del sistema de coordenadas, y corresponden a las direcciones sucesivas de las máximas varianzas de la dispersión de los puntos; ubicándolos en un nuevo sistema de coordenadas [23], [26].

Dicho análisis se visualiza en gráficas bidimensionales por facilidad de interpretación, en donde el primer componente siempre explicará la mayor variabilidad de los datos, y la varianza explicada disminuirá a medida que el componente incremente (Legendre and Legendre, 1998) [27]. El ACP permitió identificar la variabilidad entre los atributos que describen los mecanismos de trabajo de los algoritmos de consenso en Blockchain. Los primeros dos componentes (Fig. 3) describen el 87,5% de la varianza entre todas las variables (PC1 = 71,78%, PC2 = 15,73%). El primer componente muestra que la mayor variabilidad entre las variables que contiene cada algoritmo separa la mayoría de los algoritmos basados en PoW (puntos morados) que se encuentran en el extremo positivo del primer eje, de los algoritmos basados en votación (puntos rojos), que están en el extremo negativo del eje. Los algoritmos híbridos (puntos verdes) están más cerca de los algoritmos Pow puros (puntos morados) y de otro tipo de algoritmos basados en pruebas (puntos azul oscuro) (Fig. 3).

El algoritmo de estrategia GHOST (punto morado) es el único algoritmo PoW separado de los demás de la misma categoría, ubicado más cerca de otro tipo de algoritmo basados en pruebas de tipo (puntos azul oscuro). Por otro lado, los algoritmos PoS (puntos azules claros) se colocan en el lado negativo del primer eje, se colocan más cerca de los algoritmos basados en votación (puntos rojos) entre todos los algoritmos basados en pruebas (Fig. 3).

El primer componente principal separa perfectamente los algoritmos de consenso basados en trabajo (a la derecha), con respecto a los de votación (a la izquierda). Esta separación está claramente demarcada por la diferencia marcada en los atributos *number of nodes executing, decentralization, trust, nodes identities are managed, security threat, y award*; de los cuales los algoritmos basados en pruebas tienen la mayor eficiencia con respecto a aquellos basados en votación.

Adicionalmente la diferencia entre los algoritmos de los extremos positivos (*PoW based*) y negativos (*voting based algorithms*) del primer eje (Fig. 4), muestra que las diferencias se dan principalmente por las características de *modern hardware, forking, y double spending attack*, en la cual los algoritmos *byzantine fault tolerance based y crash fault tolerance based algorithms* (basados en votación) son los que tienen los mayores valores de eficiencia, mientras que los *PoW based* tienen los peores (material suplementario).

El segundo componente principal que explica el 16% de la varianza, permite separar los algoritmos *PoS based y Hybrid forms PoW & PoS* (extremo negativo), del resto de algoritmos analizados, en función que estos tienen los peores valores de eficiencia con respecto al parámetro de *Pool Mining* (Fig. 4).

IV. Categorización Propuesta

Con base en la información revisada en análisis anteriores, se desarrollo un análisis de agrupamiento (también llamado análisis de cluster), que busca clasificar individuos o variables semejantes entre sí, sin un criterio de clasificación *a priori*. El método consiste en un análisis multidimensional que divide un conjunto de objetos o descriptores, en estudio. La división mencionada se hace en subconjuntos en los que los elementos se agrupan en función de matrices de asociación que dependen de sus características. El método es empleado como una medida de asociación de objetos [23], [26].

Dentro de los métodos de agrupación se trabajó con el método de la mínima varianza, también conocido como método de Ward; el cual busca obtener la menor variabilidad intracluster, con el fin de lograr que cada agrupación sea lo más homogénea posible. Dicha homogeneidad se mide mediante la suma de los cuadrados de las diferencias entre los sujetos dentro del cluster [23], [26], [28]. Con este método, se obtuvo la ordenación de categorización propuesta de los algoritmos de consenso basados en los mecanismos de trabajo analizados en este documento. Los resultados de la categorización se muestran en la Fig. 5, donde se puede observar que la mayoría de

los grupos son similares a los que se proponen actualmente en la literatura (Fig. 1), pero con algunas diferencias importantes.

Según el sistema propuesto, los algoritmos de PoW están correctamente agrupados en una sola categoría, a excepción del algoritmo *GHOST strategy*, que se diferencia de ellos por ser mucho más eficiente por la característica de bifurcación. La categorización propuesta también mantiene la agrupación de las formas híbridas de PoW y PoS; permitiendo identificar que teniendo en cuenta las características analizadas, los algoritmos híbridos están más cerca en sus atributos de los algoritmos PoW puros que de los PoS puros. La razón de esto es que los algoritmos basados en pruebas de participación (PoS) tienen mucha más eficiencia en los atributos: *energy efficiency, modern hardware, forking, Double spending attack, y block creating speed*, que las otras dos categorías (PoW e híbridos) (material suplementario).

Así mismo, la clasificación que se propone conserva la clasificación actual de los algoritmos de *PoS (Pure PoS (Nextcoin), State of the block-based PoS, PoS by coin flipping from many nodes y Delegated PoS)*.

Uno de los principales aportes de la clasificación propuesta se basa en la separación de los algoritmos *Hyperledger with practical Byzantine fault tolerance y Symbiont, R3 Corda with BFT-SMaRt*, en función de la menor eficiencia de la velocidad de creación de bloques, con respecto a la otra agrupación de algoritmos compuesta por: *Iroha with Sumeragi, Ripple, Stellar, Quorum with Raft, y Chain*.

Otro aporte considera la recategorización de los algoritmos clasificados previamente en la categoría de "otros algoritmos basados en pruebas". La primera agrupación considera la semejanza entre los algoritmos *Puzzles designed for human PoW, Proof of burn y Proof of space*, en función del *modern hardware* que es mucho más eficaz que los otros algoritmos. Este atributo de eficiencia también los ubica más cercanamente a los algoritmos PoS. La otra categorización propone que los algoritmos *Proof of elapsed time, Proof of luck y Multichain*, en conjunto con el algoritmo de *GHOST strategy*, formen una agrupación independiente. Esta agrupación es la que debe tomarse con mayor precaución dentro de la clasificación propuesta, dado que es la que mayor distancia considera en el análisis, y sus datos muestran elevada variabilidad.

El trabajo presentado por Nguyen y Kim [5] tiene un alto grado de similitud con este trabajo, debido a que dividen los algoritmos de consenso en algoritmos basados en prueba y por votación. También hay coincidencia en las características de comparación de los algoritmos de consenso. Sin embargo, Nguyen y Kim no presentan la categorización de la forma en que se realiza en este trabajo. Por su parte Chaudhry y Yousaf en su trabajo [8] proponen una categorización de los algoritmos de consenso en sistemas distribuidos y aporta una lista de parámetros relevantes para evaluar los algoritmos de consenso, útiles para el diseño y evaluación de algoritmos.

V. Conclusiones

Este documento analiza los atributos del mecanismo de trabajo de los algoritmos de consenso de blockchain en un intento no solo de comprender, sino también de identificar los patrones que los agrupan o los separan de los demás. Por lo tanto, con base en los datos publicados, proponemos una nueva categorización de algoritmos de consenso basados en sus atributos de mecanismos de trabajo. Los resultados presentaron una separación bien definida de grupos reales (PoW, PoS, formas híbridas y basadas en votación); sin embargo, revela algunos patrones que antes no eran evidentes. Un hallazgo notable es que, incluso las formas híbridas resistentes utilizan atributos de los algoritmos PoW y PoS. El análisis de clusters (Fig. 5), así como el análisis de PCA (Fig. 3), evidencian una cercanía entre los algoritmos híbridos y PoW basados en los atributos *energy efficiency, modern hardware, forking, double spending attack*.

Otro hallazgo importante es la propuesta de reclasificación de otro tipo de algoritmos basados en pruebas, separándolos en dos grupos diferentes. Uno más cercano a los algoritmos PoS, incluido Proof of Space, retos diseñados para humanos PoW y los algoritmos Proof of Burn; mientras que el otro incluye Proof of Elapsed Time, multichain, Proof of Luck y estrategia GHOST; excluyendo este último de los algoritmos de PoW puro. Es necesario mencionar que esta categorización podría optimizarse al incluir más información sobre otros atributos de los mecanismos de trabajo u otro tipo de atributos.

Como recomendación una área en la que se puede explorar es en la definición de requerimientos del uso de cada algoritmo, es decir, de acuerdo con cada característica como consumo energético, hardware moderno y bifurcación descritos en la Tabla (I. Plantear dependiendo de la problemática que se desea resolver cuál de esas características son importantes o no relevantes para cada caso particular y así decidir qué tipo de algoritmo utilizar. Así mismo se requiere que trabajos futuros consideren las condiciones de aplicación de los algoritmos de consenso analizando características por las cuales pueden ser mas o menos eficientes dependiendo del escenario en que trabajen.

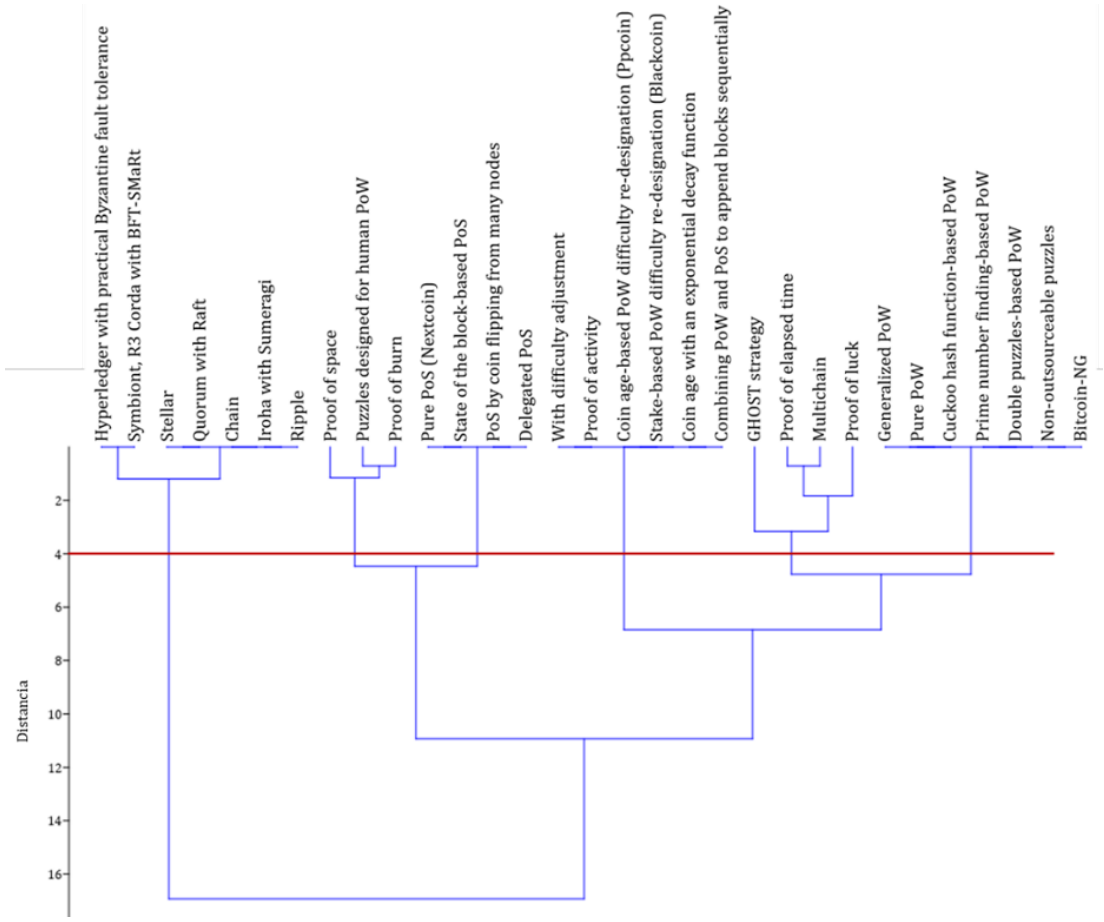

Fig. 5. Análisis de agrupamiento de los algoritmos de consenso de blockchain basados en los atributos de los mecanismos de trabajo.

REFERENCIAS

[1] T. Piscini, E., Guastella, J., Rozman, A. and Nassim, "Innovating in the digital era," tech. rep., Deloitte University Press, 2016.

[2] D. Wessel, "The Hutchins Center Explains: How blockchain could change the financial system (part 1) — Brookings Institution," *Brookings*, p. 1, 2016.

[3] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, "A review on consensus algorithm of blockchain," *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017*, vol. 2017-Janua, pp. 2567–2572, 2017.

[4] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1545–1550, May 2018.

[5] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 101–128, 2018. cited By 93.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564, 2017.

[7] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," *2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017*, 2017.

[8] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," *ICOSST 2018 - 2018 International Conference on Open Source Systems and Technologies, Proceedings*, no. December 2018, pp. 54–63, 2019.

[9] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain," *IEEE Intelligent Vehicles Symposium, Proceedings*, vol. 2018-June, no. Iv, pp. 280–285, 2018.

[10] R. Arjun and K. R. Suprabha, "Innovation and Challenges of Blockchain in Banking: A Scientometric View," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. InPress, no. InPress, p. 1, 2020.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. doi:10.1007/s10838-008-9062-0stem," *Journal for General Philosophy of Science*, vol. 39, no. 1, pp. 53–67, 2008.

[12] Bitcoin Project, "FAQ - Bitcoin." Accedido 15-06-2020.

[13] Bitcoinwiki, "SHA-256," 2016. Accedido 20-06-2020.

[14] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," tech. rep., Peercoin Foundation, 2012.

[15] P. Vasin, "Blackcoin's proof-of-stake protocol v2," *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.

[16] L. Ren, "Proof of stake velocity v2: Building the social currency of the digital age," tech. rep., Reddcoin, 2019.

[17] T. Duong, L. Fan, and H.-S. Zhou, "2-hop blockchain: Combining proof-of-work and proof-of-stake securely," Tech. Rep. 2016/716, Cryptology ePrint Archive, 2016.

[18] J. Blocki and H.-S. Zhou, "Designing proof of human-work puzzles for cryptocurrency and beyond," in *Theory of Cryptography Conference*, pp. 517–546, Springer, 2016.

[19] S. King, "Primecoin: Cryptocurrency with prime number proof-of-work," tech. rep., Primecoin, 2013.

[20] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-burn," Tech. Rep. 2019/1096, IOHK, University of Athens, University of Edinburg, 2019.

[21] S. Park, A. Kwon, G. Fuchsbauer, P. GaÅ¾i, J. Alwen, and K. Pietrzak, "Spacemint: A cryptocurrency based on proofs of space," Tech. Rep. 2015/528, SpaceMint, 2015. https://eprint.iacr.org/2015/528.

[22] R. P. D. Hammer Øyvind, Harper David A.T, "Palaeontologia Electronica," 2001. Accedido 20-10-2019.

[23] P. Legendre, *Numerical Ecology: Numerical Ecology.* Issn Ser, ELSEVIER SCIENCE B.V, 3rd ed.. ed., 2012.

[24] J. Franco, A. Rodríguez, and E. Jiménez, *Estadística Aplicada II: Estadística en Administración para Toma de Decisiones*. Económico Administrativo, Grupo Editorial Patria, 2014.
[25] D. R. Cox and C. A. Donnelly, *Principles of Applied Statistics*. Cambridge University Press, 2011.
[26] A. Catena, M. Alvarez, and H. Trujillo Mendoza, *Análisis multivariado. Un manual para investigadores.* Biblioteca Nueva, 01 2003.
[27] X. G. M. Carmen and S. M. C. Rafael, *Fundamentos de las Técnicas Multivariantes*. AULA ABIERTA, UNED, 2013.
[28] J. Sarabia Alegría, F. Prieto Mendoza, and V. Jordá Gil, *Prácticas de estadística con R*. Economía Y Empresa, Ediciones Pirámide, 2018.

Fredy Andrés Aponte Ingeniero de Sistemas y Computación. Magister en Software Libre. Estudiante Doctorado en Ingeniería de Sistemas y Computación de la Universidad del Norte. Actualmente sus áreas de Investigación son Blockchain y los ambientes virtuales de aprendizaje.

Luz Elena Gutiérrez Ingeniera de Sistemas y Magíster en Ingeniería Área Informática y Ciencias de la Computación de la Universidad Industrial de Santander. Actualmente estudiante de Doctorado en Ingeniería de Sistemas y Computación de la Universidad del Norte. Áreas de investigación: Arquitectura Software, Realidad Aumentada y Desarrollo de Software orientado a la web.

Magda L. Pineda Ingeniera de Sistemas, Magíster en dirección estratégica con énfasis en TI. Actualmente estudiante de Doctorado en Ingeniería de Sistemas y Computación, y profesor catedrático de la Universidad del Norte. Integrante del grupo de investigación Redes de Computadores e Ingeniería de Software - GReCIS. Área de investigación: Blockchain.

Inés Meriño Fuentes Ingeniero de Sistemas y Especialista en Desarrollo de Software de la Universidad del Magdalena. Especialista en Servicios Telemáticos e Interconexión de Redes de la Universidad Manuela Beltrán. Magister en Ingeniería de Sistemas y Computación de la Universidad Simón Bolívar. Estudiante Doctorado de Ingeniería de Sistemas y Computación de la Universidad del Norte. Docente de Planta e Investigadora de la Universidad del Magdalena.

Augusto Salazar Ingeniero de Sistemas de la Universidad del Norte. Maestría en Ciencias de la Computación de la National Chiao Tung University (TW). Profesor asistente en el Departamento de Ingeniería de Sistemas en La Universidad del Norte. Sus temas de investigación abarcan IoT, soluciones de múltiples realidades y analíticas de aprendizaje.

Pedro M. Wightman Ingeniero de Sistemas de la Universidad del Norte. Doctor en Ciencias de la Computación de la Universidad del Sur de la Florida, en Tampa. Actualmente profesor asociado del Departamento de Ingeniería de Sistemas de la Universidad del Norte. Director del Grupo de Investigación en Redes de Computadores e Ingeniería de Software - GReCIS. Sus áreas de investigación incluyen: privacidad de datos, aplicaciones industriales de múltiples realidades, blockchain e IoT.