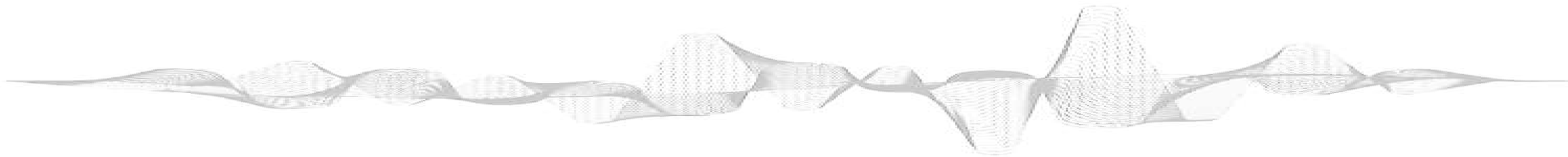
PINGPAS.com

intro pitch deck *08.09.2019v1*

For:

user security & authentication, strong cryptography, use *everywhere*



Michael Chung

chungmojo@gmail.com

PingPas has patent-pending technical and use-case innovations in the art and technology of data-over-sound and for its Phase 1, it is answering the questions --- why at this stage of tech are we still typing in our passwords and 2FAs, or inserting the USB-security keys in and out, or telling the bank rep our PIN or SSN when we are on the phone with them, and BTW, if our phones act as 2nd factor hardware for our laptops and PCs, then what is the 2nd factor hardware for our phones?

Stage and activities: Pre-funding, company is DBA, business plan and new patents applications being written, is patent pending, basic prototyping and design stage (no fundamental technology challenges, mostly design work), domains, trademarking, pingpas.eth and pingpay.eth, co-founders identified and ready, SBIR Phase 1 grant applications, etc.

PINGPAS™ (Phase 1) – the Problem, the Why, and the Answer

1. **Problem: The current user security and authentication process is "20th cent. and dated".**

   1) We are asked to lookup or remember, **2)** then type in the passwords, two-factors, or one-time passwords (OTP), **3)** into a machine that maybe key logged, **4)** or to get the token from a phone or from the SMS channel that may be unsecure, **5)** and if we are doing the two-factor authentication (2FA) on the phone, then it is extra difficult, **6)** NFC and Bluetooth have left huge gaps in security and user experience (user experience friction equates to no security or risky habits).

2. **Why: The reason is - we are using the wrong communication technology for proximity.**

   The radio spectrum technologies of NFC, Bluetooth, Wifi, and LPWAN, and the security keys (the USB or one-time token generators) – are not ideal to be the workhorse for the user security or authentication uses. The Bluetooth is vulnerable; NFC and RFID are not for challenge-response; and we have to plug in and out the USB keys and really is not suitable to be used with the mobile devices.

3. **Answer: Nature shows sound is the best – ad-hoc and near ubiquitous, and a single security *solution usable "everywhere" at home, office, or person* -** communication for proximity, with extra benefits for even interspecies uses, whether organic or digital!




The Competitive Overview:

5 companies (in the Competitive slide) are providing Data-over-sound SDKs. They started around 2013 and are collectively funded to about $40M. They are focused on the smartphones as the solution-platform and business models are to license their solutions. PingPas is focused on the fob-device as its solution-platform, although it will also have software for the phones. Also, its focus is on targeting directly the problems and market opportunities that it has identified. There are 3 notable and independent markets. **Phase 1 and 3 are disclosed, Phase 2 is stealth.**

2 other notable companies are directly targeting the payment space. Google Pay launched in India in Fall of 2017 by swapping out their QR codes and replacing with sound. (Google white paper.) ToneTag (India, $10M funding) is the largest independent company; based in India. There have been/are couple of others in payment space.

The industry is re-visiting data-over-sound because we now know after many years and huge investments, what "the NFC, Bluetooth/Beacons, WiFi can't do"; and data-over-sound is open. **PingPas discoveries advances the art.**

Our History:

We started in 2017 by exploring the use of LED (visible and infrared) based tags and badges for tracking and identification where the phone camera or webcam and app would identify the tagged object or badge wearer on a live video and the overlay their information (e.g. name and title in a "bubble" on top of the identified tag in the live video). The founder wanted something that could also work in outdoors and without the need for a LED dongle (for infrared).

We then explored ultrasound for data communication. We first targeted cryptocurrency and to build the first crypto currency point-of-sale network. **Then, looking for faster go-to-market, we found the proximity-security ("sonic-YubiKey"), then other disruptive/breakthrough uses for "over-the-air data-over-sound"**

Sound re-purposed, and the creation of a new “nearby communication” protocol.

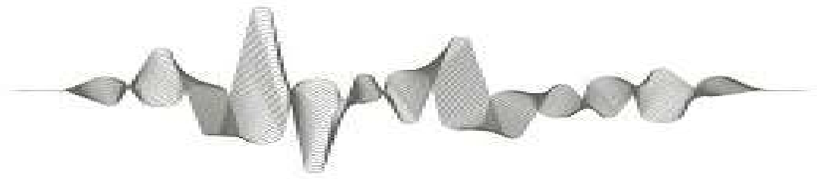
No matter how far we roam, we will always have sound, here’s to lookin’ - at sound, again.

We have:

- A communication solution for where the radio spectrum don’t go.
- Solved the friction of remembering and typing passwords, 2FAs, and secrets, especially on mobile.
- Discoveries to power new products and services in several industries.
- Innovative over-the-air data-over-sound based solutions and approaches, some which are delightful, to solve several important gaps and create new use cases and demand.

We are:

Creative, inventive, expert technologists, with business experience, and have made fundamental discoveries that enables 3 independent market – venture opportunities.



Company Purpose

PINGPAS™ will use its innovations and advances in data-over-sound to solve – universal problems and user frictions and fill critical solution gaps in - the current user security and authentication practices.

The Phase 1 market opportunity is nearly the entire “general passwords and 2FAs use space”. There are two additional and separate large emerging market opportunities for Phase 2 and 3.

Why Now? User-security is the biggest unsolved pain

The Phase 1 Opportunity and a Big Real Problem to Target.

It's 2019, why are we are we "still remembering and typing-in" our credentials?

…and for our 2FA, we have to: 1) open the Authy app or the OTP token fob; 2) look for the token-code; 3) then manually type into the web form or the app; and 4) and finally, that the hardware that we rely on for security, the **phone, itself is not secure.**

At this stage of the digital era, **we really don't want to keep typing, need to buttress the security of the phone with a separate hardware security-device, and we need an alternative to biometrics.**

And as a bonus: For the coming Voice-UI era – sonic is the ideal solution, and which also has strong-security and the challenge-response signing capabilities.

The Solution – a data-over-sound communication fob-dongle

Use a separate device to transmit the password, the 2FA, token, or secrets to the challenger – whether it's the phone, laptop, a browser, an app, or CRM rep. This is just the beginning, we have several more key use cases in stealth.

Over-the-air **data-over-sound communication, featuring: separate hardware, "quantum proof" security, air-gapped and no contact, challenge-response capable, unlicensed band, uses the "largest existing installed infrastructure", and "one-click".**

The least cost and energy to get the user-truth; & onto the DLT

What we are really solving (in Phase 1) is to have level 4 security ubiquitously at least cost:

1) The fastest way, and the least amount of energy consumed - whether at the user's behavior and cognitive level or machine to machine – for the user or machine to authenticate to the a) challenging local client, or b) to the challenge network. (Option: Even if no network or power outage, we can use piezo energy generators to store power for local clients to talk.)

2) And, because our truth is using strong security (up to level 4), we can write each such event to the Distributed ledger - thus, the path of least energy, the most cross-platform, and least cost.

Use case "n": Delivery robot drops off package and talks to door app. Door app pays robot. Both the drop and payment events are written to the blockchain.

- No need for NFC, Bluetooth, WiFi, LPWAN, or any other FCC licensed or standard communication protocols. They talk over-the-air using the most cross-platform sound, and the most pre-installed infrastructure (mic-speaker).

BTW – this link is Google's "pitch" for using data-over-sound. But we are much beyond their payment technology and use cases. https://ieeexplore.ieee.org/document/8080245

Company Status, Ask, and Use of Funds

- Pre-seed. Rudimentary prototypes and data-over-sound transmission. (BTW, plenty of open source data-over-sound on Github, and commercial SDKs.)
- Seeking $300K for company set up, and a crowdfunding campaign.
- The crowdfunding product: The PONG™ device that users can use as a security device to 1) lock/unlock their phone, and to also wall off parts of their phone; 2) to sonically tether their phone, their laptop.
  - Lock/Unlock: Instead of using the PIN or biometric – hold the PONG inches to 10s or meters from phone or laptop to lock or unlock. BECAUSE, the user don't need to do the PAIN of typing in security secret, they simply hold the PONG to gain access to a) entire parts of the phone, b) to the sand boxed parts of the phone. (Again, once we break the tyranny of needing to type in passwords, we have lot more freedom and uses for security.)
  - Sonic Tether – imagine if the phone and laptop will alert or sleep if the user walks away from them, etc.
- We will also sell or license the technology to asset, tools, and equipment tracking solutions (we may even sell to Tile, the Bluetooth tracker tag). They all currently are dependent on Bluetooth. But Bluetooth only gives vicinity. A combination BLE and Sonic-tracker tag will tell the application, exact location AND distance to the tagged objects. https://www.youtube.com/watch?v=29iE88eqU78

The need for a new user security paradigm for mobile

Mobile security is one of the biggest challenges in technology - affecting consumers, to enterprises, to cities; to governments.

- ❖ We have lot of pains and workarounds from the “limits” of the Bluetooth and Beacons, NFC, WiFi, QR codes.
- ❖ Mobile software protection is nearing its limit. Because security is based on software protecting software, it will never be as reliable as hardware-backed protection.”

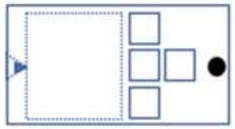
Our mobile our most important device, yet it is very vulnerable, and the technology industry has “overlooked its needs”; it needs user friendly, separate 2nd hardware device for security, and **especially usable with the phone’s smaller size and with one-hand**.

- ❖ We do and have multiple solutions and factors of security with our laptops or PC, yet we do not with our mobiles - **due to the complexity of RF based solutions and implementations**.
- ❖ “By 2020…people will use their mobile to manage their bank account 2.3 billion times, and more than internet, branch and telephone banking put together.”

Market 1 (of 3 markets) Solution for the Mobile - PONG™

Worlds first Sonic Security and Authentication – there are two uses:





The first use --- is for the user to secure their mobile, laptop, or computer to the PONG device, i.e. as a sonic lock (in lieu of PIN) and to optionally sonically tether. We will provide the app and the device. This can be implemented directly by the user and has potential to be a crowdfunding project.

The uses examples ---- To use the PONG fob-device to lock and unlock their mobile, laptop, and computer. These will talk to each other using data-over-sound. If the tethering is turned on, then these will periodically check the presence or distance of each other. The time period and the distance can be set by the user. If the tether is broken, there is an alert and/or to power-down the mobile and laptop.

The second use --- is for two-factor authentication solutions.

The uses examples --- For banks to implement the Sonic-Two-Factor on their web sites. Then, this would be an alternative to the current Google Authenticator and Authy two factors. This requires us to use industry cryptography standards. An extension of this second use is to work with security key manufacturers (e.g. YubiKey™, etc.) to partner or license our IP to them.

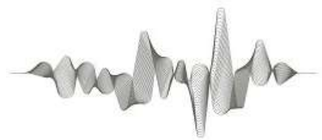
Competitive Advantages

Team and Strategies

- We ***see sound*** like no others have yet; 😉 and we have well planned road map in several sectors.
- World class expertise in the use of sound, and a supplementary LEDs (light) for transmitting data.
- We also have LEDs, or light-communication expertise and will use it. YT vids LED tags
- Expertise in broad range of technology and business - cryptography, hardware, encryption, software and hardware development; merchant payment systems; patent strategies. Etc.

Technology

- The focus and the leveraging of the most powerful, overlooked communication technology.
- First mover in our go-to-market, and in the Phases 1, 2, and 3.
- Strong patent portfolio is expected.



Appendix 1 for Phase 1 - About Data-over-sound vs. NFC/BT

Industry References for Sound, and limits of the Radio spectrum

- **Google's white paper** on data-over-sound for their payment app - Google Tez: "Ultrasonic communication using consumer hardware". (Google swapped out the QR code component of their Google Pay with "audio QR".)
- (06/2019) "Sending Data Over Sound: How and Why?... demand grows for better IoT connectivity…
- "NFC, Bluetooth and RFID: Unraveling the Wireless Connections"
- https://www.itproportal.com/features/data-over-sound-and-the-future-of-frictionless-data-transmission/
- https://lisnr.com/resources/blog/history-data-over-sound/

Market potentials (broadly) – Phase 1

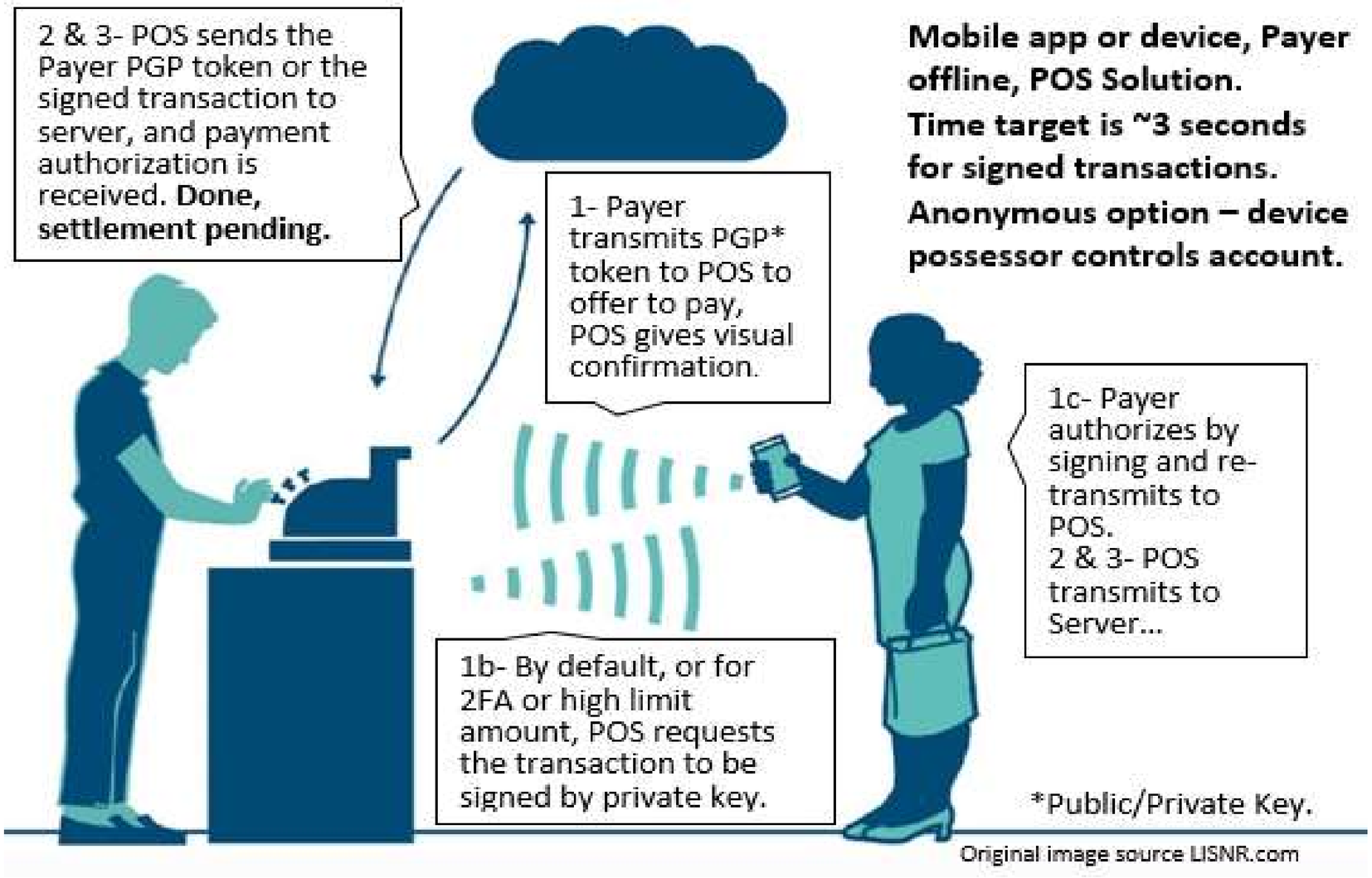
- "…the total RFID market (rise to) $13.4 Billion in 2022. This includes tags, readers and software/services for RFID labels, cards, fobs and all other form factors…"
- "The near field communication (NFC) market is expected to reach US$ 21.84 Billion by 2024, at a CAGR of 17.1% between 2017 and 2024.
- "Nearly 4 billion Bluetooth® devices are forecasted to ship in 2018…

Appendix 2 for Phase 1 – About USB-security keys, 2FAs

Market potentials (broadly) – Phase 1 – USB Security keys market size

- "**Two Factor Authentication** technology is perceiving **a huge uptake and demand across the world**…the global market will reach USD ~8.78 Billion…CAGR of ~19.6% between 2017 and 2023." Two-Factor Authentication Market
- "**Multi-factor Authentication Market Size Worth $17.76 Billion By 2025**…Authentication (for) secure online transactions, log on to online services, and access to corporate resources…biometric technologies, hardware and software applications, and cloud-based authentication services are projected to provide extensive growth opportunities…issues related to cost and complexity involved in implementing MFA solutions and the ever-changing security…"
- "MFA…Market by Model (Two, Three, Four, and Five Factor), By Application (Banking & Finance, Government, Military & Defense, Commercial Security, Consumer Electronics, Healthcare), and Geography…is expected to grow from **USD 5.2 billion in 2016 to USD 18.5 billion by 2015"**
- "…drivers of the global USB key market are…mobile phones, tablets, laptops, and computers…The major players in the global USB key market are spending heavily.."

Appendix for Phase 3 – A payment authorization example



Team

Michael Chung - Founder, Inventor, the Chief Grinder https://www.linkedin.com/in/chungmojo

We grinded for 2.5 years into PingPas and its predecessor (Badgii, for the LEDs).

30 years of real estate, retail, and merchant services mashed with 6 years of technology and startups.

Since 2013, full-time into technology startups. Mostly his own. He “invents business models”. In terms of hardware, have been involved or started several projects in the past several years – cellular tags, nano devices (semiconductor). Cryptography and encryption expertise, especially in designing for user experience, and blockchain use case models. Also, notably had a patent on email sorting which was referenced and cited over 225 times by 2010, where over 50% were by the top technology companies such as AOL, ATT, Bell Labs, Google, Microsoft, Yahoo!, Red Hat, etc. even the U.S. Postal Service. All-in on the blockchain” – read some 200+ white papers, “it’s our inflection point to Type 1 civilization”, etc.

Below are advisors who have advised PingPas and are available for more active roles.

John Sokol (in) - http://johnsokol.com/ , **“John is one of the 300 guys that created the Internet” said a friend.**
Pioneered several Internet protocols; created the first live streaming video in 1990s for 2500 web sites; he did the world’s first cybercast in 1997 for Arthur Clarke Cybercast Hal's Birthday.

Jeff Flowers College Professor (Tenured) with extensive professional experiences in Management, Programming, Blockchain Technologies. https://www.linkedin.com/in/flowersjeff/

Masahiro Mizuno hardware and prototyper par excellence https://www.linkedin.com/in/masahiromizuno/

Scott Moran. Financial, Blockchain, Cryptos. https://www.linkedin.com/in/scottdmorgan/

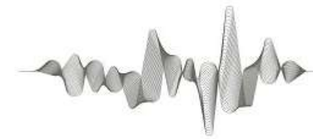
P. Dinh - over 26 years of engineering leading edge technologies. Holds 2 patents in system cryptography and has worked on the design and development of RISC, CISC, GPU processors, infrastructure and edge networking SoC, and data protection ASICs.

Software. Cryptography. Etc. etc.

The following slides are another take and intro-pitch to the PingPas Phase 1. Additional details on Phase 3 crypto-currency strategy and advantages are available. Phase 2 is in stealth at this time.

Solution Attributes

1) **Leverage the biggest and most open communication:** The sound-data
2) **Solve for the highest-grade security.**
3) **New delightful products: “One-click” fob-device or a free app**.
4) **Design for scale and cost: Bill-of-materials starting at few dollars.**
5) **Design for multi - purpose, function, versatility:**
   - Usable inches to several meters.
   - The **first wireless tether** with features of both security and distance control, for phones, laptops, or things.



Solution Background

“THE ENABLING DISCOVERY”:

1) **Sound** is **the most universal cross-platform “interspecies”** data exchange communication.

2) Its **proximity and over-the-air attributes** are particularly useful to solve the problems.

3) Sound enables uses and **applications which the radio frequency (RF) cannot do**.

4) **Challenge-response capable**, but with much less attack vectors than Bluetooth.

THE 2+ YEAR R&D, AND EXTENSIVE EXPLORATIONS, ITERATIONS, & PIVOTS.

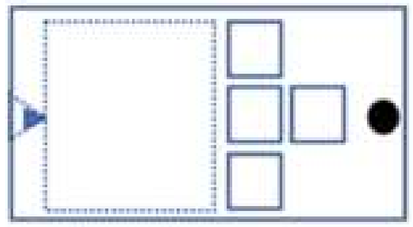
1) **“One-click” NSA grade security:** automatic ~3 seconds to authenticate or authorize vs. the 5-10 secs. for lookup, copy-pasting or typing in the security codes or passwords into the forms.

2) **New and delightful uses** to eliminate pain and workarounds.

- Easy new Sonic-Tether security and control for mobile and laptops.
- Use SONNECT™ and **authenticate using sound-data** - to Alexa™, Voice UIs, during the phone call to the CRM rep or to the company operator.

3) Our SONNECT™ cryptography security and user protocols are **design option, to be plug and play with existing security** keys and cryptography standards.

Solution – Go-to Market: PONG™



Worlds first Sonic-Tether and User-security fob:

- ✓ **An easy to use (sonic) and secure lock for your phone**, laptop, and PC. Usable from distance of ~1 to 10s of meters (adjustable). The distance can be controlled by adjusting the volume, similar to “whispering or shouting”.

- ✓ **We may do a crowdfunding** (Kickstarter or Indiegogo) as go-to-market roll out. If we do, we will also offer a new type of asset and things locating tags. **Sonic-Tags** to be attached to things such as tools and equipment, so that at a yard or job site, they can be located by directional and distance located. This may have BLE function as well.

- ✓ **Bill-of-Materials under $10** for the device; **Sonic-Tags** are about $2 with BLE.

PONG™ Specs. (Some features are in stealth.)

This is one of several designs.

Final designs are TBD; and based on the features and go-to-market strategy.

The other styles are predominantly rectangular.

- Communication: Sound. ~18.5 kHz to ~19.5 kHz; plus, additional bands. Optional second channel using light (LEDs) for higher-grade security and cryptography; added cost is minimal.
- Data rate is estimated to be ~2000 bits/second at the ~18.5 kHz to ~19.5 kHz.
- Power – Two versions. Rechargeable; AAA replaceable.
- Cryptography – Private-key storage; installed at factory, or after purchase; other cryptography options such as 2FA, one-time-password, etc.
- Other: Bill-of-materials is about $5; some designs will have screen and buttons or touch sensitive pad (we found a manufacturer for a concaved shape); some designs will be disposable.

Preamble, 3 pages.

What:

Reinventing communication at the proximity and nearby distance. Solving big gaps left by the RF communications.

How:

Using the technology of data-over-sound by "focusing on" one of its attributes – **the over-the-air*** communication and exchanging data. (Kind of what people do when they talk face to face, or over the phone line. *This took me 2 years to get that it's not about data-over-sound, instead that it's about its over-the-air aspects that I wanted to home in on…this alone is worth the price of admission.)

The other very useful part: Sound-communication is unlicensed and really no* "standards and protocols" – thus, only limited by our imagination and creativity. NFC, Bluetooth, RFID, are all licensed, regulated, etc.

The Current art. Please see competition slide. Facts:

1. Data-over-sound is good enough for Google Pay to roll out in India. They are at 100 bits/ps. We intend to range from the 100 bps to 2000 bps (for our main uses), to over 100K bps for special uses (only that for the special uses, it will require additional hardware (but at about $1 BOM) to be attached to phone's mini-USB/jack.
2. Question: With no budget, starting with zero knowledge of data-over-sound 2.5 years ago – you have thought of, and have invented data-over-sound technical solutions and methods that Google, and the other data-over-sound companies have not? **Yes.**

TL;DR: "I invent stuffs", target a big problem or opportunity, and then grind and grind….why? B/c I am not a trained engineer and often don't know where to start or stop in the technology innovation search (initially). Thus, my ignorance of the limits of the technology results in me asking an inordinate variety of whys and doing explorations. Thus, huge amount of circling and multiple looks – but this approach often results in big discoveries. **And, I have done this before…**

- My 2001 patent described email sorting scheme to folders and tabs of “priority”, “ads”, “friends”, etc. In 2007, 2 years after Gmail was launched, they started the Gmail tabs. In 2001, I had filed the patent, not knowing the difference between SMTP vs. HTTP. I was only 1 year into “the internet”. By 2015 or so, the patent had 225 references and citations – over 50% were by the top technology companies such as AOL, ATT, IBM, Google, Microsoft, Yahoo!, and even some by the U.S. Postal Service.

- In 1992, I mashed together a Motorola radiophone and a credit card terminal to result in a “wireless credit card authorization” solution and initiated a pilot project with an agency of NYC to put the wireless credit card reader into their tow trucks.

Why is the data-over-sound and especially, its over-the-air properties important?

Because, we can create new products, solutions, and services for the society (consumers, enterprises, government) that the current RF technology-based solutions can't directly, or only indirectly for some. **There is a gap in “communication” and thus, huge pain points and workarounds.** Again: The competition is “not focusing, nor seems to be aware” of the extra gift of over-the-air.

The data-over-sound has 2 critical attributes that NFC and Bluetooth don’t have.

1) The most cross-platform communication channel.

2) Microphone and speaker are the most installed infrastructure in the world.

NFC is not designed to be “smart”, subject to man-in-middle (scanning, etc.), not good for challenge response or data storage (passwords, cryptography, etc.). Bluetooth requires pairing and can be attacked (e.g. Google’s 2FA authentication recently).

PINGPAS™ Over-the-air data-over-sound can be used for these things:
A) Ad-hoc communication at distance of inches to 10s of meters – user can decide “if to whisper or shout”.

B) Security and cryptography. We have innovated an additional optical solution to give us “perfect in-the-field updatable security”. (This is in stealth. It is also patent pending.) It will enable non-prime number-based cryptography and quantum-proof --- as needed.

C) Direction and distance. Think of talking. Talking is data-over-sound. Thus, we can whisper to yell and thus, enable direction and distance. RF can't. Now that we share this, imagine the new things the DIYs and hackers can build.

1) Besides taking on the data-over-sound current art, why are we different? We are different, because we from the beginning tried for the small cheap devices and to have data-over-sound and cryptography possible at the 8-bit and 16-bit CPU computing levels. The reason was that, we wanted a payment fob that poor people around the world could use when they don't have or want to carry the phone. Etc. I did not know that the data-over-sound industry had not solved for that.

2) Only later, when we looked at the existing SDKs, did we realize that NONE of the top 4 to 5 commercial SDKs would fit the lower CPUs. They were all solving for the phone platform. Also, their opportunity focus was for basic communication use cases like using sound for admission tickets. For example, Ticketmaster tested them for admitting ticketholders, as they could be admitted in groups instead of single file.

3) Thus, grinding away, we made several major discoveries:

   a) We invented the "sonic YubiKey" – **this then, made us question: WHY are we still typing in our passwords?**

   b) We have others – but ATM, allow us to be stealth. This document describes about 50% of our IP and market opportunities.

Thank you and please excuse the bit unorthodox presentation.