xBOUNTY

A Decentralize Blockchain to Reward Anonymous Tipsters

White Paper version 1.2 Dallas, TX 2017

ABSTRACT

XBounty is an anonymous tipster service that allows tipsters to maintain full anonymity while performing the life-threatening act of providing the right information to law enforcement, helping them solve a crime whilst also being able to collect bounty in total anonymity and protection of their privacy and from harm.The platform is based on a decentralized zero knowledge blockchain service that is optimized for use by non-programmers.

The Problem

Crime reporting by eye witnesses or by individuals with knowledge of the crime and the culpable individuals involved in the crime is at its lowest across the world and in the USA in particular. Most crimes although, having very much key witnesses, often go unreported and for various reasons such as threat to life of the concerned, or the threat to life or business of the friends and family of the concerned (Witness).

Following unresolved crimes, police departments, the FBI or other crime fighting unit, often rely on the help of their local citizens and communities for case-making tips and information to make progress. Different methods are created to incentivize people coming forward and sharing valuable information. News channels and police websites offer crime hotline numbers and promise anonymity. For serious crimes, cash rewards may be offered. In one case, a police department published billboards asking for tips in a child murder case. Some Police Department has as well taken a more direct route of personally visiting the affected neighborhoods to distribute flyers and solicit information from locals. Despite these outreach efforts, many crimes still remain unsolved without adequate evidence.

The scale of the challenge can better be appreciated when viewed from the lens of the amount of losses incurred, immeasurable human and great financial losses running into billions of dollars. In the USA alone, according to the FBI's UCR (Uniform Crime Reporting 2015) there was an increase in violent crimes and property crimes which resulted in 14.3 billion dollars in losses. This is not taking into account the cost of Cyber Crimes, Human Trafficking, White Collar Crime, Drug Dealers, Missing Peoples, Terroristic threats and Public Corruption that are on the increase and are quite recurring.

The world over, the menace of crime can be put in check by a community willing to play a greater role in ensuring a crime free environment for themselves by providing valuable information to law enforcement. Especially in severe cases where bounty has be declared, a community can play a crucial role in catching criminals and preventing crime, but only if citizens speak out. According to an Accenture survey, 88% of citizens across six countries believe that citizens are important participants in crime fighting and reporting crimes is a key role for citizens in police services. This large number can make all the difference if given the right platform to play a greater role.

The Solution:

Xbounty is a decentralize platform to keep the anonymous tipsters in full anonymity. It is use to reward a solution and to protect the tipsters.

In spite of the efforts of the police in its Crime Stoppers campaign and bounties for terrorist, solicitation for information on crime has yielded very little result. Many individuals are unwilling to come forward to claim bounties on crimes they have knowledge of, most times, foregoing the bounty due to mistrust of the government and the uncertainty surrounding the award of the cash bounty. Depending on the nature of the crime, some police precinct and the FBI would often offer bounties for information leading to the arrest of prime suspects or a fortuitous break in the case. They use rewards as a tactic to squeeze information out of informants yet leaving them empty handed. What **xBounty** does is to guarantees **true** anonymity and **true** bounty amount.

By developing the **xBounty** platform, Police officers, Federal agents, Teachers, and community members would set an amount of Bounty and offer bounty tokens to the anonymous tipster by using a decentralize BlockChain and smart contract to execute the payment.

Our BlockChain DAPP is a completely decentralized system which includes the tools necessary to create smart contracts, as well as its our own cryptocurrency token **xBounty** which is needed for those contracts to work.

Smart contracts are digital algorithms which describe a set of terms, which are automatically fulfilled by the **xBounty** network. They enable law enforcement (the FBI and the Police) and informants to enter mutually agreed contracts with each other without having to worry about the default on the part of either of the party. The purpose is for the informant to provide valuable intel on unresolved case, and get paid the bounty if their information leads to the arrest of the criminals.

xBounty is a platform used to mitigate and escrow the transactions from the **rewarders** to the **tipsters**. The rewarders would set a bounty on **Xbounty** DAPP and the anonymous users would reply with a tip. Once tip is confirmed positive and the problem is solved, rewards would be released by confirmation and smart contract of both parties. **Xbounty** would then hold the bounty in escrow via smart contract to be transparent among the XB Scan in the BlockChain.

The terms of a smart contract are established before the offer is made. Then their fulfillment is ensured by software code without human interference. Thus, the smart contract technology represents an ideal tool for low-risk deal-making, maintaining full anonymity of all parties involved. This is outlined and executed by program code and the contract between the counterparties can be fulfilled or broken only in accordance with the originally established terms.

Due to the technological specifics of the blockchain - the distributed database where the smart contract is stored - any interference aimed at changing the terms of the deal after it has been signed is nearly impossible.

The **xBounty** smart contract works as an “escrow agent”, a sort of bank cell, where the terms of the deal and the money (cryptocurrency) are stored until the contract is fulfilled.

Xbounty is made to disrupt all criminal enterprise. We plan to be the Uber of Anonymous Information.

Our solution ensures full anonymity for the informants and we ensure that they are duly compensated for their information which leads to a break in any case that requires the public’s assistance.

The advantages of our solution

xBounty platform offers a range of advantages compared to the traditional ways of soliciting for information from the general public;

1. There is guaranteed full anonymity of the **tipster** and this will allow for confidence to share valuable information that can lead to the solving of a crime. The platform ensures that rewards and compensation which are duly earned are disbursed to the deserving **tipster**. The terms of the contract are established before it is signed and are stored on the BlockChain and it is impossible to change its terms after both sides have agreed to them. The contract can only be closed or broken according to the original arrangements.

2. All transactions on the **xBounty** platform are made with the use of **xBounty** token and this completely eliminates all barriers to payment. The absence of an intermediary, such as a bank, makes the counterparties free from unnecessary oversight procedures and removes the possibility of a payment cancellation due to an external decision.

Another advantage of using cryptocurrencies for payments is the fact that the process of signing a contract and paying for it are inseparable. Launching a contract requires the presence of the sum of money which the counterparties have agreed on. After that the money can only move according to the terms of the contract.

Advantages over existing alternatives

At the current moment, alternative BlockChain-based, integrated platforms for providing this same service to law enforcement do not exist.

It is possible to use the **xBounty** BlockChain to create smart-contracts manually, however that requires programming skills, or incurs the additional cost of hiring a programmer.

There are also a number of services, which allow non-programmers to create smart contracts with the use of a simplified interface. But these services cannot be considered integrated platforms for services such as this, because they do not offer the guaranteed protection of the individuals.

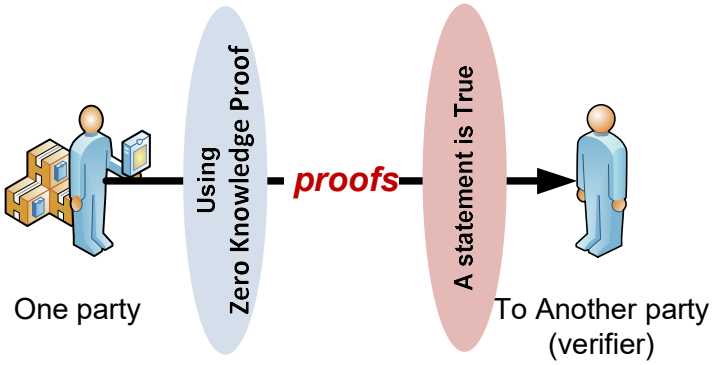
The Architecture:

Three eclectic structure to xBountys utilization of **zero knowledge proof**

1. The **Anonymous Tipsters**(informants, witness, victims, users)
2. The **xBounty** BlockChain platform which is to broker and keep the tipsters anonymous.
3. The **Rewarder** (FBI agents, Insurance Fraud units, Teachers etc)

What is Zero Knowledge Proof?

➔ It is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true [1][2][3][4][5].



Zero-knowledge proofs

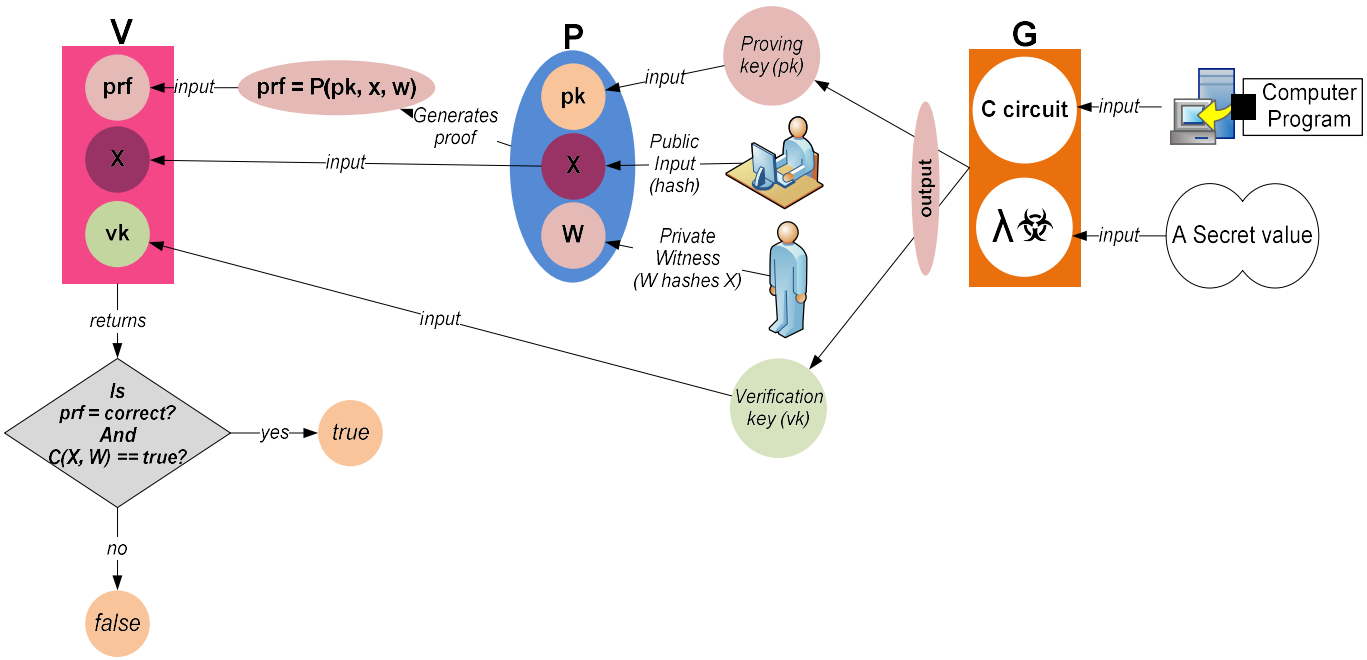
This is for a verifier to be able to convince herself that a prover possesses knowledge of a secret parameter, called a witness, satisfying some relation, without revealing the witness to the verifier or anyone else.

zk-SNARK is the sample program of Zero-knowledge proofs
It consists of three algorithms G, P, V

- The key generator G takes a secret parameter lambda and a program C, and generates two publicly available keys, a proving key pk, and a verification key vk.
- The prover P takes as input the proving key pk, a public input x and a private witness w. It generates a proof prf = P(pk, x, w).
- The verifier V computes V(vk, x, prf) which returns true if the proof is correct, and false otherwise. Thus this function returns true if the prover knows a witness w satisfying C(x,w) == true.

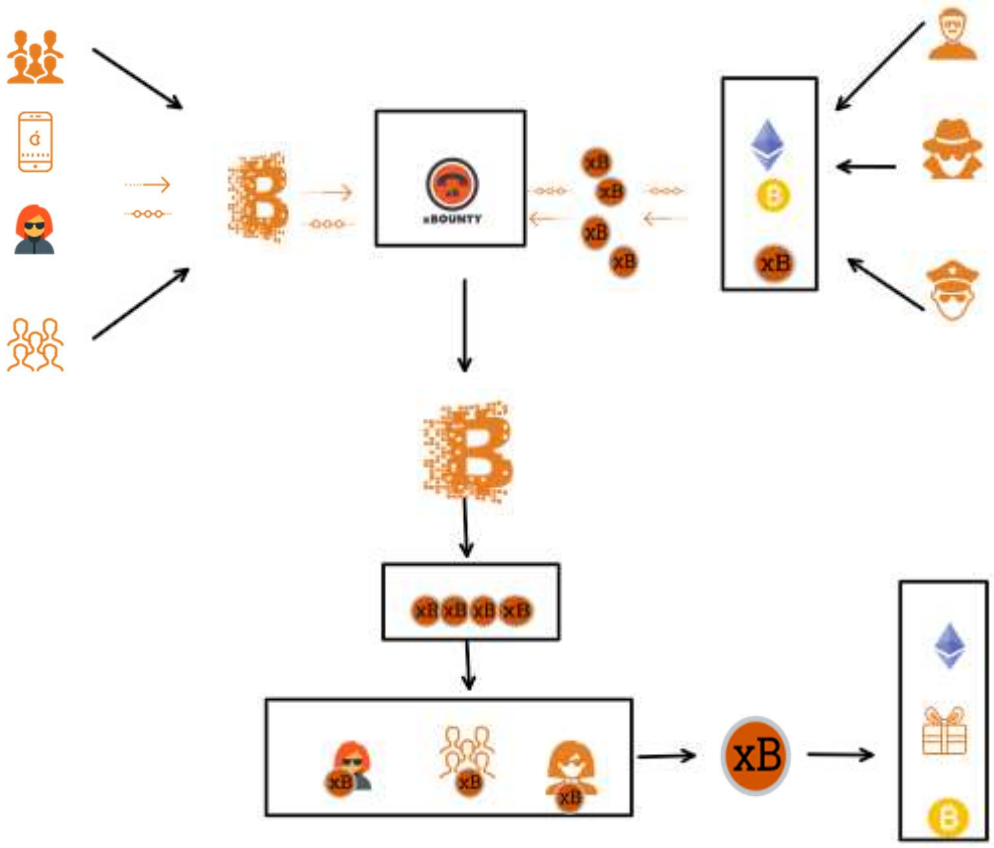
Risks

If anyone knows the secret parameter (Lambda) can generate fake proofs. Specifically, given any program C and public input x a person who knows lambda can generate a proof fake_prf such that V(vk, x, fake_prf) evaluates to true without knowledge of the secret w.
Thus actually running the generator requires a very secure process to make sure no-one learns about and saves the parameter anywhere.



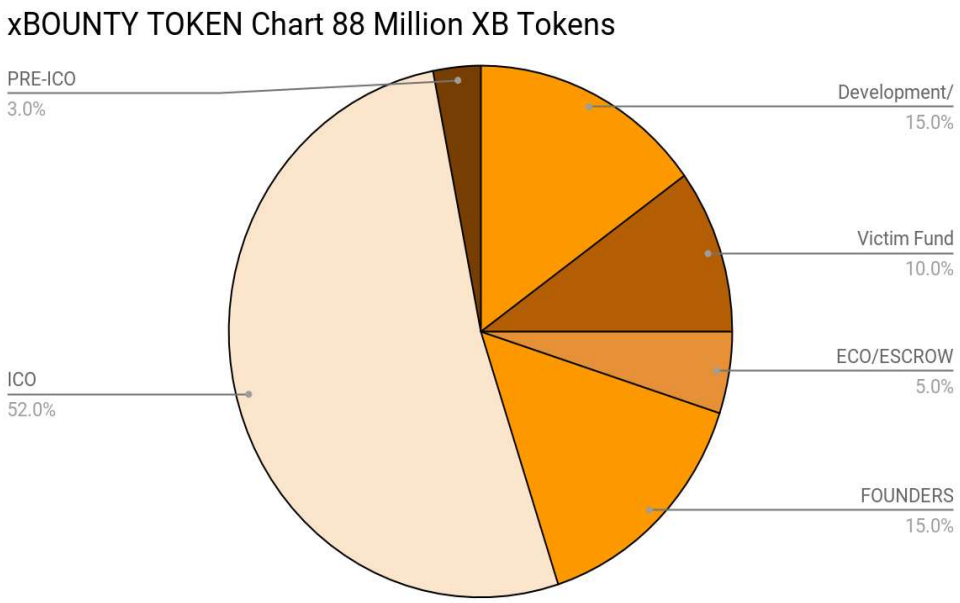
Generator (C circuit, λ is ☣): (pk, vk) = G(λ, C)
Prover (x pub inp, w sec inp): π = P(pk, x, w)
Verifier: V(vk, x, π) == (∃ w s.t. C(x,w))

Simplified Diagram



Basically, **xBounty** is a platform used to mitigate and escrow the transactions from the **rewarders** to the **tipsters**. The rewarders would set a bounty on our xbounty DAPP and the anonymous users would reply with a tip. Once tip is confirmed positive and the problem is solved, rewards would be released by confirmation and smart contract of both parties. **Xbounty** would then hold the bounty in escrow via smart contract to be transparent among the blockchain.

Token Allocation:



88,000,000 XB TOKENS

Fundraise	52%	45,760,000
Development/ Foundation	15%	13,200,000
Advisors/ Founding Team	15%	13,200,000
Victims Foundation	10%	8,800,000
Miscelleneous Cost/ Escrow	5%	4,400,000
Early Adopters	3%	2,640,000
Total	**100%**	**88,000,000**

Pre- Seed Investor

Total XB Token for sale	2,640,000
Discount	40%
XB Token Per ETH	1400
Total Eth Raise	1,886

Allocation	Tokens	Discounts	XB Token	ETH Raise
25%	11,400,000	20%	1200	9,533
25%	11,400,000	10%	1100	10,400
25%	11,400,000	5%	1050	10,895
25%	11,400,000	0%	1000	11,440
100%	**45,760,000**		**ETH Raise ICO**	**42,269**

The purpose of the token allocation is to have our own currency(**XB**) in which **XB** tokens would be rewarded to the anonymous tipsters or solution solvers. **XB** tokens then could be traded into prizes or cryptocurrency. **XB** tokens can be bought with Ethereum or Bitcoins. **Xbounty** would then take a 3% cut on all XB rewarded to keep the ecosystem and pay for marketing and operations. If problem is not solved, **XB** Tokens would be refunded to the rewarders.

- 52% ICO is schedule to start right on New Year's day 2018.
- 3% Pre-seed will be announced
- 15% will be spread to early adopters, founders and investors
- 20% of tokens will be held in escrow for operations and marketing
- 10% will be held in a trust to help Victims of crimes

Our minimum goal for the Token Sale is to sell 25,000,000 **XB** Tokens and Raise 15,000 Ether.

Future Plans:

From a simple service for getting anonymous tipping and helping to provide a safe environment for all to thrive, we plan to turn **xBounty** into a full-fledged security awareness platform which will solve a number of unresolved cases plaguing the security agencies.

The platform's further development will include the following steps:

Hellenistic **White Paper, Pre-ICO, ICO**

Matrioshka

Stage 1 **Development, DAPP in full production** **Q1 2018**

Stage 2 **Utilize by Crime Stoppers, FBI, Police stations across America, Insurance companies, Public schools in America, Colleges and universities** **Q2 2018**

Stage 3 **In partnership with the International Criminal Court** **Q3 2018**

Stage 4 **Globalize platforms to work with law enforcements throughout the world** **Q4 2018**

Topopolis

Stage 5 **Projected to be profitable by partnering up with world anti-criminal enterprises, this platform would be used worldwide to combat criminal activities and to keep humanity in check** **Q1 2019 and Beyond**

Elysium

Team:

Chuck Yang - **CEO, Founder**

Opinder Preet - **Head Blockchain Developer, Towards BlockChain Inc, New Dehli**

Jittendra Chittoda - **Blockchain Developer**

Pushkar- **Government Blockchain Developer**

Manvita Vempati- **Big Data Analysis, Solidity**

Advisor - **James Wealthy, Tech Investor**

Advisor - **Jeff Hoffman, Founder of Priceline**

Future Full time positions include:

- Chief Operating Officer (which will include compliance and legal)
- Chief Marketing Officer
- Chief Technical Officer (responsible for security)
- Business Development and strategic partnerships
- Marketing support
- Development positions
- Customer Support
- Chief Financial Officer
- External Marketing and PR
- Legal counsel
- Company secretary

References

[1] Blum, Manuel; Feldman, Paul; Micali, Silvio (1988). "Non-Interactive Zero-Knowledge and Its Applications". Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988): 103–112. doi:10.1145/62212.62222.

[2] Wu, Huixin; Wang, Feng (2014). "A Survey of Noninteractive Zero Knowledge Proof System and Its Applications". The Scientific World Journal. 2014: 1–7. PMC 4032740 Freely accessible. PMID 24883407. doi:10.1155/2014/560484

[3] Manuel Blum, Paul Feldman, and Silvio Micali. Non-Interactive Zero-Knowledge and Its Applications. Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988). 103–112. 1988

[4] Oded Goldreich and Yair Oren. Definitions and Properties of Zero-Knowledge Proof Systems. Journal of Cryptology. Vol 7(1). 1–32. 1994 (PS)

[5] Shafi Goldwasser and Yael Kalai. On the (In)security of the Fiat–Shamir Paradigm. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS'03). 2003