



MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER BLOTICK – EL TICKET INTELIGENTE

Autor: Alejandro Aparicio Blasco
Director: Fernando Monzón Delgado

Madrid
Enero de 2019

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESIS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. Alejandro Aparicio Blasco

DECLARA ser el titular de los derechos de propiedad intelectual de la obra: *Blotick – El ticket inteligente*, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

- a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar “marcas de agua” o cualquier otro sistema de seguridad o de protección.
- b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
- c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
- d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
- e) Asignar por defecto a estos trabajos una licencia Creative Commons.
- f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente*).

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

- a) Que la Universidad identifique claramente su nombre como autor de la misma
- b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
- c) Solicitar la retirada de la obra del repositorio por causa justificada.
- d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

- a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
- b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
- c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.

- d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusiva del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 18 de Enero de 2019

ACEPTA

Fdo.....



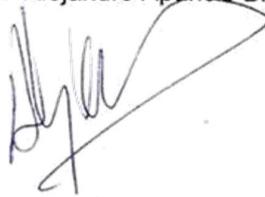
Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título
Blotick – El ticket inteligente

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el
curso académico 2018/2019 es de mi autoría, original e inédito y
no ha sido presentado con anterioridad a otros efectos. El Proyecto no es
plagio de otro, ni total ni parcialmente y la información que ha sido tomada
de otros documentos está debidamente referenciada.

Fdo.: Alejandro Aparicio Blasco

Fecha: 24/01/2019



Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Fernando Monzón Delgado

Fecha: 24/01/2019





MÁSTER UNIVERSITARIO EN INGENIERÍA INDUSTRIAL

TRABAJO FIN DE MÁSTER BLOTICK – EL TICKET INTELIGENTE

Autor: Alejandro Aparicio Blasco
Director: Fernando Monzón Delgado

Madrid
Enero de 2019

RESUMEN

Blotick es una plataforma digital de gestión de tickets de papel basada en blockchain. Descrita por primera vez en 1991 por Stuart Haber y W. Scott Cornetta¹ y popularizada por Bitcoin, una blockchain o cadena de bloques es un libro de contabilidad descentralizado que permite que los datos contenidos en él se vinculen criptográficamente y se aseguren a través de una red. Un libro de contabilidad es un registro de las transacciones que tienen lugar en un banco o una empresa. Registra las interacciones entre cuentas y sus saldos para que los contables puedan realizar un seguimiento y hacer consultas de manera rápida y ordenada.

Estas estructuras de datos se denominan bloques, y contienen transacciones realizadas en la blockchain. Pueden considerarse como las páginas de un libro de contabilidad. Cuando una página está llena de transacciones, se incorpora a la cadena de bloques. Cada bloque debe contener una cadena de datos relacionada con el bloque anterior de la cadena, llamadas *punteros hash* en la jerga de blockchain. Un bloque de datos se revisa cuando está lleno, lo que proporciona un puntero hash que se escribirá en el siguiente bloque.

Una función de hashing toma una serie de datos como entrada y genera como salida una cadena de longitud fija que está unida inequívocamente a los datos que se le proporcionan como entrada. Sirve para validar que la estructura de datos no ha cambiado desde el último proceso de hashing. Cualquier modificación de los datos originales resulta por diseño de la propia función en una alteración del hash, indicando que los datos están dañados o manipulados y, por lo tanto, no son de confianza. Sólo la misma cadena de datos puede obtener el mismo valor de hash para una función de hashing dada. Un puntero de hash al bloque anterior de la cadena de datos garantiza que ese bloque no se modificará de ninguna manera sin que los punteros hash cambien a partir de ese punto, certificando la validez (o falta de ella) de los datos que componen la cadena de bloques.

Pero una blockchain no es un libro de contabilidad cualquiera. Nadie se encarga de mantenerlo o certificar su validez. Funciona bajo el principio de descentralización, proporcionando un sistema *confiable*² sobre el que nadie es reina en particular, si no que lo hace una gran cantidad de servidores que no se conocen entre sí, ni están en la misma localización física, ni tienen el mismo propietario.

Asimismo, las blockchains viven en redes *Peer-to-Peer*, en las que los sistemas que forman la infraestructura se denominan nodos. Cada nodo conserva una copia del libro de contabilidad, anotando cada transacción que tiene lugar en la red en un bloque de datos, verificando las claves criptográficas del remitente y el destinatario y el hash del bloque de datos. Cuando un bloque está lleno, los nodos deben llegar a un consenso sobre las transacciones que lo definen, y una vez que se alcanza, el bloque de datos se incorpora a la cadena de bloques para siempre. En este sentido, una infraestructura blockchain es similar a la del protocolo BitTorrent, en la que los ordenadores no están directamente

¹ Stuart Haber, W. Scott Cornetta. *How to time-stamp a digital document*. Journal of Cryptology, January 1991. <https://link.springer.com/article/10.1007/BF00196791>

² En un sistema confiable, no es necesaria la confianza entre los participantes que lo componen

conectados pero usan el mismo protocolo, y pueden compartir archivos entre ellas como resultado.

Por lo tanto, una blockchain es segura por diseño. Cualquier atacante motivado y con recursos que quisiera tomar el control de la cadena y corromper deliberadamente sus datos internos, tendría que piratear no sólo uno de los servidores que alojan uno de los nodos de la cadena de bloques, sino el 51% de ellos³, lo que hace que el ataque no sea factible para redes formadas por un número suficientemente grande de nodos.

La primera aplicación general de una blockchain apareció en 2009, cuando la criptomoneda Bitcoin hizo uso de la tecnología de cadena de bloques para verificar las transacciones en una red descentralizada, permitiendo a los usuarios eliminar la necesidad de que los bancos u otras entidades supervisaran el mantenimiento, la integridad y la protección del libro de contabilidad. Las cadenas de bloques han sido un tema de estudio frecuente desde entonces, y muchas aplicaciones diferentes en diversas industrias emergen cada día a un ritmo creciente.

Las transacciones de datos que tienen lugar en la cadena de bloques pública de Bitcoin y llenan los bloques son bastante simples: sólo identifican el remitente, el destinatario y la cantidad a enviar. Otro tipo de transacción registra la cantidad de Bitcoin que se creará como recompensa por crear un bloque (denominada operación de minado), al igual que se imprime el dinero. Y eso es todo lo que se permite hacer.

En 2015, Vitalik Buterin, inspirado por la tecnología y el futuro potencial que presentaba, publicó el primer paper del protocolo Ethereum⁴, una nueva cadena de bloques pública alimentada por una nueva criptomoneda, el Ether. Pero la blockchain de Ethereum no se parece en nada al protocolo de Bitcoin. Las transacciones de datos que tienen lugar en la red Ethereum no sólo registran los intercambios de moneda, si no que la transacción en sí misma puede ser código de ordenador. Estos scripts se conocen como contratos inteligentes o smart contracts, y en ellos reside el verdadero poder de la tecnología blockchain, que aún está esperando a ser explorado y perfeccionado.

Se garantiza que los contratos inteligentes se ejecutan una vez que están escritos en un bloque dentro de la cadena y no pueden manipularse, son transparentes para cualquier persona con acceso a la cadena de bloques y, por este mismo motivo, convierten a la red Ethereum en la primera computadora descentralizada distribuida globalmente. Una vez que un contrato está firmado criptográficamente por el titular de la cuenta, se ejecuta en cada nodo de la red, los cuales actualizan su estado consecuentemente al mismo tiempo y no se puede detener, lo cual no se parece en nada a una base de datos, una tecnología que es confundida con frecuencia con la tecnología blockchain.

Los smart contracts también pueden interactuar entre ellos, llamarse y consultarse entre sí, y ejecutarse en un entorno sin jueces: los nodos de la red se aseguran de que el código se ejecute de la forma en que los programadores lo crearon cuando lo firmaron originalmente.

³ Siendo estrictos, un atacante necesitaría hacerse con el control del 51% del poder computacional de la red independientemente del número de nodos.

⁴ The Ethereum White paper - <https://github.com/ethereum/wiki/wiki/White-Paper>

Tanto Bitcoin como Ethereum son ejemplos perfectos de blockchains públicas, a las que todos pueden unirse y realizar transacciones en ellas. Sin embargo, en un entorno empresarial, una cadena de bloques permissionada es más adecuada, pues el gobierno de la red pertenece a los administradores de la aplicación. Quorum⁵ y Hyperledger Fabric⁶ son buenos ejemplos de redes blockchain permissionadas, y Blotick utilizará esta última para su MPV.

Haciendo uso de esta novedosa tecnología, este Trabajo de Fin de Máster propondrá Blotick, una infraestructura segura, transparente y basada en blockchain para la recepción y gestión de recibos y garantías de bienes de consumo. Esta solución facilitaría enormemente el proceso de certificación de propiedad de cualquier producto.

Esta solución Fintech, similar a una cartera de tickets, eliminaría la molestia de administrar y hacer un seguimiento de los recibos y garantías en caso de devoluciones o consultas relacionadas con el servicio de atención al cliente. Podría haber muchas aplicaciones derivadas del producto: los propietarios de tiendas de segunda mano, así como bazares online, podrían imponer el uso de la plataforma para garantizar que el origen de los productos que se venderán en sus plataformas es legítimo, no robado ni falsificado.

El proceso comenzaría en los puntos de venta, donde el vendedor emitiría un código QR al cliente después de la compra, quien lo escaneará a través de Blotick en su teléfono. Este código QR contiene toda la información relacionada con la venta, y la plataforma ejecutaría un contrato inteligente como consecuencia. El propietario firma digitalmente el contrato en su teléfono y comienza el período de garantía. La aplicación también ofrece recursos fuera de la cadena: etiquetas de productos, fotos o guías de usuario para facilitar su uso y clasificación.

Blotick convertiría el ticket en un activo digital, el centro de la venta. Cada operación y transacción se realizaría modificando las propiedades de este activo digital, proporcionando transparencia y trazabilidad de extremo a extremo desde la venta del producto hasta el final de su ciclo de vida.

⁵ <https://www.jpmorgan.com/global/Quorum>

⁶ <https://www.hyperledger.org/projects/fabric>

ABSTRACT

Blotick is a digital platform dedicated to the management of paper tickets based on blockchain technology. First described in 1991 by Stuart Haber and W. Scott Cornetta⁷ and made popular by Bitcoin, a blockchain is a decentralised ledger that allows data structures to be cryptographically linked and secured over a network. A ledger, a term mainly used in accounting, is a record of the transactions that take place in a bank or a company. It registers interactions in between accounts and their balances for the bookkeepers to track and query.

These data structures are called blocks, and they contain transactions made inside a blockchain. They can be thought of as the pages of a ledger, and when a page is full, it is incorporated into the blockchain. Each block must contain a data string that is related to the previous block in the chain, the so-called *hash pointers* in the blockchain jargon. A data block is hashed when full, providing a hash pointer that will be written into the next block.

A hashing function takes a string of data as an input and outputs a fixed-length string that is unequivocally linked to the one provided. It serves to validate that the data structure has not been changed since the last hashing process. Any modifications of the original data resulting by design in an alteration of the hash, indicating that the data is corrupted and thus, untrusted. Only the very same data string can obtain the same hash value from a given hashing function. A hash pointer to the previous block in the data chain ensures that that block will not be changed in any way without the hash pointers changing from that point on, certifying the validity (or lack thereof) of the data from which the blockchain is comprised of.

But a blockchain is not a ledger per se. Nobody is in charge of maintaining it or certifying its validity. It works under the principle of decentralisation, providing a *trustless*⁸ system in which nobody in particular reigns over but a myriad of computers that do not know each other does.

Admittedly, blockchains live in *Peer-to-Peer* networks, in which the systems forming the infrastructure are referred to as nodes. Each one of them maintain a copy of the ledger, annotating every data transaction that takes place in the network into a data block, verifying the cryptographic keys of the sender and recipient and hashing the data block. When a block is full, the nodes must then reach consensus on the pending transactions, and once it is reached, the data block is incorporated into the blockchain forever. In this regard, a blockchain infrastructure is similar to that of the BitTorrent protocol, where computers that are not directly connected but use the same protocol can share files between them as a result.

Therefore, blockchains are secure by design. Any motivated attacker that wanted to take over the chain and purposely corrupt the data within would need to hack not only

⁷ Stuart Haber, W. Scott Cornetta. *How to time-stamp a digital document*. Journal of Cryptology, January 1991. <https://link.springer.com/article/10.1007/BF00196791>

⁸ In a trustless environment, the necessity for trust between members does not exist.

a server hosting a node of the blockchain, but 51% of them⁹, making the attack unfeasible for networks formed by a moderately large number of nodes.

The first mainstream application of a public blockchain appeared in 2009, when the Bitcoin cryptocurrency made use of blockchain technology to verify transactions in a decentralised network, empowering the users by removing the need for banks or other entities to oversee the maintenance, integrity and protection of the ledger. Blockchains have been a subject of study ever since, and many different applications in diverse industries emerge at a growing rate.

The data transactions that take place in the Bitcoin public blockchain and fill in the blocks are rather simple: they only track sender, recipient and the amount to be sent. Another type of transaction registers the amount of Bitcoin to be created, just like money is printed. And that is all there is to it.

In 2015, Vitalik Buterin, inspired by the technology and the future potential it posed, published the first white paper of the Ethereum protocol¹⁰, a new public blockchain fuelled by a new cryptocurrency, the Ether. But the Ethereum blockchain is nothing quite like the Bitcoin protocol. The data transactions that take place in the Ethereum network not only track monetary exchanges, but the transaction itself can be computer code. These scripts are referred to as *Smart Contracts*, and inside them resides the true power of the blockchain technology, still waiting to be explored and perfected.

Smart Contracts are guaranteed to run once they are written in a block inside the chain, cannot be manipulated or tampered with, are transparent to anyone with access to the blockchain and effectively makes the Ethereum network the first globally distributed decentralised computer. Once a contract is cryptographically signed by the account holder it runs in every node of the network and updates its status accordingly at the same time and cannot be stopped, which is nothing like a database.

Smart Contracts can also interact between them, calling and consulting each other, and run on a judgeless environment: the network nodes make sure the code is run the way its programmers intended to when they signed it in the first place.

Both Bitcoin and Ethereum are perfect examples of public blockchains, which everybody can join and perform transactions in them. In an enterprise environment however, a *permissioned* blockchain is more suitable, for the governance of the network remains with the administrators of the application. Quorum¹¹ and Hyperledger Fabric¹² are good examples of permissioned blockchain networks, and this application will use the latter for its MVP.

Making use of this novel technology, this thesis will propose Blotick, a paperless, blockchain-based, transparent and secure infrastructure for consumer goods'

⁹ To be more precise, an attacker would need to gain control of 51% of the computational power of the network regardless of the number of nodes, which makes the prospect equally unlikely, for the number of online nodes (and as a consequence, the computational power) of a public blockchain is sufficiently high at any given time.

¹⁰ The Ethereum White paper - <https://github.com/ethereum/wiki/wiki/White-Paper>

¹¹ <https://www.jpmorgan.com/global/Quorum>

¹² <https://www.hyperledger.org/projects/fabric>

receipts and warranties acquisition and management. This solution would enormously facilitate the process of certificating ownership of any given product.

This wallet-like fintech solution would eliminate the hassle of managing and keeping track of receipts and warranties in case of returns or customer service-related inquiries. There could be many derived applications from the product: second-hand store owners as well as online bazaars could enforce the use of the platform to ensure that the origin of the to-be-sold goods is legitimate, e.g. not stolen or counterfeited.

The process would begin in points of sale, where the retailer would issue a QR code to the customer after the purchase, who scans it via the smartphone wallet app. This QR code contains all the information related to the sale, and the platform would then create a Smart Contract accordingly. Once created, the owner digitally signs the contract and the warranty period kicks in. Off-chain resources would also be available from the app: product tags, pictures or user guides for ease of use and management.

Blotick would make the ticket a digital asset, the centre of the sale. Every operation and transaction would be performed modifying the properties of this digital asset, providing transparency and end-to-end traceability since the sale of the product until the end of its lifecycle.

ÍNDICE

1.	INTRODUCCIÓN	3
2.	DESCRIPCIÓN DEL PROBLEMA.....	5
3.	METODOLOGÍA	7
4.	BUSINESS MODEL CANVAS	9
4.1.	ACTIVIDADES CLAVE	9
4.2.	RECURSOS CLAVE	10
4.3.	PROPUESTA DE VALOR	11
4.4.	RELACIONES CON CLIENTES	11
4.5.	CANALES.....	12
4.6.	SOCIOS CLAVE.....	12
4.7.	SEGMENTOS DE CLIENTES	12
4.8.	ESTRUCTURA DE COSTES.....	13
4.9.	FLUJO DE INGRESOS	13
4.10.	ESQUEMA VISUAL DEL CANVAS	14
5.	PLAN DE NEGOCIO.....	15
5.1.	DESCRIPCIÓN DEL SERVICIO.....	15
5.2.	VENTAJAS COMPARATIVAS	17
5.3.	ESTUDIO DE MERCADO.....	18
5.3.1.	Descripción del sector	18
5.3.2.	Análisis de la clientela potencial	20
5.3.3.	Análisis de la competencia. Estado del arte	20
5.3.4.	Análisis DAFO	22
5.4.	ESTRATEGIA DE NEGOCIO Y PLAN DE MARKETING.....	23
5.4.1.	Producto	24
5.4.2.	Precio.....	25
5.4.3.	Distribución.....	26
5.4.4.	Promoción	27
5.5.	PLAN DE OPERACIONES.....	28
5.5.1.	Procedimientos y necesidades técnicas	28
5.5.2.	Compras	29
5.6.	ESTRATEGIA DE RECURSOS HUMANOS	29
5.6.1.	Organigrama.....	29

5.6.2.	Necesidades de personal.....	31
5.6.3.	Contratos y retribuciones	31
5.7.	ESTUDIO ECONÓMICO-FINANCIERO	32
5.8.	ESTRUCTURA JURÍDICA.....	41
5.8.1.	Protección de la idea	41
5.8.2.	Organización legal del proyecto.....	41
5.8.3.	Posible ICO	42
5.8.4.	Uso de la plataforma	42
5.8.5.	Empleados y proveedores.....	43
6.	MÍNIMO PRODUCTO VIABLE.....	45
6.1.	ELECCIÓN DE LA TECNOLOGÍA BLOCKCHAIN.....	45
6.2.	CONCEPTOS CLAVE DE HYPERLEDGER FABRIC.....	47
6.2.1.	Elementos básicos	47
6.2.2.	Cantidad y distribución de nodos.....	48
6.2.3.	Número de canales	48
6.3.	ARQUITECTURA PROPUESTA	49
6.4.	INFRAESTRUCTURA CLOUD NECESARIA.....	51
6.5.	BLOTICK API	52
6.6.	APLICACIÓN WEB	52
7.	BIBLIOGRAFÍA	53
	ANEXO A. ENCUESTA CIUDADANA	55
	ANEXO B. EQUIPO PROMOTOR.....	59
	ANEXO C. PARTICIPACIÓN EN CONCURSOS DE EMPRENDIMIENTO	63

1. INTRODUCCIÓN

Blotick es una infraestructura segura y transparente que pretende acabar con los tickets y garantías de papel, facilitando su gestión y adquisición informatizada en puntos de venta físicos gracias a la tecnología blockchain o cadena de bloques. Esta solución facilitará enormemente el proceso de certificar la pertenencia de un producto frente a terceros. Blotick elimina el dolor de cabeza generado debido a la pérdida, deterioro y almacenamiento de tickets de papel. La sustitución del ticket de papel por el ticket inteligente es la idea en torno a la que gira el modelo de negocio y permite al consumidor ejercitar sus derechos en casos de devolución u otros servicios postventa.

Existen muchas aplicaciones que se desprenden del producto: tiendas de segunda mano podrían utilizar la plataforma para certificar que la procedencia de los productos que van a ser vendidos en su comercio es legal o que se trata de productos auténticos. Productos de financiación y seguros al instante, pagos con dinero tokenizado o programas de fidelización a medida son algunos de los servicios que se podrían incorporar a la aplicación gracias a su estructura modular.

Blotick aporta valor al consumidor final, pues sin más esfuerzo que el de desbloquear su smartphone y enseñar su ID en forma de código QR, el usuario podrá adquirir su prueba de compra y ejercitar sus derechos con ella, incorporando al framework Blockchain-as-a-Service una prueba inmutable y eterna de adquisición y pertenencia.

Los puntos de venta verán el servicio como una oportunidad de diferenciación en un sector cada vez más competitivo. Se pretende proporcionar al retail físico una herramienta que les permita crear un nuevo canal de comunicación con sus clientes e incorporar nuevos productos y servicios que les ayuden a traer características propias del comercio electrónico al punto de venta físico.

2. DESCRIPCIÓN DEL PROBLEMA

Como se enunciará a lo largo de esta memoria, el problema identificado afecta tanto a los clientes finales como a los puntos de venta.

Por una parte, es patente la dificultad e inconveniencia de guardar tickets de papel por cada compra que se efectúa, perdiendo de vista fácilmente aquellos tickets que son importantes para ejercitar posteriormente nuestro derecho a devolución, cambio o reparación en periodo de garantía. Los usuarios finales deben hacer frente a una gran cantidad de pruebas de compra de diferentes formatos que se deterioran con el tiempo, son fáciles de traspapelar y contienen poca información acerca del producto comprado.

De igual manera, los puntos de venta experimentan también dificultades a la hora de fidelizar clientes, perdiendo la comunicación entre los clientes y ellos mismos en el momento de la compra. Es habitual en la venta física que un cliente compre un producto y el punto de venta no ofrezca ningún tipo de servicio postventa o modelo de fidelización ajustado al historial de compras del cliente, algo muy común en el modelo de negocio y marketing del comercio online.

Los clientes poco fieles a un comercio en concreto son reacios a participar en engorrosos programas de fidelización como tarjetas de puntos, tarjetas de crédito específicas o bonos de descuento cuando se produce un determinado número de compras de cierto producto. Principalmente esto es debido a la gran cantidad de modelos de fidelización existentes y la poca voluntad del cliente final a participar en un gran número de ellos, optando únicamente por aquellas formas de fidelización que se les ofrece desde sus puntos de venta habituales, cuando el cliente ya está fidelizado.

Blotick pretende resolver este problema dual a través de la estandarización del ticket, creando un activo digital en blockchain que simboliza la prueba de pertenencia del producto y creando una plataforma que construya un nuevo canal de comunicación entre puntos de venta y clientes a través de economía basada en tokens.

Los usuarios podrán fácilmente demostrar que son los auténticos propietarios del bien sin necesidad de haber guardado durante meses un ticket de papel que probablemente ya se haya borrado por el propio paso del tiempo o se haya extraviado. Este activo digital es susceptible también de ser transferido, logrando una trazabilidad del producto en el caso de que se desee intercambiar o vender a una tienda de segunda mano para su posterior reventa. De esta forma, las tiendas de segunda mano pueden certificar que la procedencia del producto es legítima, lo cual es indudablemente beneficioso para sus potenciales clientes, que se aseguran de que el producto no es robado o falsificado, pues pueden ver la fecha y lugar exactos de la compra, ya que el ticket digital en blockchain es inmutable e imperecedero.

A lo largo de los siguientes apartados se describirá en más profundidad el modelo de negocio de Blotick, cuáles serían las claves necesarias para su éxito, los recursos necesarios para su desarrollo, la proposición de valor que ofrece tanto a puntos de venta

como clientes, la tecnología blockchain utilizada en un Mínimo Producto Viable y la estrategia de marketing a emplear para lograr una gran penetración en el competitivo mercado de las aplicaciones móviles; así como un plan de operaciones y un estudio económico y financiero que asegure la sostenibilidad de la empresa en el tiempo.

3. METODOLOGÍA

La metodología principal empleada a lo largo del desarrollo de este proyecto está basada en torno al lienzo del modelo de negocio o Business Model Canvas.

El Business Model Canvas es una herramienta que facilita el desarrollo de nuevos modelos de negocio mediante un gráfico intuitivo dividido en diferentes categorías que describen la propuesta de valor de la empresa, la infraestructura necesaria, ayuda a identificar sus futuros clientes y potenciales socios y anima a cuadrar las finanzas del modelo de negocio desde el principio, para así tener un marco de desarrollo que permita estudiar la viabilidad económica de la empresa en base a su proposición de valor.

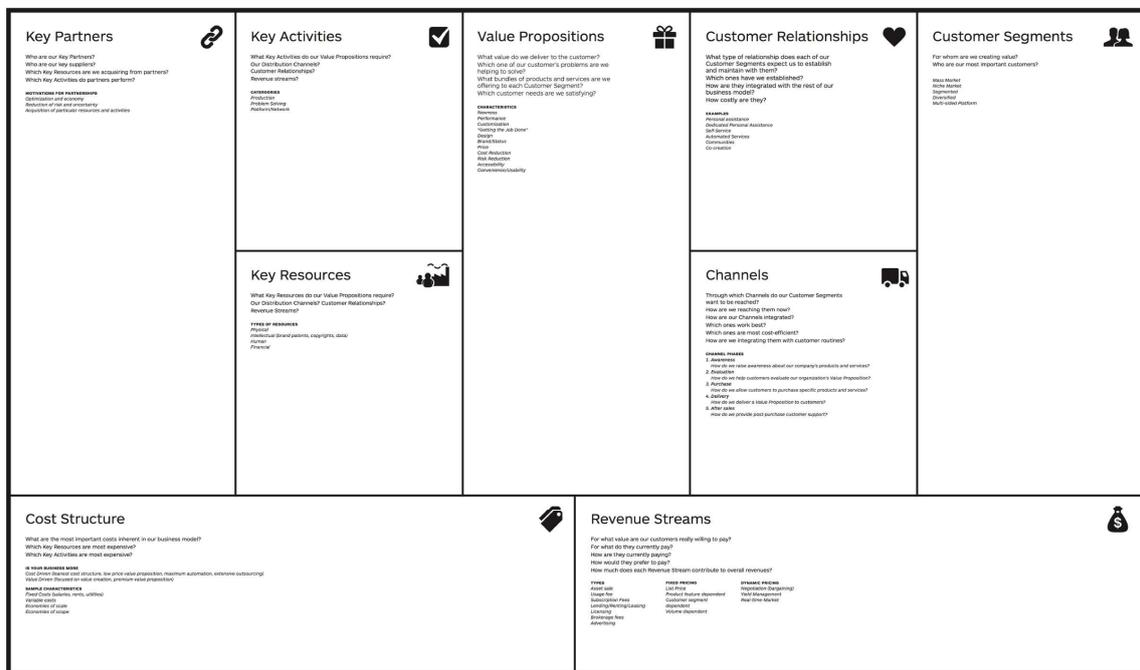


Figura 1 – Business Model Canvas

Inicialmente el Business Model Canvas fue propuesto por Alexander Osterwalder¹, un emprendedor suizo conocido por su trabajo en diseño de modelos de negocio. El lienzo de modelo de negocio consiste en 9 elementos clave divididos en distintas categorías:

- Infraestructura:
 - Actividades clave: cuáles son las actividades más importantes de cara a ejecutar con garantías la propuesta de valor de la empresa.
 - Recursos clave: qué recursos son necesarios para la creación de valor.

¹ <http://alexosterwalder.com/>

- Socios clave: qué relaciones serán fundamentales para el desarrollo del negocio y de su actividad principal.
- Oferta
 - Proposición de valor: qué productos y servicios distinguen a tu modelo de negocio, aportando valor final al cliente y satisfaciendo sus necesidades.
- Clientes
 - Segmentos de clientes: qué clientes se identifican como potenciales clientes del negocio
 - Canales: a través de qué medios se va a comunicar y entregar a los clientes la proposición de valor
 - Relación con clientes: de qué manera se va a interactuar con los clientes y establecer la relación con ellos
- Finanzas
 - Estructura de costes: cuál es el modelo de monetización de la empresa y en qué tipo de costes se incurren
 - Fuentes de ingresos: cómo se producen los ingresos en la empresa, de qué se obtiene beneficio

En el próximo apartado se describirá el Business Model Canvas de Blotick, detallando cada una de sus partes.

Como complemento al Business Model Canvas, este proyecto se propuso para la V Edición del concurso Comillas Emprende, por lo que la metodología y las ayudas propuestas por la organización del concurso definitivamente han influido en el desarrollo de este Trabajo de Fin de Máster.

4. BUSINESS MODEL CANVAS

Tal y como se ha descrito en el apartado anterior, la metodología fundamental para el desarrollo del modelo de negocio de Blotick será el Business Model Canvas. En él se definirá qué problemas se ayudará al cliente a resolver, cómo se resolverán y qué beneficios reportará a la compañía la resolución de dichos problemas.

En los siguientes puntos se describirán con detalle cada uno de los elementos del Canvas en arreglo a sus distintas categorías.

4.1. ACTIVIDADES CLAVE

- Estudio de la tecnología blockchain: puesto que todo el modelo de negocio gira en torno a la estandarización del ticket, y esto lo proporciona blockchain, será fundamental estudiar esta incipiente tecnología a fondo para comprender todo su potencial de cara a su aplicación en Blotick. Existen diferentes tipos de redes blockchain que habrá que estudiar por separado para ofrecer un estudio comparativo que permita decidir la mejor opción. Puesto que la tecnología avanza rápidamente, será preciso estar al tanto de los numerosos cambios que se avecinan tanto tecnológicos como a nivel regulatorio, jurídico y administrativo.
- Desarrollo del MVP: el mínimo producto viable será clave a la hora de medir la viabilidad del producto y su evolución a lo largo de distintos estados futuros de madurez. Será fundamental encontrar un punto de venta dispuesto a realizar una rápida implantación que permita iterar el producto y aplicar mejoras con suficiente frecuencia.
- Diseño de los smart contracts: es el núcleo de la red blockchain que permitirá el registro, modificación de atributos e intercambio del ticket virtual como activo digital. Los contratos inteligentes contienen la lógica de negocio y deberán cumplir la regulación específica referida a las garantías en España que se detallará en el punto 5.3.1.
- Networking: será imprescindible contactar a distintos puntos de venta y a sus respectivos responsables del área de operaciones/IT para explicar el potencial de Blotick y su capacidad de adopción.
- Integración con los sistemas actuales de los puntos de venta: ésta es quizá una de las actividades más importantes. En las primeras exploraciones se ha encontrado una gran resistencia al cambio en los puntos de venta físicos en este aspecto. Los sistemas actuales son herramientas informáticas -en muchos casos muy anticuadas- que los puntos de venta son reacios a cambiar o modificar. Será necesario, por tanto, que Blotick sea fácil y rápido de implementar, y requiera de los mínimos cambios posibles de cara al punto de venta.

- Desarrollo y diseño de la aplicación: debido a la gran relevancia que toma la aplicación en sí en el éxito de Blotick, su desarrollo es una actividad fundamental. El usuario medio de smartphones es muy estricto en cuanto al número de aplicaciones que almacena en su móvil, y el tiempo que permanecen instaladas en su dispositivo hasta ser borradas es muy bajo para la inmensa mayoría de aplicaciones que se descarga. Es por ello que se debe primar la calidad y la experiencia de usuario para lograr que la aplicación sea atractiva para el cliente y se convierta en una herramienta fundamental a la hora de efectuar sus compras.
- Integración de múltiples soluciones: Blotick tiene el potencial de agrupar bajo su plataforma servicios adicionales como seguros, financiación o servicios de atención al cliente personalizados. Estas soluciones aportan valor más allá de la idea fundamental del negocio y se estudiará su implantación en futuras versiones de la aplicación. Dichos servicios pueden marcar la diferencia a la hora de captar nuevos usuarios y retener a los más fieles.

4.2. RECURSOS CLAVE

- Plataforma blockchain: la elección del tipo de red marcará el desarrollo de la arquitectura y la infraestructura en la nube necesaria para alojar los nodos de Blotick.
- Equipo promotor: un equipo equilibrado que limite las carencias globales antes de producir cualquier contratación es de vital importancia. El buen rollo, la compenetración entre los miembros y las sinergias entre sus diferentes perfiles serán necesarios para llevar la idea a buen puerto.
- Desarrolladores: tanto de blockchain, como de aplicaciones, como back-end y front-end, los programadores serán un recurso clave de Blotick, sin los cuales la empresa está condenada al fracaso. Atraer los perfiles adecuados en un mercado laboral con gran demanda de profesionales de este sector será una tarea tan ardua como fundamental.

4.3. PROPUESTA DE VALOR

- Para usuarios:
 - Gestión informatizada de tickets y garantías.
 - Prueba de pertenencia inmutable e imperecedera.
 - Facilidad para conseguir financiación en el momento de la compra.
 - Facilidad a la hora de contratar un seguro adicional en el momento de la compra.

- Para puntos de venta:
 - Almacenamiento descentralizado de las pruebas de compra.
 - Informatización y modernización de procesos.
 - Mayor control y transparencia.
 - Mejora del servicio postventa.
 - Nuevas capacidades de fidelización a través de la creación de un nuevo canal de comunicación.
 - Diferenciación respecto del resto de sus competidores.
 - Recorte de distancias respecto del comercio online en ámbitos de captación, procesado y análisis de datos.

- Para fabricantes:
 - Asignación en tiempo real de las garantías y monitorización sobre su número y vigencia.
 - Mayor control sobre la venta de productos y veracidad de su procedencia.

- Para tiendas de segunda mano:
 - Fácil comprobación de la legitimidad del producto a comprar/vender.

4.4. RELACIONES CON CLIENTES

A los usuarios finales no se les ofrecerá una atención personalizada, permitiendo sin embargo el contacto con el servicio de soporte de Blotick a través de la app y página web.

Los puntos de venta serán el foco de toda la atención y se deberá cuidar la relación con ellos como parte imprescindible del éxito de la idea. Se les ofrecerá una atención personalizada y rápida con el fin de establecer una relación estrecha y de confianza.

Respecto a bancos y aseguradoras, cuando se pretendan incluir estas nuevas funcionalidades, se necesitará de igual manera un trato preferente hacia ellos para implementar servicios de financiación y seguros en la aplicación de manera orgánica.

4.5. CANALES

El canal principal de comunicación con los usuarios será a través del portal web y la aplicación, donde podrán encontrar un apartado de Preguntas Más Frecuentes (FAQ) y un soporte de manera individual a través de correo electrónico.

Para el resto de las empresas -puntos de venta, bancos y aseguradoras- se recurrirá a reuniones presenciales, contacto telefónico y correo electrónico. En el caso de tener un cliente de gran envergadura, se dedicará un miembro del equipo al rol de *client manager*, con el fin de establecer una relación mucho más estrecha y duradera con un importante cliente al que se le deberá prestar una atención extra.

4.6. SOCIOS CLAVE

Para el lanzamiento de la idea, se contará con la ayuda de Comillas Emprende, organizador del concurso de emprendimiento que ha dado pie a este proyecto. El gran número de actividades organizadas, talleres, encuentros con mentores y personas de interés, son herramientas que se deberán utilizar para hacer nuevos contactos y establecer relaciones con nuevos socios clave.

La consultora tecnológica everis y el mentor de este proyecto en el concurso de emprendimiento Comillas Emprende, Moisés Menéndez, son socios clave que han mostrado su interés y apoyo desde el primer momento de concepción de la idea y han ayudado enormemente a aterrizar el modelo de negocio.

4.7. SEGMENTOS DE CLIENTES

- Usuarios:
 - Toda persona que disponga de teléfono móvil y realice compras de productos con o sin garantía comercial o de productos que quiera financiar/asegurar.
 - Debido a la penetración y uso de los smartphones, confianza en la tecnología y frecuencia de compra de objetivo, los usuarios principales tendrán entre 22 y 45 años

- Puntos de venta:
 - Grandes almacenes.
 - Tiendas de electrónica y electrodomésticos.
 - Sector textil.
 - Posibilidad de incluir a tiendas online.
 - Puntos de venta que tengan dificultades para captar clientes y/o fidelizarlos y puedan ayudarse de una economía basada en tokens para sus nuevos modelos de fidelización.

- Fabricantes:
 - Empresas con problemas de falsificación de sus productos
 - Empresas que deseen tener una trazabilidad completa de las garantías vigentes de sus productos.

- Entidades financieras:
 - Entidades con servicios de financiación al consumo.

- Empresas aseguradoras:
 - Empresas que quieran ofrecer seguros adicionales en productos específicos

4.8. ESTRUCTURA DE COSTES

La estructura de costes está detallada en el Estudio Económico-Financiero, descrito en el punto 5.7.

4.9. FLUJO DE INGRESOS

El flujo de ingresos está detallado en el Estudio Económico-Financiero, descrito en el punto 5.7.

4.10. ESQUEMA VISUAL DEL CANVAS

<p>SOCIOS CLAVE</p>  	<p>ACTIVIDADES CLAVE</p> <ul style="list-style-type: none"> • Diseño de los <i>Smart Contracts</i> • Estudio de la tecnología <i>blockchain</i> • Integración de la solución con los sistemas del cliente • <i>Networking</i> • Mínimo Producto Viable • Desarrollo y diseño de la aplicación • Integración de múltiples soluciones en la <i>app</i> 	<p>RECURSOS CLAVE</p>   	<p>PROPUESTA DE VALOR</p> <ul style="list-style-type: none"> • USUARIOS - Gestión informatizada de las garantías y tickets - Prueba de pertenencia - Facilidad para conseguir financiación - Facilidad a la hora de asegurar la compra • PUNTOS DE VENTA - Almacenamiento descentralizado de las firmas de los contratos - Informatización de procesos - Mayor control y transparencia - Mejora del servicio - Diferenciación • FABRICANTE - Asignación en tiempo real de las garantías - Mayor control sobre la venta de productos y veracidad de su originalidad • TIENDAS DE SEGUNDA MANO - Fácil comprobación de la legitimidad del producto a comprar/vender 	<p>RELACIONES CON CLIENTES</p> <ul style="list-style-type: none"> • USUARIOS - Atención no personalizada • EMPRESAS, BANCOS Y ASEGURADORAS - Atención personalizada y rápida 	<p>CANALES</p> <ul style="list-style-type: none"> • USUARIOS - Canal de "Preguntas Frecuentes" con respuestas - Servicio de atención vía correo electrónico y atención FIFO (<i>First In First Out</i>) sobre la marcha • EMPRESAS, BANCOS Y ASEGURADORAS - Reuniones presenciales, contacto telefónico y correo electrónico - <i>Key Account Managers</i> 	<p>SEGMENTO CLIENTES</p> <ul style="list-style-type: none"> • USUARIOS - Toda persona que disponga de teléfono móvil y realice compras de productos con o sin garantía comercial o de productos que quiera financiar/asegurar - Debido a la penetración y uso de los smartphones, confianza en la tecnología y frecuencia de compra de objetivo, los usuarios principales tendrán entre 22 y 45 años • PUNTOS DE VENTA - Grandes almacenes - Grandes empresas de <i>e-commerce</i> • FABRICANTE - Empresas con problemas de falsificación por terceros • ENTIDADES FINANCIERAS - Entidades con servicios de financiación al consumo • EMPRESAS ASEGURADORAS - Empresas que quieran ofrecer seguros en productos específicos
<p>ESTRUCTURA DE COSTES</p>		<p>FLUJO DE INGRESOS</p>				
<p>Punto 5.7.</p>		<p>Punto 5.7.</p>				

5. PLAN DE NEGOCIO

5.1. DESCRIPCIÓN DEL SERVICIO

Blotick es una plataforma que proporciona a los consumidores una forma fácil, transparente y fiable de gestionar sus tickets y garantías. Para los puntos de venta, Blotick significa ceder todos los servicios de emisión y gestión de ticketing y protección de datos a una plataforma descentralizada y segura, permitiéndoles reducir sus costes operacionales y asegurándoles cumplir con nuevas normativas de privacidad como la GDPR. Por otro lado, la propia plataforma crea un nuevo canal de comunicación entre punto de venta y consumidor, pues ambos estarán permanentemente conectados mediante nuestro servicio.

El factor diferencial del punto de venta físico frente a otros canales de compra es precisamente el momento de la compra, cuando el cliente, después del proceso de elección del producto, se dirige a caja a pagar el producto escogido. Este momento es considerado como el clímax de la compra física, cuando el cliente se lleva el producto de manera directa consigo mismo. Se entiende que existe una desconexión entre punto de venta y cliente en este momento, debido a la dificultad para ofrecer programas de fidelización atractivos y fáciles de usar y entender. Blotick pretende estandarizar el ticket, y convertirlo en el centro de la experiencia de la compra física.

Para aunar todas estas funcionalidades, se hace uso de la tecnología blockchain, famosa por ser el protocolo detrás de criptomonedas como Bitcoin o Ethereum. Esta nueva tecnología permite la transferencia de valor a través de internet, convirtiendo todo activo, tangible o intangible en un activo digital susceptible de ser almacenado y transferido, con todo el valor que contenga el mismo. En el internet tradicional, un archivo se puede copiar y transferir infinitas veces, lo que imposibilita el cuantificar su valor o determinar el propietario del mismo. Sin embargo, el internet del valor que la tecnología blockchain ha creado, permite la transferencia de activos digitales mediante robustos protocolos criptográficos de código libre, ampliamente contrastados en diferentes industrias como el sector bancario.

En un mundo en el que la seguridad informática toma cada vez más relevancia, es imperativo que una plataforma de estas características sea segura e impenetrable. Una infraestructura Blockchain vive simultáneamente en un número determinado de nodos, servidores que componen la red y ejecutan las operaciones pertinentes para llevar a cabo las transacciones. Puesto que todos los nodos poseen la misma información en todo momento y se actualizan simultáneamente, un atacante nunca podrá tomar el control de la red accediendo a uno de los nodos, pues el resto vería que la información del nodo atacado no se corresponde con la de los demás y la desecharían. En teoría, un atacante podría tomar el control de la plataforma si controlase el 51% del poder computacional de la red al mismo tiempo, una tarea titánica para una infraestructura compuesta por un

número moderado de nodos. A día de hoy, ninguna infraestructura blockchain ha sido hackeada.

Blockchain abre la puerta al mundo descentralizado, en el que los intermediarios no existen. Una infraestructura que pretende agrupar a todo tipo de puntos de venta debe estar por encima de cualquier actor centralizado que gobierne la plataforma, para dar garantías a todos los participantes de que nadie puede trampear el sistema o manipularlo a su antojo; un sistema en el que las reglas son predefinidas, que todo participante debe acatar, y que funcionará de manera autónoma y permanente mientras exista al menos un nodo activo.

En contraposición a un blockchain público, como el de Bitcoin o Ethereum, en el que cualquiera puede ver u ordenar una transacción y toda la información queda guardada de manera pública en la cadena de bloques, un blockchain permissionado tiene una estructura jerárquica, en la que se pueden dar permisos individuales de lectura y/o escritura para una parte o toda la cadena de bloques. Como consecuencia, puede haber una serie de participantes que interactúen con una misma plataforma de manera que sus transferencias se sucedan de manera opaca entre ellos: las aplicaciones corren simultáneamente en la misma red, pero aisladas unas de otras, y nadie puede ver transacciones de una cadena si no se le ha dado permiso expresamente.

El diseño a alto nivel de la arquitectura de la aplicación sería el siguiente, que se detallará más adelante en el apartado 6:

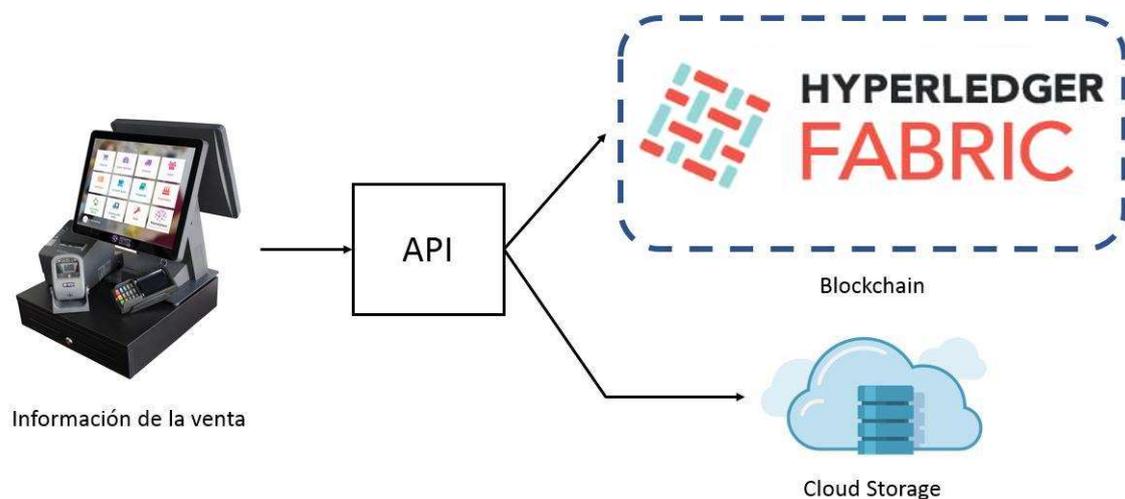


Figura 2 – Arquitectura a alto nivel de Blotick

En primer lugar, el cliente aporta su identidad digital (identidad en blockchain en forma de código QR) en el momento de la compra. El punto de venta gestiona la venta y produce una información (ID producto, ID fabricante, garantía, precio, fecha de compra, condiciones específicas...) que es comunicada a la API, junto con la ID del cliente.

La API de Blotick es la encargada de recolectar esa información, junto con otra proporcionada en la web del fabricante (si procede), procesarla y enviarla tanto a

blockchain como al almacenamiento en la nube. En la nube se almacenan los documentos relativos a la garantía, manual de instrucciones y metadatos de la venta.

La infraestructura blockchain estará basada en Hyperledger Fabric, un producto de código libre cuyo desarrollo está avalado y financiado por la Linux Foundation. En el apartado 6 se detallará su funcionamiento con mayor profundidad.

5.2. VENTAJAS COMPARATIVAS

Existen o han existido otras aplicaciones similares a Blotick que han intentado digitalizar pruebas de compra y todas ellas o bien han fracasado o no han llegado a tener una repercusión importante en ningún mercado. Blotick pretende triunfar allí donde otros fracasaron, por diversos motivos:

- Otras soluciones únicamente realizan una copia del ticket en papel respaldada en una aplicación. Esto no aporta ningún valor más allá de conservar los tickets en formato digital y evitar pérdida y deterioro de los mismos. Sin embargo, todas estas soluciones tienen un punto débil: si la aplicación acaba fracasando el cliente puede potencialmente perder todos sus tickets y todo depende de un agente centralizado, el desarrollador. Con una solución basada en blockchain el ticket es eterno e inmutable, no depende de ninguna empresa ni desarrollador, y el ticket seguirá vivo mientras la red de Hyperledger Fabric disponga al menos de un nodo activo. Es de esperar que una red del tamaño apropiado, en el caso de desaparecer, fuera un proceso que se prolongara en el tiempo lo suficiente como para establecer una nueva infraestructura a la que migrar fácilmente todos los datos sin riesgo de pérdida, sabiendo además que la migración es sencilla de un servidor a otro.
- Los tickets de papel portados a una aplicación de smartphone tradicional en ningún caso pueden representar una prueba de pertenencia, pues podrán ser fácilmente falsificados o copiados. En blockchain todos los activos registrados son únicos, protegidos criptográficamente e infalsificables.
- El hecho de ofrecer a los clientes una copia digital del ticket de papel obviamente aporta valor a los consumidores finales, pero al punto de venta en sí no le aporta nada a su modelo de negocio. Blotick quiere elevar el ticket al centro de la experiencia de compra, sirviendo como base para un nuevo canal de comunicación, uniendo a punto de venta y cliente incluso después del momento de la compra, ofreciendo nuevos programas de fidelización basados en economía de tokens (o *tokenomics*) y promociones específicas.

Siendo una plataforma construida desde el principio con la idea de tener gran modularidad, se pretende alcanzar el objetivo a dos años vista desde su puesta en funcionamiento el incluir servicios adicionales. Los que recibirán nuestra atención inmediata una vez se ha logrado la estabilidad y escalabilidad de la plataforma serán la financiación y contratación de seguros específicos en el momento de la compra. Estos

servicios ya se ofrecen de manera manual, es nuestra intención integrarlos en la plataforma para una mayor visibilidad y facilidad de contratación, aumentando potencialmente el mercado de estos productos financieros al llegar a más clientes.

Como objetivo a largo plazo, se contempla la posibilidad de incluir pagos móviles basados en dinero tokenizado, una tecnología que ya están explorando grandes bancos como Santander y que sería muy fácilmente implementable en nuestra plataforma existente. Sin embargo, a pesar del potencial que existe en el mundo de los pagos móviles, se trata de una tecnología que todavía no está preparada para ser adoptada en masa.

5.3. ESTUDIO DE MERCADO

5.3.1. Descripción del sector

El sector al que está destinado el producto es el comercio minorista o terciario. A continuación, se describe el contexto legal, económico y cultural para alcanzar un mayor entendimiento del nicho de mercado en el que encaja Blotick y las necesidades que cubre tanto de comercios como de consumidores.

En el ámbito legal, el Real Decreto de Consumo 1/2007 destaca la obligación por parte del comercio de entregar al comprador un justificante de compra. Dicho justificante puede ser expedido en papel o en cualquier otro soporte duradero como por ejemplo vía email o SMS.

Al adquirir un producto, se tienen una garantía legal y una garantía comercial asociadas al justificante de compra:

- La garantía legal tiene 2 años de duración en España y es obligatoria para todos los productos. Se puede ejercitar cuando el producto comprado no es conforme con el contrato. Es decir, que el producto no presente la calidad o prestaciones habituales que se esperan de él o que no sea apto para el fin para el que está destinado. El consumidor recibirá los servicios adecuados de reparación del producto de manera gratuita. En caso de no ser posible dicha reparación, se llevará a cabo la sustitución del producto o el reembolso del importe.
- La garantía comercial es especificada por el punto de venta o fabricante. Ésta no debe afectar a los derechos que otorga la garantía legal. En el comprobante de compra deben quedar reflejadas las nuevas condiciones que aporta la garantía comercial.

El Real Decreto 1/2007 hace hincapié en que para que el consumidor pueda ejecutar cualquiera de las garantías, deberá disponer del justificante de compra, así como del comprobante de garantía si este estuviera en un documento separado.

En cuanto al contexto económico, debido al alivio de la crisis económica, desde el año 2013 se está dando un aumento de ventas en casi todos los sectores. En la última década, el sector se ha visto revolucionado con el gran desarrollo del mundo de la tecnología y de la información. El comercio electrónico o “*e-commerce*” está creciendo a pasos agigantados y plataformas online como Amazon han cobrado gran importancia en el mercado.

Muchas marcas ya existentes anteriormente en formato de puntos de venta físicos han optado por ofrecer también servicios online a sus consumidores. Y es que el comercio electrónico ofrece numerosas ventajas tanto a consumidores como a compañías. Por citar algunas, el usuario tiene un mayor rango de selección de productos, no tiene que desplazarse al punto de venta y le da una mayor rapidez de compra. El comercio electrónico por su parte puede aplicar herramientas como *Big Data* o *Business Intelligence* con mayor efectividad para hacer un estudio más adecuado de las necesidades de sus clientes.

Con el gran avance de la tecnología, los puntos de venta físicos tienen que evolucionar para poder reducir costes, aumentar productividad y mejorar servicios para seguir siendo competitivos. A continuación, se muestran algunas pautas y tendencias que los comercios han de tener en cuenta para no quedarse atrás en la carrera por atraer al mayor número de consumidores posibles:

- A través de la automatización de procesos, diseño de algoritmos y *Business Intelligence*, se puede realizar cambios en precios y toma de decisiones con mayor rapidez y con menor personal.
- Tendencia hacia Servicios IT subcontratados en vez de tenerlos todos internos
- La ventaja competitiva se la lleva el negocio que se mueve más rápido y conoce mejor al cliente. Las empresas que mejor se están posicionando tienen los siguientes valores:
 - El valor que ofreces no tiene por qué ser generado por ti
 - La transparencia es buena, no una amenaza
 - Conseguir la atención del consumidor es la única ventaja
 - El valor está en los servicios y todo serán servicios. Por lo tanto, será indispensable conocer al consumidor
- A partir de mayo 2018 debido a la ley de protección de datos (GDPR), el usuario tendrá el derecho de a elegir qué información quiere que una compañía tenga o no sobre él
- Cobra importancia el establecimiento de canales digitales con el consumidor para llamar su atención. El consumidor ya no busca las tradicionales ofertas masivas sino que busca una recomendación o promoción personalizada.

- Blockchain puede ser la clave para añadir y mantener la fidelidad del cliente sin añadir complicaciones a sus programas ya existentes.

Aún con la gran emergencia y rápido crecimiento del comercio electrónico, la venta física sigue teniendo una gran mayoría de porcentaje de mercado. En 2016, según la Comisión Nacional de los Mercados y la Competencia, solo el 7,2% de los productos vendidos en el sector textil y el 4,2% en electrodomésticos, imagen y sonido fueron realizados a través de comercio electrónico.

Es por todo lo mencionado que Blotick es una plataforma que puede otorgar a los puntos de venta físicos el canal de comunicación que necesitan, y del que ahora mismo carece, para poder atraer a sus clientes y ponerse a la altura del e-commerce en determinados aspectos.

5.3.2. Análisis de la clientela potencial

El producto es aplicable a cualquier punto de venta que lo quiera integrar. Aun así, se ha procedido a realizar una primera reducción del mercado a estudiar a los sectores de comercio terciario en las líneas de textil, electrodomésticos de gama blanca, ordenadores y teléfonos. Debido a que estas líneas de comercio ofrecen productos que son más propensos a requerir una devolución o una avería dentro del plazo de garantía, los consumidores van a ver una mayor necesidad de disponer de una aplicación como Blotick.

Adicionalmente, en estas líneas, se encuentran grandes marcas que cuentan con mayores márgenes de beneficios y que destinan más dinero a innovación. Y es por ese motivo que estos son los clientes a los que se debe apuntar en un inicio para conseguir realizar pruebas de concepto con ellos y poder producir un MPV (Mínimo Producto Viable). Como ya se ha comentado con anterioridad, este tipo de puntos de venta tienen interés en adoptar una solución como Blotick para poder abrir un nuevo canal de comunicación con el cliente, o mejorar el existente, en el momento de la compra y poder aplicar métodos de fidelización y atracción que ahora solamente pueden aplicar con el bajo porcentaje de compras que realizan online.

Además, la integración de Blotick para el punto de venta supone una mayor facilidad del registro de sus tickets y añade seguridad al proceso de ticketing ya que utiliza tecnología blockchain, con todas las ventajas que ya se han introducido, por lo que al final estarían reduciendo sus costes de gestión, permitiéndoles de esta forma mejorar sus márgenes.

5.3.3. Análisis de la competencia. Estado del arte

Una vez realizado un estudio de la competencia de Blotick, son varios los proyectos que han intentado implementar soluciones similares pero que al parecer no han tenido

suficiente éxito. Basándose en el estudio de las debilidades que han hecho fracasar a los distintos proyectos, Blotick pretende ofrecer un nuevo ángulo y triunfar dónde el resto de los intentos fracasó.

Todos estos proyectos han centrado sus esfuerzos en la resolución de la necesidad básica del usuario: la gestión de sus tickets y garantías asociadas. Para ello han utilizado una base de datos tradicional. Al punto de venta le ofertan la mejora de servicio hacia su cliente en cuanto a la gestión de sus tickets y además consiguen un ahorro económico en cuanto a papel y tinta.

Estos proyectos no han incluido en su solución lo que para Blotick parece indispensable que es la posibilidad de apertura de un nuevo canal con el consumidor del que ya se ha hablado anteriormente. Además, ninguno de los competidores encontrados incluye la tecnología blockchain, la cual es el núcleo del proyecto, ya que aporta numerosos beneficios tanto a consumidores como comercios.

Se ha procedido a clasificar a los competidores según si se trata de competencia directa o indirecta:

- Competencia directa: esta categoría engloba a todos aquellos directamente comparables con Blotick, al tratarse de empresas creadas únicamente con el objetivo de solucionar la problemática actual del ticket en papel. Los principales competidores hallados tanto a nivel nacional como a nivel internacional son los siguientes:
 - Warranteer: se trata del principal competidor encontrado a nivel internacional, la solución que proponen es la de realizar una foto al ticket en papel, para su posterior almacenamiento en su base de datos centralizada.
 - Byetick: es sin lugar a dudas, el competidor directo con Blotick. Comparte más similitudes, ambos proyectos se crearon a principios de 2017 por un grupo de estudiantes a través de un programa de emprendimiento de la universidad; en el caso de Byetick, la Universidad de Sevilla. Aunque las soluciones que plantean son comparables a las de Blotick, la principal diferencia se halla en la ausencia de la tecnología Blockchain, lo que les dificulta la unificación del ticket y su almacenamiento perenne y seguro.
- Como competencia indirecta se encuentran algunos puntos de venta que han creado su propia aplicación para otorgar descuentos a sus clientes (Mango, Zara, etc.). Muchas de estas aplicaciones aún no tienen incorporadas la funcionalidad de adjuntar tickets online una vez comprado el producto, con lo cual, Blotick quedaría por encima. Para las que sí tienen dicha funcionalidad, Blotick es diferencial en el sentido en el que es una única aplicación para todos los puntos de venta socios, lo cual es más atractivo para el usuario ya que no tiene que descargarse numerosas aplicaciones de distintos negocios ni tener su información registrada en cada uno de ellos. Con Blotick, le valdrá con registrarse una sola vez

y podrá dotar de la información que él mismo crea conveniente a cada punto de venta en cada momento.

5.3.4. Análisis DAFO

	Positivas	Negativas
Externas	<p>Oportunidades</p> <ul style="list-style-type: none"> • Aumento de ventas, mayor crecimiento de empresas de retail, más dinero para innovación • La sociedad demanda la sustitución del ticket en papel • La escalabilidad y replicación en otros países es sencilla, si somos los primeros podemos penetrar fácilmente • Contexto en el que los puntos de venta físicos tienen que transformarse para poder aprovechar el big data y subsistir 	<p>Amenazas</p> <ul style="list-style-type: none"> • Ausencia total del hábito de pagar con el teléfono móvil por parte de la mayoría de los usuarios • Desconocimiento sobre la tecnología blockchain por parte de los usuarios, puede llevar a falta de valoración del producto o incluso al no entendimiento del valor que ofrece • Solución potente para su adaptación en punto de ventas físicos cuando hay una tendencia de reducción de este tipo de mercado en favor del electrónico u online • Pueden surgir fuertes competidores que adopten soluciones parecidas a la nuestra y la implementen con mayor rapidez, aprovechando nuestras inversiones en intentar cambiar los hábitos de los consumidores
Internas	<p>Fortalezas</p> <ul style="list-style-type: none"> • Oferta de un nuevo canal de comunicación con el consumidor en un entorno en el que el KYC es más importante debido a que el usuario quiere oferta de servicios • Uso de Blockchain, solución descentralizada y transparente resultando en una mayor confianza entre Punto de Venta – Blotick – consumidor • Equipo comprometido con apoyos en la Universidad Pontificia Comillas 	<p>Debilidades</p> <ul style="list-style-type: none"> • La empresa necesita mucho dinero en los primeros años, lo que no va a permitir tener un crecimiento tan rápido como se quisiera y se necesita a un socio financiero para alcanzar el éxito • Desconocimiento inicial de la marca Blotick en un entorno en el que el marketing digital es importante • Carencia de un programador de Blockchain en el equipo promotor con la dificultad actual para encontrar gente con ese perfil.

5.4. ESTRATEGIA DE NEGOCIO Y PLAN DE MARKETING

La elección de una acertada estrategia comercial y de un buen plan de marketing puede significar el éxito o el fracaso del proyecto. Para poder elegir la vía acertada con la que Blotick debe acercarse a sus clientes, primero ha de ser consciente de cuáles son sus necesidades o problemas actuales. Al ser distintos los clientes de los usuarios es necesario realizar estrategias distintas con las que acercarse a cada uno de ellos.

Por un lado, se encuentra el colectivo de usuarios finales, que lo formarán todas aquellas personas que hagan uso de Blotick, a través de sus dispositivos móviles, cada vez que realicen un pago. Para entender el problema/necesidad en profundidad de este colectivo se procedió a realizar más de 250 encuestas a personas de distinto sexo y edad con el fin de poder obtener una visión del problema/necesidad lo más amplia posible (Anexo A). El resultado de la encuesta muestra que más del 80% opina que el sistema actual de ticketing y garantías no está todo lo optimizado que podría llegar a estar. Más del 70% ha perdido alguna vez el ticket de compra teniendo la necesidad de devolver/cambiar el producto. Y casi la mitad de los encuestados no recuerda cuando vence la garantía de sus compras. Por lo tanto, Blotick tiene que ser capaz de resolver esas carencias actuales del sistema de forma sencilla y atractiva para el usuario. Dotándolo de disponibilidad total para poder acceder a todos sus tickets de compra con las respectivas garantías de los productos.

Por el otro lado se encuentran los puntos de venta, los verdaderos clientes, dado que son aquellos que van a pagar por el servicio. Es hacia ellos a donde Blotick debe de dirigir su estrategia comercial y su plan de marketing. Pero... ¿Qué opinan los puntos de venta del sistema de ticketing actual? ¿En qué les podría beneficiar a ellos Blotick? Una cosa está clara, y es que siempre que la solución les permita ahorrar costes e incrementar los ingresos se estará cubriendo las necesidades generales de cualquier punto de venta y por lo tanto es esta la línea por la que Blotick debe desarrollar el producto final. Pero Blotick no sólo pretende quedarse en la superficie, la idea es tratar de detectar qué puede ofrecerles a los puntos de venta que mejore su situación actual. Para ello, se procede a hablar con varias personas del gremio y todas ellas coinciden en que uno de los principales problemas es el escaso poder de fidelización actual que sufren los puntos de venta y que es muy difícil sacar provecho del clímax de la compra, momento del pago en caja en el que se mantiene un contacto directo con el usuario.

5.4.1. Producto

Una vez comprendidas las necesidades de nuestros usuarios y de los puntos de venta se procede al diseño del producto dando lugar a la creación de Blotick. ¿Qué es Blotick? Blotick es una plataforma unificada de gestión de tickets y garantías basada en blockchain. El producto es atractivo tanto para el cliente, los puntos de venta, como para los usuarios, los consumidores finales.

En cuanto a los puntos de venta, como ya se ha comentado en otros apartados anteriores, se les ofrece un nuevo canal de comunicación con sus consumidores a través del cual puede poner en marcha métodos de fidelización de clientes y programas de descuentos o cupones personalizados. Además, a través de Blotick, el punto de venta va a poder llevar a cabo un control de las garantías vivas a tiempo real.

Blotick es el gancho que el punto de venta necesita para atraer a su cliente, para poder sacar partido a la experiencia de la compra en establecimiento físico y poder conocer a su cliente mejor para ofrecerle el servicio que necesita.

En la otra cara de la moneda se encuentra el usuario. Éste va a beneficiarse aún más si cabe de las ventajas que ofrece Blotick. En primer lugar, va a poder gestionar sus tickets y garantías asociadas de manera gratuita, sencilla y organizada. La forma en la que Blotick pretende acercarse a los usuarios es mediante el mensaje de que ya se pueden olvidar de almacenar sus tickets en carteras, bolsos o cajones. Con Blotick, el usuario no sólo va a llevar un registro digital de sus tickets, sino que además va a poder conocer de manera sencilla las condiciones y plazos restantes de sus garantías.

Pero, sobre todo, Blotick va a servirle al usuario como una herramienta para acercarse a los puntos de venta, para hacerles llegar las necesidades que tienen y le va a permitir tener acceso a servicios nuevos que hasta ahora no habían sido posibles. A continuación, se citan algunos ejemplos:

- En caso de avería, el usuario va a poder ponerse en contacto con atención al cliente con un solo click.
- Posibilidad de pedir una prolongación o modificación de su garantía comercial.
- Contratación de un servicio de financiación sobre alguno de sus productos.
- Contratación de un seguro adicional que cubra el estado de su producto para situaciones que la garantía no lo haga por sí misma.
- Traspasar tickets y garantías asociadas a otros usuarios en caso de regalar el producto o de venderlo en mercado de segunda mano.

En definitiva, con Blotick, el usuario va a tener un mayor control sobre su información y la de sus productos y además no va a tener que confiar en terceros y en sus bases de datos para que su información y su registro de tickets estén seguros, ya que cuenta con la

inmutabilidad y transparencia que ofrece blockchain. Los tickets pasarán a ser únicos y eternos.

5.4.2. Precio

Una vez desarrollada la idea de negocio surge la necesidad de estudiar su viabilidad económica. ¿Cuánto se debe cobrar por el servicio, para que la idea sea viable económicamente y a su vez les permita a los puntos de venta reducir costes? Debido a los resultados obtenidos en la encuesta y a la experiencia personal de los socios fundadores, se ha decidido que la App Blotick sea de uso gratuito para los usuarios y no muestre ningún tipo de publicidad con el que obtener ingresos, dado que empeora la experiencia del usuario, algo que es crucial para que estos estén cómodos a la hora de usarla.

Pero ¿cómo hacerse una idea de lo que cobrarles a los clientes cuando no existe una solución parecida en la que fijarse para tener una mínima referencia? Una de las ventajas de basar el proyecto en blockchain es que los costes por transacción son muy pequeños. Esto ya proporciona de por sí un margen para poder obtener beneficio a la vez que permites al punto de venta ahorrar en costes de gestión.

Al no disponer de competencia directa, Blotick ha tenido que estimar el precio que quería ponerle por su servicio. Pero, ¿qué es realmente lo que se vende a los puntos de venta? ¿Cómo se piensa cobrarles? Después de realizar varias hipótesis se llegó a la conclusión que había que dividir los ingresos en dos ramas diferentes. Primeramente, cobrar a los puntos de venta por la integración de la plataforma en sus sistemas (setup) y una vez hecho esto, cobrarles por cada ticket gestionado. Con la primera rama de ingresos no se pretende obtener beneficio sino cubrir costes. Para ello primero hay que ser conscientes del coste aproximado que supondría el hecho de realizar el setup a un punto de venta. Por un lado, se encuentran los costes de personal, compuesto por los programadores y los socios fundadores y por otro todos los costes necesarios para el desarrollo de la plataforma.

A continuación, se muestra una tabla en la que se desglosan los principales costes asociados al setup. Tal y como se ha comentado previamente, con esta parte no se pretende obtener beneficio si no cubrir costes, por lo que se dividen los costes totales entre el número de setups estimados para ese año. Debido a que el número estimado de setups durante el año 1 es muy reducido y que los costes se mantienen prácticamente constantes se ha estimado oportuno dividir la suma de los costes del año 1 y 2 entre el número total de setups estimados para los dos años.

	Año 1		Año 2		Año 3		Año 4					
Empleados totales	5	-	6	-	6	-	6	-				
Sueldo programador	1	54,000	54,000	2	56,700	113,400	2	59,535	119,070	2	62,512	125,024
Sueldo equipo	4	1,350/mes	64,800	4	1,418/mes	68,040	4	1,488/mes	71,442	4	1,563/mes	75,014
Oficina		300/mes/persona	18,000		300	21,600		300	21,600		300	21,600
Licencia Red Alastría	1	500	500	1	500	500	1	500	500	1	500	500
Material Varios	3	80/cliente	240	40	80/cliente	3,200	150	80/cliente	12,000	300	80/cliente	24,000
Web	12	500/mes	6,000	12	500/mes	6,000	12	500/mes	6,000	12	500/mes	6,000
Marketing	12	500/mes	6,000	12	1,500/mes	18,000	12	4,500/mes	54,000	12	13,500/mes	162,000
Opex total			149,540			230,740			284,612			414,138
# setups			3			40			150			300
coste setup			8,844			8,844			1,897			1,380

Tabla 1 – Cálculo del coste por setup

Con esto llegamos a un coste unitario por setup durante los dos primeros años de 8.844 €. A partir del año 3 el precio/coste se reduce enormemente debido a que la estimación de número de setups se multiplica llegando a un coste/precio total de 1.897€/setup en el año 3 y de 1.380 €/setup en el año 4.

Para poder cobrar a sus clientes y obtener unos ingresos, Blotick procede a venderles packs de “utility tokens”. Estos tokens funcionan como el combustible de la plataforma. Cada vez que se registra una venta, se quema un token.

1 token = 1 registro de ticket

De esta manera se consigue que los puntos de venta compren directamente el pack con el número de tokens aproximado a los tickets/garantías que esperan emitir, obteniendo de esta forma ingresos previos a costes, aportando liquidez a la plataforma.

Poniéndonos en un escenario pesimista se estimó oportuno un precio de 0,08€ por token o ticket. Esta comisión fija es totalmente transparente y es proporcional al coste computacional de registrar el ticket en blockchain.

5.4.3. Distribución

Al igual que en apartados anteriores los canales de distribución varían entre los usuarios y los puntos de venta.

Los principales canales de distribución para llegar a los usuarios se encuentran en las Apps y por lo tanto, a través de los dos mayores portales de descarga de Apps que son App Store (para iOS) y Play Store (para Android). También podrán acceder a través de la aplicación web desde cualquier dispositivo electrónico con acceso a internet.

Dado que también existe un interés por parte de los puntos de venta -que hayan decidido incorporar Blotick como sistema de gestión- de que sus usuarios hagan uso de la aplicación, se promocionará en los puntos de pago (caja) mostrando a la gente la utilidad y facilidad de aplicación.

Los canales de distribución de los puntos de venta varían en gran medida debido a la dificultad de implantación que conlleva con respecto a los de los usuarios. En este caso se procederá a realizar reuniones presenciales en las que se negociarán y acordarán los puntos claves para la implantación de la plataforma.

5.4.4. Promoción

La principal promoción que se va a realizar es la de vender packs de utility tokens. Cuantos más tokens se adquieran, más barata sale cada unidad. Con esta medida lo que se pretende es incitar a los puntos de venta a que compren grandes cantidades de tokens de una sola vez, lo que conlleva una gran inyección de liquidez.

De igual manera, a los grandes almacenes que tienen puntos de venta distribuidos por toda España les interesa realizar la mayor cantidad de setups posibles para que el precio por unidad disminuya, ya que los costes totales apenas variarían y se repartirían entre el número total de setups.

Una de las posibilidades que incorporará Blotick es la gestión de promociones dentro de un punto de venta. Ejemplo: compra 10 cafés y te invitamos al siguiente. Con este servicio, se evita a los usuarios el hecho de tener que guardar todas las tarjetas de promociones que va acumulando a lo largo de su vida, creando una fidelización con el punto de venta.

Para conseguir desarrollar un plan de marketing para habituar a los usuarios al uso de Blotick y familiarizarlos con la App se ha destinado un presupuesto creciente exponencialmente año a año.

Blotick es consciente de que habituando al usuario a un uso frecuente de la aplicación se fuerza de manera indirecta a los puntos de venta a integrar Blotick dentro de su negocio, dado que les permite diferenciarse de sus competidores y por otro lado establecer una relación más cercana con sus clientes.

Las redes sociales representan uno de los principales medios de comunicación, puesto que además de tener un coste considerablemente menor al del resto de los medios, tienen una gran llegada dentro de nuestro target.

En el año 4 se lanzará el primer spot publicitario en televisión, con el que se pretenderá cubrir no solo al sector joven, al que ya esperamos haber llegado a través de las redes sociales y otros eventos, sino a la población con más de 40 años habituada a la tecnología.

5.5. PLAN DE OPERACIONES

A continuación, se detalla el proceso de desarrollo de los componentes necesarios para hacer de este proyecto una realidad. Puesto que Blotick es un servicio a puntos de venta, no existe un proceso productivo tradicional asociado, sino un proceso modular de creación de cada una de las entidades que conformarán la infraestructura.

5.5.1. Procedimientos y necesidades técnicas

El primer objetivo es el de desarrollar un Mínimo Producto Viable que implantar en unos pocos puntos de venta de nuestro primer cliente con el fin de que se familiarice con la tecnología y sus características de uso.

El primer paso, por lo tanto, es el de crear la aplicación móvil que permita el almacenamiento de claves criptográficas que habiliten la posibilidad de hacer transacciones en blockchain. En paralelo a este desarrollo, se necesitará crear una API que recoja los datos del punto de venta, los organice y clasifique, y los suministre a la red blockchain. También deberán desarrollarse los contratos inteligentes de Hyperledger Fabric, así como el levantamiento de la infraestructura IT requerida.

Ya en el punto de venta, se deberá instalar un lector de códigos QR en cada punto para llevar a cabo la lectura de la clave pública del cliente en el caso de la venta, o del activo digital asociado al producto en caso de devolución o ejecución de la garantía.

Una vez establecido el MPV en pre-producción, se monitorizará constantemente la estabilidad y correcto funcionamiento de la plataforma, con el objetivo de corregir *bugs* y aportar mejoras constantes con el *feedback* del cliente para ofrecerle el mejor servicio posible y aprender de su experiencia para lograr un producto cohesionado de cara a ofrecerle nuevos servicios a futuros clientes a medida que la plataforma evolucione.

El siguiente paso será garantizar la escalabilidad de la solución, estudiando las continuas mejoras de Hyperledger Fabric para anticiparse a posibles problemas derivados de la actualización de la propia red y coordinarse con el objetivo de hacer una transición suave hacia un número más elevado de puntos de venta. Esta etapa será clave para el futuro éxito de Blotick, pues se necesitará una adopción rápida de muchos puntos de venta a partir de 2020 si se pretende convertir a la plataforma en un estándar de la industria. Blotick debe prepararse para hacer frente a un gran número de implantaciones mensuales en puntos de venta en el caso de que la iniciativa iguale o supere nuestras expectativas.

Para todo ello se necesitará un espacio de trabajo común, bien sea una oficina tradicional o preferiblemente un espacio de *crowdworking*, en el que se puedan desarrollar más rápidamente las habilidades del equipo fundador dentro del mundo del emprendimiento, aprendiendo constantemente y ampliando la red de influencia y de asesores.

5.5.2. Compras

Por lo que respecta al desarrollo de Blotick, su modelo de negocio no se basa en la producción de bienes materiales ni de gestión de stocks. Sin embargo, ha de adquirirse material y mobiliario de oficina, así como equipamiento informático, principalmente ordenadores portátiles para los miembros del equipo.

Otra ventaja de optar por un espacio de *crowdworking*, es el ahorro en tiempo y esfuerzo de gestionar los gastos asociados a mobiliario y diseño de interiores de las oficinas.

Sí que se tendrá en cuenta la contratación de servicios de *hosting web* y *cloud frameworks*, y aunque la gran mayoría de las herramientas de desarrollo son de código abierto, habrá necesidad de adquirir licencias de Office 365 y otras herramientas productivas como Slack o Trello que ayuden a funcionar de la manera más eficiente posible, adoptando la filosofía Lean Startup aplicada al desarrollo de servicios IT.

5.6. ESTRATEGIA DE RECURSOS HUMANOS

5.6.1. Organigrama

El organigrama de la Figura 3 muestra los distintos departamentos que configuran la empresa con su correspondiente jerarquía.



Figura 3 – Estructura organizacional de Blotick

En la cabeza de la pirámide se encontraría el Administrador General o CEO que tiene como función la implementación del plan de negocio descrito en este apartado. Es el nexo entre los distintos departamentos de la empresa y debe planificar, organizar, controlar y dirigir la empresa. El CEO tiene además la última palabra en la toma de decisiones

significativas para la empresa y es el pilar más importante en la definición e implementación de la estrategia de la misma.

En un segundo nivel en la pirámide se encuentra el Departamento de Desarrollo de Producto y el de Desarrollo de Negocio.

En el departamento de Desarrollo de Producto se van a llevar a cabo todas aquellas tareas para la elaboración de Blotick. El CTO está a la cabeza de este bloque. Tiene como funciones la dirección, supervisión y coordinación de los integrantes del departamento y de sus tareas.

En este departamento se cuenta además con programadores de blockchain y back-end de la plataforma y App y con programadores de front-end. Los primeros se encargan de desarrollar las tripas del producto. Son los encargados de programar los smart contracts de Blotick, desarrollar el protocolo de garantías y los servicios y el back-end de las DApps (Distributed Apps) que se encuentren en la capa superficial del protocolo. Todo esto se debe crear sobre la arquitectura base de Hyperledger Fabric.

Por otro lado, los programadores de front-end son los encargados de desarrollar la parte superficial del producto. Lo que el cliente y usuario van a ver. Se encargan de desarrollar la web y las aplicaciones móviles en Apple y Android. Deben tener un perfil más orientado a diseño y funcionalidad. Desde Blotick pensamos que es indispensable conseguir un diseño atractivo y funcional. Una máxima a seguir es que la App sea sencilla y rápida de usar, para que no se generen colas en los supermercados.

Además, Blotick va a contar con uno o dos programadores de front-end destinados a la instauración de los set-up en los puntos de venta que contraten nuestros servicios.

El departamento de Desarrollo de Negocio contiene los subdepartamentos de Finanzas, Marketing, Recursos Humanos y Ventas. En un inicio de la empresa, al ser estos departamentos pequeños, serán el CEO, COO y CFO las personas que desempeñen todas las funciones que se requieran.

EL CFO, evidentemente, estará más orientado a llevar las finanzas de la empresa con el apoyo del CEO y del COO en caso de ser necesario. Este departamento es fundamental para tener una estrategia sólida y coherente que promueva crecimiento en los primeros años de vida.

El departamento de marketing estará dirigido por el COO y tendrá como misión hacer llegar el producto tanto al cliente como al usuario.

El departamento de RRHH estará dirigido por el COO y el CEO, pero también contará con la participación del CFO y CTO dependiendo del departamento para el que trate la incorporación o materia a tratar.

El departamento de ventas se encuentra inicialmente cubierto por el CEO y el COO.

5.6.2. Necesidades de personal

Actualmente somos cuatro socios cofundadores en el equipo que vamos a desempeñar los papeles de CEO, COO, CTO y CFO.

En los comienzos de la compañía necesitaremos contratar al menos a otro programador de blockchain y a otro front-end para poder empezar a desarrollar un MPV y el producto final a posteriori. La idea del equipo promotor es de encontrar dicho personal en alguna empresa colaboradora con Blotick y muy relacionada con el mundo del blockchain, y que también tengan inquietudes y la motivación necesaria para embarcar en una aventura emprendedora.

5.6.3. Contratos y retribuciones

A continuación, se muestran las tablas de sueldos de los empleados de la empresa incluyendo al equipo promotor para los tres primeros años. La seguridad social se supone un 35 % de media.

Año 1

En el año 1 además del equipo promotor, se cuenta con un programador blockchain y dos programadores front-end, uno dedicado al desarrollo de aplicaciones web y móviles, y otro a la implementación de set-ups.

En Euros

Costes de personal	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Total
Promotor	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	12,000
													Seguridad Social
													16,200
													x4
													64,800
Programador Blockchain	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	60,000
													Seguridad Social
													81,000
													x1
													81,000
Programador Front End	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	40,000
													Seguridad Social
													54,000
													x2
													108,000
													TOTAL COSTE PERSONAL
													253,800

Tabla 2 – Necesidades de personal. Año 1.

Año 2

En el año 2 se contrata a un programador front-end adicional para la implementación de set-ups

En Euros

Costes de personal	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Total
Promotor	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	12,000
													Seguridad Social
													16,200
													x4
													64,800
Programador Blockchain	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	60,000
													Seguridad Social
													81,000
													x1
													81,000
Programador Front End	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	40,000
													Seguridad Social
													54,000
													x3
													162,000
													TOTAL COSTE PERSONAL
													307,800

Tabla 3 – Necesidades de personal – Año 2.

Año 3

En el año 3 se contrata a un programador front-end más para el desarrollo y mantenimiento de la web y las aplicaciones móviles

En Euros

Costes de personal	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Total
Promotor	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	12,000
													Seguridad Social x4
													16,200
													64,800
Programador Blockchain	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	60,000
													Seguridad Social x1
													81,000
													81,000
Programador Front End	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	3,333	40,000
													Seguridad Social x4
													54,000
													216,000
													TOTAL COSTE PERSONAL
													361,800

Tabla 4 – Necesidades de personal. Año 3.

5.7. ESTUDIO ECONÓMICO-FINANCIERO

A la hora de contemplar la viabilidad de un proyecto es muy importante no sólo hacer un buen estudio de mercado y de producto, sino que también se ha de proyectar la realidad financiera esperada en un futuro. De esta manera, se consiguen planificar las necesidades de capital y justificar la viabilidad económica del proyecto. Igualmente, este tipo de información permite controlar y gestionar el día a día de la compañía.

Para ello, se han proyectado los dos Estados Financieros más importantes -Cuenta de Pérdidas y Ganancias, y Balance- a lo largo del periodo 2018-2021.

Antes de construir los Estados Financieros especificados, se realizará un desglose de datos económicos del año 1. Los datos que se tienen son:

- Costes operativos:
 - Sueldo programador: 54.000€, tiene en cuenta el coste de seguridad social y se actualiza a razón de un 5% anual. Hace referencia al sueldo de los programadores con perfil enfocado a la realización de los servicios de integración de la plataforma y el punto de venta.
 - Sueldo fundador: 1.350€ mensuales, tiene en cuenta el coste de seguridad social y se actualiza a razón de un 5% anual.
 - Marketing: 500€ mensuales. Se triplica la cantidad destinada al marketing cada año, a medida que se tienen puntos de venta integrados en la plataforma.
 - Oficina: 300€ mensuales por persona, según una búsqueda realizada de diferentes alternativas de espacios de coworking.
 - Material y varios: 80 euros por punto de venta. Se tiene en cuenta en todos los periodos y hace referencia a gastos para preparación de material comercial, entrega de documentación, etc.

- Web: 500€ mensuales. Hace referencia a los costes asociados al hosting de la página web, contratación de Google Analytics y posicionamiento SEO
- Inversión en activos:
 - Ordenadores: 1.000€ por ordenador. Cada vez que se incorpora gente nueva, se habrá de tener en cuenta
 - Registro de marca “Blotick”: 188€, incluyen 149€ de solicitud y 39€ de concesión. Sólo se ha de realizar en el año 1.
 - Compra del dominio web: 50€. Sólo se ha de realizar en el año 1.
 - Sueldo programador blockchain: 81.000€, tiene en cuenta el coste de seguridad social y se actualiza a razón de un 5% anual. Hace referencia al sueldo del programador experto en blockchain que construirá la infraestructura de la plataforma.
 - Sueldo programador: 54.000€, tiene en cuenta el coste de seguridad social y se actualiza a razón de un 5% anual. Hace referencia al sueldo de los programadores con perfil enfocado a desarrollo *front-end* y *back-end*, que realizarán la puesta a punto de la plataforma e interfaces de interacción con la misma.
- Ingresos:
 - Únicamente se cobrará por servicio de setup los costes incurridos en el mismo. En el caso de los años 1 y 2, se cobrará c.9.000€. En el caso de los años 3 y 4, se cobrará c.2.000€ y c.1.400€ respectivamente.
 - Se considera que se realizarán las siguientes implantaciones:
 - Año 2018: 3 setups, a modo de prueba de concepto y testeo del mínimo producto viable.
 - Año 2019: 40 setups, justificando el número en cuanto a que el cliente que ha probado la prueba de concepto quiere implantar la solución en otros puntos de venta y otros puntos de venta quieran probar la solución.
 - Año 2020: 150 setups, justificando el número en cuanto a que los clientes que tienen implantada la solución quieren integrar más puntos de venta y otros puntos de venta nuevos quieran probar la solución.
 - Año 2021: 300 setups, justificando el número en cuanto a que los clientes que tienen implantada la solución quieren integrar más puntos de venta.

- Los servicios de setups se cobrarán en un plazo de cobro de 30 días.
- Se prevé cobrar una media de 0.08€ por token a lo largo del periodo estudiado, como se ha reflejado en el apartado 5.4.2.

Por otro lado, la penetración del mercado de tickets estimada en 3 años es del 1%, llegando a un volumen de tickets gestionados objetivo de c.8 millones de tickets. Se empezarán a vender tokens en 2019, cuando esté listo el mínimo producto viable de la plataforma y realizados los primeros setups. Para ello, se ha tenido en cuenta una curva de adopción de la tecnología de la siguiente manera:

- Año 2019: 0,5%, equivalente a 40.155 tickets gestionados.
- Año 2020: 20%, equivalente a 1.606.187 tickets gestionados.
- Año 2021: 100%, equivalente a 8.030.936 tickets gestionados.
- La venta de tokens se realizará con un periodo de cobro nulo, ya que el pago se realiza en el momento de la compra.
- Relación con instituciones financieras:
 - Se tiene en cuenta que la concesión de un préstamo por una entidad financiera tendrá un plazo de 5 años y un coste del 7% anual. Estos valores se han obtenido tras realizar un estudio de alternativas. Igualmente, la cuantía de la concesión del préstamo puede ser sustituida o reducida por una subvención o premios de concursos de emprendedores. A continuación, se obtendrán las necesidades de financiación, cuadrando la deuda y la participación de inversores externos.
- Relación con inversores externos:
 - Se emitirá un contrato específico con cada inversión realizada por parte de los inversores externos. Se buscará en todo momento realizar contratos con objetivos donde:
 - Se emiten acciones preferentes convertibles en acciones ordinarias en caso de no cumplimiento de los objetivos.
 - De esta manera, los fundadores conservan la mayor parte del control de la compañía si cumplen con los objetivos.
 - Los inversores externos convierten en acciones ordinarias sus acciones preferentes, ganando control de la compañía, si los objetivos no son cumplidos
- Relación con la Agencia Tributaria
 - Se ha tenido en consideración un Impuesto de Sociedades del 30% sobre el beneficio antes de impuestos.

Una vez establecidas las bases, se presentan los Estados Financieros².

En primer lugar, se presenta el Balance de Situación a lo largo de los periodos, en miles de euros:

Balance Sheet				
Period	2018	2019	2020	2021
Fixed Assets	135,00	276,75	485,12	703,91
Acc. Depreciation	13,50	41,18	89,69	160,08
Non-Current Assets	121,50	235,58	395,44	543,84
Inventories				
Receivables	2,20	29,66	33,95	87,09
Cash	1,48	2,40	3,16	4,63
Current Assets	3,69	32,06	37,11	91,72
Total Assets	125,19	267,63	432,55	635,56
Shareholders	177,02	103,86	232,38	23,43
Retained Earnings	(98,19)	70,13	53,91	397,27
Equity	78,83	173,99	286,29	420,71
Non-Current Liabilities	31,52	69,65	114,67	168,53
Notes Payable	2,25	4,98	8,19	12,04
Accounts Payable				
Accrued Accounts	12,58	19,01	23,39	34,29
Current Liabilities	14,83	23,99	31,58	46,32
Equity & Liabilities	125,19	267,63	432,55	635,56

Tabla 5 – Balance de situación

² En el año 2018, ya que los promotores del proyecto tienen intención de constituir la sociedad y empezar con la contratación en septiembre, los costes anuales han sido prorrateado a una tercera parte. Esto se debe a que los meses de septiembre a diciembre incluido, son una tercera parte del total de meses que hay en un año.

Se puede apreciar fácilmente cómo la plataforma se activa en el balance como un activo intangible, crucial para el desarrollo de la actividad. Por otro lado, no hay Inventario en el Balance debido a que Blotick vende servicios, y los utility tokens vendidos son generados en el momento de la transacción.

A continuación, se presentan los flujos con respecto inversores e instituciones bancarias. El proceso que se ha seguido es el siguiente:

1. Determinación del flujo de caja con respecto de inversores
2. Ejecución de una macro en VBA que determina la deuda necesaria, iterando y haciendo el encaje de intereses financieros entre la cuenta de Pérdidas y Ganancias y el Balance.

1 Sales increase/decrease				
2 Inflation				
3 Fixed costs	153,09	231,34	284,61	417,14
4 Investments	135,00	141,75	208,37	218,79
Average depreciation	10 years			
5 Days in inventory	0 days	0 days	0 days	0 days
365 days a period	30 days	30 days	30 days	30 days
Collection period	30 days	30 days	30 days	30 days
Cash ratio	10,0%	10,0%	10,0%	10,0%
Days to pay suppliers	0 days	0 days	0 days	0 days
Days to pay accruals	30 days	30 days	30 days	30 days
6 First round	98,21	(75,54)	(65,78)	(416,61)
Second round	78,81	100,57	124,16	153,75
Shareholders	177,02	25,03	58,39	(262,86)
Preferred dividends				
7 Debt	33,78	43,10	53,21	65,89
Debt's time horizon	15 years			
8 Financing	112,59	143,67	177,38	219,65
	Ws: 70,0%		rs: 33,9%	
	Wd: 30,0%		rd: 3,0%	
			g: 3,5%	
	Minimum interest: 3,0%		rRF: 3,0%	
	Interest: 3,0%		rM: 30,0%	
	Maximum interest: 25,0%		beta (assets): 0,80	
	Desired leverage (for banks): 40,0%			
				WACC
				24,3%

Tabla 6 – Flujos con respecto a inversiones

En cuanto a las relaciones con los inversores se puede determinar lo siguiente:

- Se está teniendo en cuenta la financiación de un Business Angel en el año 2018, al que se le devolverá el dinero en el año 2021 con una TIR del 31%. Se ha escogido la figura del Business Angel debido a la madurez del proyecto en el año 2018 y las necesidades de capital dadas.
- Se está teniendo en cuenta la financiación de un Venture Capital en el año 2019, al que se le devolverá el dinero a partir del año 2022 incluido. Se ha escogido la figura del Business Angel debido a la madurez del proyecto en el año 2018 y las necesidades de capital dadas.

En cuanto a la relación con las instituciones financieras se puede determinar lo siguiente:

- Se va a necesitar captar financiación de un banco todos los años. De todas maneras, el apalancamiento de la compañía a duras penas llega al 50% en los años en los que la empresa no es generadora de caja (año 2018, 2019 y 2020).
- Ya en el año 2021, los bancos no tendrán problemas para ofrecernos financiación debido a la generación de caja de los siguientes años y la visibilidad de la misma.

En segundo lugar, se presenta la Cuenta de Pérdidas y Ganancias en miles de euros:

		1.000 \$			
Income Statement					
Period	2018	2019	2020	2021	
Revenues	26,82	360,82	413,11	1.059,61	
COGS					
Gross Margin	26,82	360,82	413,11	1.059,61	
Fixed Costs	153,09	231,34	284,61	417,14	
EBITDA	(126,27)	129,48	128,49	642,48	
Depreciation	13,50	27,68	48,51	70,39	
EBIT	(139,77)	101,81	79,98	572,08	
3,0% Interests	0,51	1,63	2,96	4,55	
Pretax Profit	(140,28)	100,18	77,02	567,53	
30,0% Taxes	(42,08)	30,05	23,11	170,26	
Earnings	(98,19)	70,13	53,91	397,27	
Less preferred dividends					
Retained Earnings	(98,19)	70,13	53,91	397,27	

Tabla 7 – Cuenta de pérdidas y ganancias

Tal y como se puede observar, no se tiene beneficio hasta llegado el año 2019. Esto se debe a que la principal fuente de ingresos en el modelo de negocio de Blotick, suponiendo que la empresa está ya establecida y reconocida en el mercado, es la venta de tokens. Y, se ha construido un escenario muy conservador a lo que esto respecta. Cabe mencionar que, una vez llegados a este punto, la empresa se vuelve muy rentable ya que la construcción de la plataforma y la integración de puntos de venta se ha realizado con éxito, dejando paso a tareas de mantenimiento. Hay que tener igualmente en cuenta que no se han tenido en cuenta otros futuros ingresos como:

- Ingresos por servicios modulares, entre los que se incluyen: venta de seguros, acceso a financiación al consumo y otros. Blotick no se encargaría de realizar esos servicios, pero sí de ser la plataforma que permite el punto de encuentro entre las partes.

- Ingresos en otros países. Una vez alcanzada la escalabilidad sería sencillo para Blotick acompañar a grandes clientes a otras geografías o simplemente penetrar otros países a parte de España.

Se estima un EBITDA positivo y creciente a partir del año 2019. El EBITDA, o beneficio operativo, es un buen indicador de la solvencia operativa de una empresa.

Estimación de los Flujos de Caja:

NOPAT	(97,84)	71,26	55,99	400,46
Depreciation	13,50	27,68	48,51	70,39
OCF	(84,34)	98,94	104,50	470,85
- CAPEX	(135,00)	(141,75)	(208,37)	(218,79)
- Increase in NWC	8,89	(21,94)	(0,68)	(43,72)
CFFA	(210,44)	(64,75)	(104,55)	208,34
TV				1.035,20
FCF	(210,44)	(64,75)	(104,55)	1.243,54

Tabla 8 – Flujos de caja

Se puede apreciar cómo no se alcanza un flujo de caja positivo hasta el 2021. Esto se debe a las altas necesidades de CAPEX que ocurren durante los primeros periodos. Una vez alcanzada la escalabilidad del proyecto, empieza a generar un margen EBIT creciente, dado que los ingresos crecen a un mayor ritmo que los costes.

A continuación, se refleja la tercera y última parte de los estados financieros:

Statement of Cash Flow

Period	2018	2019	2020	2021
1. Cash Flow from Operations				
Net Income	(98,19)	70,13	53,91	397,27
Depreciation	13,50	27,68	48,51	70,39
Op. Cash Flow	(84,69)	97,80	102,43	467,66
(-) Incr. Inventories				
(-) Incr. Receivables	(2,20)	(27,45)	(4,30)	(53,14)
Incr. Accounts Payable				
Incr. Accrued Accounts	12,58	6,43	4,38	10,89
Cash Flow from Operations	(74,31)	76,78	102,51	425,42
2. Cash Flow from Investments	(135,00)	(141,75)	(208,37)	(218,79)
3. Cash Flow from Financing				
Common Shareholders	177,02	25,03	58,39	(262,86)
Preferred Shareholders (-)				
Banks	33,78	40,85	48,24	57,70
Cash Flow from Financing	210,80	65,88	106,62	(205,15)
Cash Flow	1,48	0,92	0,76	1,47
Cash at the beginning		1,48	2,40	3,16
Cash Flow	1,48	0,92	0,76	1,47
Cash at the end	1,48	2,40	3,16	4,63

Tabla 9 – Cash Flow Statement

Como último capítulo del análisis de la viabilidad financiera del proyecto, se ha procedido a calcular diferentes ratios, con el fin de poderse los presentar a los inversores en el corto plazo.

Ratios

Period	2018	2019	2020	2021
Liquidity				
Current Ratio	0,25	1,34	1,18	1,98
Acid Test	0,25	1,34	1,18	1,98
Cash Ratio	10,0%	10,0%	10,0%	10,0%
Management				
Inventory Turnover				
Days of Inventory	0 days	0 days	0 days	0 days
Receivables Turnover	12,17	12,17	12,17	12,17
Collection Period	30 days	30 days	30 days	30 days
Payables Turnover				
Days to Pay Payables	0 days	0 days	0 days	0 days
Accruals Turnover	12,17	12,17	12,17	12,17
Days to Pay Accruals	30 days	30 days	30 days	30 days
Total Asset Turnover	0,21	1,35	0,96	1,67
Debt				
Leverage Ratio	37,0%	35,0%	33,8%	33,8%
Credit Ratio	27,0%	27,9%	28,4%	28,4%
Times Interest Coverage	(275,87)	62,61	27,00	125,69
Cash Coverage Ratio	(249,23)	79,63	43,38	141,16
Equity Multiplier	1,59	1,54	1,51	1,51
Wd				
Profitability				
ROE	(124,6%)	40,3%	18,8%	94,4%
ROA	(78,4%)	26,2%	12,5%	62,5%
Profit Margin	(366,1%)	19,4%	13,1%	37,5%
Total Asset Turnover	0,21	1,35	0,96	1,67
Equity Multiplier	1,59	1,54	1,51	1,51
Plowback Ratio	100,0%	100,0%	100,0%	100,0%

Tabla 10 – Análisis de ratios

5.8. ESTRUCTURA JURÍDICA

La organización de Blotick implica la adopción de toda una serie de acciones de contenido legal más allá de la propia constitución de la Sociedad que va a servir de base para sostener su actividad. Revisaremos a continuación cada uno de estos aspectos.

5.8.1. Protección de la idea

- Acuerdo de promotores-fundadores: el equipo fundador establecerá un acuerdo para coordinar su posición común ante terceros y entre ellos mismos (financiadores, nuevos socios, no competencia, propiedad intelectual, etc.).
- Acuerdo de confidencialidad: se elaborará un modelo de NDA estándar para acompañar presentaciones del proyecto. Esto será crítico en el caso de presentaciones comerciales o a potenciales partners y distribuidores que podrían violar nuestros derechos de propiedad.
- Cláusulas específicas en acuerdos con potenciales empleados y proveedores: en los acuerdos de prestación de servicios a Blotick incluiremos las previsiones contractuales necesarias para proteger la propiedad intelectual y evitar actos de competencia desleal.
- Marcas y dominio: registro de:
 - Marca europea “Blotick”.
 - Dominios internet para .es, .com, .io y .eu.
 - Estudio de posibles patentes en US.

5.8.2. Organización legal del proyecto

- Constitución de la Sociedad y Pacto de Socios: la Sociedad adoptará la forma de Sociedad de Responsabilidad Limitada conforme a la legislación española de Sociedades de capital: Razones principales:
 - Tipo de entidad estándar para terceros (nuevos socios-inversores)
 - Permite la inclusión de pactos para su mejor organización (financiación, clases de participaciones, gobernanza, etc.)
 - Neutral y facilita el acceso a fuente de financiación para I+D
 - Gestión de la responsabilidad patrimonial de los socios.

Además de lo anterior, el Pacto de Socios incluirá:

- Organización del órgano de gobierno
 - Organización del equipo gestor
 - Gobierno. (Materias reservadas: derechos de voto).
 - Mecanismos de resolución de conflictos.
 - Encaje de los acuerdos principales de financiación.
- Financiación “estándar”: Se plantean dos modalidades principales para la incorporación de financiadores del proyecto
 - Capital (más probable): implicaría la organización de la primera “ronda” mediante la entrega de participaciones que representan derechos de voto y económicos en el proyecto. El problema principal será la valoración de la Sociedad y los pactos como socios que implicarán cierta rigidez en un estado temprano o seed del proyecto.
 - Préstamo convertible (preferible): cada vez más habitual en el emprendimiento tecnológico, sería un bono para distribuir entre uno o varios inversores, que permitiría originar la financiación necesaria. En la siguiente ronda, este bono se podría convertir a elección del inversor en capital en condiciones preferentes -con importante descuento en la valoración de la compañía en esa ronda- o ser devuelto con un interés.

5.8.3. Posible ICO

Al ser un proyecto basado en blockchain, se está considerando la organización de una *Initial Coin Offering* basada en la venta anticipada de los utility tokens que se han configurado como modelo de ingresos de la actividad de Blotick. Consultados diferentes expertos, se aconseja su estudio en profundidad, si bien debe ser analizado conjuntamente con los primeros inversores en la compañía y siempre que quedara aclarado el panorama regulatorio de las ICOs en nuestro país.

5.8.4. Uso de la plataforma

- Acuerdos de comercialización: Preparación de los acuerdos para uso por fabricantes y comercios.
- Términos de uso de la plataforma: Acuerdos para usuarios finales regulando ejercicio y condiciones de sus derechos. Tema delicado por el carácter legal de las garantías en muchas ocasiones, y tratarse de ciudadanos-consumidores.

- Políticas generales de la Web, APP y plataforma: Privacidad, términos legales del sitio, otras requeridas en cada momento por la legislación aplicable. Posible gestión del sello “confianza legal”.
- Especificidades blockchain: Los contratos de uso de la plataforma tendrán que resolver las cuestiones GDPR y de privacidad que están planteándose a la utilización de la blockchain por personas físicas.

5.8.5. Empleados y proveedores

- Acuerdos con empleados: Modelo de incentivos ligado al plan de negocio para el equipo *core* de Blotick. Necesidad de contratación de recursos propios de la Compañía en la fase inicial para la protección del modelo.
- Acuerdos con proveedores: Preparación de los acuerdos básicos con las posibles compañías de servicios tecnológicos para la construcción del producto.

6. MÍNIMO PRODUCTO VIABLE

El Mínimo Producto Viable ha sido definido como la implantación más sencilla que puede procurarse a un punto de venta de manera que la solución sea operativa a nivel de emisión del ticket y recepción por parte del usuario. Para ello será necesario definir una arquitectura blockchain apropiada, una infraestructura en la nube que la aloje, una API de comunicaciones entre el terminal del punto de venta y la red blockchain, y una aplicación web en la que el usuario pueda registrarse y obtener su clave pública para identificarse en la red blockchain.

6.1. ELECCIÓN DE LA TECNOLOGÍA BLOCKCHAIN

El primer paso que se debe dar hacia la elección de la tecnología blockchain más apropiada disponible es determinar si se necesita una blockchain pública o privada-permisionada. Las blockchain públicas, como la de Bitcoin, Ethereum o Ripple por mencionar algunas, se definen por las siguientes características.

- Son de código abierto.
- Cualquier persona puede participar en ellas y realizar transacciones.
- Cualquier persona o entidad puede alojar un nodo de la red para añadir poder computacional y verificar transacciones (comúnmente conocidos como *mineros* de una red blockchain).
- La cadena de bloques es pública y cualquiera -no sólo un participante o un minero- puede ver y auditar todas las transacciones de principio a fin en el libro contable.

Estas características hacen de las blockchain públicas candidatas ideales para aplicaciones como las criptomonedas, que buscan la descentralización del sector bancario y abren las puertas a que cualquiera pueda hacer uso de ellas, estableciendo las reglas del juego de manera transparente, y certificando la posesión de los activos asociados a una clave pública.

Sin embargo, para una aplicación como Blotick, en la que los datos de las compras son de carácter sensible, tanto para usuarios como para puntos de venta, es mucho más apropiado el uso de una blockchain permisionada, que permite crear una jerarquía de usuarios y establecer ciertos criterios de registro y alojamiento de los nodos.

Existen dos soluciones fundamentales de blockchain permisionadas de código libre de las que se podría hacer uso:

- Quorum: desarrollado por el banco de inversión JP Morgan Chase, Quorum es un blockchain permisionado basado en la tecnología Ethereum, a la que añade una capa de privacidad para poder cifrar las transacciones que tienen lugar en la red

para los usuarios que se deseen. Puesto que por debajo Quorum sigue siendo Ethereum (literalmente es una copia del código de Ethereum excepto por esa capa de privacidad llamada Constellation que desarrolla JPMorgan), muchas de sus características se comparten con la blockchain de Ethereum: existen comisiones por transacción, los smart contracts deben ser desarrollados en el lenguaje de programación de Ethereum (Solidity), y el desarrollo del código base está sujeto a las directrices que proporciona la Ethereum Enterprise Alliance.

- Hyperledger Fabric: es una solución de blockchain permissionado de código abierto que se desarrolla bajo el paraguas de Hyperledger; un conjunto de productos blockchain de código abierto avalado y financiado por la Linux Foundation, la entidad más importante de software libre a nivel mundial. Fabric es el producto con estado de madurez más avanzado dentro de Hyperledger, y al igual que el resto de sus productos, es desarrollado en conjunto por diferentes empresas, siendo IBM la que más código aporta a la iniciativa. Fabric está pensado principalmente para su aplicación en el ámbito empresarial, ofreciendo gran capacidad de adaptabilidad a distintos modelos organizacionales dependiendo de los requerimientos funcionales de la empresa que desee utilizarlo. La arquitectura de Fabric es altamente modular, por lo que se puede distribuir la carga computacional entre distintos servidores para lograr una escalabilidad y robustez que otras soluciones no pueden proporcionar sin tener que renunciar a determinadas funcionalidades. Fabric permite también encriptar la totalidad o parte de las transacciones que tienen lugar en la red, definiendo distintos tipos de participantes con distintos tipos de permisos.

Es por la gran configurabilidad, modularidad, estado de madurez, y capacidad de escalado que se ha elegido Hyperledger Fabric para la definición de la arquitectura blockchain de este MVP. En los siguientes apartados se detallará con más profundidad el funcionamiento de Hyperledger Fabric para facilitar la comprensión de la arquitectura propuesta para Blotick.

6.2. CONCEPTOS CLAVE DE HYPERLEDGER FABRIC

El conjunto de aspectos que deben ser estudiados desde una perspectiva de diseño de arquitectura son múltiples, y dependen de la forma en la que vaya a trabajar el sistema. Es necesario por este motivo tener un mayor conocimiento de la forma de trabajar de la tecnología base: Hyperledger Fabric v1.3. En esta sección, se introduce, de forma breve y genérica dicha tecnología y su forma de operar, una vez ya configurada.

6.2.1. Elementos básicos

- **Peer:** son módulos aportados por las entidades participantes en la blockchain. Estos nodos contienen tanto el libro contable, como una base de datos que recoge el estado actual de la cadena y que será leída por los smart contracts. Fabric define varios tipos de peers: committing peers, endorsing peers, leader peers y anchor peers. Todo peer es de tipo committing peer, es decir, almacena la cadena de bloques y mantiene el World State (ver Ledger). Todo peer que tenga un chaincode instalado es al mismo tiempo un endorsing peer. Cada organización puede tener uno o más leader peers. Estos se encargan de propagar los bloques recibidos desde un orderer peer (ver Ordering Service) a todos los committing peers del canal. Un anchor peer es empleado para la comunicación con peers de otras organizaciones en el canal.
- **Channel (canal):** se trata de un canal de comunicación privado entre peers, de forma que sólo los participantes con permisos para ello puedan participar en el canal. Cada canal mantiene una blockchain propia, junto con su chaincode, y sólo los participantes del canal pueden ver la blockchain y las transacciones registradas en ella. Por tanto, se puede decir que cada canal equivale a una blockchain distinta. Es un mecanismo que permite alcanzar un mayor nivel de separación entre participantes si se estima oportuno. Hay que destacar que un mismo peer puede participar en más de un canal simultáneamente, manteniendo aisladas sus respectivas blockchain.
- **Chaincode:** es la denominación que reciben los smart contracts en Fabric. Estos pueden desarrollarse en lenguajes de programación comunes como Java, Node.js o Golang; y pueden interactuar con la blockchain a través de una API configurada en consecuencia. En Fabric hay dos tipos de chaincode: de usuario –programado por los administradores del canal donde se encuentre– y de sistema –que aporta la lógica necesaria para ejecutar parte del flujo de las transacciones, y es programado por el administrador de la red.
- **Ordering Service:** es el servicio encargado de crear los bloques para cada canal, alcanzando el consenso entre los diferentes orderer peers que lo componen. Este componente es totalmente modular y ofrece distintos protocolos de consenso. Este

servicio puede estar conformado por un conjunto de nodos. De hecho, para lograr mayor tolerancia a fallos, es interesante que no se restrinja a un único nodo.

- **Ledger:** el libro contable en cada canal está conformado por su cadena de bloques y el World State, base de datos clave-valor que mantiene el estado actual del blockchain. De forma que cada uno de los peers que pertenecen a un canal mantienen una copia local de ambos. Además, Fabric es compatible con dos tipos de bases de datos que pueden almacenar el World State: LevelDB o CouchDB, con diferentes características.
- **Private Data Collection:** colección de datos privados al que sólo pueden acceder los peers del conjunto de organizaciones de un canal autorizados a ello. Se trata de un mecanismo que permite intercambiar información entre una serie de organizaciones de un canal sin necesidad de crear otro. La base de datos en la que se almacenan las colecciones de datos privados se denomina SideDB.
- **Cliente:** se define como aplicación cliente aquella que está autorizada para participar en la red y propone transacciones. La aplicación cliente envía la transacción a uno o más endorsing peers en función de la política de aprobación establecida en dicho canal. Una vez ha recibido suficientes respuestas con la aprobación adecuada, manda la transacción junto con los endorsements obtenidos al Ordering Service, que la incluye en un bloque y la propaga para su posterior validación y confirmación en el registro.

6.2.2. Cantidad y distribución de nodos

Por cantidad de nodos se entiende como el conjunto de nodos que deben coordinarse y sincronizarse en su operación. De esta manera, a menor número de nodos, menor será el tiempo de respuesta, si bien la carga de trabajo que podrá hacer frente será proporcional, y la tolerancia a fallo y disponibilidad de la solución serán igualmente menores. De manera contraria, a mayor número de nodos, el sistema será más robusto y estable frente a contingencias y podrá soportar mayor número de transacciones por segundo, aunque las comunicaciones entre nodos serán más lentas, llegando al punto de que una combinación de latencias altas y gran número de transacciones pueda saturar el sistema. Este problema es particularmente grave si su distribución geográfica está muy repartida y la calidad de los canales de comunicación a utilizar entre ellos no es la apropiada.

6.2.3. Número de canales

Los canales son uno de los mecanismos que proporciona Fabric para aislar registros de transacciones, generando para cada uno de ellos su propia blockchain. De esta forma, la carga de trabajo global es procesada por los peers que componen el canal al que son

enviadas las transacciones. Por tanto, los canales de forma implícita introducen una forma de realizar trabajo en paralelo. Es interesante por tanto definir el número adecuado de canales a utilizar.

Hay que destacar en este punto, que un mismo peer (de tipo endorsing o committing) puede participar en más de un canal. En este caso habrá que asignar más recursos al peer para que pueda hacer frente a la operación en diferentes canales.

6.3. ARQUITECTURA PROPUESTA

Para el MVP de Blotick se propone una arquitectura compuesta por dos organizaciones de Fabric, una que actúe como administrador de la red y otra que englobe a todos los usuarios y puntos de venta.



Figura 4 – Modelo de gobernanza de la red para el MVP

Para el MVP se aborda un caso con dos puntos de venta y un número indeterminado de usuarios. Todos los participantes de la red deberán adquirir sus credenciales oportunas para poder operar en la red. Estas credenciales serán emitidas por el administrador de la organización (Certificate Authority, CA) según se detalla en la Figura 5.

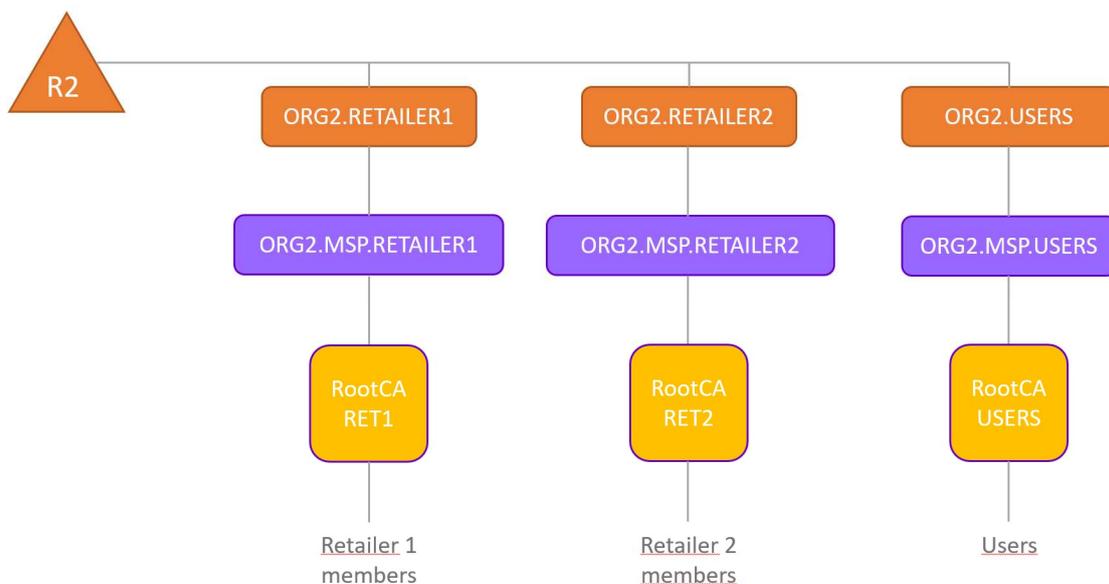


Figura 5 – Estructura de autoridades certificadoras

Una arquitectura provisional completa podría aproximarse a la descrita en la Figura 6. Estaría compuesta por un endorsing peer de la organización que actúa como administrador y dos endorsing peers de la segunda organización, dedicada a la operación de los dos puntos de venta, que comparten el canal 2 para dar de alta los activos digitales que definen los tickets virtuales.

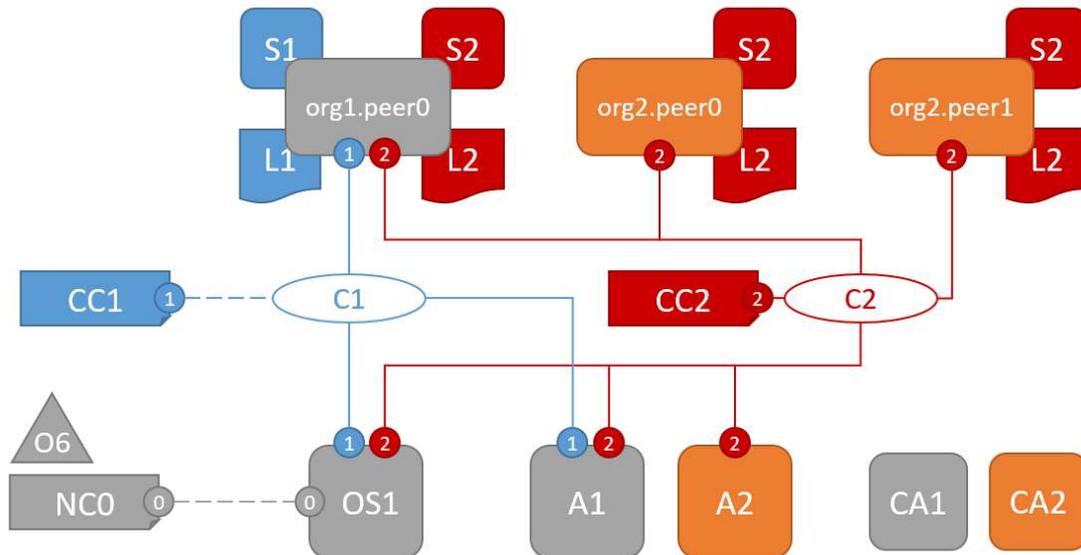


Figura 6 – Arquitectura de Hyperledger Fabric propuesta para el MVP

Leyenda:

- S: Chaincode
- L: Ledger (World State + Blockchain)
- C: Channel
- CC: Channel Configuration
- NC: Network Configuration
- A: Application
- OS: Ordering Service
- CA: Certificate Authority

6.4. INFRAESTRUCTURA CLOUD NECESARIA

Para alojar la arquitectura anteriormente descrita, será necesario contratar un servicio de máquinas virtuales en la nube para que contengan todos los módulos de Hyperledger Fabric necesarios para la operación del sistema (peers, orderers, CAs, aplicaciones cliente...). Esta infraestructura se contratará a un proveedor de servicios cloud reconocido para garantizar la compatibilidad futura con próximas versiones de Fabric. Posibles candidatos para la contratación podrían ser Amazon Web Services, Microsoft Azure o Google Cloud.

Una aproximación sensata con coste moderado que podría servir para el MVP estaría compuesta por cuatro máquinas virtuales basadas en Linux con las siguientes especificaciones de hardware:

- Procesadores de dos núcleos
- 8GB de memoria RAM
- 200GB de disco duro
- No es necesaria capacidad de computación gráfica para esta aplicación

Quedaría entonces determinar la distribución de los diferentes módulos de Hyperledger Fabric en las máquinas virtuales de forma que no se produzca la saturación de ninguna en condiciones normales de operación. Una posible distribución de la infraestructura se detalla en la Figura 7.

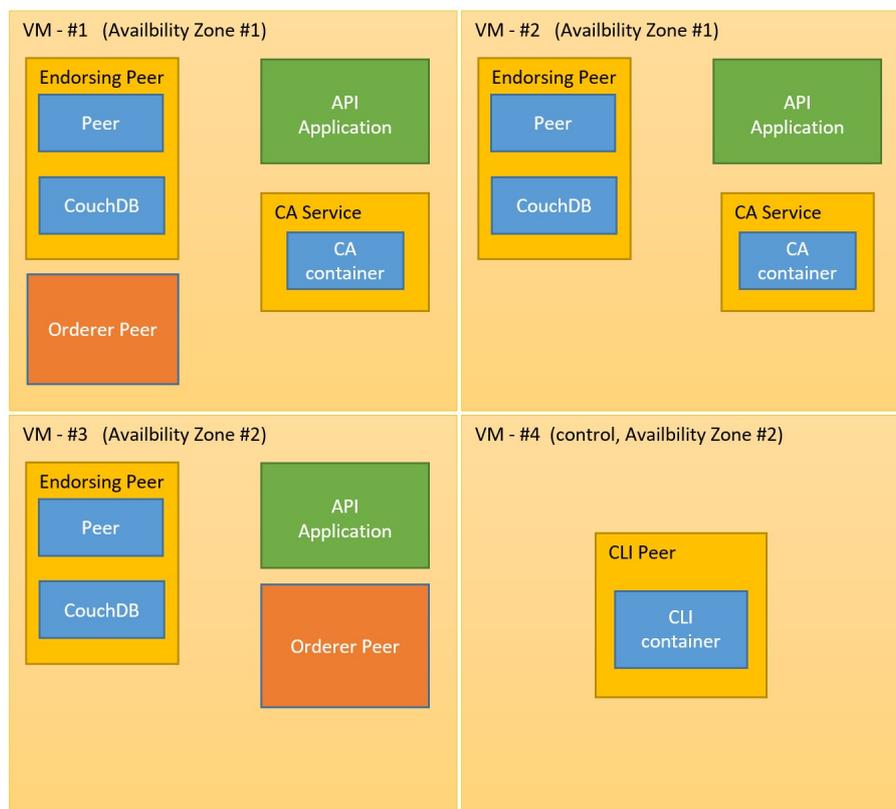


Figura 7 – Infraestructura Cloud y distribución de componentes Fabric para el MVP

6.5. BLOTICK API

El objetivo de la API de Blotick será el de recibir los eventos generados en el punto de venta en el momento de la compra. Estos eventos tendrán una estructura de datos determinada en función del sistema utilizado por cada punto de venta. La API deberá ser capaz de recibir esa estructura de datos, interpretarla, y producir como resultado un archivo de formato de texto estructurado que sirva como entrada a los smart contracts de la red Fabric. El diseño funcional a alto nivel de la solución y cómo encaja en la plataforma a nivel global se detalla en la Figura 8.

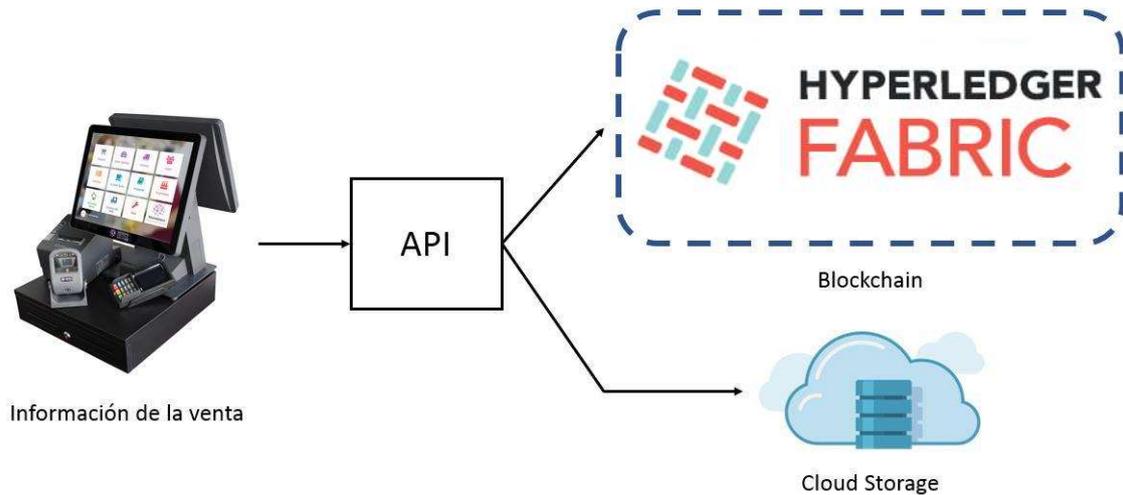


Figura 8 – Situación de la API frente al resto de componentes

6.6. APLICACIÓN WEB

La aplicación web a desarrollar para el MVP será extremadamente sencilla. Únicamente tendrá la funcionalidad de permitir el registro vía correo electrónico de los usuarios y asignarles un identificador en forma de *clave pública*³. Este identificador permite dar de alta al usuario en Fabric, y su representación física será en forma de código QR, que deberá mostrar en el momento de la compra para poderle transferir los tickets relativos a sus productos recién adquiridos.

³<https://es.wikipedia.org/wiki/X.509>

7. BIBLIOGRAFÍA

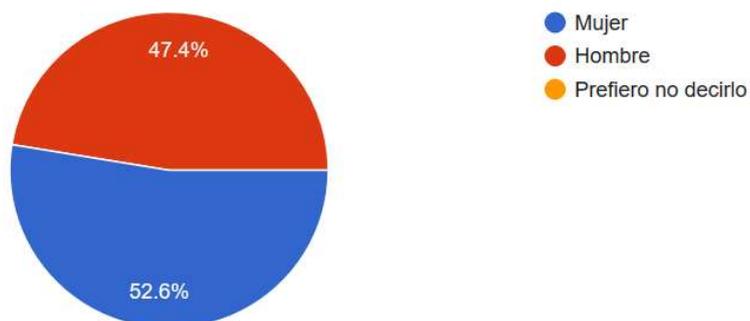
- [RIES11]. Ries, Eric, “The Lean Startup”, Currency, 2011
- [SINE11] Sinek, Simon, “Start with Why: How Great Leaders Inspire Everyone to Take Action”, Portfolio, 2011
- [RABA17] De Rábago Marín, Jaime, “Entrepreneurship Course. Module 2: The Business Model Canvas”, Universidad Pontificia de Comillas, 2017
- [RABA17] De Rábago Marín, Jaime, “Entrepreneurship Course. Module 6: Lean Start-up”, Universidad Pontificia de Comillas, 2017
- [GAUR18] Gaur, Nitin; Desrosiers, Luc; Novotny, Petr; Ramakrishna, Venkatraman; O’Dowd, Anthony; Baset, Salman A., “Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric”, Packt, 2018
- [ANTO17] Antonopoulos, Andreas M., “Mastering Bitcoin: Programming the Open Blockchain”, O’Reilly, 2017

ANEXO A. ENCUESTA CIUDADANA

En marzo 2018 se realizó una encuesta a 251 potenciales usuarios cuyos resultados se detallan a continuación.

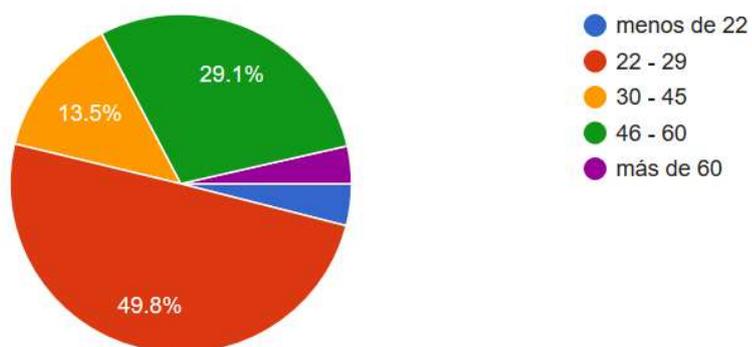
Sexo

251 respuestas



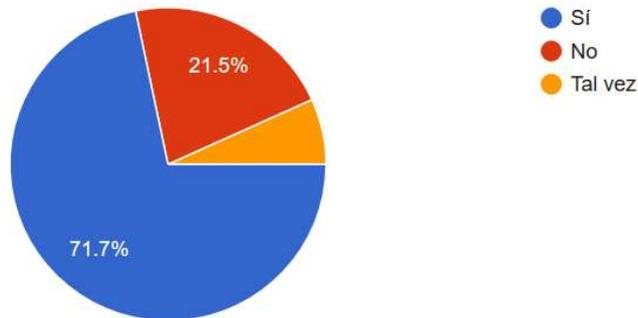
Edad

251 respuestas



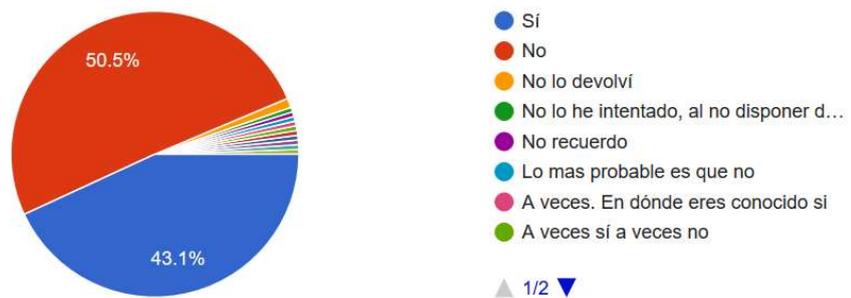
¿Alguna vez has perdido un justificante de compra y has necesitado devolver el producto?

251 responses



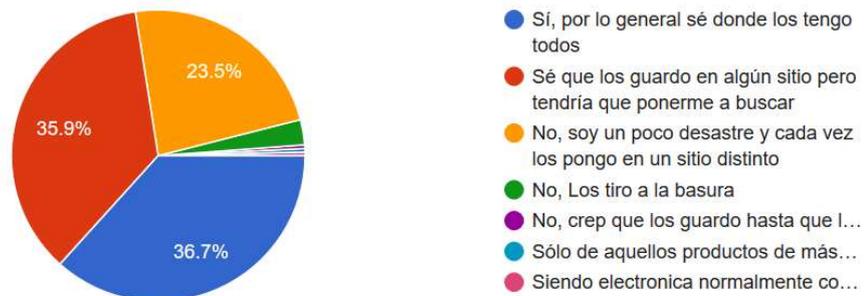
Si respondiste sí a la anterior pregunta, ¿Conseguiste devolverlo?

188 responses



¿Guardas las garantías de este tipo de productos durante más de dos años? ¿Sabes donde los guardas?

251 responses



¿Piensas que el sistema de tickets funciona adecuadamente?

251 responses



¿Usarías una app que en el momento de la compra, te almacenara tus garantías y tickets de forma electrónica? Así no se perderían nunca y te avisaría cuando queda poco para el vencimiento del plazo de devolución o garantía

251 responses



ANEXO B. EQUIPO PROMOTOR

Alejandro Aparicio Blasco

Información personal:

- Teléfono: +34 637509309
- Email: alej.aparicio@gmail.com
- Fecha y lugar de nacimiento: 16/01/1991, Alicante

Educación:

- Master en Ingeniería Industrial, Escuela Técnica Superior de Ingeniería (ICAI), Universidad Pontificia de Comillas, Madrid (2016 -)
- Official Master's Degree in the Electric Power Industry, Escuela Técnica Superior de Ingeniería (ICAI), Universidad Pontificia de Comillas, Madrid (2016 -)
- Grado en Ingeniería en Tecnologías Industriales, Universidad Politécnica de Valencia, Spain (2011-2016)
- Cambridge Certificate of Proficiency in English (C2), January 2016

Experiencia laboral:

- Técnico de mantenimiento eléctrico, prácticas en Fertiberia S.A., Puerto de Sagunto, Valencia (septiembre 2015- junio 2016)
- Investigador colaborador en el Instituto de Investigación Tecnológica (IIT), Universidad Pontificia de Comillas, Madrid (noviembre 2016 – diciembre 2017)
- Business Analyst en everis Digital - Blockchain Team, Madrid, Spain (febrero 2018 - actualmente)

Hugo Garcés Gómez

Información personal:

- Teléfono: +34 697747282
- Email: hugo_g92@hotmail.com
- Fecha y lugar de nacimiento: 11/05/1992, Alicante

Educación:

- New Venture Creation Summer School, Business. Tulane University, Junio 2016
- Master in Business Administration (MBA), Universidad Pontificia de Comillas (2015-2016)
- Grado en Ingeniería Eléctrica, Universidad Miguel Hernández de Elche (UMH) (2010-2015)
- Curso en Energías Renovables y Tecnologías del Hidrógeno, Fachhochschule Stralsund, Alemania (2012-2013)

Experiencia laboral:

- Becario en CIB - Investment Banking en BBVA, Madrid (2016 - 2017)
- Becario en el departamento de M&A en BBVA, Madrid (2017)
- Analista en el departamento de M&A en Indra Sistemas, Madrid (2017)
- Analista Junior en Colliers International Spain Corporate Finance (2017-actualmente)

Enrique Gómez Limia

Información personal:

- Teléfono: +34 608 898 075
- Email: enriquegomezlimia@gmail.com
- Fecha y lugar de nacimiento: 18/05/1994, Madrid

Educación:

- Master en Ingeniería Industrial, Escuela Técnica Superior de Ingeniería (ICAI), Universidad Pontificia de Comillas, Madrid (2016 – 2018)
- Master in Business Administration (MBA), ICADE Business School, Universidad Pontificia de Comillas, Madrid (2016 – 2019)
- Grado en Ingeniería Electromecánica, Escuela Técnica Superior de Ingeniería (ICAI), Universidad Pontificia de Comillas, Madrid (2012 - 2016)
- Intercambio académico en Ingeniería Eléctrica en la Universidad École Polytechnique Fédéral de Lausanne (EPFL), Suiza, (2015-2016)

Experiencia laboral:

- Ingeniero eléctrico, prácticas en Gas Natural Fenosa, Departamento de Innovación, Madrid (junio 2017 - enero 2018)
- Blockchain Product Owner en ioBuilders, Madrid (octubre 2018 – actualmente)

Gabriel de Muguerza Peña

Información personal:

- Teléfono: +34 680738938
- Email: gabriel.de.muguerza@gmail.com
- Fecha y lugar de nacimiento: 16/06/1993, Bilbao

Educación:

- Master en Ingeniería Industrial, Escuela Técnica Superior de Ingeniería (ICAI), Universidad Pontificia de Comillas, Madrid (2016 - 2018)
- Diploma en Modelización Financiera, Wharton Business School, online (2017)
- Diploma en Gestión Internacional, Stanford University, Management Science & Engineering Department, Palo Alto (verano 2013 y verano 2014)
- Grado en Ingeniería Industrial, Universidad de Deusto, Bilbao (septiembre 2011 - junio 2016)
- Grado en Administración y Dirección de Empresas, Deusto Business School, Bilbao (septiembre 2011 - junio 2016)

Experiencia laboral:

- Becario en Alantra Private Equity, Madrid (2017 - 2018)
- Becario en Bluecap Management Consulting (verano 2017)
- Becario en el Departamento de Control de Gestión Corporativa, Gamesa Corporación Tecnológica (2015 - 2016)
- Co-fundador del Club de Consultoría de Deusto (2014 - 2016)
- Ayudante de Investigación en Deusto Global Center for Sustainable Business (2013 - 2014)

ANEXO C. PARTICIPACIÓN EN CONCURSOS DE EMPRENDIMIENTO

Blotick, el ticket inteligente se presentó como proyecto a la categoría Ideando del V Concurso de emprendimiento organizado por Comillas Emprende de la Universidad Pontificia de Comillas, resultando ganador, obteniendo un premio de 3000€ en metálico destinado a la constitución de la sociedad.



Figura 9 – Equipo Blotick. De izquierda a derecha: Enrique Gómez, Hugo Garcés, Moisés Menéndez (mentor), Alejandro Aparicio y Gabriel de Muguerza

Esta oportunidad nos permitió representar a la Universidad Pontificia de Comillas en la X edición del Startup Programme, un concurso de emprendimiento universitario a nivel nacional, en el que Blotick consiguió dos premios y tres nominaciones:

- Premio Visa “Connected Commerce” a la mejor startup de e-commerce, dotado con la invitación a presentar nuestro proyecto en el Visa Day, sesiones de mentoring y un premio en metálico de 1000€.
- Premio Fundación Rafael del Pino a la mejor startup tecnológica, dotado con la participación en el Programa Emtech Internacional en el Massachusetts Institute of Technology (MIT).



Figura 10 – Gabriel de Muguerza durante el pitch de Blotick en el X Startup Programme



Figura 11 – Enrique Gómez durante el pitch de Blotick en el Visa Day

