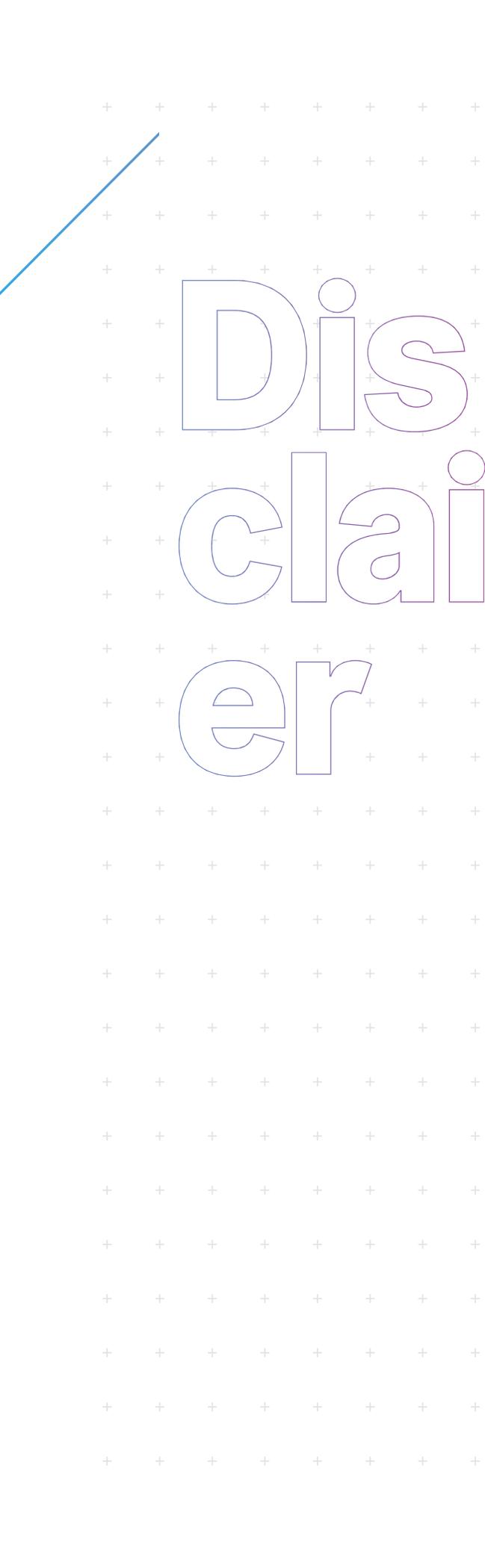


BIDIPASS



White Paper





Disclaimer

Disclaimer

This paper is for information purposes only and is not a statement of future intent.

Unless expressly specified otherwise, the products and innovations set out in this paper are currently under development. BidiPass makes no warranties or representations as to the successful development or implementation of such technologies and innovations, or achievement of any other activities noted in this paper, and disclaims any warranties implied by law or otherwise, to the extent permitted by law. No person is entitled to rely on the contents of this paper or any inferences drawn from it. BidiPass disclaims all liability for any loss or damage of whatsoever kind which may arise from any person acting on any information and opinions relating to BidiPass.

For more information, please visit [this link](#).



Identity is under attack.

Blockchain is one of the most transformative technologies in recent history, a platform not just for distributed hosting and execution of code but for a more equitable future, as well. It's spawned a whole class of utopian thinkers who are sure that the cryptographically secured future will be better and more just than any time that's come before – but there's a problem. Week after week, month after month, blockchain and associated cryptocurrency businesses are repeatedly hit with potentially reputation-destroying attacks, regularly losing cryptocurrencies in the millions or tens of millions of US dollars in value.

The problem runs deeper than crypto-theft, however. There is now a fundamental lack of trust in online services – and with good reason. Are our e-commerce transactions

secure? Are our communications? Taken and counted via connected electronic devices, is even the vote to be trusted?

The inherent concern that connects all of these topics is authentication. The question is how, when we aren't standing in front of our customers and looking them directly in the eyes, can we be sure that we're not actually talking to a professional criminal, or even a bored teenager? How can we be sure that every online interaction is not in fact a breach by malicious actors?

In other words, how do we fix the digital economy?

How do we fix identity verification in a rapidly growing digital economy?

Past solutions have failed.

Attempts to solve this problem have mostly come down to increased password security – but that can only take us so far.

Users are reluctant to adopt strong security practices, and there are plenty of password attacks that ignore the complexity of the password itself. Large-scale data breaches regularly begin by compromising a single users' account, either to steal through this user directly or to use them as a foothold to deeper access.

It has also failed to stop the equally harmful rise of so-called "synthetic identities." These are attacks in which hackers create plausible but entirely fictional identities that are accepted as genuine by KYC services, allowing hackers to interface with an exchange or online store under false pretenses.

The next attempt to fix the problem of online security was the blockchain itself, which incorporated all kinds of encryption and transparency to prevent direct hacking. It has been very successful at preventing these direct cyber-attacks – but thanks to the need for many exchanges to integrate custom user interfaces and so-called "hot wallets," crypto-breaches are common, nonetheless.

How is this possible? The answer, in part, has to do with KYC itself. KYC providers are only as secure as the data that they receive – so if a process can be hacked in the steps between the blockchain and the KYC provider, then the KYC provider might well authenticate an inauthentic user. That sort of mistaken cyber-identity is the crux of a huge proportion of today's cyber-crime. How can we shore up this crucial interface and let the internet get back to its full potential?

BidiPass is the secure, easy-to-use ID verification solution that the whole digital economy has been waiting for, both in and out of the cryptocurrency space.

It leverages the blockchain and its own proprietary BidiKey transfer protocol to shore up the security holes in existing KYC systems. BidiPass doesn't replace KYC as a service, but acts as a platform for accurate authentication of a user's identity during a standard KYC check.

Best of all, this all happens via the user's mobile device, in a quick and user-friendly manner that will finally bring top-tier security to the average internet user. Now, a hacker with access to a user's account can only do so much damage without also having access to that user's mobile device.

It will streamline the authentication process for both users and service providers, ensuring that a platform capable of delivering full digital security can also allow a quick, painless experience that doesn't get in the way of completing a purchase or other form of communication. And since it complements existing KYC infrastructure, BidiPass cannot run afoul of laws mandating use of KYC, nor can it throw a wrench into existing authentication processes.

With an easy-to-use, open source API for quick integration of the BidiPass protocol into any existing app, the choice is simple. Do online service providers want to be able to trust that their KYC provider is always correct? If so, BidiPass is the solution they need.

The
answer
is
here.

BidiPass is...



Fast

Any security measure that introduces hassle and excess waiting will drive users away from the service we mean to protect. BidiPass is dedicated to improving security online by introducing a solution that is quick and truly painless.

By using QR codes and the our proprietary public key encryption scheme, we can validate a connection quickly enough to keep the user on track for their purchase.



Secure

BidiPass uses a patented bi-directional public key encryption scheme that extends an extra layer of security over the traditional KYC validation scheme. *(For more, see p.8).*

By pairing this security protocol to the physical device in a user's pocket and administrating all transfers via the Ethereum blockchain, BidiPass can offer unparalleled security for validation of KYC transactions.



Mobile

Greater security should never have to mean lesser convenience or useability. Unlike many other high-tier security schemes, BidiPass will integrate into your service's existing user flow, in any context. It will never freeze out users based on their device type, or limit their potential use cases.

BidiPass utilizes industry standard mobile technology to ensure that virtually every potential user can become a real user without issue.

BidiPass is the new industry standard for user authentication.



What makes BidiPass unique?



The main driver of BidiPass's unique level of security is the patented bidirectional encryption process.

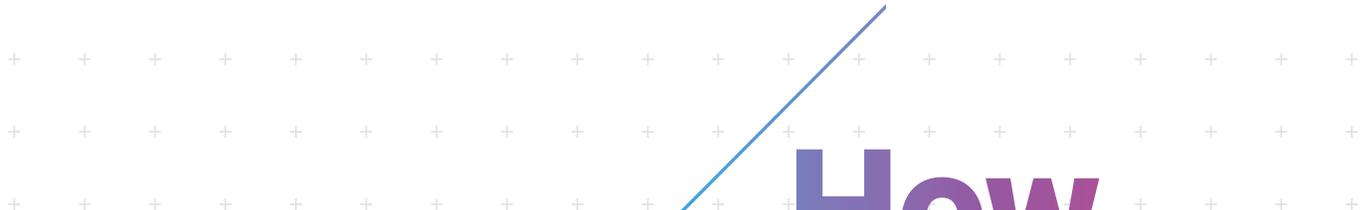
The proprietary approach uses secure, industry-standard elliptic curve encryption in a patented bidirectional process that ensures that you really are dealing with the customer you think you are. This allows total peace of mind about the security of data, both for the service provider and their users.

Unlike existing verification solutions like Civic and TheKey, BidiPass is not a replacement for existing KYC providers, and does not duplicate their user-ID solution. Instead, BidiPass is positioned as a provider of technological infrastructure for verification of queries for these existing ID databases.

To learn more about the proprietary BidiKey encryption process, check out the patent itself by following this [link](#), or by scanning the QR code to the left.

The BidiPass Financial Passport, issued when the user completes the initial BidiPass sign-up process, will be respected by every service provider using BidiPass, no matter where they are in the world. Since BidiPass doesn't interfere with existing authentication structures, but simply enhances them, it will not become a legal issue for existing institutions or startups. By staying out of international legal quagmires, BidiPass should be able to approach fixation in the market.

BidiPass is powered by the Ethereum blockchain. Ethereum has long been the standard for secure, reliable blockchain services. We use the blockchain to administer secure funds transfers in tandem with BidiPass user authentication, which allows the system to be self-sustaining and profitable without charging users – ever.



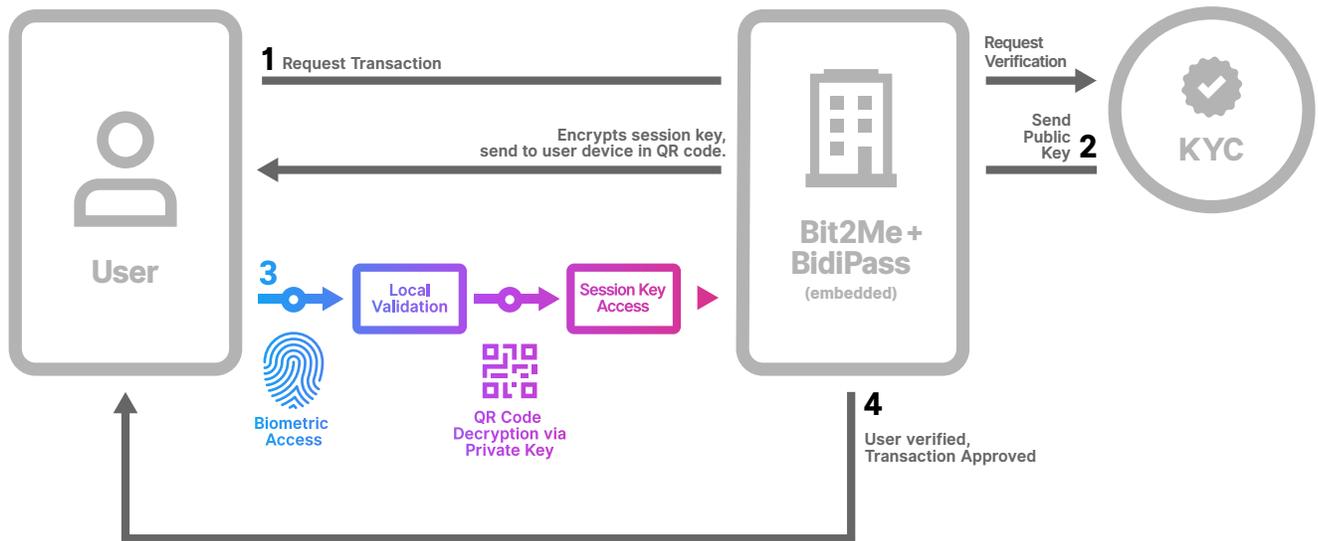
How it works.

BidiPass is a platform for secure authentication of KYC-based personal identification records, protecting both users and service providers from the risks of fraud and identity theft.

The proprietary BidiPass solution, called BidiKey, authenticates existing customer records to validate individual transactions and ensure that only the intended user is granted access.

Thanks to an easy-to-use API, the BidiPass protocol can be quickly integrated with virtually any existing app infrastructure. Anyone from crypto-exchanges to banks to online stores will be able to integrate BidiPass into their codebase quickly and easily, reducing development costs.

How it works.



1

The service provider receives a request for a transaction and looks up the appropriate public encryption key, hosted securely at an accredited KYC provider. Service provider performs function to encrypt a unique session key with this public key. Service provider then displays this encrypted key to the user in the form of a QR code.

2

The user scans this QR code with their mobile device, BidiPass challenges the user with a biometric (fingerprint) security check.

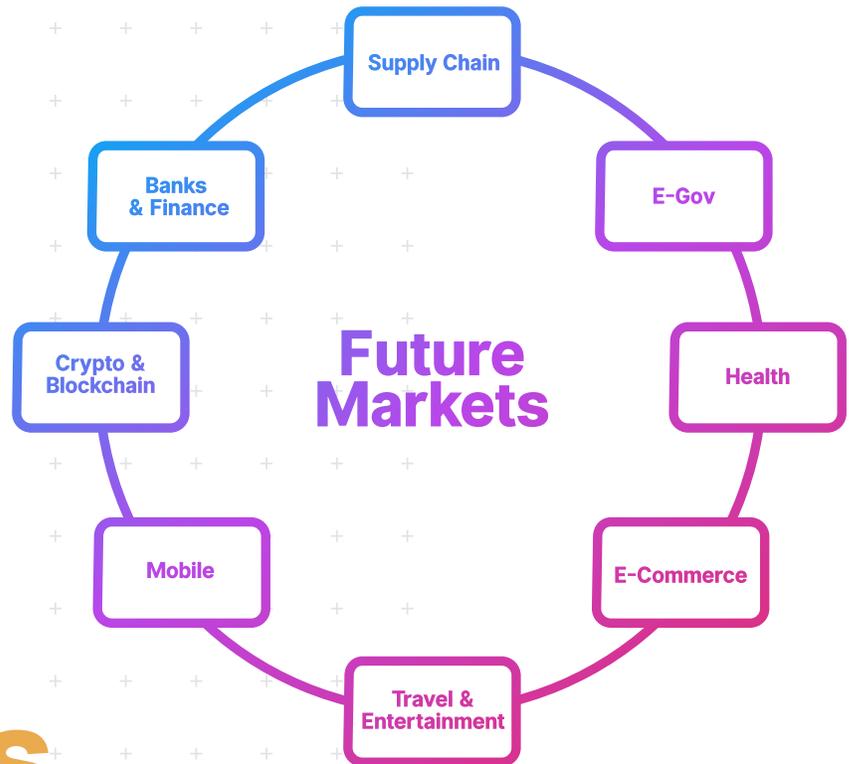
If validated, BidiPass decrypts the QR code with the user's private key, regenerating the one-time session code.

3

Successful decryption reveals the code. Which is input to the service provider page to prove that the user holds the private key.

Confirmed session key input by the user acts as verification of their mobile device, and thus their identity.

Our business model.



The BidiPass model derives from the need for service providers to assure their customers of a high level of data security, without driving those customers away with excessive wait times.

Validation with BidiPass is always 100% free to users, with service providers adding an appropriate number of Ethereum-standard "BDP Tokens" to the regular transaction fee for executing the smart contract. This fee is retained by BidiPass as payment for services rendered.

The eventual target market for BidiPass is the entire online ID verification space – any online service that needs to verify a user's actual identity is a potential BidiPass customer. However, the first focus for marketing and roll-out will be the crypto space, including markets, exchanges, wallets, dApps, ICOs, and more. These services have experienced

a disproportionate number of attacks and attempted thefts, and already do business in cryptocurrencies. Blockchain and cryptocurrency services have the easiest path to BidiPass integration, including exchanges, wallets, and wider blockchain-based services.

Once this foundation of reliable, cryptocurrency-based earnings is in place, expansion to larger and more historically profitable industries like banking and insurance can begin.

BidiPass will also initially focus marketing on the European and Asia-Pacific regions, where the team has the greatest level of experience and can leverage the strongest existing relationships. The American markets will come next, once revenue streams are established.

Collectively, these businesses will be known as the BidiPass Network.

Use Case

Bit2Me

Bit2Me
Cryptocurrency
Exchange

BidiPass has already signed a memorandum of understanding with Bit2Me, Spain's leading cryptocurrency exchange, which already serves customers all over the world. Bit2Me already serves customers all over the world, and every time Bit2Me receives a request for a transaction it must rely on the stated identity of the user – even though anyone could be sitting behind the keyboard. With such rampant user ID fraud, that's a problem. Bit2Me has to trust the integrity of a single login with all of its financial security and the trust of its customers.

With BidiPass, the service provider can make use of the most established and ubiquitous KYC services while still incorporating an all-new, high-security option

for user ID. Having integrated the BidiKey code into their own application infrastructure, Bit2Me can begin to sell itself as the secure crypto-exchange, where even a traditional hacks can't truly bring them down. Providers using BidiPass suffer reduced loss of funds due to fraud, but more importantly reduced loss of customer trust due to the loss of those funds. Again, the most important thing BidiPass brings to its partner services is the ability to maintain the trust of their users in an increasingly perilous online space.

For Bit2Me, these advantages more than make up for the costs of BidiKey, from their perspective. For their users, who never pay for authentication with BidiPass, the choice is even clearer.



**Our
Partners**

bit 2 me

Travala.com



Service providers can incorporate BidiPass into their interface through our user-friendly API. This open-source solution will be both transparent and easy to use, bringing BidiPass functionality to any backend with minimal development time. With the GitHub crowd development platform, we can quickly address any issues with BidiPass that may arise in specific software ecosystems.

The BidiPass protocol is thus a platform for user authentication, across a wide variety of KYC providers and payment systems. By focusing on giving service providers the tools they need to safely interact with customers, BidiPass can facilitate more trust in online interactions. Its distinctive,

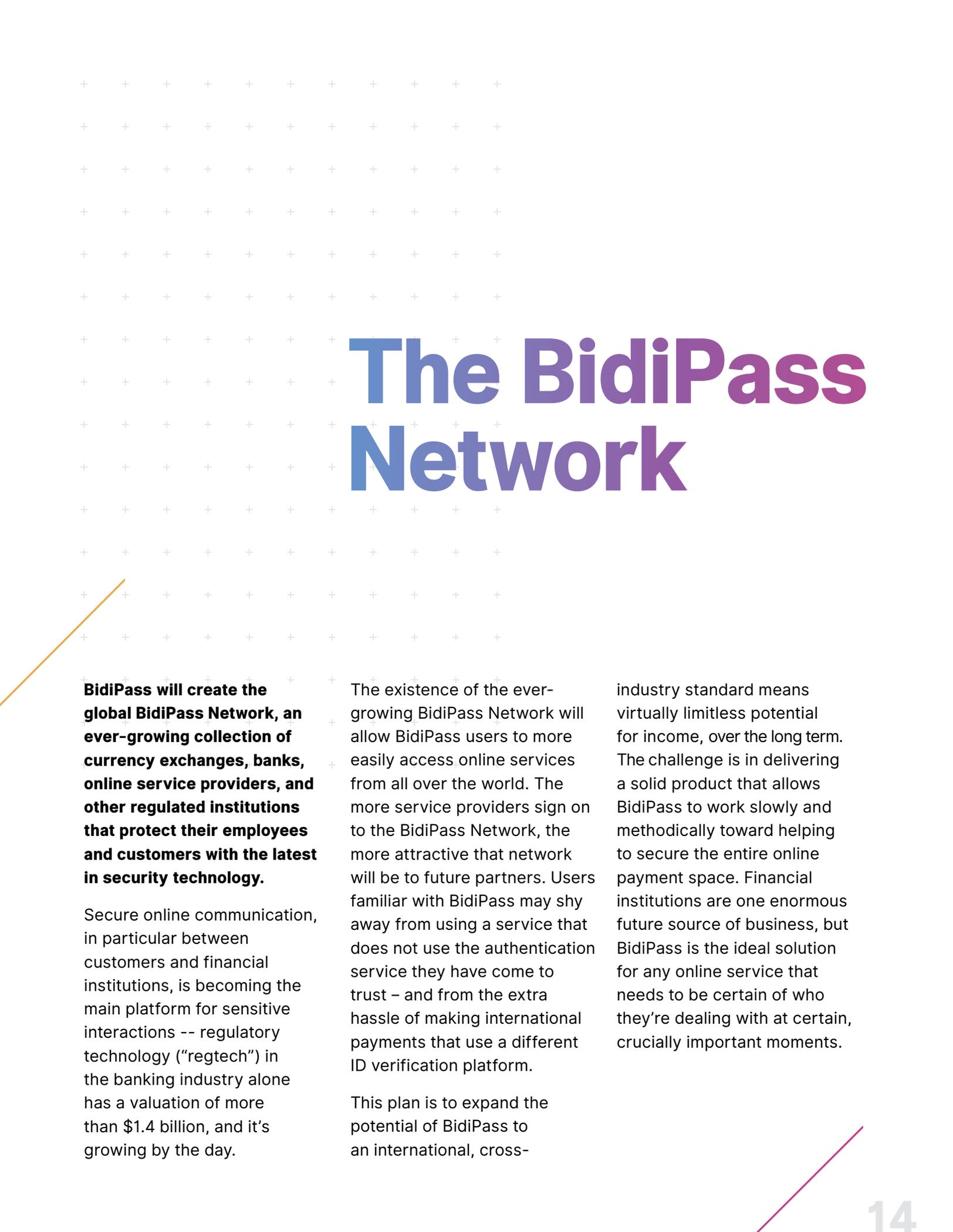
The BidiPass Protocol

QR-code check will be memorable to users, who will associate the process with increased peace of mind.

Much like the CAPTCHA insets of years gone by, a BidiPass insert in an otherwise traditional page will become iconic of a moment that requires increased security, online. Once that happens, those without it may struggle to justify its absence to their users and paying customers.

Service providers who use BidiPass will join an exclusive club: the BidiPass Network.





The BidiPass Network

BidiPass will create the global BidiPass Network, an ever-growing collection of currency exchanges, banks, online service providers, and other regulated institutions that protect their employees and customers with the latest in security technology.

Secure online communication, in particular between customers and financial institutions, is becoming the main platform for sensitive interactions -- regulatory technology ("regtech") in the banking industry alone has a valuation of more than \$1.4 billion, and it's growing by the day.

The existence of the ever-growing BidiPass Network will allow BidiPass users to more easily access online services from all over the world. The more service providers sign on to the BidiPass Network, the more attractive that network will be to future partners. Users familiar with BidiPass may shy away from using a service that does not use the authentication service they have come to trust – and from the extra hassle of making international payments that use a different ID verification platform.

This plan is to expand the potential of BidiPass to an international, cross-

industry standard means virtually limitless potential for income, over the long term. The challenge is in delivering a solid product that allows BidiPass to work slowly and methodically toward helping to secure the entire online payment space. Financial institutions are one enormous future source of business, but BidiPass is the ideal solution for any online service that needs to be certain of who they're dealing with at certain, crucially important moments.

Roadmap

2 0 1 8



- Concept Development
- Patent System Development
- Definition of the BidiPass Protocol



- Development of the cryptographic system
- Development and initial testing of the MVP
- Definition of the Vision for the global BidiPass Network



- Release of MVP Apps on iOS & Android
- Release of MVP API
- Token Generation Event (TGE)



- International Roadshow
- Definition of the smart contract technology platform with built-in KYC verification
- Set up of the BidiPass monetary Policy Board

2 0 1 9



- Rigorous testing on the Ethereum Testnet
- Implementation of the smart contract technology platform with built-in KYC verification
- Expansion to the European and Asia-Pacific regions



- Release on the Ethereum Mainnet
- Version 1.0 iOS & Android Apps
- First implementations of the BDP token powering the Bidipass Network



- Deployment of third party Certification Open System
- Release of version 1.0 of the BidiPass API
- Expansion to the American markets

BDP TOKEN

BDP Token is the crypto-token that powers the Bidipass Network.

The BDP token is:

- An ERC20 standard Ethereum blockchain-based token. BidiPass is based in a secure and trusted software technology.
- The token that keeps all BidiPass transactions running, and which acts as the sole form of payment within the BidiPass Network.
- Extremely straightforward to use. BDP Token is integrated into BidiPass transactions with no extra delays hassle for the user or service provider.
- A form of reward for using the BidiPass Network. Part of all BDP Token fees will be distributed directly to the user whenever they make a transaction using the BidiPass Network. These tokens can then be exchanged for security-related products provided by BidiPass and other Network service providers.

Monetary Policy Goals

1. To reward early adopter and promoters of the network through an appreciating token;
 - Token appreciation should be comparable to the underlying growing market for KYC verifications and digital asset tokenization operations. As this asset class grows, Bidipass' serviceable obtainable market grows as well.
2. To increase the velocity of money for the token in short-run;
3. To ensure that there is sufficient liquidity of BDP tokens on the platform exchange and public exchange;

Monetary policy

The monetary policy of BDP tokens are determined directly by a Monetary Policy Board and indirectly by BDP token holders who are eligible to vote for Monetary Policy Board Members (TCR mechanism) and participate in other list-based referendums. This governance mechanism allows the token economics of the platform to adapt and evolve responsibly and with the input and participation of stakeholders.

The initial board, comprising a minimum of 5 members and a maximum of 9, will be appointed by Bidipass Ltd. prior to the TGE. BDP token holders can vote for board members on an annual basis via a governance module that is available to any token holder. The TCR is deployed when a minimum of 3 mining nodes" second" the TCR. Once deployed, token holders are able to stake their tokens in different smart contract addresses representing different governance decisions.

Token Sale Details

Sale Date:

August 16, 2018

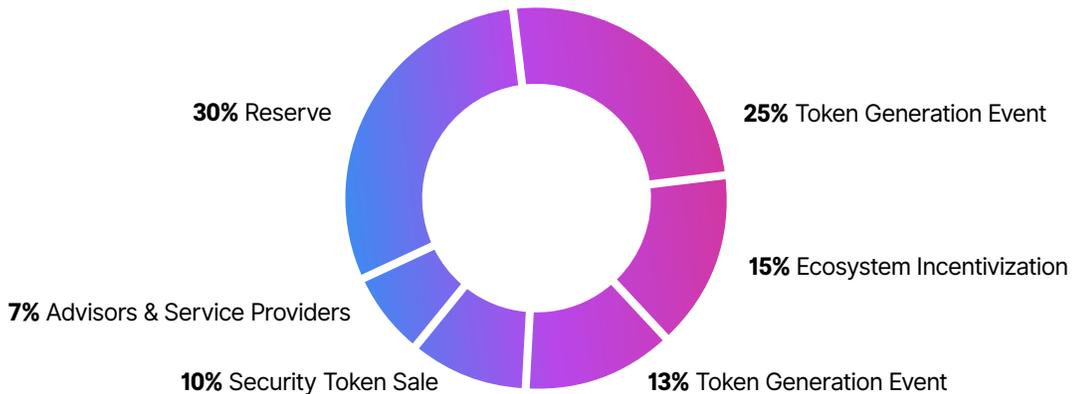
Soft Cap:

\$3,500,000

Hard Cap:

\$16,000,000

Token Allocation

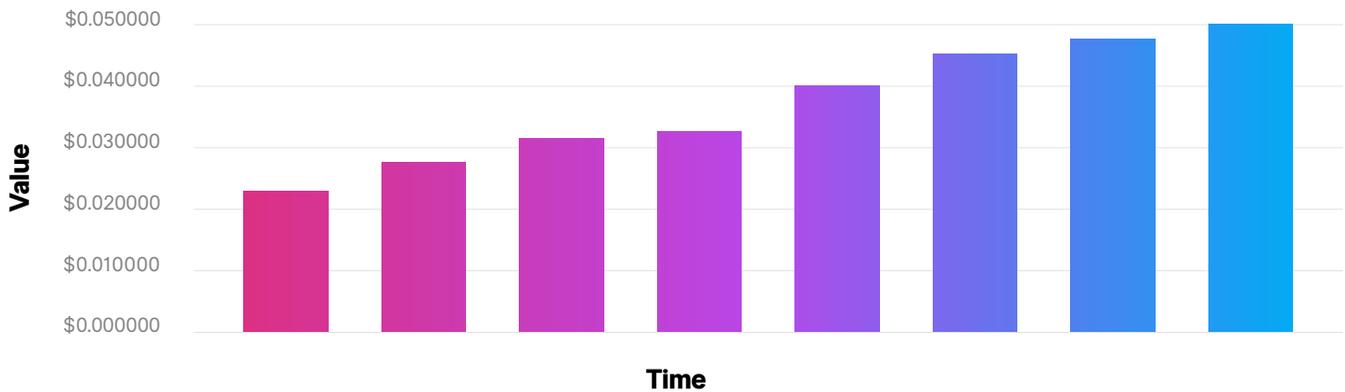


Fund Allocation	
Research & Development	50.0%
Marketing & Sales	27.8%
Reserve	14.4%
Admin & Operations	5.0%
Legal	2.8%

Bonus Structure	
Day 1	25%
Stage 1	20%
Stage 2	12%
Stage 3	5%
Stage 4	0%

Crowdsale

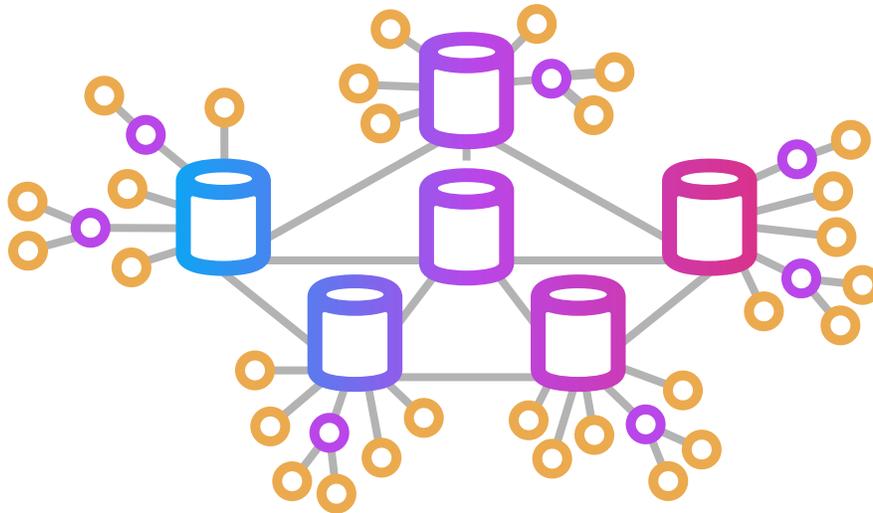
Crowdsale Price Over Time



Crowdsale Base Price	
Security Token - \$500k Bulk Buy	\$0.022500
Security Token - \$100k Bulk Buy	\$0.027500
Security Token - Small (below \$100k)	\$0.031250
TGE - Phase 1 (Base Price)	\$0.032500
TGE - Phase 2 (Base Price)	\$0.040000
TGE - Phase 3 (Base Price)	\$0.045000
TGE - Phase 4 (Base Price)	\$0.047500
TGE - Price	\$0.050000

TGE Discounts					
	<50k (VD)	50k (VD)	100k (VD)	500k (VD)	1,000k (VD)
Phase 1	0%	5%	10%	15%	20%
Phase 2	0%	5%	10%	15%	20%
Phase 3	0%	5%	10%	15%	20%
Phase 4	0%	5%	10%	15%	20%

Token Economics



Economic Agents

○ Users

Following our Airdrop, a User's wallets will contain enough BDP tokens to both register their identity on the Bidipass platform and conduct a handful of verifications.

Users verify themselves via the Bidipass software before conducting a business transaction that requires KYC. This process will require a transaction fee that is a function of the current hash rate (difficulty for miners).

○ Service Providers

Service providers require a means of verifying their user base with KYC, especially certain activities like white-listing or pre-ICO screening. Companies in the blockchain industry ought to pay for the verifications of each User. Service providers are able to bulk purchase tokens to "fuel" the verification of their consumer base.

An API will be made available to deploy tokenized versions of digital assets. These smart contracts will include the balance of the assets and a history of its previous owners. A transaction fee will be required to deploy the asset.

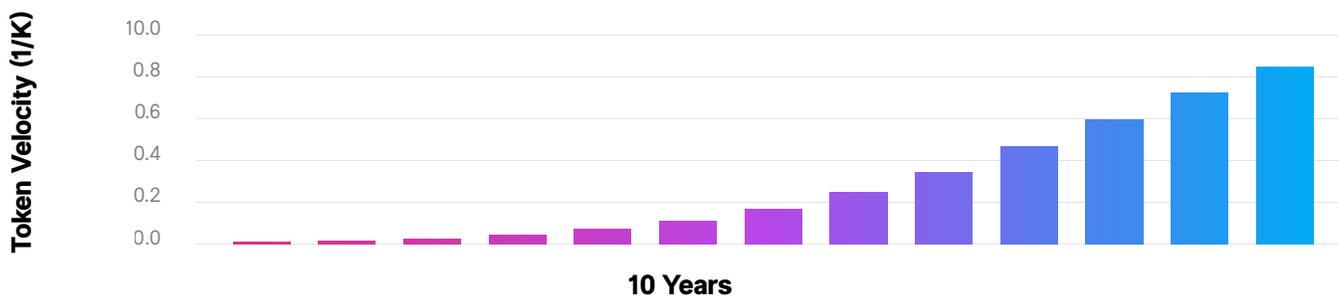
📁 Miners

Miners are incentivized to record all inbound registrations and verifications. Miners not only receive the transaction fees from inbound registration and verification, but will be given block rewards after the successful confirmation of 5 blocks. This Proof of Work scheme holds the Nakamoto consensus algorithm which is also dictated by the mining difficulty rate.

Miners are also incentivized to confirm the creation and deployment of smart contracts and the set of owners following deployment. These transactions are placed within a block and include transaction fees to incentivize miners to confirm and register them on the ledger.

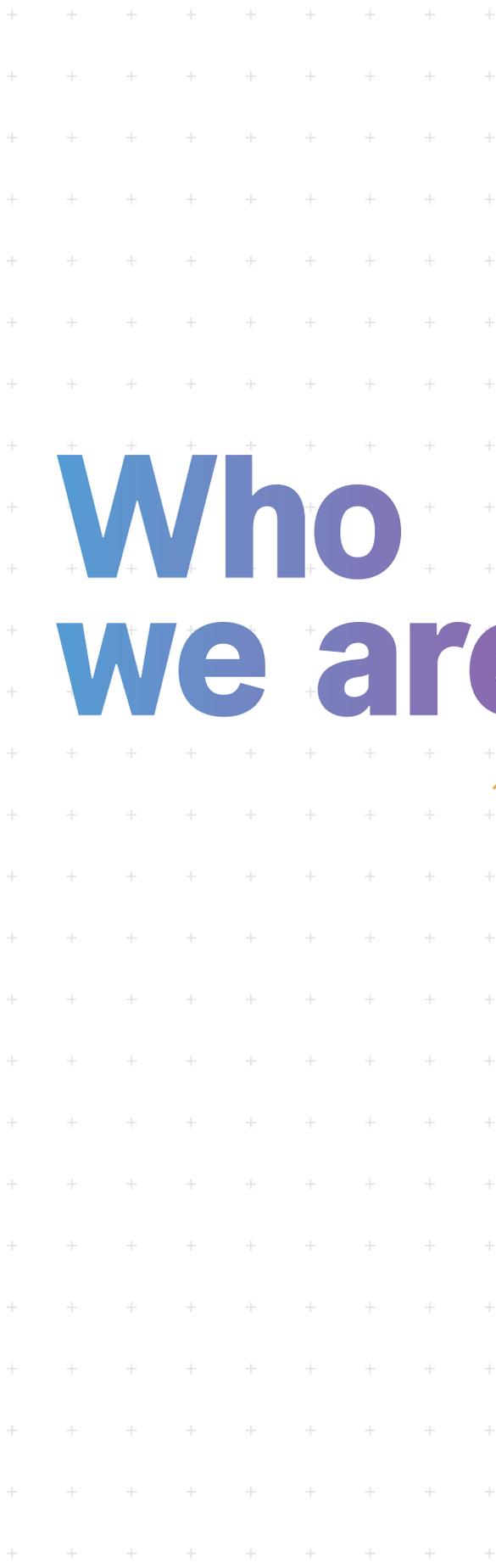
Token Economics

BDP Token Velocity Analysis



Token Usage				
Token Usage	Event Info	Event Type	Token?	Qty.
Identity Registration	Company or user gets issued a private key and its public key pair.	Single	Y	N/A
Identity Verification (SP side)	Service provider (SP) requires identity verification of User before engaging in business transaction. This counts as a transaction a miner has to confirm.	Multiple	Y	N/A
BDP Token Transfer	Network fee (gas) paid to miner to verify a transaction. Ex. Payment of good or service.	Multiple	Y	N/A
Smart Contract Deployment	Creation of a digital asset, governance module (Ex. TCR) , asset trades/swaps	Multiple	Y	N/A
Smart Contract Transaction	Digital transfers, governance participation (Ex. staking in a TCR)	Multiple	Y	N/A

Token Velocity	
Event Type	Target User/ Usage/Year
BDP Transfer	3
BDP Asset Transfer	1
Crypto Asset Wallet Transfer	4
Exchange Transfer	3
ICO Participation	1
Velocity	12
Rounded Velocity	12



Who we are.

The BidiPass team has decades of experience in some of the largest and most competitive tech companies in the world.

Our parent company, LeverIT, has been a successful developer of IT service management for over 17 years. In that time, LeverIT built a strong base of connections with the core institutions of the finance industry, both in Spain and around the world.

BidiPass has taken this foundation of experience in financial technology development and financial sector networking, and combined it with an all new team of experts in advanced cryptography, the blockchain, cyber-security, and token economics. This unique collection of skill sets gives BidiPass a leg up on any potential competitors, who usually enter the space from either a technological or fintech perspective. Since the BidiPass team understands both worlds, we won't be caught off guard by an unforeseen difficulty.

Now, meet the BidiPass team members...

BidiPass Team



Fernando Albarrán / CEO

[LinkedIn](#)

Fernando is a seasoned businessman with 25+ years of experience founding, developing, and leading world-class tech companies in Spain's financial sector. He's that sort of roll-up-the-sleeves, commercially-hardened, tech-savvy professional that a modern startup needs. Fernando serves as CEO at numerous companies, and has managed teams of more than 500 members.



Juan Otero / Chief Strategy Officer (CSO)

[LinkedIn](#)

Juan brings more than 15 years experience with disruptive tech companies. He has previously worked with companies like Sun Microsystems, Oracle, and Booking.com.



Juan José Ruiz / VP Technology

[LinkedIn](#)

Juan José is an experienced businessman from the software industry. For over a decade, he has managed mobile development companies and platforms certified by top BlackBerry, Unity, and Samsung, among others. He has also worked in the development of official Samsung applications for mobile and wearable devices.

Our team is too large to list here – more than 25 members!
To see them all, check out [company website](#).

BidiPass Team



Samuel Izquierdo / VP Operations

[LinkedIn](#)

Samuel lives and breathes blockchain tech. With 25+ years of background as a Coordinator of the Innovation and Laboratory area, Samuel is a veteran technical consultant who has been responsible for anti-fraud and vulnerability alerts. He's now dedicated to fixing the security of the blockchain industry with BidiPass as the all-in-one solution.official Samsung applications for mobile and wearable devices.



Antonio Segovia / Cryptography Engineer

[LinkedIn](#)

Antonio is a software developer with experience in domestic systems coded for Arduino hardware. He has also worked in secure systems that implement two-phased authentications.



Carlos Javier Gutierrez / BlockChain Engineer

[LinkedIn](#)

Carlos has developed several large-scale multilayered, distributed Java applications. In addition to mastering Java, he is familiar with an incredible array of programming languages. Drop him a challenge to tackle with his dev skills portfolio!

Our team is too large to list here – more than 25 members!
To see them all, check out [company website](#).

BidiPass Advisors



Juwan Lee / FinTech Expert Advisor

[LinkedIn](#)

Juwan is a veteran CEO and fintech entrepreneur with 30 years of experience in the financial services and investment industries. He has served as head of equity for JP Morgan and co-founded the Blockchain Center of Hong Kong. Juwan is currently the CEO of Arrakis Ventures.



Santiago Vázquez / FinTech Expert Advisor

[LinkedIn](#)

Santiago is a successful entrepreneur, investor, and innovator. Over several decades, he has participated in the tech, telecoms, private equity, and e-commerce industries. Santiago has also worked as an investment banker and as a financial analyst at the prestigious Banco Santander.



Keith Teare / Blockchain Engineer

[LinkedIn](#)

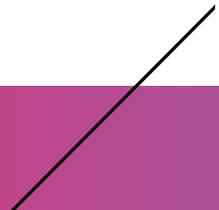
For over 30 years, Keith has built successful tech companies. He is currently executive chairman and Chair of the Investment Committee at Accelerated Digital Ventures.



Alexis Kirkia / Blockchain Expert Advisor

[LinkedIn](#)

With a background in the aviation industry, Alexis co-founded the crypto-market making firm GSR. He is an avid advisor to blockchain companies and tokenization projects.



**Thank
You**



 BIDIPASS

